

Федеральное агентство связи
Федеральное государственное бюджетное образовательное
учреждение высшего образования

Сибирский государственный университет
телекоммуникаций и информатики

Е.В. Кокорева

АРХИТЕКТУРА ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ

ЛАБОРАТОРНЫЕ РАБОТЫ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Новосибирск 2020

Кокорева Е.В. Архитектура телекоммуникационных систем и сетей: учебно-методическое пособие. – Новосибирск: СибГУТИ, 2020. – 38 с.

В пособии описан цикл лабораторных работ по дисциплине «Архитектура телекоммуникационных систем и сетей» для студентов направления 11.03.02 «Инфокоммуникационные технологии и системы связи». Лабораторные работы выполняются с использованием сетевого симулятора Cisco Packet Tracer.

В результате выполнения лабораторных работ студенты должны освоить принципы настройки и конфигурирования сетевых устройств, изучить методы статической и динамической маршрутизации, а также научиться работать с виртуальными локальными сетями (VLAN).

Кафедра систем мобильной связи

Таблиц – 2, иллюстраций – 30, литературы – 3 наим.

Рецензент – доцент кафедры телекоммуникационных сетей и вычислительных средств О.И. Моренкова

Утверждено редакционно-издательским советом СибГУТИ в качестве учебно-методического пособия.

© Сибирский государственный университет
телекоммуникаций и информатики, 2020

ОГЛАВЛЕНИЕ

Оглавление	2
Памятка по выполнению лабораторных работ	3
Различные теоретические сведения	4
Лабораторная работа №1	16
Лабораторная работа №2	21
Лабораторная работа №3	27
Список литературы	37

Памятка по выполнению лабораторных работ

Лабораторные работы требуют для своего выполнения наличия на компьютере сетевого симулятора Cisco Packet Tracer.

Ссылка на бесплатную версию СРТ для студентов:

<http://blog.netskills.ru/2015/02/cisco-packet-tracer-62-download-cisco.html>

В качестве результата выполнения лабораторной работы студент должен выслать преподавателю **два** файла: **отчёт** в формате **Office** или **PDF** и файл **модели** в формате **.pkt**.

Отчёт оформляется в соответствии с требованиями ГОСТ 7.32–2017 «Отчет о научно-исследовательской работе» и ГОСТ 2.105–95 «Общие требования к текстовым документам» и состоит из следующих элементов:

1. Титульный лист.
2. Содержание (с нумерацией страниц).
3. Задание в соответствии с вариантом.
4. Структурная схема сети в соответствии с заданием.
5. Выполнение лабораторной работы в соответствии с заданием с описанием всех значащих этапов.
6. Скриншоты результатов (команд и откликов на них) выполнения пунктов задания лабораторной работы.
7. Выводы по проделанной работе.
8. Список литературы (по ГОСТ 7.1-2019).

Рисунки (графики, скриншоты, схемы, диаграммы и пр.), таблицы, формулы и другие объекты отчёта должны быть пронумерованы и подписаны в соответствии с ГОСТ 2.105-95.

Различные теоретические сведения

I Интерфейс пользователя Cisco Packet Tracer и его основные инструменты

Интерфейс пользователя Cisco Packet Tracer выглядит следующим образом (здесь и далее описана версия 6.2.0 Student):

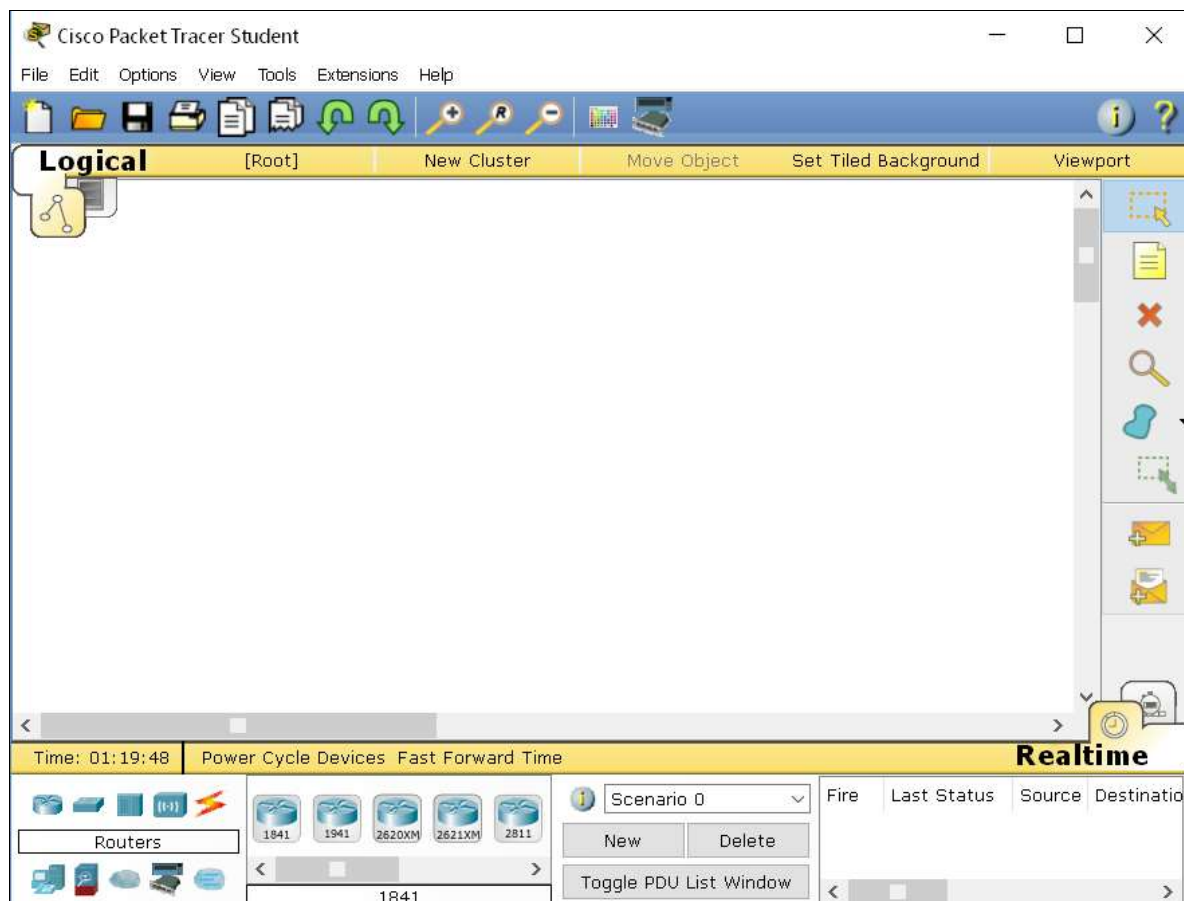


Рис. 1. Интерфейс программы Cisco Packet Tracer

Интерфейс приложения достаточно прост и интуитивно понятен.

В верхней части графического окна программы находится обычный для приложений Windows набор инструментов (строка меню, панель инструментов), с помощью которых можно создавать, сохранять и открывать модель, а также выполнять копирование, удаление элементов, а также печать, отмену или повторение операций и т.д.

Для создания сетевой топологии необходимо выбрать в панели устройств (левая нижняя панель рис. 2) левой кнопкой мыши необходимые устройства и поместить их в рабочую область (окно в центре см. рис. 1) щелчком мыши. Из этой же панели выбираются соединительные линии. Как правило симулятор сам выбирает тип соединения, достаточно нажать  – Automatically Choose Connection Type (рис. 3).

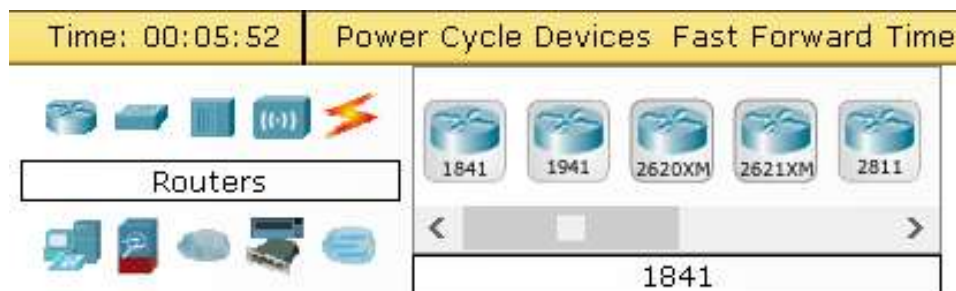


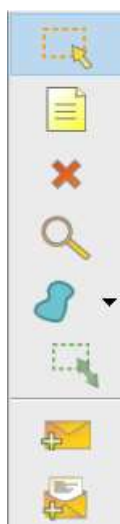
Рис. 2. Панель устройств

Заметим, что тип устройства или соединения отображается в нижней части панели при наведении курсора на его ярлычок.



Рис. 3. Типы соединений

Справа находится ещё одна панель инструментов для выполнения некоторых действий в рабочей области:



- выбор элемента (Select)
- примечание (Place Note)
- удаление элемента (Delete)
- просмотр свойств элемента (Inspector)
- рисование и закрашивание фигуры (Draw Polygon/Rectangle/Ellipse/Line)
- изменение размера фигуры (Resize Shape)
- добавить простой пакет (Add Simple PDU)
- добавить составной пакет (Add Complex PDU)

Допустим, мы поместили в рабочую область модель, представленную на рис. 4. Щелчок левой кнопкой мыши на изображении устройства открывает окно настроек этого устройства. На рис. 5 показано окно настроек хоста, а на рис. 6. – окно настроек коммутатора.

Можно видеть, что окно конфигурирования хоста содержит вкладки:

- Physical;
- Config;
- Desktop;
- Custom Interface.

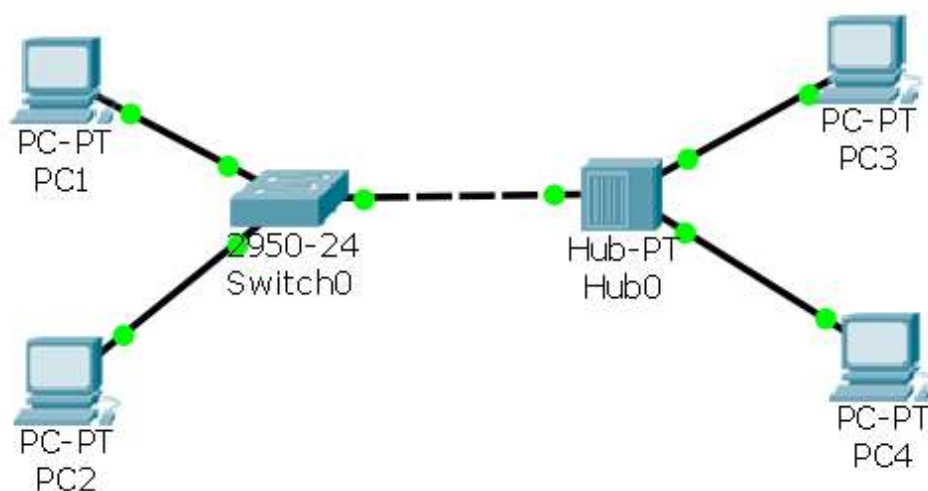


Рис. 4. Пример модели сети в Cisco Packet Tracer

Чтобы задать сетевые настройки хоста проще всего перейти на вкладку **Config** (рис. 7), выбрать требуемый интерфейс, например, **FastEthernet0** (рис. 7 – 1) и ввести IP адрес и маску сети в соответствующие поля раздела **IP Configuration** (рис. 7 – 2). Аналогично настраиваются остальные сетевые устройства.

