

Лабораторная работа №1.

Способы конфигурирования сетевых компонентов на основании симуляторов Cisco Packet Tracer и GNS.

Реализация физической топологии сети с помощью Cisco Packet Tracer и GNS

Эмулятор сети, это программа, позволяющая строить и анализировать сети на разнообразном оборудовании в произвольных топологиях с поддержкой разных протоколов. Эти программы позволяют получить возможность изучать работу различных сетевых устройств: маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров и т.д. В данной работе демонстрируются базовые навыки использования программных продуктов Cisco Packet Tracer и GNS.

Цель: научиться создавать сеть на базе программ Cisco Packet Tracer и GNS

Время выполнения лабораторной работы: 90 минут.

Теоретический материал: Cisco Packet Tracer:

Интерфейс программы Cisco Packet Tracer

На рис. 1.2 представлен *интерфейс* (главное окно) программы Cisco Packet Tracer.

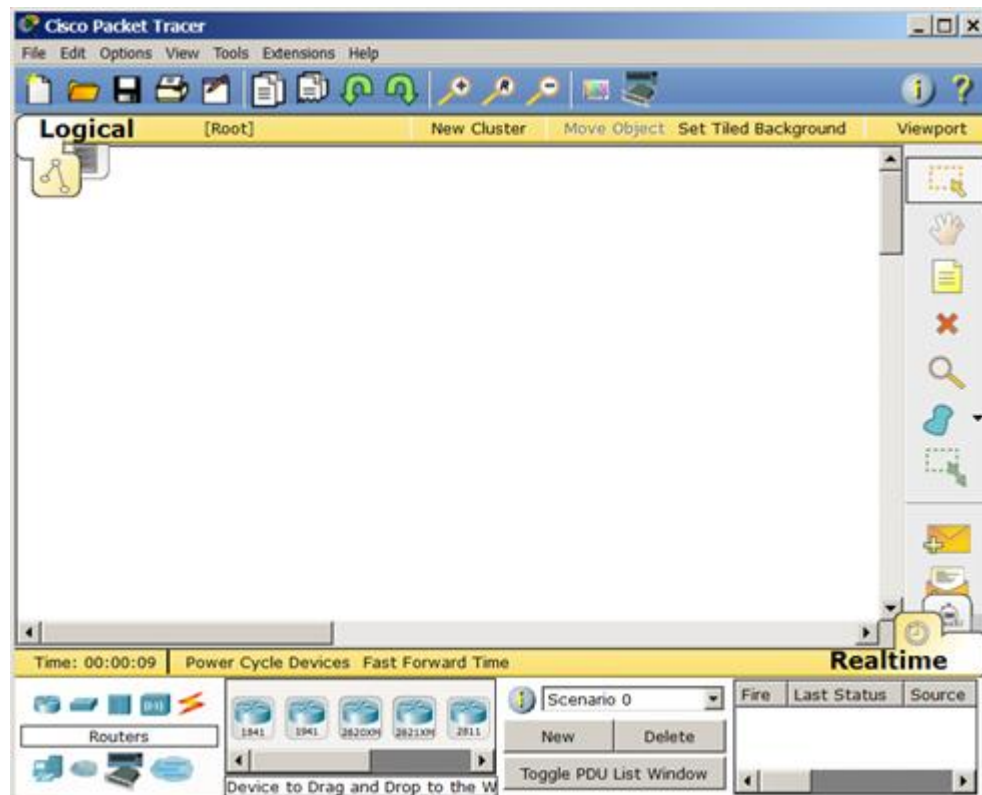


Рис. 1.2. Интерфейс программы Cisco Packet Tracer (CPT)

Главное меню

Главное меню показано на рис. 1.3.

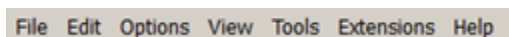


Рис. 1.3. Главное меню

File (Файл) - содержит *операции* открытия/сохранения документов.

Edit (Правка) - содержит стандартные *операции* "копировать/вырезать, отменить/повторить";

Options (Настройки) – содержит настройки программы. В частности, здесь расположена кнопка **Change Language**, позволяющая производить локализацию программы на другие языки.

View (Вид) - содержит инструменты изменения масштаба рабочей области и панели инструментов;

Tools (Инструменты) - содержит цветовую палитру и окно пользовательских устройств;

Extensions (Расширения) - содержит мастер проектов и ряд других инструментов;

Help (Помощь) – содержит помощь по программе.

Панель инструментов

Панель инструментов приведена на рис. 1.4.



Рис. 1.4. Панель инструментов

Панель инструментов с помощью пиктограмм дублирует основные пункты главного меню программы.

Оборудование

Снизу, под рабочей областью, расположена панель оборудования. Данная панель содержит в своей левой части типы (классы) устройств, а в правой части – их наименование (модели). При наведении на каждое из устройств, в прямоугольнике, находящемся в центре между ними будет отображаться его тип. Типы оборудования представлены на рис. 1.5.



Рис. 1.5. Панель оборудования Packet Tracer (Основные типы оборудования)

Маршрутизаторы (роутеры) используется для поиска оптимального маршрута передачи данных на основании алгоритмов маршрутизации.

Коммутаторы - устройства, предназначенные для объединения нескольких узлов в пределах одного или нескольких сегментах сети. *Коммутатор* (свитч) передаёт пакеты информации на основании таблицы коммутации, поэтому трафик идёт только на тот *MAC-адрес*, которому он предназначается, а не повторяется на всех портах, как на концентраторе (хабе).

Беспроводные устройства в программе представлены беспроводным маршрутизатором и тремя точками доступа.

Среди **конечных устройств** вы увидите ПК, ноутбук, *сервер*, принтер, телефоны и так далее. *Интернет* в программе представлен в виде облаков и модемов *DSL*. Пользовательские устройства и облако для многопользовательской работы показаны на рис. 1.6.



Рис. 1.6. Пользовательские устройства и облако для многопользовательской работы

Линии связи

С помощью линий связи создаются соединения узлов сети в единую топологию и при этом каждый тип кабеля может быть соединен лишь с определенными типами интерфейсов устройств (рис. 1.7).



Рис. 1.7. Типы линий связи

Автоматический тип – при данном типе соединения *Packet Tracer* автоматически выбирает наиболее предпочтительные тип соединения для выбранных устройств.

Консоль – консольные соединения. Консольное соединение может быть выполнено между ПК и маршрутизаторами или коммутаторами.

Медь прямой – соединение медным кабелем типа *витая пара*, оба конца кабеля обжаты в одинаковой раскладке.

Медь кроссовер – соединение медным кабелем типа *витая пара*, концы кабеля обжаты как кроссовер.

Оптика – соединение при помощи оптического кабеля, необходимо для соединения устройств, имеющих оптические интерфейсы.

Телефонный кабель – кабель для подключения телефонных аппаратов. Соединение через телефонную линию может быть осуществлено между устройствами, имеющими модемные порты. Пример - ПК, дозванивающийся в сетевое облако.

Коаксиальный кабель – соединение устройств с помощью коаксиального кабеля. Используется для соединения между кабельным модемом и облаком.

Серийный DCE и серийный DTE - соединения через последовательные порты для связей *Интернет*. Для настройки таких соединений необходимо установить синхронизацию на стороне *DCE*-устройства. Сторону *DCE* можно определить по маленькой иконке "часов" рядом с портом.

Графическое меню

На рис. 1.8 показано графическое меню программы.



Рис. 1.8.
Графическое меню

На этом рисунке слева направо:

Инструмент **Select** (Выбрать) можно активировать клавишей Esc. Он используется для выделения одного или более объектов для дальнейшего их перемещения, копирования или удаления.

Инструмент **Move Layout** (Переместить слой, горячая клавиша M) используется для прокрутки больших проектов сетей.

Инструмент **Place Note** (Сделать пометку, клавиша N) добавляет текст в рабочей области проекта.

Инструмент **Delete** (Удалить, клавиша Del) удаляет выделенный *объект* или группу объектов.

Инструмент **Inspect** (Проверка, клавиша I) позволяет, в зависимости от типа устройства, просматривать содержимое таблиц (*ARP*, *NAT*, таблицы маршрутизации др.).

Инструмент **Drawapolygon** (Нарисовать многоугольник) позволяет рисовать прямоугольники, эллипсы, линии и закрашивать их цветом.

