

Министерство образования и науки Российской Федерации

Государственное образовательное учреждение
высшего профессионального образования
«Оренбургский государственный университет»

Кафедра администрирования информационных систем

Ю.А. Ушаков, М.В. Ушакова, А. Л. Коннов

КОМПЬЮТЕРНЫЕ СЕТИ

Методические указания
к лабораторным работам. Часть 1

Рекомендовано к изданию Редакционно-издательским советом
Государственного образовательного учреждения высшего профессионального
образования «Оренбургский государственный университет»

Оренбург
ИПК ГОУ ОГУ
2011

УДК 004.7 (07)
ББК 32.973-0181я7
У 93

Рецензент - кандидат технических наук, доцент Шухман А. Е.

Ушаков, Ю. А.

У 93 Компьютерные сети: методические указания к лабораторным работам: в двух частях/ Ю. А. Ушаков, М. В. Ушакова, А.Л. Коннов; Оренбургский гос. ун-т. - Оренбург: ГОУ ОГУ, 2011. ч. 1. – 52 с.

Методические указания предназначены для студентов, обучающихся по программам высшего профессионального образования по направлению 010300.62 Математика, компьютерные науки при изучении дисциплины «Сети и системы телекоммуникаций» и направлению 220100 Системный анализ и управление при изучении дисциплины «Вычислительные сети и комплексы».

УДК 004.7(07)
ББК 32.973 – 0181я7

© Ушаков Ю.А.,
Ушакова М.В.,
Коннов А.Л., 2011.
© ГОУ ОГУ, 2011.

Содержание

1 Лабораторная работа №1. Настройка параметров IP в различных операционных системах.....	4
1.1 Общие сведения.....	4
1.1.1 Основные команды.....	4
1.1.2 Настройка виртуальной машины Windows и Linux.....	7
1.2 Рабочее задание.....	16
1.3 Контрольные вопросы.....	17
2 Лабораторная работа №2. Проектирование схемы IP адресации корпоративной сети.....	17
2.1 Общие сведения.....	17
2.2 Рабочее задание.....	21
2.3 Контрольные вопросы.....	23
3 Лабораторная работа №3. Изучение системы моделирования Cisco Packet Tracer.....	24
3.1 Общие сведения.....	24
3.2 Рабочее задание.....	34
3.3 Контрольные вопросы.....	35
4 Лабораторная работа №4. Создание логической схемы сети в Cisco Packet Tracer.....	36
4.1 Общие сведения.....	36
4.2 Рабочее задание.....	43
4.3 Контрольные вопросы.....	44
5 Лабораторная работа №5. Проектирование физической схемы сети, расчет комплектующих и расходных материалов.....	45
5.1 Общие сведения.....	45
5.2 Рабочее задание.....	48
5.3 Контрольные вопросы.....	50
Список использованных источников.....	52

1 Лабораторная работа №1. Настройка параметров IP в различных операционных системах

Цель работы. Изучить настройку сети на различных операционных системах для работы в сети. Получить навыки тестирования сети и контроля параметров настройки.

1.1 Общие сведения

1.1.1 Основные команды

Для обеспечения работы сети каждый компьютер должен быть настроен соответствующим образом: или через автоматические службы или вручную. В данной работе все настройки будут производиться ручным методом. Для настройки операционных систем (ОС) есть как минимум два способа: графический и через командную строку.

Команда *ifconfig* служит для настройки параметров IP-интерфейса (Unix). Этой командой можно перенастраивать интерфейсы работающей системы, также ей пользуются скрипты начальной загрузки для конфигурации IP-модуля при старте ОС. Для различных ОС это выглядит следующим образом:

1) FreeBSD:

- *ifconfig интерфейс inet IP-адрес netmask маска;*
- *ifconfig интерфейс inet IP-адрес/длина_префикса.*

2) Linux:

- *ifconfig интерфейс inet IP-адрес netmask маска broadcast широкосетчат_адрес.*

Список интерфейсов, их текущие настройки и статус выводятся по команде *ifconfig*, введенной без параметров.