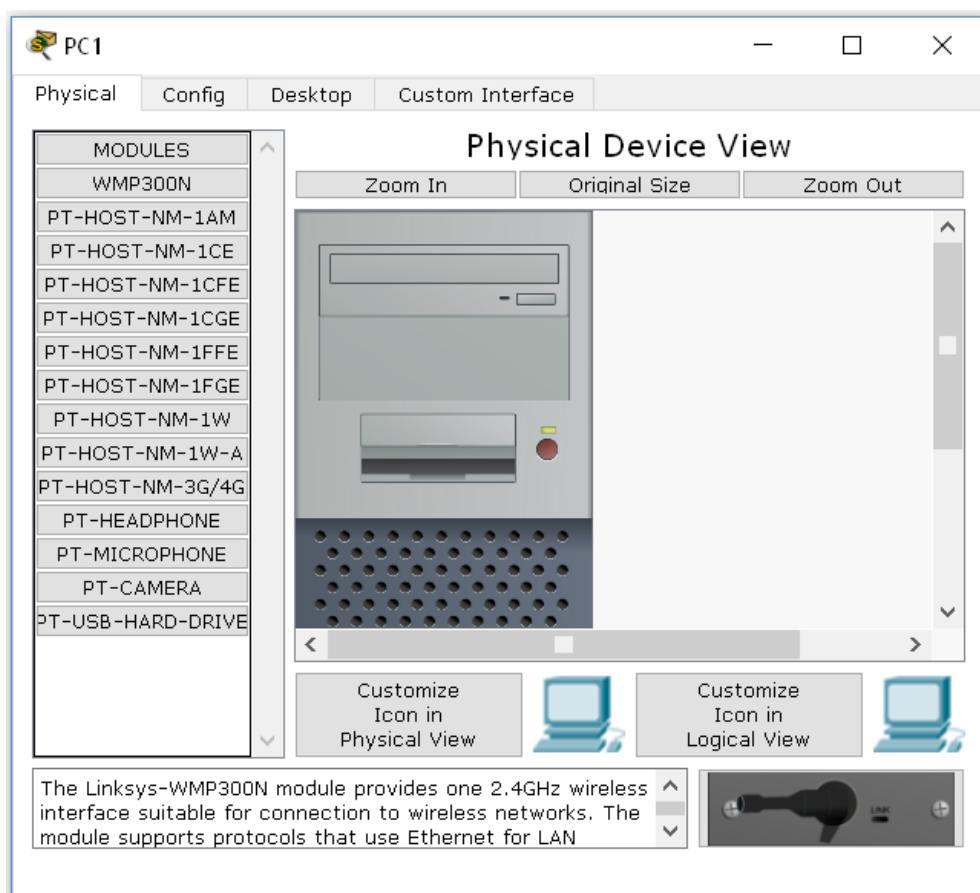


Рис. 5. Окно настройки параметров хоста

Для применения различных команд (например, **ping** или **arp**) служит вкладка **Desktop** (рис. 8) поле **Command Prompt** (командная строка) (рис. 9).

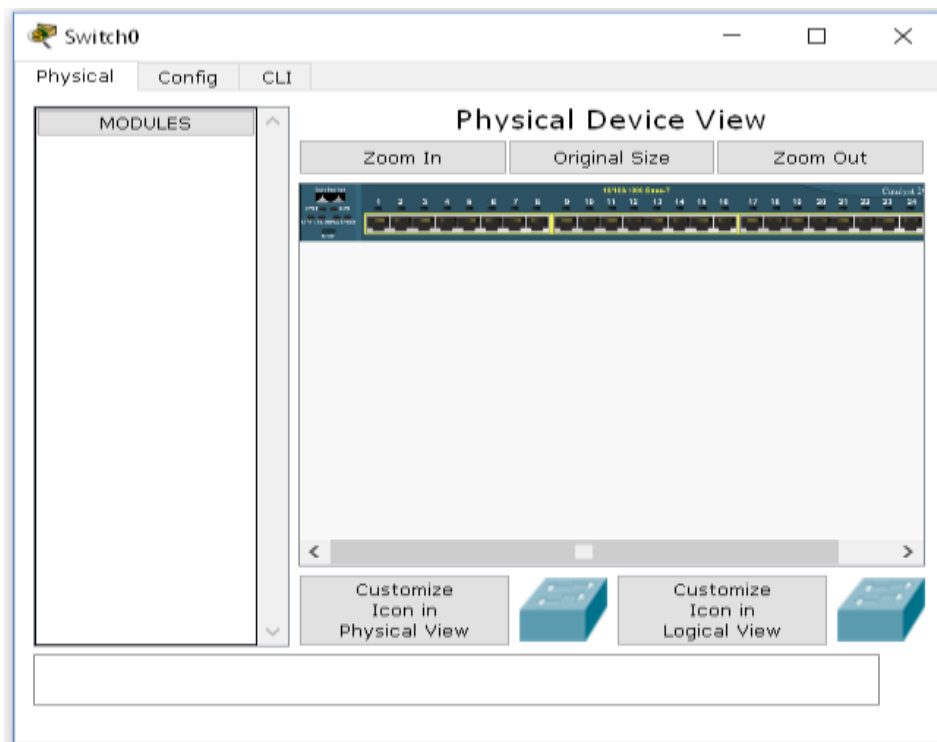


Рис. 6. Окно настройки параметров коммутатора

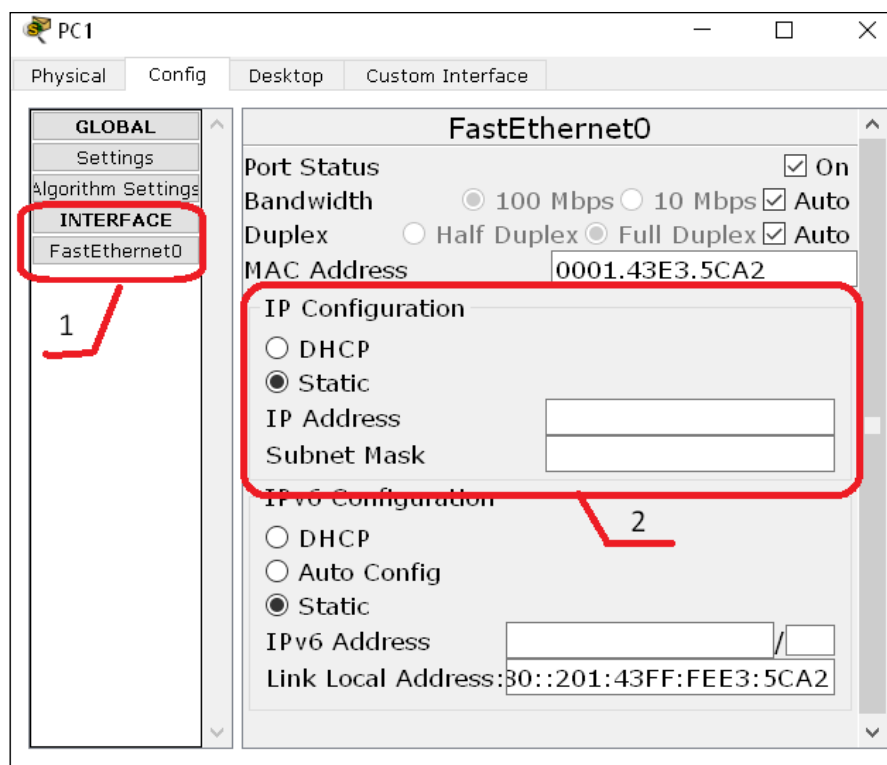


Рис. 7. Сетевые настройки хоста

Чтобы проверить соединения используется команда `ping` (передача и приём ICMP-сообщений). Синтаксис команды: `ping <-t> <ip-address>`, например, `ping 192.168.1.10`. Ключ `-t` позволяет отправлять неограниченное число ICMP-пакетов. Использование команды без ключа позволит передать четыре пакета, а ключ `-n` позволит задать ограниченное число ICMP-пакетов:

`PC>ping -n 200 192.168.1.10`

Если результат выполнения команды выглядит также как на рис. 10, значит «полет нормальный».



Рис. 8. Вкладка Desktop настроек хоста

Для того чтобы посмотреть ARP (англ. *Address Resolution Protocol*) таблицу (таблицу соответствия IP адресов MAC адресам устройств) необходимо ввести команду:

>>arp -a – ключ -a указывает на просмотр адресов всех устройств сети. Результат выполнения команды представлен на рис. 11.

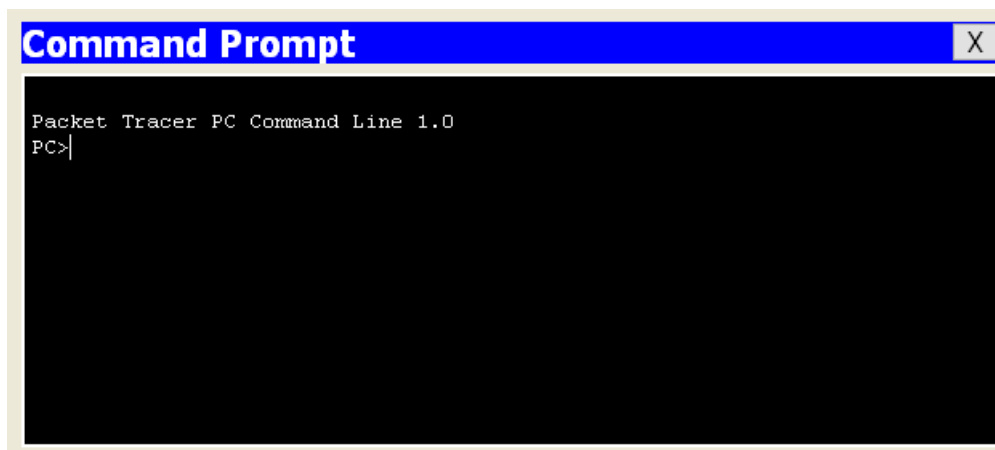


Рис. 9. Командная строка

Для просмотра информации об интерфейсе служит команда `ipconfig` (рис. 12).

```

PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128

```

Рис. 10 Пример выполнения команды ping

```

PC>arp -a

Internet Address      Physical Address      Type
192.168.1.2           0030.a3c8.d82a       dynamic
192.168.1.3           0060.5c20.204b       dynamic
192.168.1.4           0050.0f8c.31bd       dynamic

```

Рис. 11. Пример выполнения команды arp

```

PC>ipconfig

FastEthernet0 Connection:(default port)

Link-local IPv6 Address.....: FE80::201:43FF:FEE3:5CA2
IP Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 0.0.0.0

```

Рис. 12. Пример выполнения команды ipconfig

При переходе в режим симуляции **Simulation** справа от рабочей области открывается **Simulation Panel** (рис. 13).