Инструмент **Resize Shape** (Изменить размер формы, комбинация клавиш Alt+R) предназначен для изменения размеров рисованных объектов (четыреугольников и окружностей).

Элементы анимации и симуляции

Эти элементы интерфейса показаны на рис. 1.9.



Рис. 1.9. Элементы анимации и симуляции

Инструменты **Add Simple PDU** (Добавить простой *PDU*, клавиша P) и **Add Complex PDU** (Добавить комплексный *PDU*, клавиша C) предназначены для эмулирования отправки пакета с последующим отслеживанием его маршрута и данных внутри пакета.

Физическое представление оборудования

В программе возможно физическое *представление* оборудования в виде его физической конфигурации (рис. 1.10).



Рис. 1.10. Физическая конфигурация ПК

Для изменения комплектации оборудования необходимо отключить его питание, кликнув мышью на кнопке питания и перетащить мышью нужный *модуль* в свободный *слот*, затем включить питание. В качестве примера я добавил в физическую конфигурацию ПК микрофон (PT-MICROPHONE), в результате чего ПК изменил свой значок в программе (рис. 1.11).



Рис. 1.11. Изменение пиктограммы ПК после подключения к нему микрофона

Остальные модули добавляются в устройства аналогично. Так, на *компьютер* есть возможность добавить не только микрофон, но и, например, наушники или жесткий *диск* для хранения данных.

Практическая работа 1-1. Создание сети из двух ПК в программе Cisco Packet Tracer

В качестве примера для начального знакомства с программой построим простейшую *сеть* из двух ПК, соединенных кроссовым кабелем (рис. 1.12).

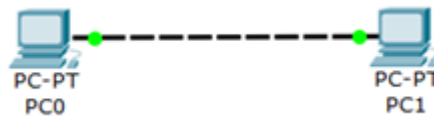


Рис. 1.12. Сеть из двух ПК

Для решения нашей задачи на вкладке **End Devices** **Ctrl+Alt+V** (Конечные устройства) выбираем тип компьютера и переносим его мышью в рабочую область программы (рис. 13).

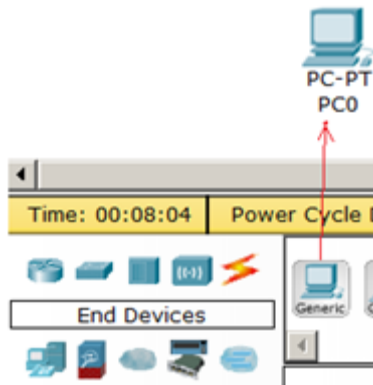


Рис. 1.13. Устанавливаем в рабочую область программы первый ПК

Компьютеры соединяем посредством медного кроссовера **Copper Cross-Over** (Перекрестный кабель).

Совет: Если при выборе кроссовера зеленые лампочки не загорятся, то выберите тип соединения **Автоматически**.

Теперь приступим к настройке левого ПК: щелкаем на нем мышью, переходим на вкладку **Ip Configuration** (Настройка IP) – рис. 1.14.



Рис. 1.14. Стрелка показывает на кнопку открытия окна IP Configuration

Для первого ПК вводим *IP адрес* 192.168.1.1 и маску подсети 255.255.255.0, окно закрываем (рис. 1.15). Аналогично настраиваем второй ПК на *адрес* 192.168.1.2 и ту же маску.

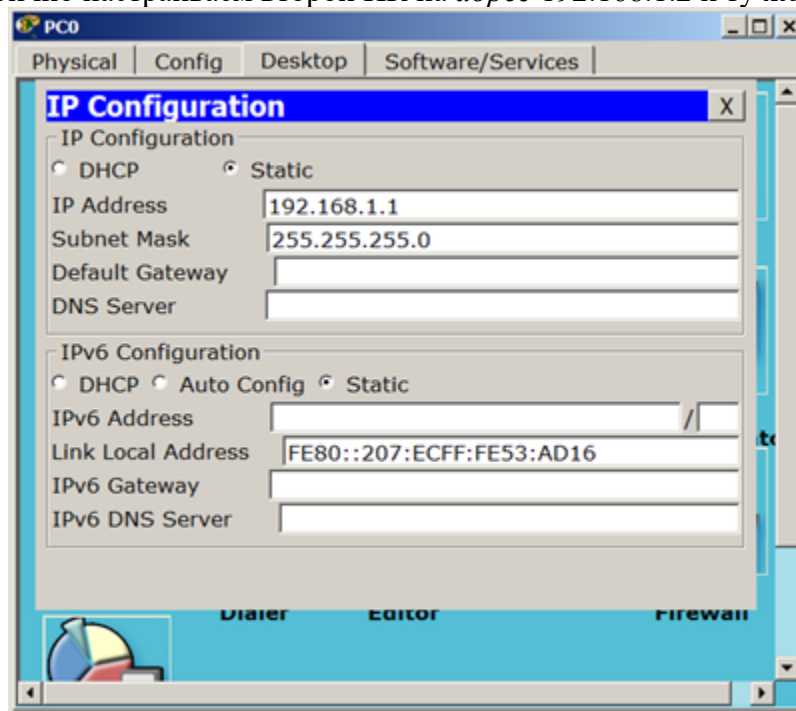


Рис. 1.15. Окно настройки PC0

Далее проверим наличие связи ПК и убедимся, что ПК0 и ПК1 видят друг друга. Для этого на вкладке **Desktop** (**Рабочий стол**) перейдем в поле *run* (*Командная строка*) и пропингуем соседний ПК (рис. 1.16).

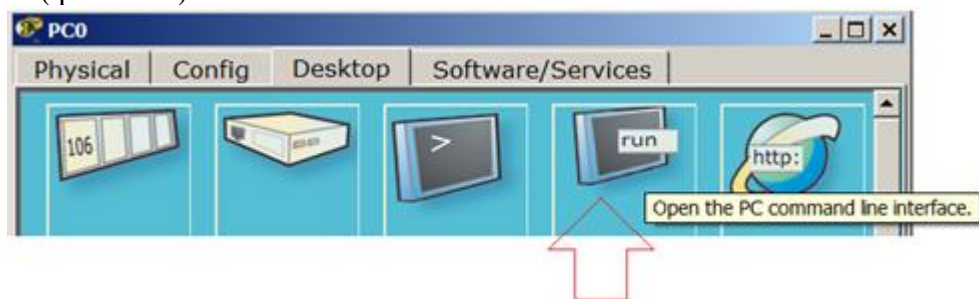


Рис. 1.16. Кнопка run

Как видно из рис. 1.17 *связь* между ПК присутствует (настроена).


```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=62ms TTL=128
Reply from 192.168.1.2: bytes=32 time=32ms TTL=128
Reply from 192.168.1.2: bytes=32 time=31ms TTL=128
Reply from 192.168.1.2: bytes=32 time=32ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 62ms, Average = 39ms

PC>
```

Рис. 1.17. Пинг прошел успешно

Теоретический материал: Режим симуляции в Cisco Packet Tracer

Cisco Packet Tracer содержит режим симуляции работы сети, в котором можно имитировать сетевые события. Рассмотрим конкретный пример.

Практическая работа 2-1.

Организация Режимы симуляции работы сети

Сформируйте в рабочем пространстве программы *сеть* из 4х ПК и 2х хабов. Задайте для ПК IP адреса и маску сети 255.255.255.0 (рис. 2.1).

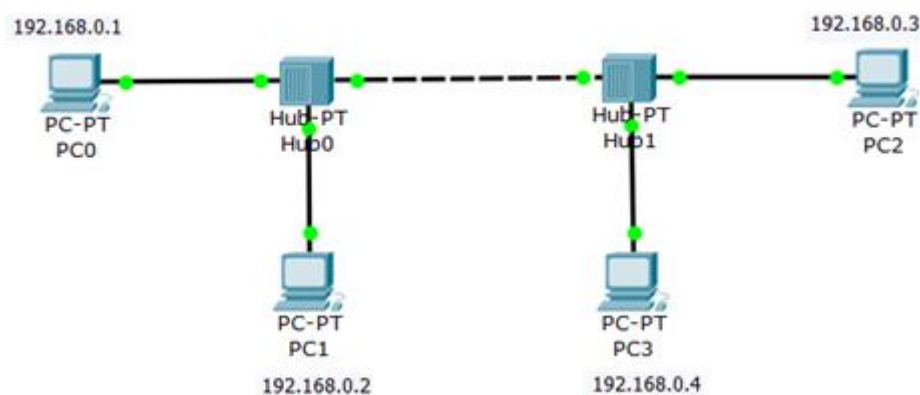


Рис. 2.1. Все ПК расположены в одной сети

Совет: Нашу схему вы можете сохранить в виде картинки с расширением *PNG командой **File-Print-Print to file**.