Команда *route* служит для внесения или удаления записей из таблицы маршрутов (как "на лету", так и при начальной загрузке), например:

- *route add -net сеть_назначения netmask маска gw след_узел;*

- *route delete -net сеть_назначения*,

где:

сеть_назначения и *маска* - IP-адрес и маска сети назначения (сети, в которой находится конечный пункт следования дейтаграммы);

след_узел - IP-адрес следующего маршрутизатора на пути к указанной сети назначения.

Указание слова *default* или адреса 0.0.0.0/0 вместо адреса сети назначения обозначает маршрут по умолчанию (в этом случае маска не требуется). В другом случае если маска не указана, *route* выберет ее из своих соображений, поэтому во избежание недоразумений маску необходимо указывать всегда.

Если устанавливается маршрут до сети, к которой узел подсоединен непосредственно, то в этом случае в поле *след_узел* указывается адрес собственного IP-интерфейса, через который эта сеть достижима; если же адрес следующего маршрутизатора не указан, то *route* сам выберет наиболее подходящий IP-интерфейс для связи с этой сетью, например:

1) В FreeBSD для маршрутов, ведущих к отдельным узлам сети:

- *route {add|delete} -host адрес_узла_назначения gw след_узел.*

2) В FreeBSD для маршрутов, ведущих к другим сетям:

- *route add -net сеть_назначения/длина_префикса -gateway след_узел;*

- *route add -net default -gateway след_узел;*

- *route add -host узел_назначения -gateway след_узел;*

- *route delete -net сеть_назначения.*

3) В Windows

- *route {add|delete} адрес_назначения MASK маска след_узел.*

Команды *sysctl* (FreeBSD, Linux) и *ndd* (Solaris) предназначены для изменения различных параметров операционной системы. В частности, эти команды позволяют разрешить или запретить ретрансляцию дейтаграмм: для этого соответствующий параметр устанавливается в 0 или 1.

В приведенных ниже примерах первая команда выводит значение параметра, отвечающего за ретрансляцию дейтаграмм, а вторая команда присваивает этому параметру значение 1 ("разрешить"), например

1) В Linux

- `sysctl net.ipv4.ip_forward`
- `sysctl -w net.ipv4.ip_forward=1`

2) В FreeBSD

- `sysctl net.inet.ip.forwarding`
- `sysctl net.inet.ip.forwarding=1`

Команда `netstat -rn` - вывод таблицы маршрутов (Unix, Windows), `netstat -n` - выводит информацию о соединениях. Для каждого соединения выводится название транспортного протокола, сокет (IP-адреса и номера портов) обеих сторон и состояние соединения. Также команда `netstat` выводит информацию об открытых портах.

В Windows информацию о настройках протокола IP можно получить командами `windowsipcfg` (Windows 95/98) или `ipconfig /all` (Windows 2000+), в Linux/Unix командой `ifconfig` без параметров.

Команда `arp` выполняет просмотр и манипуляции базой данных протокола ARP. Основные ключи (Unix, Windows):

- «-a» - показать всю `arp`-таблицу;
- «-d» *имя_хоста* - удалить сведения об указанном хосте,;
- «-s» *имя_хоста* *MAC_адрес* - внести вручную MAC-адрес Ethernet указанного хоста.

Команда `ping IP-адрес` посылает запросы ICMP Echo указанному хосту и принимает ответы ICMP Echo Reply, выводит статистику потерянных пакетов и времени отклика. Для заикливания команды в ОС FreeBSD следует указать ключ «-s», а в Windows - ключ «-t».

Команда `traceroute IP_адрес` (в Windows - `tracert`) - выводит список промежуточных узлов на пути к указанному. По умолчанию программа обращается в DNS для преобразования IP-адресов узлов в доменные имена. Если сервис DNS недоступен

пен, или необходимо ускорить вывод результата, обращение к DNS следует отключить (*tracert -n IP-адрес* для Unix, *tracert -d IP-адрес* для Windows).

1.1.2 Настройка виртуальной машины Windows и Linux

Для настройки операционных систем для работы в сети необходимо воспользоваться виртуальной машиной. Ниже показано, каким образом необходимо создать и настроить виртуальную машину для корректной работы. Для виртуализации используется бесплатная утилита VirtualBox.