Отфильтровать передаваемые пакеты, можно нажав кнопку **Edit Filters** и выбрав в появившейся панели требуемые типы пакетов крыжиками в нужных полях (рис. 14).

Запустить автоматическую симуляцию можно кнопкой **Auto Capture/Play**. Скорость симуляции можно увеличить или уменьшить движком (1) на рис. 13, потянув его вправо или влево соответственно.

II IP адрес и маска подсети

IPv4-адрес состоит из четырёх октетов в десятичном представлении без начальных нулей, разделенных точками: «192.168.11.10».

В заголовке IP-пакета есть поля **source IP** и **destination IP**: адреса источника (того, кто посылает пакеты) и адреса назначения (кому предназначены пакеты). Это напоминает информацию на почтовом конверте.

IP-адреса источника и получателя в заголовке пакета записываются без разделителей между октетами и имеют длину 32 бита каждый.

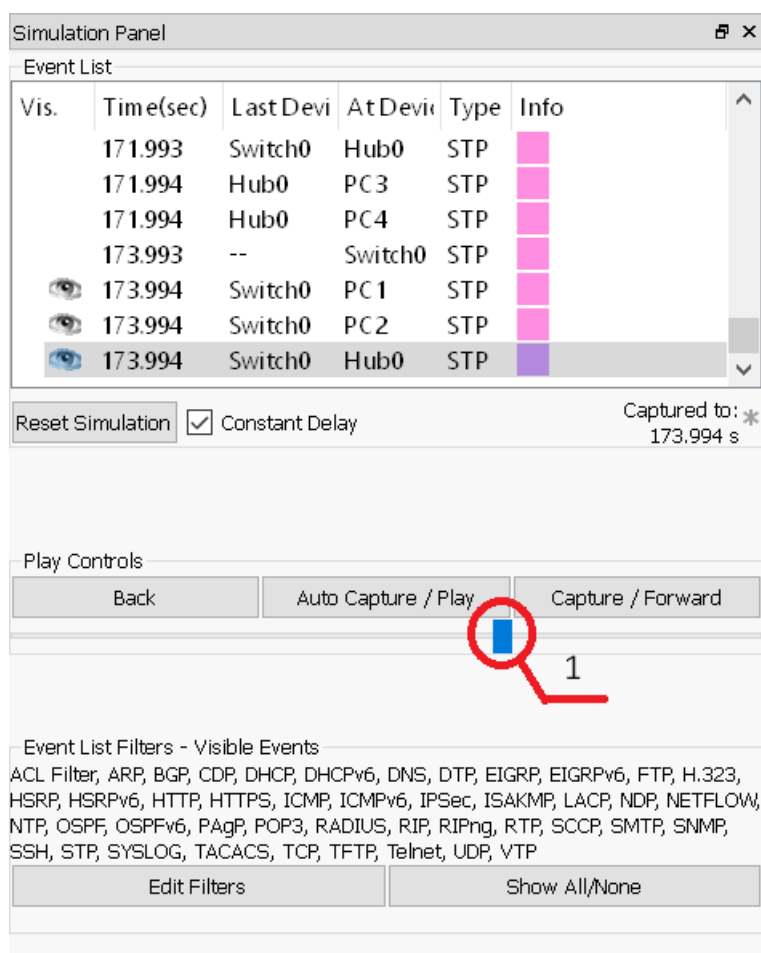


Рис. 13. Панель симуляции

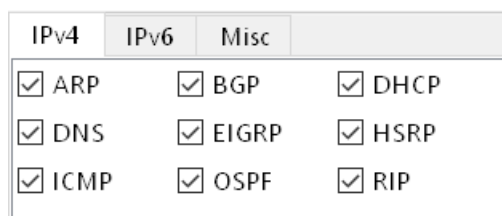


Рис. 14. Выбор типов пакетов для передачи

Когда IP-адрес присваивается интерфейсу компьютера или маршрутизатора, ему назначают еще и маску подсети. В заголовок пакета маска не заносится. Маска нужна для определения границ подсети. Чтобы каждый хост мог определить, кто находится с ним в одной подсети (или просто сети), а кто за ее пределами.

Дело в том, что внутри одной сети компьютеры обмениваются пакетами «напрямую», а когда нужно послать пакет в другую сеть, то они отправляют их шлюзу «по умолчанию», имеющему адрес интерфейса маршрутизатора, через который осуществляется выход данных в другие сети

Маска подсети также представляет собой 32 бита. Но в отличие от IP-адреса, нули и единицы в ней не могут чередоваться. Всегда сначала идет некоторое количество единиц, а потом дополняющее до 32-х разрядов количество нулей. Маска 120.22.123.12 в десятичном представлении или 01111000.00010110.01111011.00001100 в двоичном не существует. Но

может быть маска 255.255.248.0 или 11111111.11111111.11111000.00000000. Сначала N единиц, потом 32 – N нулей.

При обозначении интерфейса можно указывать IP-адрес и через слэш N – длину маски. Так и делают: пишут 192.168.11.10/21 вместо 192.168.11.10 255.255.248.0. Обе формы несут один и тот же смысл, но первая удобнее для пользователя.

Чтобы определить границы подсети, компьютер делает побитовое умножение (логическое И) между IP-адресом и маской, получая на выходе адрес с нулевыми битами в позициях нулей маски. Рассмотрим пример IP-адреса 192.168.11.10/21:

```
11000000.10101000.00001011.00001010
11111111.11111111.11111000.00000000
-----
11000000.10101000.00001000.00000000 = 192.168.8.0
```

В результате получили адрес сети, к которой относится данный хост.

Таким образом, нули в конце маски определяют количество адресов устройств данной сети. В примере, приведённом выше их количество равно $2^{10} - 1$ (один адрес, как правило, отводится под шлюз сети).

III Режим конфигурирования маршрутизаторов

Для конфигурирования маршрутизаторов необходимо войти в режим командной строки CLI (англ. Command Line Interface). Для этого нужно щёлкнуть левой кнопкой мыши по изображению устройства в рабочей области и перейти на вкладку CLI в открывшемся окне (рис. 15).

На рис. 16 показано окно консоли маршрутизатора с начальной загрузкой.

Приглашение маршрутизатора выглядит следующим образом:

Router>

Команды консоли маршрутизатора могут вводиться в контексте пользователя или администратора. В контексте пользователя выполняются самые простые команды, не связанные с настройкой устройства. Конфигурирование настроек маршрутизатора производится в контексте администратора (привилегированный режим).

Для входа в привилегированный режим вводится команда:

Router>enable

После чего приглашение изменится на:

Router#

Для получения сведений о команде нужно набрать знак ? после команды, и нажать Enter, например:

Router#show ?

Результат выполнения команды приведён на рис. 17.