Теперь нужно перейти в режим симуляции комбинацией клавиш **Shift+S**, или, щелкнув мышью на иконку симуляции в правом нижнем углу рабочего пространства (рис. 2.2).

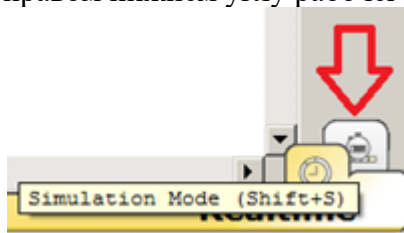


Рис. 2.2. Кнопка Симуляция

Нажмите на кнопку **Edit Filters** (Изменить фильтры) и исключите все сетевые протоколы, кроме *ICMP* (рис. 2.3).

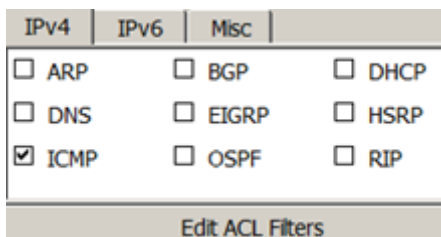


Рис. 2.3. Флажок ICMP активен

Новый термин

ICMP (Internet Control Message Protocol) — сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных.

С одного из хостов попробуем пропинговать другой узел. Для этого выбираем далеко расположенные друг от друга узлы, для того, чтобы наглядней увидеть, как будут проходить пакеты по сети в режиме симуляции. Итак, с PC1 пингуем PC2 (рис. 2.4).

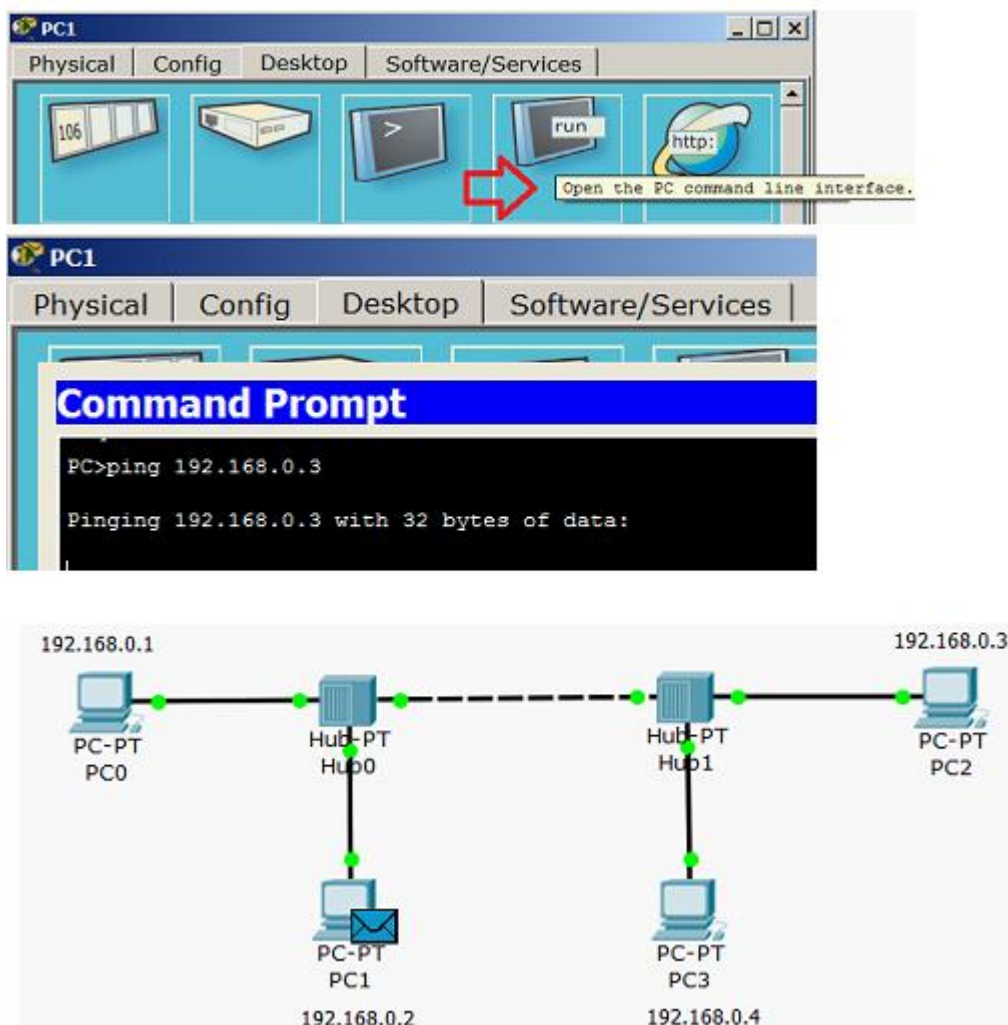


Рис. 2.4. PC1 пингует PC2 (начало процесса)

Примечание: Ping — утилита для проверки соединений в сетях на основе TCP/IP. Утилита отправляет запросы (ICMP Echo-Request) протокола ICMP указанному узлу сети и фиксирует поступающие ответы (ICMP Echo-Reply). Время между отправкой запроса и получением ответа (RTT) позволяет определять двусторонние задержки (RTT) по маршруту и частоту потери пакетов, то есть косвенно определять загруженность на каналах передачи данных и промежуточных устройствах. Полное отсутствие ICMP-ответов может также означать, что удалённый узел (или какой-либо из промежуточных маршрутизаторов) блокирует ICMP Echo-Reply или игнорирует ICMP Echo-Request.

На PC1 образовался пакет (конвертик), который ждёт начала движения его по сети. Запустить продвижение пакет в *сеть* пошагово можно, нажав на кнопку **Capture / Forward** (Вперёд) в окне симуляции. Если нажать на кнопку **Auto Capture / Play** (воспроизведение), то мы увидим весь цикл прохождения пакета по сети. В (*Список событий*) мы можем видеть успешный результат пинга (рис. 2.5).



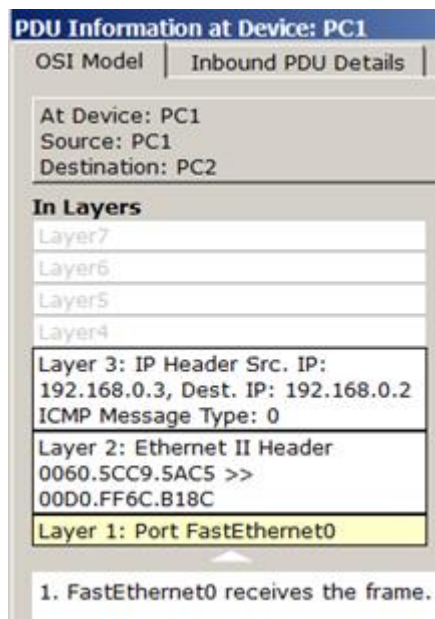
| Event List | | | | | | | | | | Simulation |
|---|-------------|--------|-------------|------|---|----------|----------|-----|--------|------------|
| Fire | Last Status | Source | Destination | Type | Color | Time(se) | Periodic | Num | Edit | Delete |
|  | Successful | PC1 | PC2 | ICMP |  | 0.000 | N | 0 | (edit) | (delete) |

Рис. 2.5. Связь PC1 и PC2 есть

Теоретический материал: Модель OSI в Cisco Packet Tracer

Щелчок мышью на конверте покажет нам дополнительную информацию о движении пакета по сети. При этом на первой вкладке мы увидим **модель OSI** (рис. 2.6). На вкладке *OSI Model* (Модель *OSI*) представлена *информация* об уровнях *OSI*, на которых работает данное сетевое устройство.



| PDU Information at Device: PC1 | |
|--|---------------------|
| OSI Model | Inbound PDU Details |
| At Device: PC1 Source: PC1 Destination: PC2 | |
| In Layers | |
| Layer7 | |
| Layer6 | |
| Layer5 | |
| Layer4 | |
| Layer 3: IP Header Src. IP: 192.168.0.3, Dest. IP: 192.168.0.2 ICMP Message Type: 0 | |
| Layer 2: Ethernet II Header 0060.5CC9.5AC5 >> 00D0.FF6C.B18C | |
| Layer 1: Port FastEthernet0 | |
| 1. FastEthernet0 receives the frame. | |

Рис. 2.6. Мониторинг движения пакета на модели OSI

На другой вкладке можно посмотреть структуру пакета (рис. 2.7).