После запуска VirtualBox необходимо через меню Машина→Создать (CTRL-N) добавить новую машину. Затем, после нажатия кнопки «Далее» в поле «Имя» ввести любое название машины (рисунок 1.1), например, BSD-1 или XP-1. В выпадающем списке «Операционная система» ввести для Windows или Unix соответственно «Windows» (поле «Версия» – Windows XP) или «BSD» (поле «Версия» – «FreeBSD»).

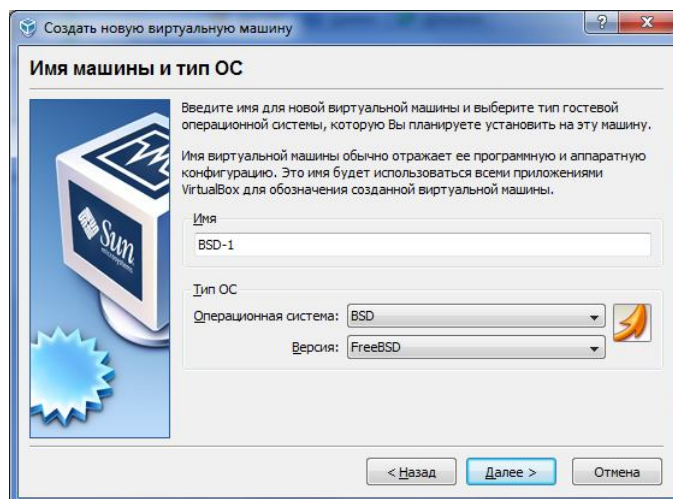


Рисунок 1.1 – Настройка общих свойств виртуальной машины.

На следующей странице настройки выбрать «128Мб» памяти и нажать «Далее» (рисунок 1.2).

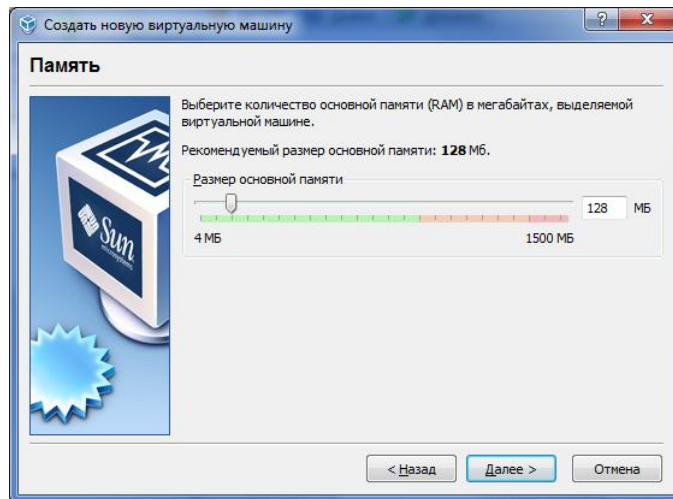


Рисунок 1.2 – Выбор объема памяти виртуальной машины

Затем необходимо выполнить одно из двух действий. При наличии уже созданного виртуального диска его нужно добавить в систему перед использованием. В окне выбора диска выбрать пункт «Использовать существующий жесткий диск», нажать значок справа (рисунок 1.3), в появившемся окне нажать кнопку «Добавить» (рисунок 1.4).