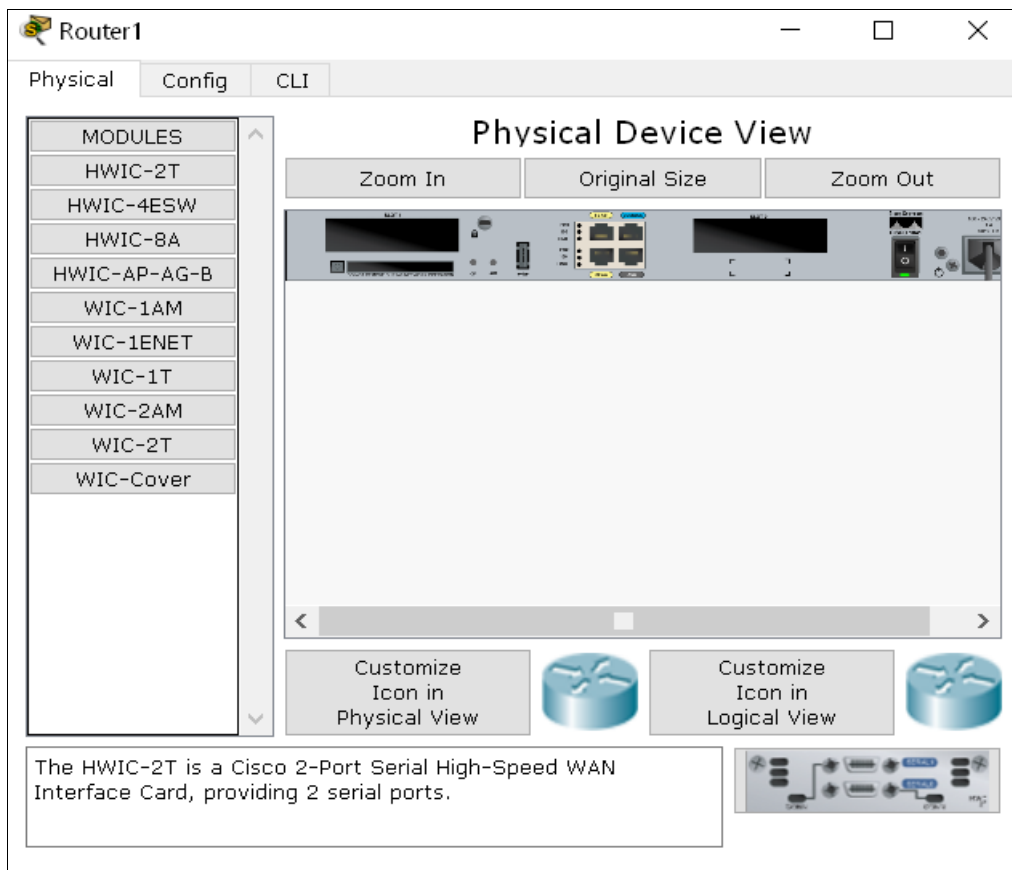


Рис. 15. Вход в режим интерфейса командной строки

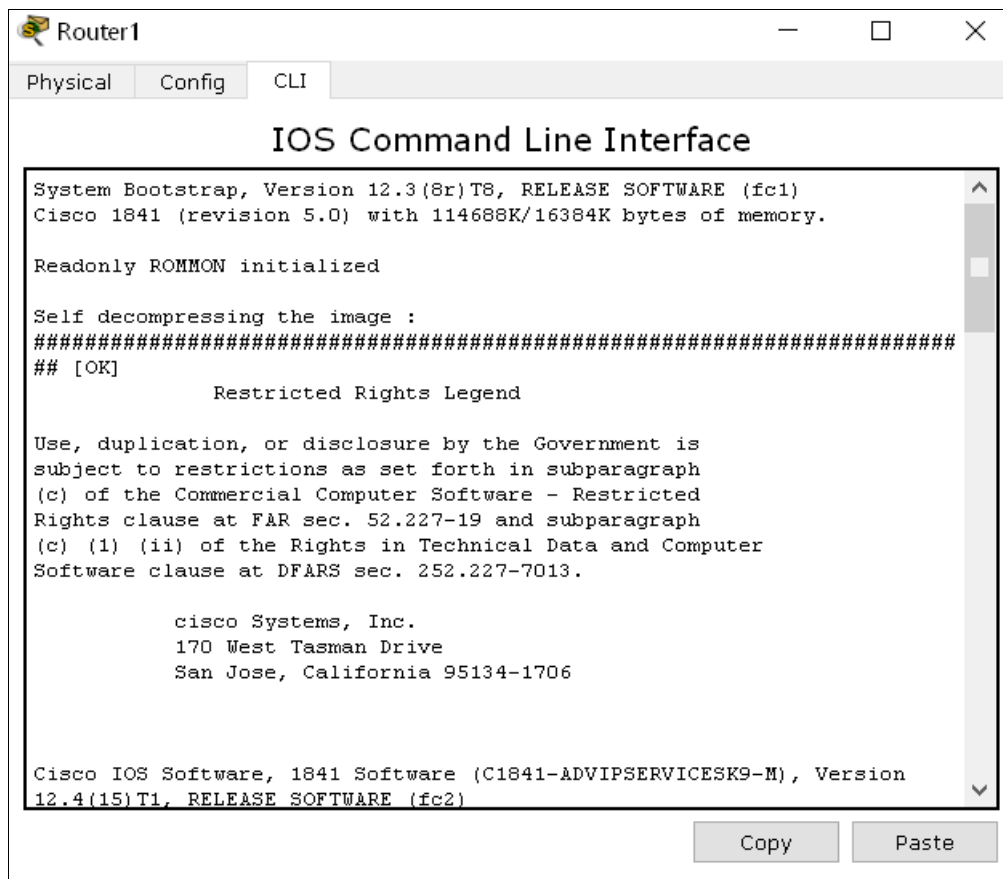


Рис. 16. Начальная загрузка маршрутизатора

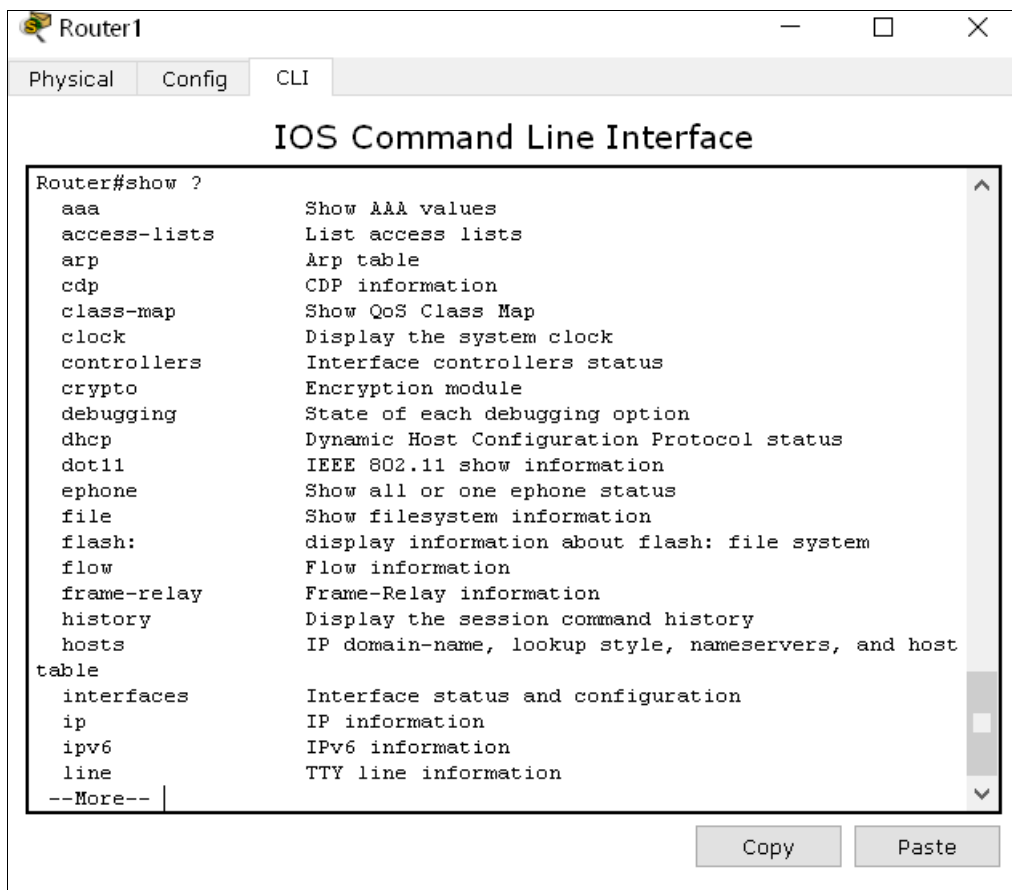


Рис. 17. Параметры команды show

Далее приводятся некоторые команды контекста администратора.

Вход в режим настройки конфигурации:

```
Router#configure terminal
```

или, сокращённый вариант:

```
Router#conf t
```

Установка пароля для привилегированного режима:

```
Router(config)#enable secret <password>
```

Изменение имени устройства:

```
Router(config)#hostname <Name>
```

Вместо <Name> указывается новое имя устройства. После чего приглашение изменится на (рис. 18):

```
<Name>(config)#
```

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
```

Рис. 18. Вход в привилегированный режим и смена имени

Далее будем использовать в качестве имен роутеров имена типа R1, R2, R3...

Включение и настройка IP адреса на интерфейсе (через который будет производиться загрузка ПО и дальнейшее конфигурирование устройства):

```
R1(config)#interface fastethernet 0/0
```

или, сокращённый вариант:

```
R1(config)#int fa0/0
```

```
R1(config-if)#ip address 192.168.0.1 255.255.255.0
```

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

 – поднять интерфейс.

или, сокращённый вариант:

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

```
R1(config-if)#exit
```

 – выйти из режима (вернуться на предыдущий уровень).

Выход на самый верхний уровень:

```
R1(config-if)#end
```

Для серийного интерфейса (Serial). Вход в режим конфигурирования интерфейса:

```
R1(config)#interface serial 0/0
```

или, сокращённый вариант:

```
R1(config)#int se0/0
```

Сохранение текущей конфигурации:

```
R1#copy running-config startup-config
```

Сокращённый вариант:

```
R1#copy run start
```

Далее надо нажать Enter на вопрос системы об имени файла (рис. 19).

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa 0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

Рис. 19. Настройка интерфейса и сохранение текущей конфигурации

Просмотр текущей работающей конфигурации:

```
<Name>#show running-config
```

или:

```
<Name>#show run
```

Просмотр сохраненной конфигурации:

```
<Name>#show startup-config
```

или:

```
<Name>#show start
```

Запуск ping-процесса:

```
<Name>#ping <IP-адрес устройства>
```

Количество передаваемых ICMP-пакетов – 5.

Остальные команды будут приведены по ходу выполнения лабораторных работ, к описанию которых мы приступим в следующих разделах.

Лабораторная работа №1

Настройка параметров простой IP-сети

Цель работы: конфигурирование сетевых интерфейсов компонентов IP-сети. Закрепление навыков работы с интерфейсом командной строки маршрутизатора. Объединение компьютеров в сеть и проверка сетевых соединений.

Краткая теория

Для добавления физических модулей к сетевому устройству, необходимо щелчком мыши открыть окно настроек устройства (рис. 18) и на вкладке Physical:

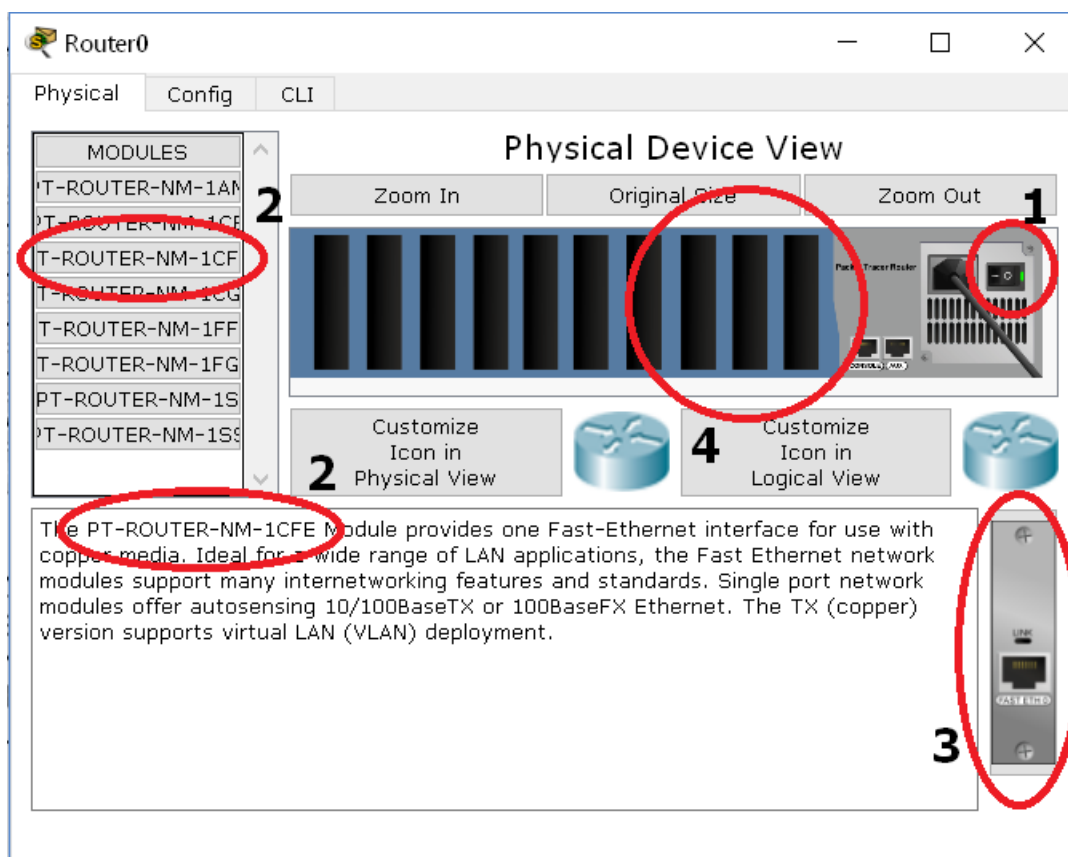


Рис. 18. Физическая конфигурация маршрутизатора

- выключить питание устройства (кнопка 1);
- выбрать в панели дополнительных модулей (2) необходимый модуль;
- курсором мыши перетащить планку, изображение которой появится в позиции 3, в пустой слот устройства (4);
- включить устройство (1).

Команды конфигурирования устройств приведены в **ПРИЛОЖЕНИИ 1**.

Настройку интерфейсов хостов следует производить в окне IP Configuration вкладки Desktop (рис. 19–20).

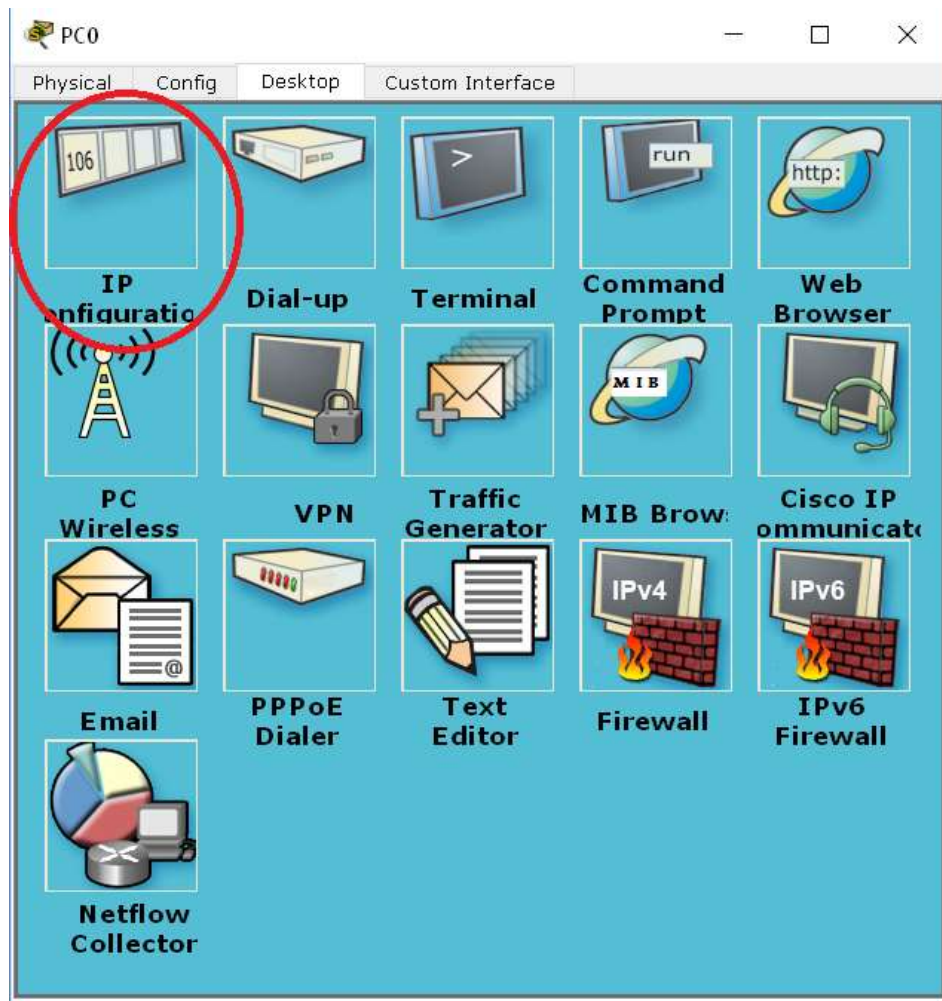


Рис. 19. Вкладка Desktop

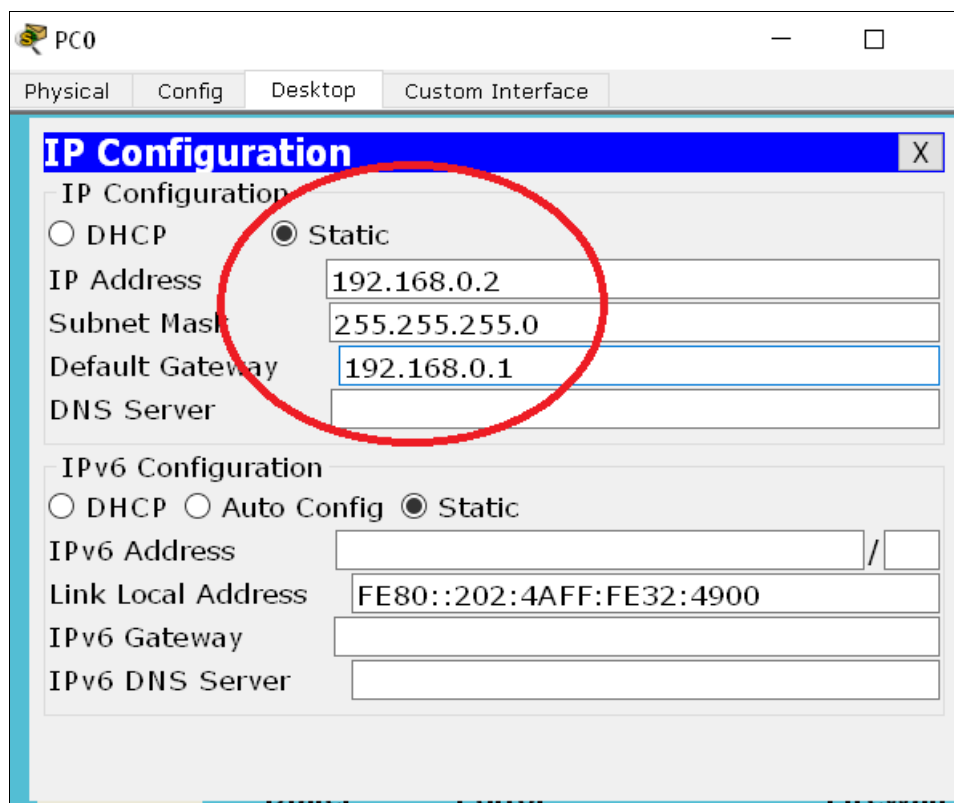


Рис. 20. Окно IP Configuration

Задание:

Собрать в симуляторе Cisco Packet Tracer схему сети, приведённую на рис. 21. Выбрать для реализации устройства Router-PT Empty, Switch 2950-24 и PC-PT. IP-адреса, обозначенные на рис. 21, являются адресами подсетей.

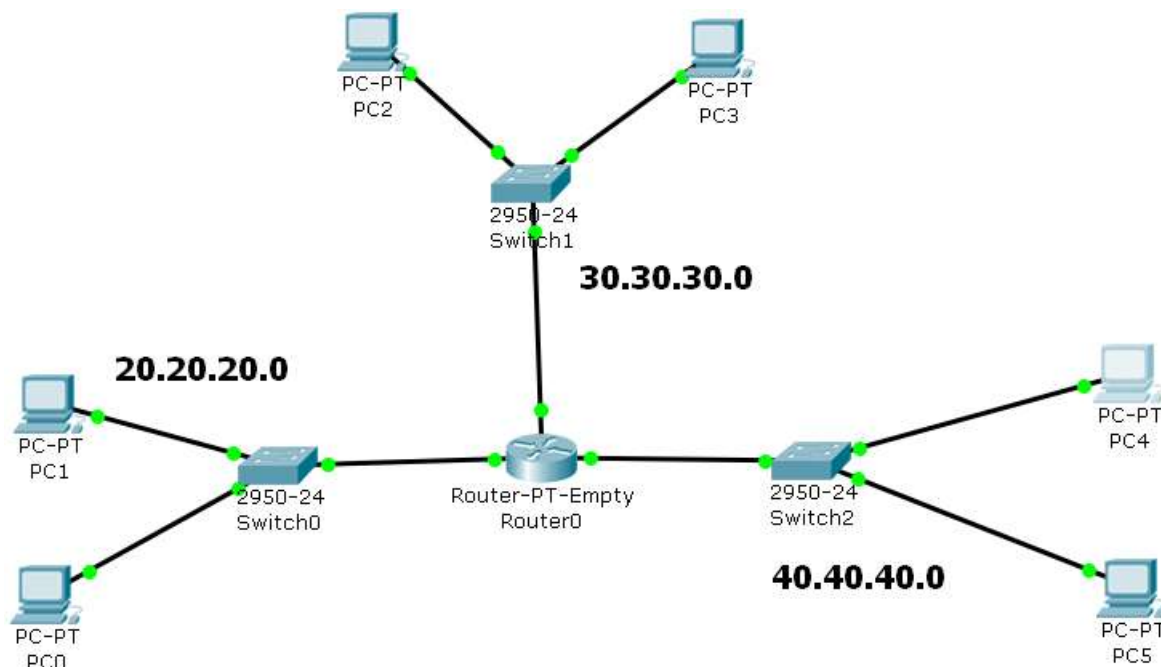


Рис. 21. Схема сети

Прежде чем соединить устройства в сеть, необходимо наполнить содержимым роутер (т.к. мы выбрали «пустой» – empty). Для этого на вкладке Physical (рис. 18) выбрать три модуля PT-ROUTER-NM-1CFE и вставить их в предназначенные для них слоты.

Сетевые соединения и настройку интерфейсов следует производить в соответствии с табл. 1. Маска всех сетей 24-хразрядная (255.255.255.0).

Таблица 1. Конфигурация сетевых интерфейсов

Устройство	Интерфейс	IP-адрес	Шлюз
Router0	Fast Ethernet 0/0	20.20.20.1	–
	Fast Ethernet 1/0	30.30.30.1	–
	Fast Ethernet 2/0	30.30.30.1	–
PC0	eth0	20.20.20.2	20.20.20.1
PC1	eth0	20.20.20.3	20.20.20.1
PC2	eth0	30.30.30.2	30.30.30.1
PC3	eth0	30.30.30.3	30.30.30.1
PC4	eth0	40.40.40.2	40.40.40.1
PC5	eth0	40.40.40.3	40.40.40.1

Порядок выполнения лабораторной работы:

1. Запустить симулятор Cisco Packet Tracer.

2. Выбрать из панели устройств маршрутизатор, коммутаторы и компьютеры, соответствующие схеме на рис. 21.
 3. Добавить к маршрутизатору необходимые модули.
 4. Соединить устройства в сеть в соответствии со схемой и табл. 1.
-



Примечание: если не соблюдать соответствия соединяемых интерфейсов и настроек, легко запутаться и построить нерабочую сеть.

5. Перейти в интерфейс командной строки (CLI) маршрутизатора Router0.
6. Войти в привилегированный режим, а затем в режим конфигурирования настроек маршрутизатора.
7. Поочерёдно войти в режим конфигурирования интерфейсов Fa0/0, Fa1/0 и Fa2/0 и задать сетевые настройки в соответствии с табл. 1.
8. Поднять интерфейсы и сохранить конфигурацию.
9. Поочерёдно задать сетевые параметры (IP-адрес, маска, шлюз) компьютерам сети.
10. Убедиться в достижимости всех объектов сети по протоколу IP командой `ping`.
11. Исправить ошибки, если таковые обнаружены и сохранить конфигурацию. Снова запустить `ping`-процесс.
12. Просмотреть настройки интерфейсов компьютеров командой `ipconfig`.
13. Оформить отчёт по лабораторной работе.
14. Сдать и защитить работу.

Структура отчета к лабораторной работе:

1. Титульный лист.
2. Содержание с нумерацией страниц.
3. Задание к лабораторной работе.
4. Структура сети.
5. Сетевые настройки устройств.
6. Ход работы:

Данный раздел состоит из последовательного описания значимых выполняемых шагов (с указанием их сути) и копий экранов (должна быть видна набранная команда и реакция системы, если она есть).

7. Выводы по лабораторной работе.

Контрольные вопросы:

1. Для чего применяется устройство коммутатор? Какие виды коммутаторов вы знаете?
2. Опишите функции маршрутизатора.
3. Что такое IP-адрес? Из чего он состоит?
4. Для чего служит маска подсети?
5. Чем адрес сети отличается от адреса хоста?
6. Сколько IP-адресов может иметь сетевое устройство?

Лабораторная работа №2

Статическая и динамическая маршрутизация

Цель работы: настройка статической и динамической маршрутизации в IP-сети. Проверка достижимости устройств до и после обрыва на линии. Сравнение двух видов маршрутизации.

Теоретические сведения:

I Особенности статической маршрутизации

Статическая маршрутизация осуществляется без участия каких-либо протоколов. Все маршруты при этом явно прописываются на интерфейсах при конфигурировании маршрутизатора. Такой способ применим только в относительно небольших сетях (с малым количеством маршрутизаторов).

Основным недостатком такого способа является то, что при обрыве любой линии связи, маршруты, связанные с ней, становятся недоступными и привязанные к этим маршрутам подсети – недостижимыми.

1. Настройка статической маршрутизации на роутере

Формат команды:

```
R1(config)# ip route <сеть назначения> <маска> <next hop>
```

В команде указывается адрес подсети, которой принадлежат адресуемые хосты, маска этой подсети и адрес шлюза – интерфейса, через который пакеты смогут переходить из данной подсети в другую подсеть (на пути к сети назначения).

Прежде чем настраивать сетевые устройства, необходимо зайти в привилегированный режим командой:

```
R1>enable
```

А чтобы получить доступ к конфигурации необходимо ввести:

```
R1#conf t
```

или

```
R1#configure terminal
```

Пример настройки маршрутизации на роутере R1 (адреса и маски, приведённые в примере, не используются в лабораторной работе):

```
R1(config)#ip route 172.16.30.0 255.255.255.0 172.16.20.1
```

```
R1(config)#ip route 172.16.40.0 255.255.255.0 172.16.20.2
```

```
R1(config)#exit
```

2. Маршрутизация по умолчанию

```
R1(config)#ip route 0.0.0.0 0.0.0.0 <next hop>
```

Например,

```
R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.20.1
```

3. Сохранение конфигурации маршрутизатора

```
R1#copy running-config startup-config
```

Сокращённый вариант команды:

```
R1#copy run start
```

4. Просмотр карты маршрутов (рис. 22)

```
R1#show ip route
```

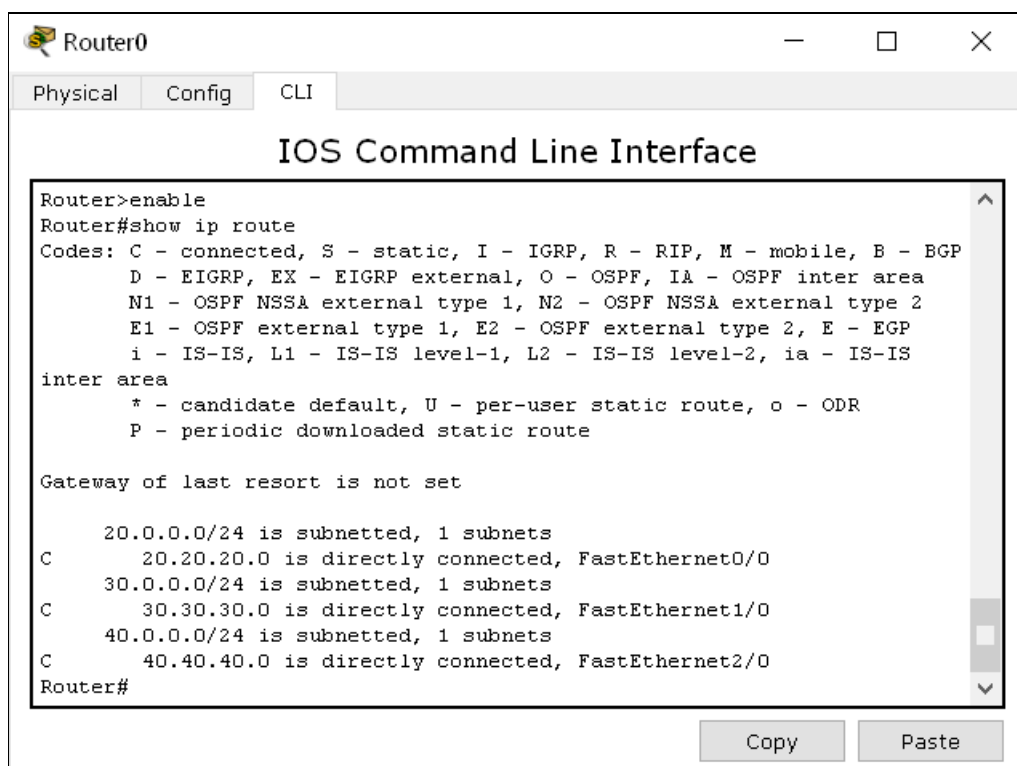


Рис. 22. Отклик на команду show ip route

На рис. 22 представлен роутер, маршрутизация на котором не настроена. Здесь можно видеть обозначения: С – сеть напрямую присоединённая к данному роутеру; S – сеть со статической маршрутизацией; R – RIP; O – OSPF и т.п.

5. Отключение сообщений консоли

```
R1(config)#no logging console
```

II Принципы динамической маршрутизации

Динамическая маршрутизация означает автоматическое построение таблиц маршрутизации на роутерах с помощью специальных протоколов. Использование протоколов маршрутизации позволяет избежать необходимости вручную прописывать маршруты на всех роутерах сети и ошибок, связанных с человеческим фактором. Эти протоколы призваны строить таблицы

маршрутизации автоматически, исходя из текущей конфигурации сети.

В IP-сетях существует два типа протоколов маршрутизации:

- дистанционно-векторные, основанные на метриках «расстояния» (например, количество роутеров) до сети назначения (RIP, IGRP, EIGRP);
- состояния связи, основанные на топологии сети и её характеристиках (OSPF, IS-IS).

Протокол маршрутной информации (англ. *Routing Information Protocol*) — один из самых простых протоколов маршрутизации. RIP применяется в небольших компьютерных сетях и позволяет маршрутизаторам динамически обновлять маршрутную информацию, получая ее от соседних роутеров.

RIP маршрутизация осуществляется на основе *дистанционно-векторного алгоритма* (англ. *Distance Vector Algorithm – DVA*) с использованием метода Беллмана-Форда.

Протокол RIP версии 2 отличается тем, что при его использовании маршрутизатор передаёт соседним роутерам сведения не только об адресах, подключенных к нему подсетей, но и об их масках, что позволяет использовать нестандартные маски этих подсетей.

1. Настройка динамической маршрутизации на роутере

Команда настройки RIP-маршрутизации

```
R1(config)#router rip
```

Протокол RIP-маршрутизации версии 2

```
R1(config-router)#version 2
```

Адреса сетей, подключенных к данному роутеру, которые он сообщает своим «соседям»

```
R1(config-router)#network <адрес сети>
```

Пример настройки RIP-маршрутизации (адреса, представленные в примере, не используются в лабораторной работе):

```
R1(config)#router rip
```

```
R1(config-router)#network 172.16.30.0
```

```
R1(config-router)#network 172.16.40.0
```

```
R1(config)#exit
```

Остальные команды (сохранения настроек, просмотр конфигурации и пр.) приведены в разделе I данной лабораторной работы или в ПРИЛОЖЕНИИ 1.

Задание:

Собрать сеть, представленную на рис. 23. Адреса, представленные на рисунке, являются адресами подсетей. Адреса интерфейсов должны быть настроены в соответствии с принадлежностью данного интерфейса конкретной подсети.

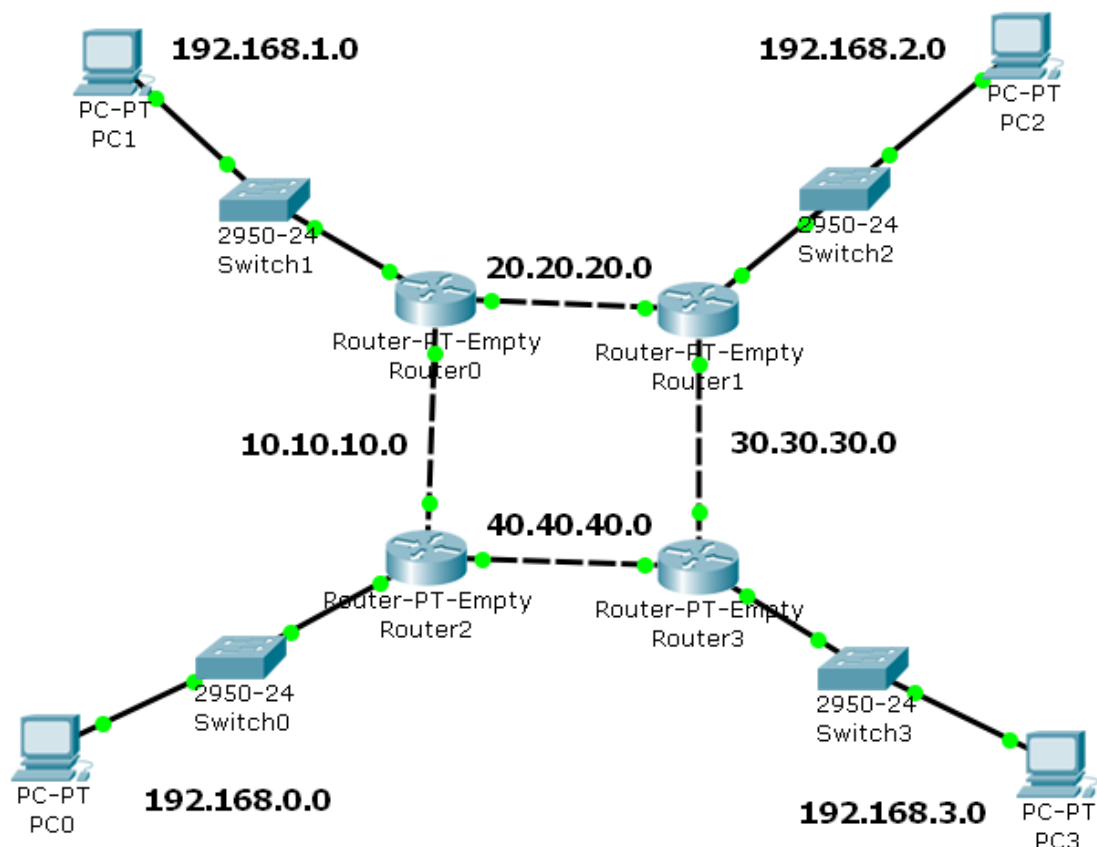


Рис. 23. Схема сети для изучения принципов маршрутизации

Выбрать для реализации устройства Router-PT Empty, Switch 2950-24 и PC-PT. Прежде чем соединить маршрутизаторы в сеть, необходимо добавить к каждому из них по три слота PT-ROUTER-NM-1CFE, как это было сделано в лабораторной работе №1.

Произвести настройку сетевых параметров хостов и маршрутизаторов в соответствии с адресами подсетей, представленных на рис. 23. Для простоты маску всех подсетей принять 24-х разрядной.

Настроить статическую маршрутизацию на роутерах сети, таким образом, чтобы все хосты оказались доступны друг для друга и для роутеров.

Проверить, как поведёт себя сеть при обрыве одной из линий.



Примечание: Не забывать сохранять настройки роутеров при внесении изменений в конфигурацию.

Заново собрать схему, представленную на рис. 23 (это проще, чем удалять статическую маршрутизацию на роутерах).

Настроить динамическую маршрутизацию RIP на роутерах сети, таким образом, чтобы все хосты оказались доступны друг для друга и для роутеров.

Проверить, как поведёт себя сеть при обрыве одной из линий.

Порядок выполнения работы:

1. Запустить Cisco Packet Tracer.

2. Выбрать из панели устройств маршрутизатор, коммутаторы и компьютеры, соответствующие схеме на рис. 23.
3. Добавить к маршрутизатору необходимые модули.
4. Соединить устройства в сеть в соответствии со схемой на рис. 23.
5. Отключить консольные сообщения (`no logging console`).
6. Настроить интерфейсы маршрутизаторов в интерфейсе командной строки (CLI) в соответствии с адресами подсетей.
7. Поднять интерфейсы (`no shut`).
8. Просмотреть настройки интерфейсов командой `show`.
9. Сохранить настройки маршрутизаторов (`copy run start`).
10. Проверить командой `ping` недоступность маршрутизаторов, находящихся в разных подсетях.
11. Проверить командой `ping` доступность интерфейсов, находящихся в одной подсети.
12. Настроить интерфейсы хостов в окне IP Configuration вкладки Desktop.
13. Проверить доступность шлюза для хоста командой `ping`.
14. Если какие-либо из команд пп.10–13 не работают, исправить ошибки и выполнить пп.6–13 повторно.
15. Настроить статическую маршрутизацию на каждом из роутеров. Предусмотреть обрыв любой линии связи между роутерами.
16. Проверить доступность хостов командой `ping`.
17. Просмотреть полученную таблицу маршрутизации на каждом из роутеров.
18. Удалить линию связи между любыми роутерами.
19. Пропинговать с хоста PC3 хосты PC0 и PC1 и PC2.
20. Объяснить полученные результаты.
21. Собрать схему на рис. 23 заново, (добавив к маршрутизатору необходимые модули).
22. Повторить пп.5–8, 9, 12–14 с новой сетью.
23. Настроить динамическую маршрутизацию RIP версии 2 на каждом из роутеров сети.
24. Повторить пп. 16–20.
25. Оформить отчёт по лабораторной работе.
26. Сдать и защитить работу.

Содержание отчета к лабораторной работе:

1. Титульный лист.
2. Содержание с нумерацией страниц.
3. Задание к лабораторной работе.
4. Структура сети.
5. Сетевые настройки устройств со скриншотами.
6. Ход работы:

Данный раздел состоит из последовательного описания значимых выполняемых шагов (с указанием их сути) и копий экранов (должна быть видна набранная команда и реакция системы, если она есть).

7. Выводы по лабораторной работе.

Контрольные вопросы:

1. Что такое маршрутизация?
2. Опишите разницу между статической маршрутизацией и динамической.
3. Приведите примеры команд Cisco для настройки статической маршрутизации.
4. Для чего применяется команда ping?
5. Какие поля содержит таблица маршрутизации?
6. Какие виды динамической маршрутизации вы знаете?
7. Что такое метрика маршрута?
8. Чем протокол RIP v1 отличается от RIP v2?
9. Как реагируют на обрыв линии связи роутеры в сетях со статической и динамической маршрутизацией?

Лабораторная работа №3

Маршрутизация между VLAN

Цель работы: изучение метода создания виртуальных локальных сетей и передачи информации между ними.

Краткая теория

I Определение VLAN

VLAN (англ. *Virtual Local Area Network*) — логическая («виртуальная») локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были расположены в одной подсети, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть и позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств.

Если порт коммутатора принадлежит одной VLAN, то он работает в режиме **access** (`switchport mode access`), если через порт коммутатора могут передаваться данные нескольких VLAN, то он работает в режиме **trunk** (`switchport mode trunk`). Если порт не принадлежит ни одной VLAN, то не используется ни один из этих режимов (`no switchport`).

II Настройка VLAN на Ethernet switch 3-го уровня

Рекомендуется, чтобы отличать коммутатор 3-го уровня от коммутаторов 2-го уровня, переименовать его, например, как показано ниже:

```
Switch>enable
```

```
Switch#conf t
```

```
Switch#hostname R1-SW
```



Примечание: Далее в примерах будут представлены сокращенные варианты команд конфигурирования, уже описанных ранее.

Создание базы данных VLAN на коммутаторе (двух виртуальных сетей):

```
R1-SW#vlan database
```

```
R1-SW#vlan 2
```

```
R1-SW#vlan 3
```

Отклик системы виден на рисунке 24.

```
R1-SW(vlan)#vlan 2
VLAN 2 added:
      Name: VLAN0002
R1-SW(vlan)#vlan 3
VLAN 3 added:
      Name: VLAN0003
R1-SW(vlan)#
```

Рис. 24. Создание базы данных VLAN на коммутаторе

Для маршрутизации между VLAN необходимо

1. Включить ip routing

```
R1-SW(config)#ip routing
```

2. Назначить IP-адреса соответствующим VLAN, для этого выполняются следующие команды:

- a. Вход в режим конфигурирования

```
R1-SW(config)#int vlan <Номер>
```

- b. Задание IP-адреса и маски VLAN

```
R1-SW(config-if)#ip address <Адрес> <Маска>
```

- c. Подъем VLAN

```
R1-SW(config-if)#no sh
```

- d. Выход из режима конфигурирования

```
R1-SW(config-if)#ex
```

Настройка интерфейса коммутатора третьего уровня для работы с трафиком VLAN состоит из следующих шагов:

1. Вход в режим конфигурирования

```
R1-SW(config)#int <Имя интерфейса>
```

2. Подъем интерфейса

```
R1-SW(config-if)#no sh
```

3. Указание режима работы

access:

```
R1-SW(config-if)#switchport mode access
```

trunk:

```
R1-SW(config-if)#switchport mode trunk
```

4. Подключение VLAN к порту:

access:

```
R1-SW(config-if)#switchport access vlan <Номер>
```

trunk:

```
R1-SW(config-if)#switchport trunk encapsulation dot1q
```

```
R1-SW(config-if)#switchport trunk allowed vlan add <Номер>
```

5. Выход из режима конфигурирования

```
R1-SW(config-if)#ex
```

6. Если порт не принадлежит ни одному VLAN, необходимо указать:

```
R1-SW(config-if)#no switchport
```

III Настройка VLAN на Ethernet switch 2-го уровня

Пример настройки VLAN на портах коммутаторов SW1 и SW2 показан на рис. 25.

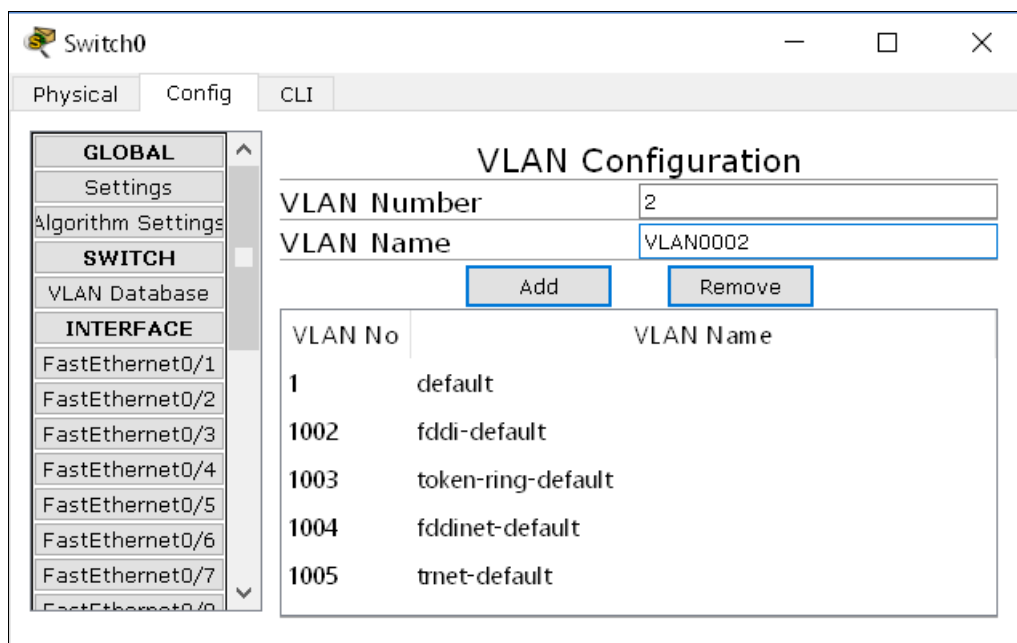


Рис. 25. Настройка VLAN на локальных коммутаторах

Интерфейсы FastEthernet (0/1, 0/2, 0/3) должны быть настроены на соответствующий режим работы, как это показано в разделе II для R1-SW.

IV Другие команды CLI

1. Просмотр настроек VLAN:

```
R1-SW#show vlan brief
```

Отклик на команду приведён на рис. 26.

```

R1-SW#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/4, Fa0/5, Fa0/6,
Fa0/7                    Fa0/8, Fa0/9, Fa0/10,
Fa0/11                   Fa0/12, Fa0/13, Fa0/14,
Fa0/15                   Fa0/16, Fa0/17, Fa0/18,
Fa0/19                   Fa0/20, Fa0/21, Fa0/22,
Fa0/23                   Fa0/24, Gig0/1, Gig0/2

2    VLAN0002                active
3    VLAN0003                active
1002 fddi-default           active
1003 token-ring-default     active
1004 fddinet-default        active
1005 trnet-default          active

```

Рис. 26. Команда просмотра настроек VLAN

2. Просмотр настроек интерфейсов, работающих в режиме trunk:

`R1-SW#show interface trunk`

Отклик на команду приведён на рис. 27.

```

R1-SW#show interface trunk

Port      Mode      Encapsulation  Status        Native vlan
Fa0/2     on        802.1q         trunking      1
Fa0/3     on        802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/2     1-1005
Fa0/3     1-1005

Port      Vlans allowed and active in management domain
Fa0/2     1,2,3
Fa0/3     1,2,3

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/2     1,2,3
Fa0/3     1,2,3

```

Рис. 27. Команда просмотра интерфейсов

3. Просмотр режимов работы интерфейсов:

`R1-SW#show interface switchport`

Отклик на команду приведён на рис. 28.