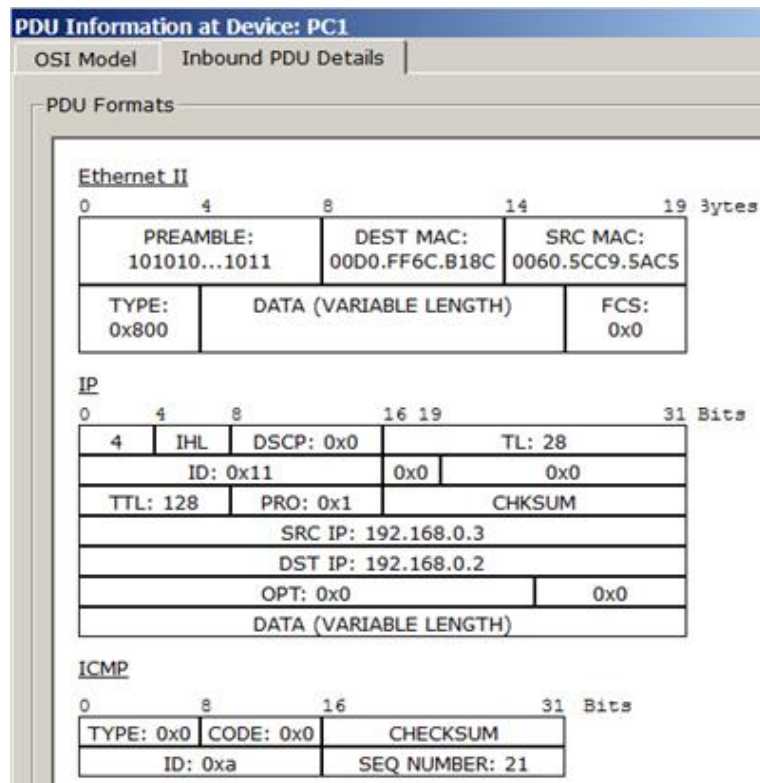


Рис. 2.7. Структура пакета

Итак, подведем некий промежуточный итог нашей работы. В *Packet Tracer* предусмотрен режим моделирования (Симуляции), в котором показывается, как работает утилита *Ping*. Чтобы перейти в данный режим, необходимо нажать на значок **Simulation Mode** (Симуляция) в нижнем правом углу рабочей области или комбинацию клавиш **Shift+S**. Откроется **Simulation Panel** (Панель симуляции), в которой будут отображаться все события, связанные с выполнения *ping*-процесса. Моделирование прекращается либо при завершении *ping*-процесса, либо при закрытии окна симуляции. В режиме симуляции можно не только отслеживать используемые протоколы, но и видеть, на каком из семи уровней модели *OSI* данный протокол задействован. В процессе просмотра анимации мы увидели принцип работы хаба. Концентратор (*хаб*) повторяет пакет на всех портах в надежде, что на одном из них есть получатель информации. Если пакеты каким-то узлам не предназначены, эти узлы игнорируют пакеты. А когда пакет вернется отправителю, то мы увидим галочку "принятие пакета". (рис. 2.8).

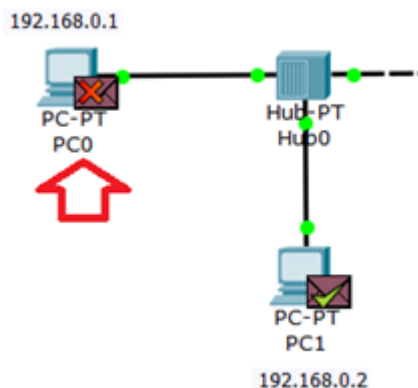


Рис. 2.8. Значки игнорирования пакетов и подтверждение соединения

Командная строка

Если нажать на кнопку **Auto Capture / Play** (воспроизведение), то мы увидим весь цикл прохождения пакета по сети (процесс повторится 4 раза) – рис. 2.9.

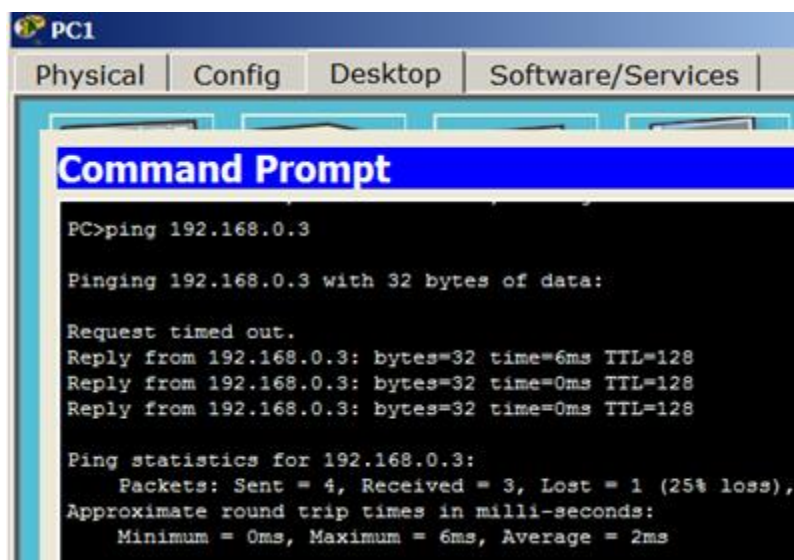


Рис. 2.9. Пинг от ПК1 до ПК2

Здесь:

TTL- время жизни отправленного пакета (определяет максимальное число маршрутизаторов, которое пакет может пройти при его продвижении по сети),

time - время, потраченное на отправку запроса и получение ответа,

min - минимальное время ответа,

max - максимальное время ответа,

avg - *среднее время* ответа.

Практическая работа 2-2.

Настройка сетевых параметров ПК в его графическом интерфейсе

Добавим в нашу *сеть* еще один ПК – PC4. Пример измененной сети из пяти ПК и 2-х хабов (рис. 2.10).

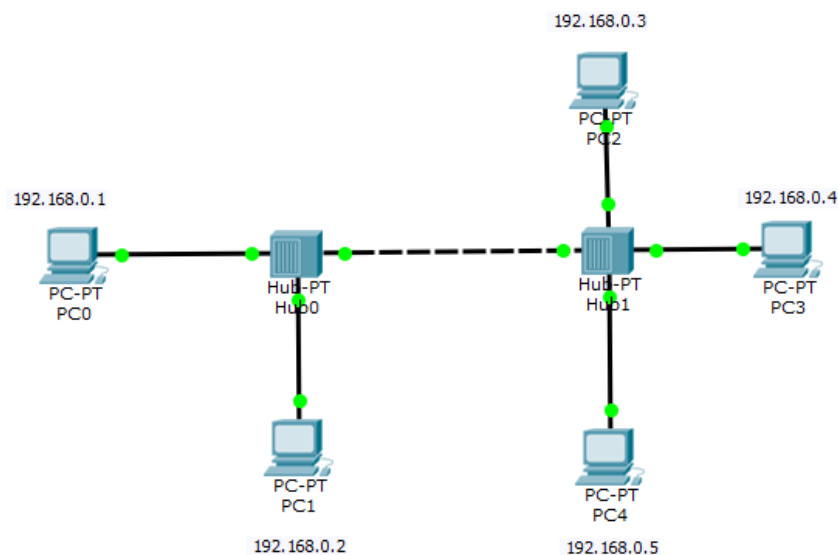


Рис. 2.10. Схема сети

Откроем свойства устройства PC4, нажав на его изображение. Для конфигурирования компьютера воспользуемся командой **ipconfig** из командной строки (рис. 2.11).