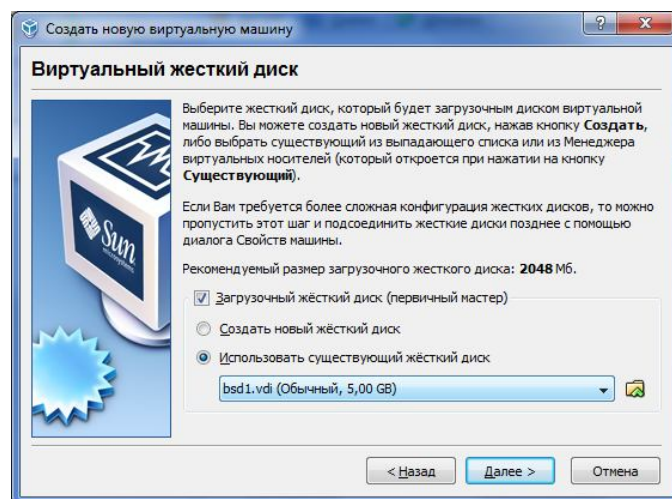


Рисунок 1.3 – Выбор жесткого диска

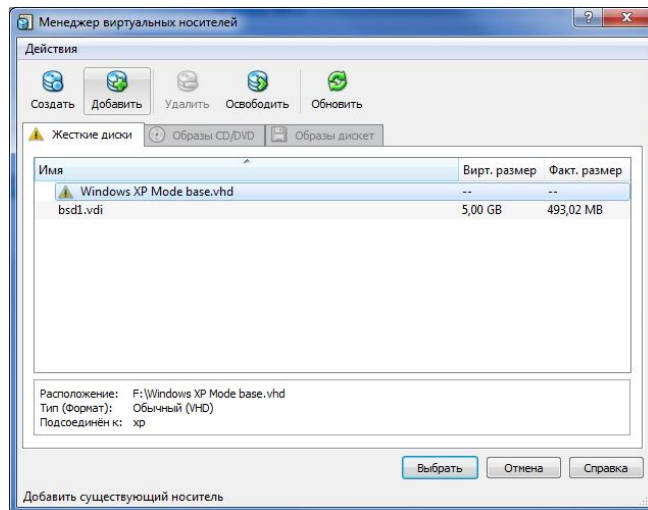


Рисунок 1.4 - Добавление диска в систему

В появившемся диалоге выбрать путь к диску и указать файл с содержимым диска (обычно он имеет расширение «vdi»).

Если файла с жестким диском нет, необходимо создать новый диск. В появившемся окне (рисунок 1.5) необходимо выбрать размер диска 2 Гб и путь для сохранения файла с данными (можно оставить по умолчанию) и нажать «Далее».

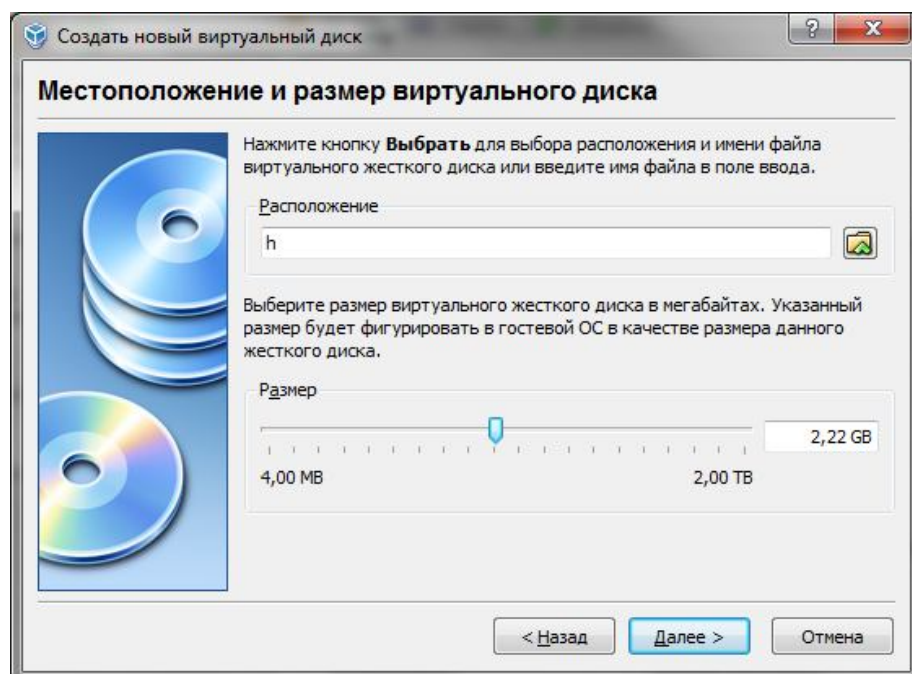


Рисунок 1.5 – Выбора размера диска

После этих действий виртуальная машина создана, но не настроена. Правой кнопкой мыши необходимо кликнуть на нужной виртуальной машине и выбрать пункт «Свойства» (рисунок 1.6).