```

R1-SW#show interface switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
--More--

```

Рис. 28. Команда просмотра режимов работы интерфейсов

Задание:

Настроить две виртуальные сети и маршрутизацию между ними на примере структуры, представленной на рис. 29.

Выбрать для реализации устройства Cisco Router 1841, четыре PC-PT, а также два Ethernet коммутатора второго уровня и один Multilayer Switch 3560 коммутатор третьего уровня (с функциями маршрутизатора, обозначенный на схеме R1-SW). В Ethernet switch 3-го уровня будут задействованы интерфейсы коммутатора (FastEthernet 0/1, FastEthernet 0/2, FastEthernet 0/3).

Произвести конфигурирование сетевых интерфейсов хостов (рис. 30) и просмотреть настройки.

Произвести настройки VLAN и маршрутизации между ними. Настроить маршрутизацию между коммутатором 3-го уровня и маршрутизатором. Сконфигурировать интерфейсы коммутаторов 2-го уровня.



Примечание: Маску подсети для простоты сделать 24-разрядной.

Просмотреть настройки VLAN. Пропинговать сетевые устройства, оценить полученные результаты.

Сетевые настройки устройств приведены в табл. 2.

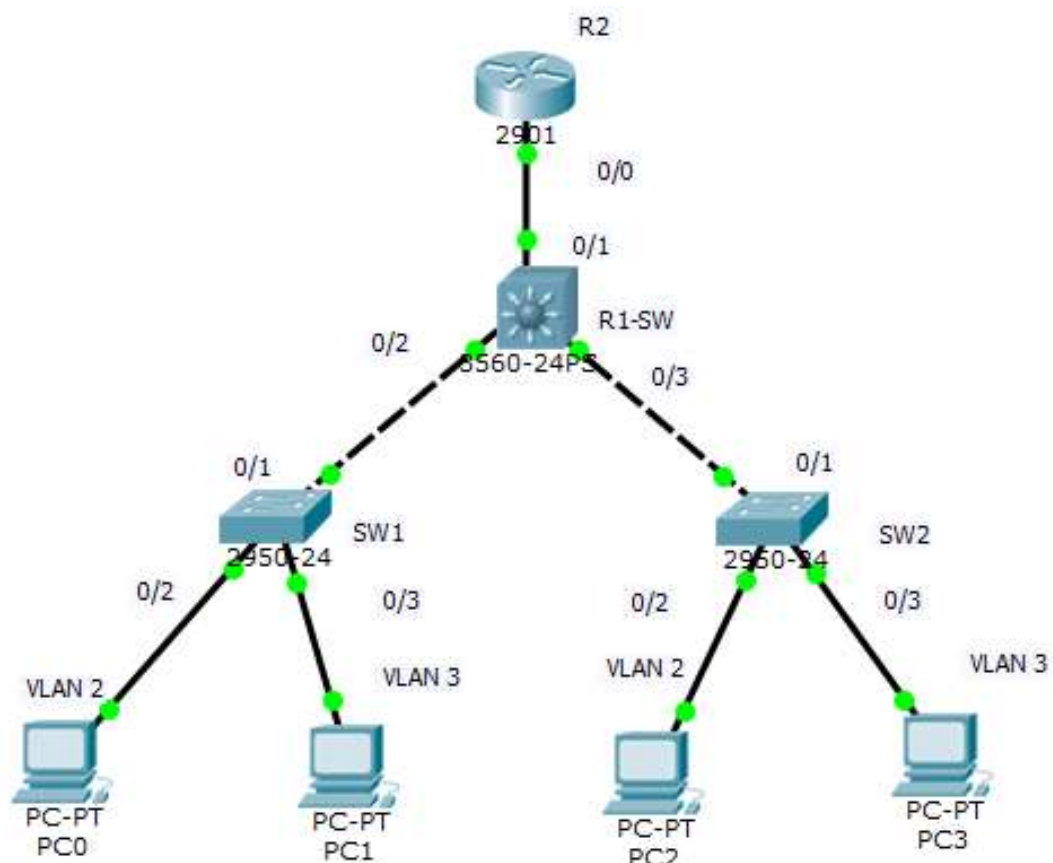


Рис. 29 – Схема сети

Таблица 2 – Сетевые настройки интерфейсов и VLAN

Устройство	Интерфейс	IP-адрес	Режим	VLAN	Шлюз
R1	Fa 1/1	-	trunk	vlan 2-3	-
	Fa 1/2	-	trunk	vlan 2-3	-
	Fa 1/0	10.10.10.1	no switchport	-	10.10.10.2
R2	Fa 0/0	10.10.10.2	-	-	10.10.10.1
PC0	Eth 0	20.20.20.2	-	vlan 2	20.20.20.1
PC1	Eth 0	30.30.30.2	-	vlan 3	30.30.30.1
PC2	Eth 0	20.20.20.3	-	vlan 2	20.20.20.1
PC3	Eth 0	30.30.30.3	-	vlan 3	30.30.30.1
SW1	0/1	-	dot1q (trunk)	vlan 1-3	-
	0/2	-	access	vlan 2	-
	0/3	-	access	vlan 3	-
SW2	0/1	-	dot1q (trunk)	vlan 1-3	-
	0/2	-	access	vlan 2	-
	0/3	-	access	vlan 3	-

Устройство	Интерфейс	IP-адрес	Режим	VLAN	Шлюз
Vlan 2	...	20.20.20.1	-	-	-
Vlan 3	...	30.30.30.1	-	-	-



Примечание: VLAN 1 не нужно настраивать, поскольку она определяется по умолчанию.

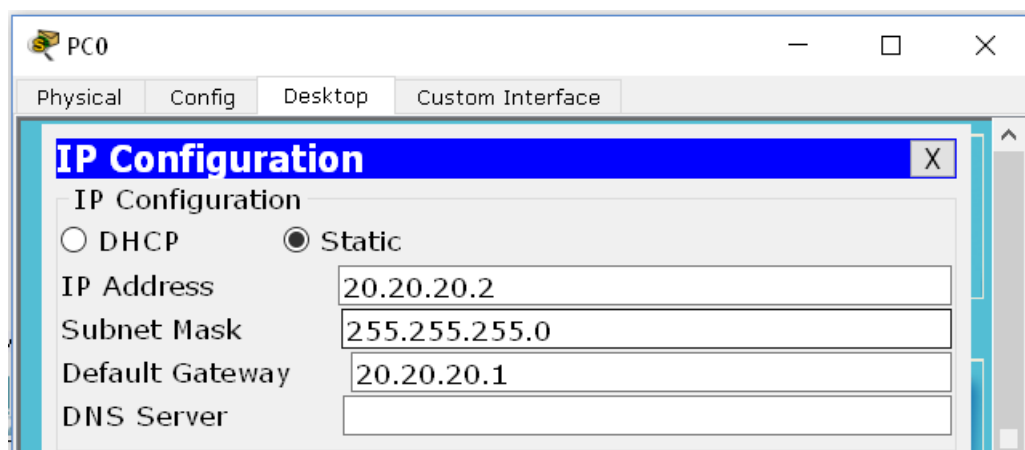


Рис. 30. Сетевые настройки хостов

Порядок выполнения лабораторной работы:

1. Создать новый проект Cisco Packet Tracer.
2. Построить сетевую структуру, представленную на рис. 29.
3. Настроить PC0–PC3 (задать IP-адрес, 24-разрядную маску и шлюз по умолчанию) в соответствии с табл. 2
4. Настроить роутер R2 в соответствии с табл. 2.
5. Сохранить настройки маршрутизатора.
6. Настроить интерфейсы коммутатора третьего уровня R1-SW.
7. Настроить VLAN 2–3 на R1-SW (раздел II). Поднять интерфейсы.
8. Поднять VLAN 1 на R1-SW.
9. Настроить trunk-интерфейсы на R1-SW (раздел II).
10. Настроить соединение и маршрутизацию (статическую или динамическую по вашему выбору) между R1-SW и R2.
11. Сохранить настройки R1-SW.
12. Настроить VLAN на локальных коммутаторах (рис. 25). Применить настройки.
13. Интерфейсы FastEthernet 0/1 SW1 и SW2 должны работать в режиме trunk, остальные интерфейсы – в режиме access.

14. Просмотреть информацию о VLAN, интерфейсах и режимах их работы (раздел IV).
15. Убедиться в достижимости всех объектов сети друг для друга (PC0, PC1, PC2, PC3) по протоколу IP командой ping.
16. Исправить ошибки, если таковые обнаружены, и сохранить конфигурацию. Снова запустить ping-процесс.
17. Оформить отчёт по лабораторной работе.
18. Сдать и защитить работу.

Структура отчета по работе:

1. Титульный лист.
2. Содержание с нумерацией страниц.
3. Задание к лабораторной работе.
4. Структура сети.
5. Сетевые настройки устройств со скриншотами.
6. Ход работы:

Данный раздел состоит из последовательного описания значимых выполняемых шагов (с указанием их сути) и копий экранов (должна быть видна набранная команда и реакция системы, если она есть).

7. Выводы по лабораторной работе.

Контрольные вопросы:

1. Что отличает локальную сеть LAN от других типов сетей (глобальная, персональная, городская...)?
2. Опишите понятие виртуальной локальной сети VLAN.
3. Охарактеризуйте технологию Ethernet и её разновидности.
4. Чем отличаются режимы TRUNK и ACCESS интерфейсов VLAN?
5. Обрисуйте разницу между коммутаторами 2-го и 3-го уровня.
6. Каким образом настраиваются VLAN на коммутаторах 3-го и 2-го уровня?

Некоторые команды CLI

Привилегированный режим:

```
R1#enable
```

Режим конфигурирования:

```
R1#configure terminal
```

или, сокращённый вариант:

```
R1#conf t
```

Изменение имени устройства (вместо <Name> поставить имя):

```
R1(config)#hostname <Name>
```

Отмена вывода всякого мусора в консоль:

```
R1(config)#no logging console
```

Настройка маршрутизации по умолчанию (вместо <next hop> подставить адрес следующего на пути к точке назначения маршрутизатора):

```
R1(config)#ip route 0.0.0.0 0.0.0.0 <next hop>
```

Вход в режим конфигурирования интерфейса (Fast Ethernet):

```
R1(config)#interface fastethernet 0/0
```

или, сокращённый вариант:

```
R1(config)#int fa0/0
```

Вход в режим конфигурирования интерфейса (Serial):

```
R1(config)#interface serial 0/0
```

или, сокращённый вариант:

```
R1(config)#int se0/0
```

Настройка IP-адреса и маски:

```
R1(config-if)#ip address 192.168.0.1 255.255.255.0
```

Поднять интерфейс:

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

или, сокращённый вариант:

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

Выйти из режима (вернуться на предыдущий уровень).

```
R1(config-if)#exit
```

Вернуться на самый верхний уровень

```
R1(config-if)#end
```

Сохранение текущей конфигурации:

```
R1#copy running-config startup-config
```

или сокращённый вариант:

```
R1#copy run start
```

Далее надо нажать Enter на вопрос системы об имени файла.

Просмотр текущей работающей конфигурации:

```
R1#show running-config
```

или:

```
R1#show run
```

Просмотр сохраненной конфигурации:

```
R1#show startup-config
```

или:

```
R1#show start
```

Запуск ping-процесса:

```
R1#ping <IP-адрес устройства>
```

Просмотр конфигурации интерфейсов:

```
R1#show interfaces
```

Просмотр маршрутной информации:

```
R1#show ip route
```

Список литературы

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы // СПб.: Питер, 2011. – 863 с.
2. Столлингс, В. Современные компьютерные сети: пер. с англ. – 2-е изд. // СПб.: ПИТЕР, 2003. – 782 с.
3. Таненбаум Э., Уэзеролл Э. Компьютерные сети : 5-е изд. // СПб.: ПИТЕР, 2013. – 960 с.

В разработке

Елена Викторовна Кокорева

АРХИТЕКТУРА ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ

АЛГОРИТМЫ МАРШРУТИЗАЦИИ

Лабораторный практикум

Учебно-методическое пособие

Редактор: К.И. Шурыгина

Корректор:

Подписано в печать

Формат бумаги 62×84 1/16, отпечатано на ризографе, шрифт №10,

Изд. л. 2,5, заказ №, тираж 5 экз.

СибГУТИ 630102, Новосибирск, ул. Кирова, 86