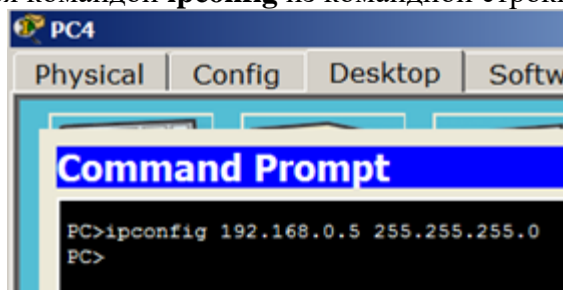


Рис. 2.11. Назначаем для ПК ip адрес и маску сети

Совет: вместо команды **ipconfig** можно использовать **show ip all**

Как вариант, *IP адрес* и маску сети можно вводить в графическом интерфейсе устройства (рис. 2.12).

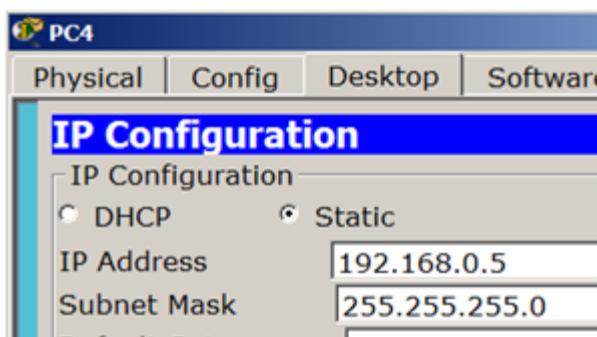


Рис. 2.12. Второй способ конфигурирования компьютера (настройки узла сети)

На каждом компьютере проверим назначенные нами параметры командой **ipconfig/show ip all** (рис. 2.13).

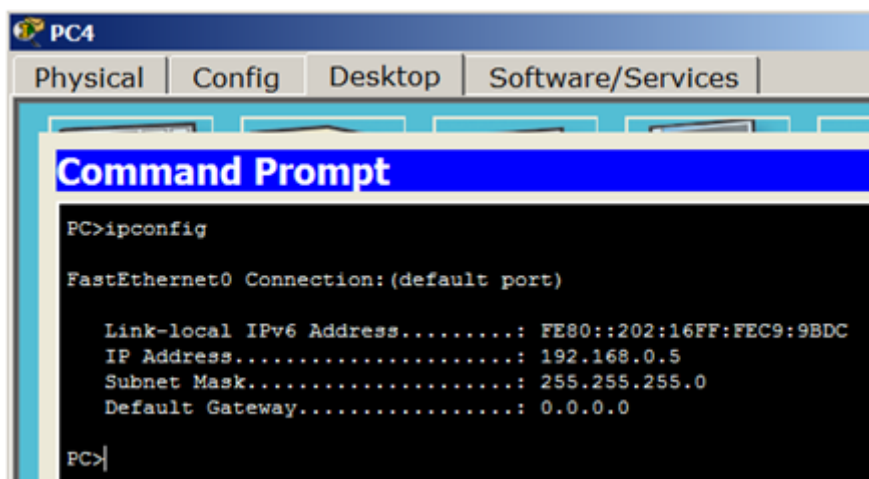


Рис. 2.13. Проверка конфигурирования ПК3

Теоретический материал: Graphical Network Simulator - GNS3:

Одной из альтернатив Cisco *Packet Tracer* является бесплатная программа **GNS3** – Графический Симулятор Сети. GNS3 позволяет моделировать работу реальных сетей, что крайне важно для обучения сетевого персонала. Фактически вы получаете имитацию полноценной компьютерной сети с дорогостоящим оборудованием – на вашем ПК или сервере.

GNS3 (Graphical Network Simulator) - среда моделирования компьютерных сетей, использующих сетевое оборудование, функционирующее на базе процессоров с архитектурой MIPS. К таким сетевым устройствам относятся, в том числе, большинство сетевых коммутаторов и маршрутизаторов, производимых компанией CISCO.

Свою историю среда GNS3 начинает с 2007 года, в котором Джереми Гроссман (Jeremy Grossman) занимался выполнением выпускной квалификационной работы и ему было необходимо создать среду моделирования компьютерных сетей. В основу создаваемого программного продукта легла разработка эмулятора MIPS устройств Dynamips и его графического интерфейса Dynagen.

В дальнейшем среда GNS3 получила широкое распространение и теперь является одним из популярных сред для изучения компьютерных сетей и отработки различных промышленных решений.

В текущей версии для своего функционирования среда GNS3 использует следующее программное обеспечение:

- WinPCAP – системный драйвер и библиотека функций, позволяющая получить доступ к сетевым интерфейсам физического компьютера и передаваемой/получаемой информации по ним. Используется для анализа трафика, передаваемого по сети;
- Wireshark – графический анализатор сетевого трафика. Позволяет наглядно отобразить подробнейшую информацию о сетевом трафике. Используется как внутри среды GNS3, так и позволяет анализировать трафик с реальной компьютерной сети (считывая его с физических интерфейсов с помощью драйвера WinPCAP);
- Dynamips – среда моделирования сетевых устройств, реализованных на базе процессоров с MIPS архитектурой. Для своего функционирования требует наличие образов операционных систем iOS сетевых устройств CISCO. Допускает выполнение и иных операционных систем.
- VPCS, VirtualBox, QEMU – среды моделирования ЭВМ. Используются для эмулирования оконечных сетевых устройств или промежуточных устройств, реализованных на базе ЭВМ с архитектурой IBM/PC;

- SolarWinds Response – среда для анализа сетевого трафика. Используется для графического отображения информации, подготовленной Wireshark;
- SuperPUTTY – система виртуальных терминалов. Позволяет подключаться к сетевым устройствам для управления ими.
- Cpulimit – средство ограничения объемов потребления процессорного времени.

Интерфейс среды GNS3 и её начальное конфигурирование

После установки и запуска среды GNS3 пользователь видит главное рабочее окно (см. рисунок 3.1), содержащее традиционные элементы (строку заголовка, меню, строку состояния) и шесть рабочих областей:

- Панели инструментов (1 и 2), используются для доступа к основным инструментам работы с моделью компьютерной сети, включая сохранение проекта, его открытие и создание нового;
- Окно сетевых устройств (блоков, для построения модели сети, 3), используется для выбора элементов для размещения в создаваемой модели сети;
- Рабочая область, отражающая созданную модель сети (4);
- Перечень устройств, которые задействованы в модели сети (5);
- Командная панель, используется для управления моделью с использованием командной строки (6). Перечень команд и их описание доступны по команде help.