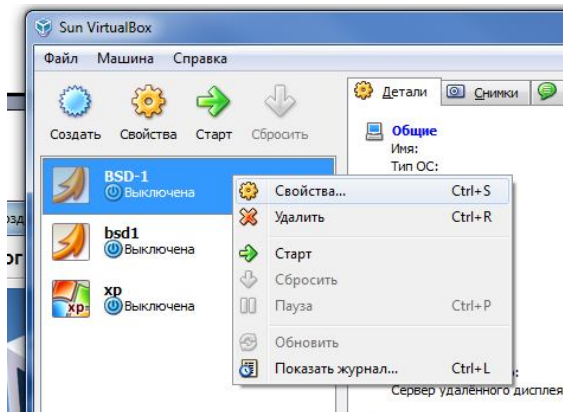


Рисунок 1.6 – Настройка машины

В свойствах сети (вкладки слева) в выпадающем списке «Тип подключения» нужно выбрать «Сетевой мост». Затем нажать «Дополнительно» и в поле «Тип адаптера» выбрать адаптер «PC-NET II» (рисунок 1.7).

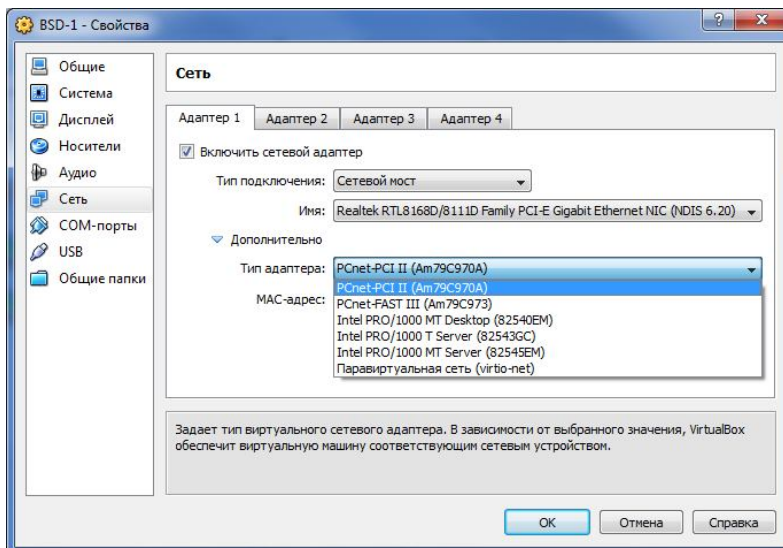


Рисунок 1.7 – Настройка сети машины

Теперь настройка закончена. Можно запустить машину. Если диск был создан заново, на него необходимо установить операционную систему. При первом запуске появится мастер первого запуска (рисунок 1.8).