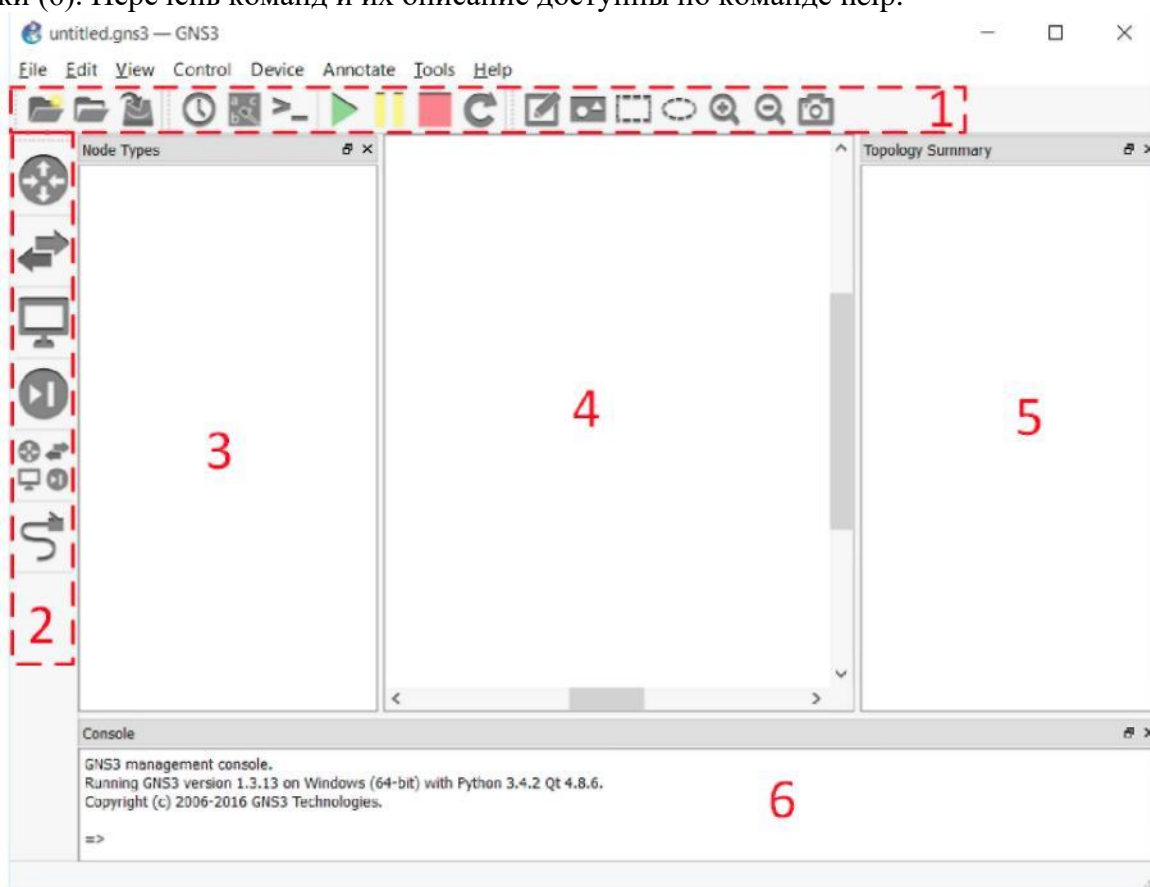


Рис. 3.1: Главное окно программы GNS3

Рассмотрим подробнее панели инструментов 1 и 2 (все кнопки рассматриваются слева направо, рис. 3.2):



Рис. 3.2: Панель инструментов программы GNS3

Управление отдельным сетевым устройством осуществляется через контекстное меню, доступное при наведении на него курсора мышки и нажатии правой кнопки мышки (см. рисунок 3.3.). В этом меню доступны также элементы включения (Start), выключения (Stop) и приостановки (Suspend), а также: конфигурирования устройства (Configure, см. рисунок 3.4), изменения имени устройства (Change hostname), изменения изображения устройства в модели (change symbol), доступ к консоли управления (Console), доступ к порту управления (Auxiliary console), Сохранения и восстановления конфигурации устройства (import config, export config, save config), просмотр сетевого трафика (capture), настройка модельных параметров (idle-pc, auto idle-pc), изменения прикрепления к слоям отображения модели (raise one layer, lower one layer) и удаления устройства из модели (Delete).

Управление файлами с моделью сети (создать новый проект, открыть существующий проект, сохранить текущий проект).

Доступ к элементам, используемым для построения модели компьютерной сети (маршрутизаторы, коммутаторы, оконечные устройства, устройства безопасности сети, все устройства и соединители).

Средства работы с изображением модели компьютерной сети (текстовая запись, рисунок из файла, прямоугольник, круг, увеличить масштаб отображения модели (визуально приблизить модель), уменьшить масштаб отображения модели, сделать копию изображения модели компьютерной сети).

Управление моделью компьютерной сети (управление снимками текущего состояния модели, управление отображением наименований сетевых интерфейсов, подключиться ко всем консолям сетевых устройств модели, «включить» все сетевые устройства модели, приостановить работу всех сетевых устройств модели, «выключить» все устройства модели, привести все устройства модели в исходное состояние).

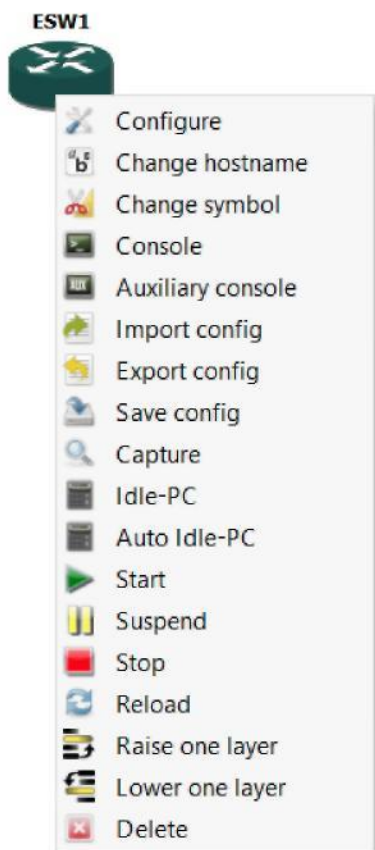


Рис.3.3 Контекстное меню управления элементом модели (на примере маршрутизатора)

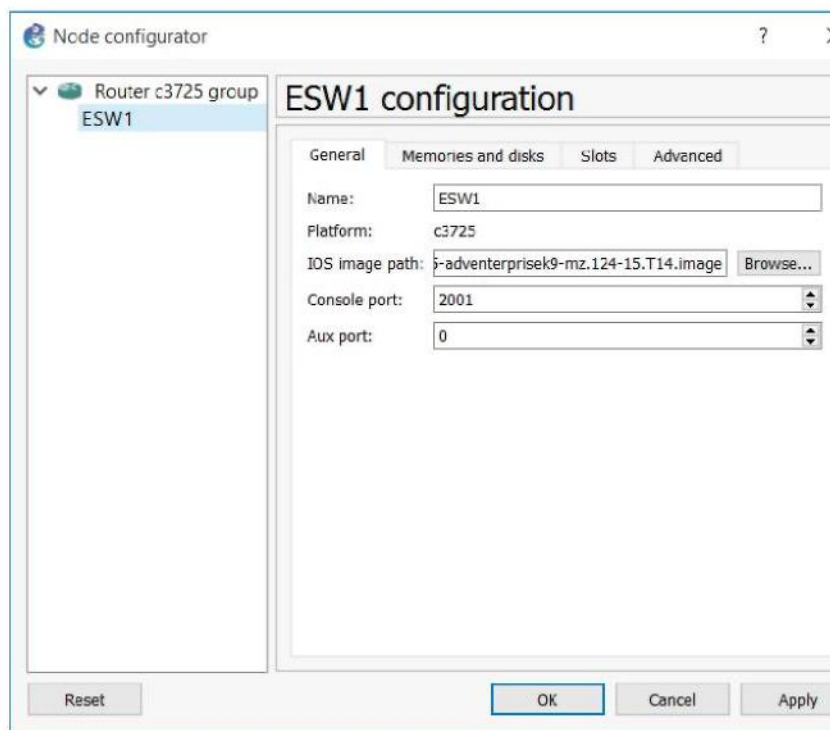


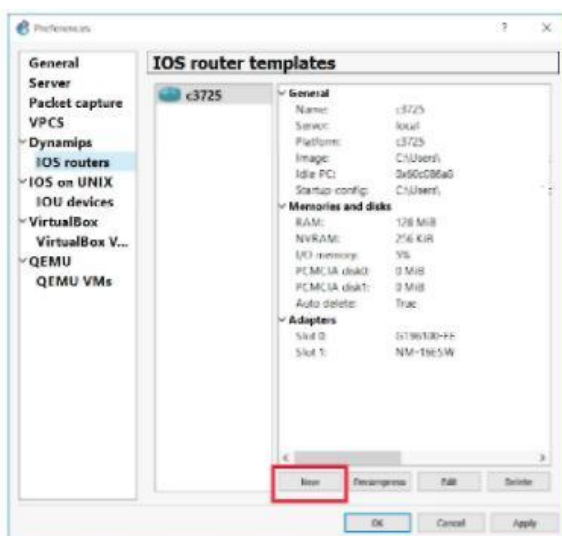
Рис.3.4 Окно конфигурации маршрутизатора

Параметры конфигурирования зависят от типа устройств. Некоторые из параметров будут рассмотрены ниже.

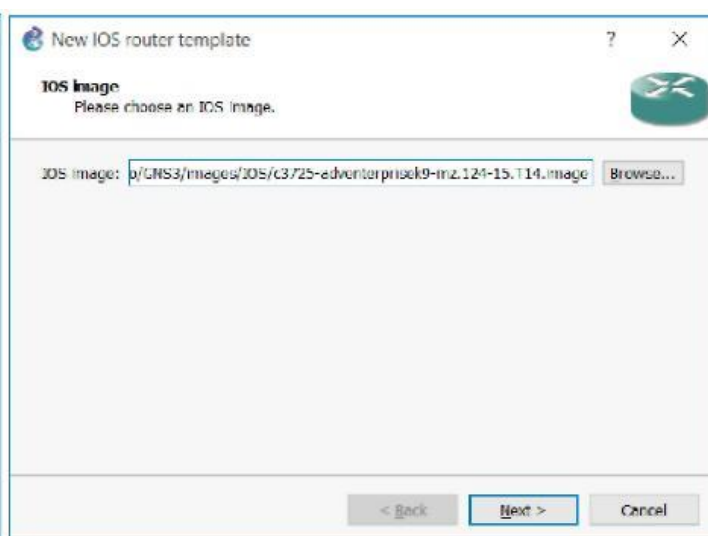
При первом запуске системы GNS необходимо создать модели устройств, которые будут использоваться в создаваемом проекте компьютерной сети. В рамках лабораторной работы планируется использование трех типов устройств: коммутатор, маршрутизатор, персональный компьютер.

В качестве коммутатора будет использоваться встроенная модель коммутатора, имеющая несколько интерфейсов Ethernet. В режиме конфигурирования для этой модели доступны следующие параметры: количество интерфейсов, режим работы интерфейса (access или trunk) и номер VLAN, к которому этот интерфейс относится. В рамках лабораторной работы будет использован только параметр «количество интерфейсов».

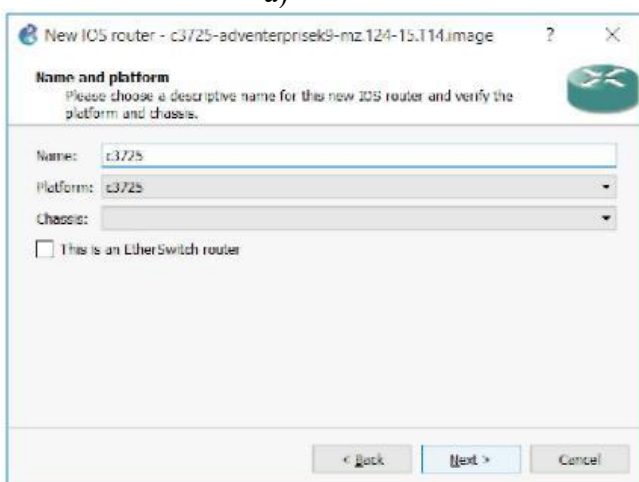
Для создания маршрутизаторов необходимо загрузить в систему моделирования образ операционных системы и сформировать соответствующий модельный элемент. Сделать это можно в режиме настройки среды (пункт меню Edit->Preferences), далее выбрав в дереве параметров пункт Dynamips->iOS routers (см. рисунок 3.5).



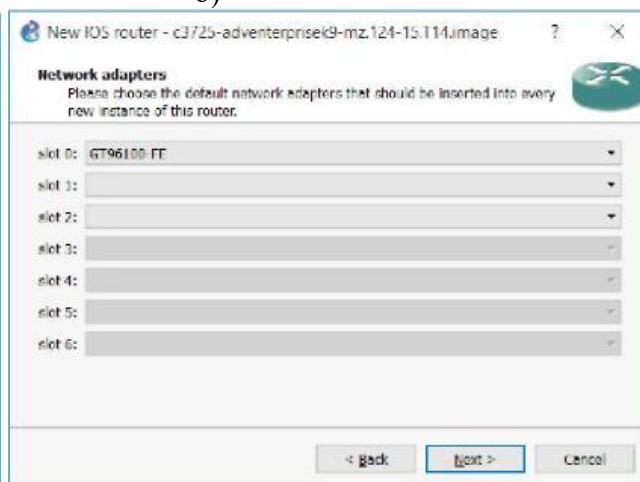
а)



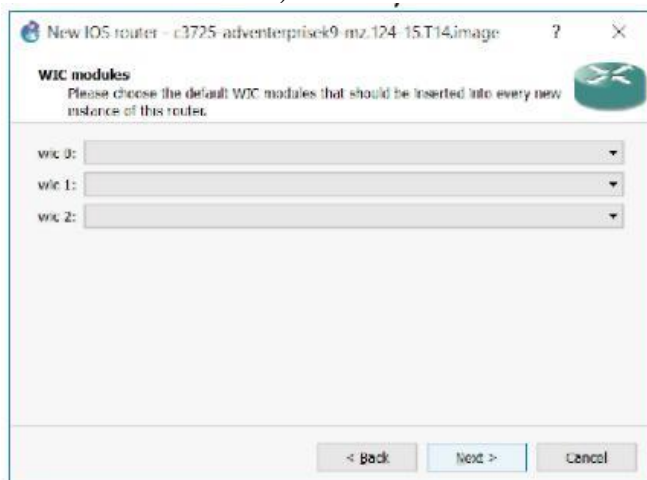
б)



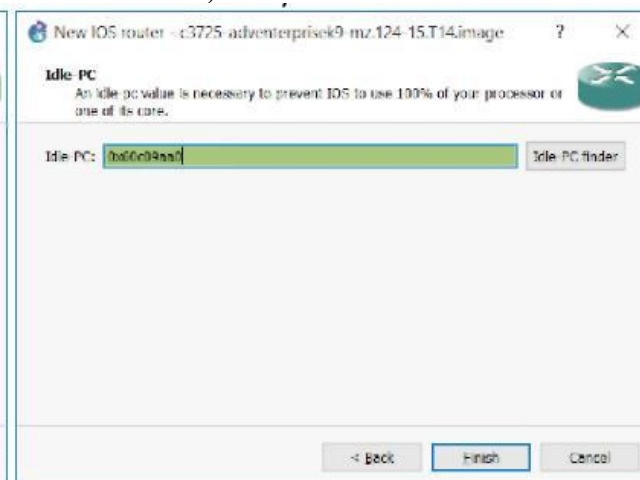
в)



г)



д)



е)

Рис. 3.5 Окно создания модельных элементов – маршрутизаторов
(а – начальное окно, б – выбор файла с «образом» операционной системы, в) выбор типа модели создаваемого сетевого устройства и его корпуса, г) определение заполнения «больших» слотов расширения, д) определение заполнения «малых» слотов расширения, е) число Idle-PC)

Конфигурация слотов расширения для оборудования CISCO производится аналогично, как и в системе Cisco Packet Tracer.

Объем памяти, необходимый для функционирования операционной системы определяется в соответствии с техническим описанием соответствующих устройств компании CISCO.

Особое внимание при создании модельных маршрутизаторов необходимо обратить на параметр Idle-PC, определяющий степень максимальной загрузки процесса, которую может достичь выполнение dynamips, реализующей этот маршрутизатор. Этот параметр предлагается системой автоматически при создании модельного объекта. Одна рекомендуется после создания модели сети и первого запуска модели провести перерасчет этих параметров, используя контекстное меню (пункт меню IdlePC). При этом перерасчет этого значения производится сразу для всех объектов сети, созданных на базе одного модельного объекта.

Для создания моделей персональных компьютеров необходимо настроить одну из сред виртуализации: VirtualBox, QEMU или VirtualPC. В рамках лабораторной работы будет использована среда VirtualBox, в которой создаются пустые контейнеры (см. рисунок 3.6).

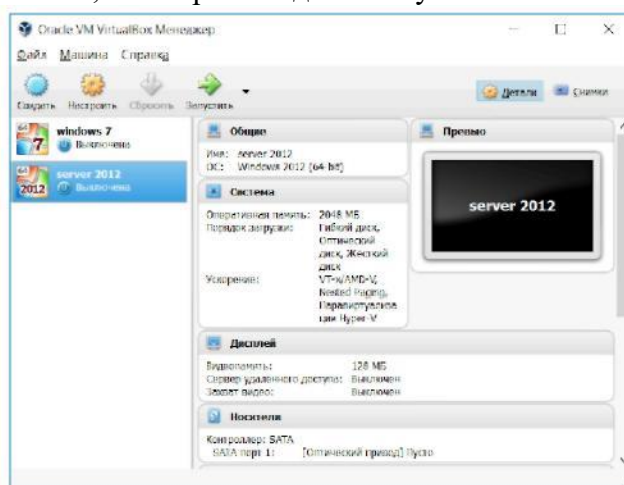


Рис.3.6 Окно менеджера VirtualBox с двумя пустыми контейнерами

После создания виртуальных машин их необходимо подключить к среде моделирования GNS3. Сделать это можно также в режиме настройки среды (пункт меню Edit->Preferences), далее выбрав в дереве параметров пункт VirtualBox->VirtualBox VM templates (см. рисунок 3.7).

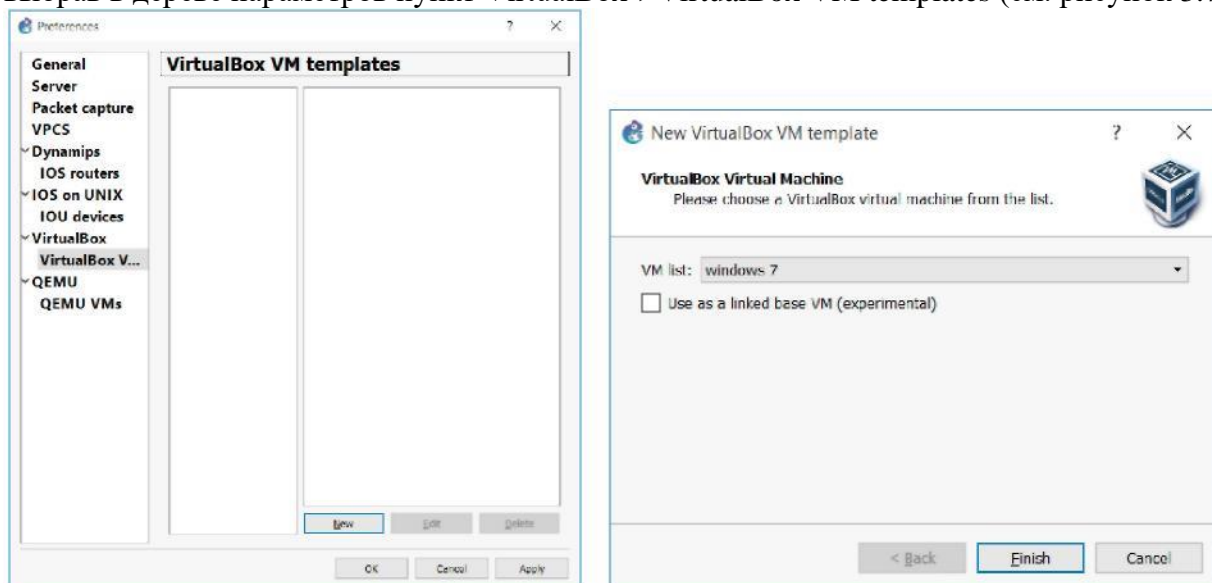


Рис.3.7 Подключение виртуальных машин и их конфигурирование

Здесь следует отметить, что для связи с виртуальными машинами по эмулируемой компьютерной среде будет использоваться протокол TCP/IP и потребуются разрешить доступ двух сред к соответствующим сетевым портам.

Для взаимодействия с физической сетевой средой в модели предусмотрено два объекта – Host и Cloud.

Задание 1: Создайте свою *сеть* из 2х ПК (по схеме согласно рис. 1.12) с помощью симулятора Cisco Packet Tracer и настройте ее работу. Параметры сетей должны использовать выделенный диапазон адресов по вариантам, представленным в приложении №1. Каждый студент осуществляет конфигурацию сети по индивидуальным параметрам. Результат настройки сети из двух компьютеров при выполнении практической работы следует сохранить в формате *.pkt и представить в приложении к отчету по лабораторной работе.

Задание 2: Создайте свою *сеть* из 4х ПК и 2х хабов (по схеме согласно рис. 2.1), с помощью симулятора Cisco Packet Tracer и настройте ее работу. Параметры сетей должны использовать выделенный диапазон адресов по вариантам, представленным в приложении №1. Каждый студент осуществляет конфигурацию сети по индивидуальным параметрам. Результат настройки сети из двух компьютеров при выполнении практической работы следует сохранить в формате *.pkt и представить в приложении к отчету по лабораторной работе. Симулируйте пинг с PC1 на PC2 и сохраните результаты в виде картинки пошагово и представьте их в отчете.

Задание 3: Создайте свою *сеть* из 5-и ПК и 2х хабов (по схеме согласно рис. 2.10), с помощью симулятора Cisco Packet Tracer и настройте ее работу. Параметры сетей должны использовать выделенный диапазон адресов по вариантам, представленным в приложении №1. Каждый студент осуществляет конфигурацию сети по индивидуальным параметрам. Результат настройки сети из 5 компьютеров при выполнении практической работы следует сохранить в формате *.pkt и представить в приложении к отчету по лабораторной работе. Конфигурирование и проверка конфигурации сети компьютера 5 осуществляется с помощью командной строки и сохраните пошагово действия в виде картинки в отчете.

Задание 4: Установить среду моделирования GNS3 и произвести начальную конфигурацию добавив два пустых контейнера с виртуальными машинами от VirtualBox. Создайте свою *сеть* из 2х ПК (по схеме согласно рис. 1.12) с помощью симулятора GNS3 и настройте ее работу. Параметры сетей должны использовать выделенный диапазон адресов по вариантам, представленным в приложении №1. Каждый студент осуществляет конфигурацию сети по индивидуальным параметрам. Результат настройки сети из двух компьютеров при выполнении практической работы следует сохранить в формате *.gns3 и представить в приложении к отчету по лабораторной работе.

Задание 5: Создайте свою *сеть* из 4х ПК и 2х хабов (по схеме согласно рис. 2.1), с помощью симулятора GNS3 и настройте ее работу. Параметры сетей должны использовать выделенный диапазон адресов по вариантам, представленным в приложении №1. Каждый студент осуществляет конфигурацию сети по индивидуальным параметрам. Результат настройки сети из 4 компьютеров при выполнении практической работы следует сохранить в формате *.gns3 и представить в приложении к отчету по лабораторной работе. Симулируйте пинг с PC1 на PC2 и сохраните результаты в виде картинки пошагово и представьте их в отчете.

Задание 6: Создайте свою *сеть* из 5-и ПК и 2х хабов (по схеме согласно рис. 2.10), с помощью симулятора GNS3 и настройте ее работу. Параметры сетей должны использовать выделенный

диапазон адресов по вариантам, представленным в приложении №1. Каждый студент осуществляет конфигурацию сети по индивидуальным параметрам. Результат настройки сети из 5 компьютеров при выполнении практической работы следует сохранить в формате *.gns3 и представить в приложении к отчету по лабораторной работе. Конфигурирование и проверка конфигурации сети компьютера 5 осуществляется с помощью командной строки и сохраните пошагово действия в виде картинки в отчете.

ПРИЛОЖЕНИЕ №1

Варианты использования выделенного диапазона адресов для лабораторной работы №1

| Вариант | Выделенный диапазон адресов | Маска подсети | Примечание |
|---------|-----------------------------|---------------|------------|
| 1 | 192.168.0.1/24 | 255.255.255.0 | |
| 2 | 10.255.0.1/24 | 255.255.255.0 | |
| 3 | 10.25.0.1/24 | 255.255.255.0 | |
| 4 | 10.10.0.1/24 | 255.255.255.0 | |
| 5 | 10.100.0.1/24 | 255.255.255.0 | |
| 6 | 172.185.0.1/24 | 255.255.255.0 | |
| 7 | 98.11.0.1/24 | 255.255.255.0 | |
| 8 | 192.172.0.1/24 | 255.255.255.0 | |
| 9 | 98.33.0.1/24 | 255.255.255.0 | |
| 10 | 25.25.0.1/24 | 255.255.255.0 | |
| 11 | 198.11.0.1/24 | 255.255.255.0 | |
| 12 | 30.30.0.1/24 | 255.255.255.0 | |
| 13 | 188.168.0.1/24 | 255.255.255.0 | |
| 14 | 95.168.0.1/24 | 255.255.255.0 | |
| 15 | 155.120.0.1/24 | 255.255.255.0 | |
| 16 | 178.120.0.1/24 | 255.255.255.0 | |
| 17 | 98.200.0.1/24 | 255.255.255.0 | |
| 18 | 96.166.0.1/24 | 255.255.255.0 | |
| 19 | 125.167.0.1/24 | 255.255.255.0 | |
| 20 | 189.145.0.1/24 | 255.255.255.0 | |