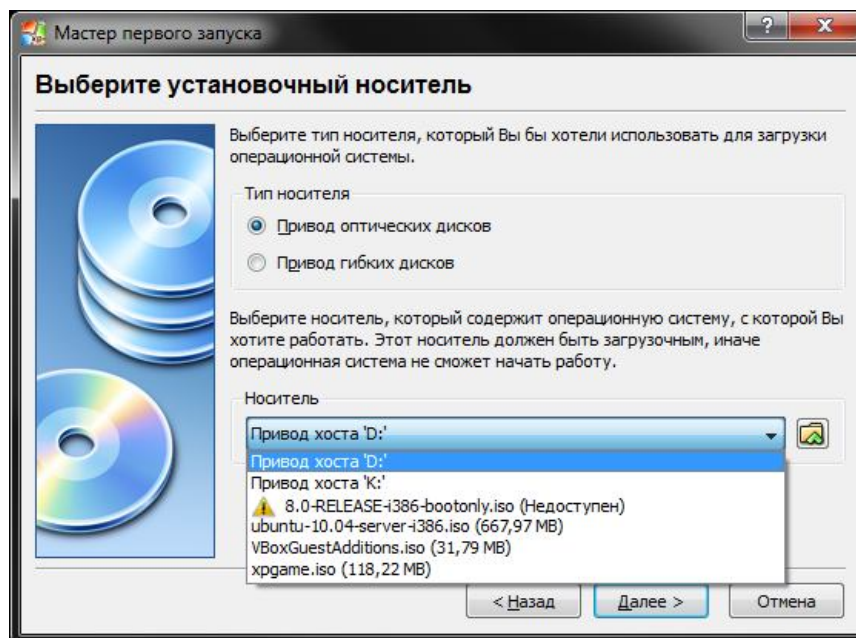


Рисунок 1.8 – Выбор метода установки операционной системы

Если в выпадающем списке нет нужного образа, его необходимо добавить в систему аналогично добавлению файла жесткого диска (рисунок 1.4). Установка ОС происходит в штатном режиме.

После запуска ОС необходимо провести авторизацию. Для Windows системы логин не требуется, для FreeBSD используем логин «root» пароль «123123». В Windows системе возможна неправильная установка драйверов. Для корректной установки необходимо сначала установить «Дополнения Гостевой ОС» из меню «Устройства» (рисунок 1.9). После выбора этого пункта в виртуальный CDROM устанавливается образ с драйверами. Для установки общих драйверов необходимо запустить с этого диска файл VBoxWindowsAdditions.EXE и следовать инструкциям на экране.

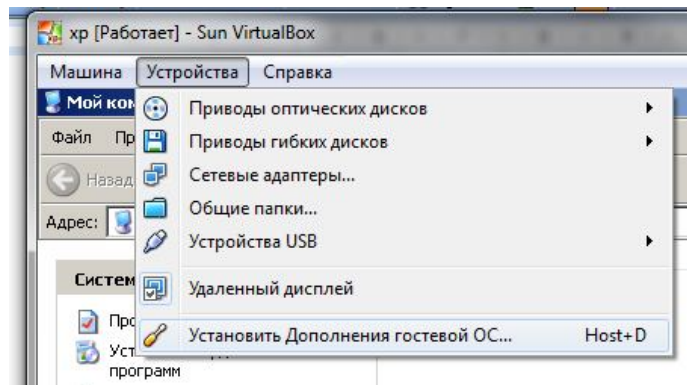


Рисунок 1.9 – Установка дополнительных драйверов

Однако драйвера на сетевую карту могут не установиться в автоматическом режиме. Для установки вручную необходимо распаковать драйвера командой «D:\VBoxWindowsAdditions /extract» (рисунок 1.10).

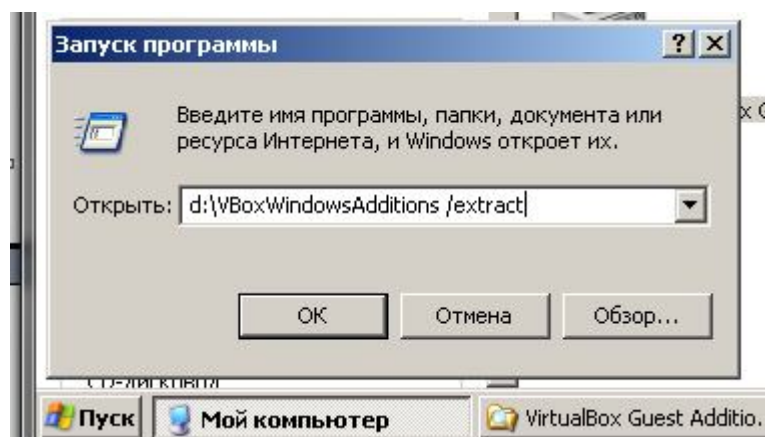


Рисунок 1.10 – Распаковка драйверов

Затем в диспетчере устройств (он находится в пункте меню «Управление», которое появляется при клике правой кнопкой мыши на иконке «Мой компьютер») необходимо выбрать на устройства «Ethernet-контроллер» пункт «Обновить драйвер» (рисунок 1.11).

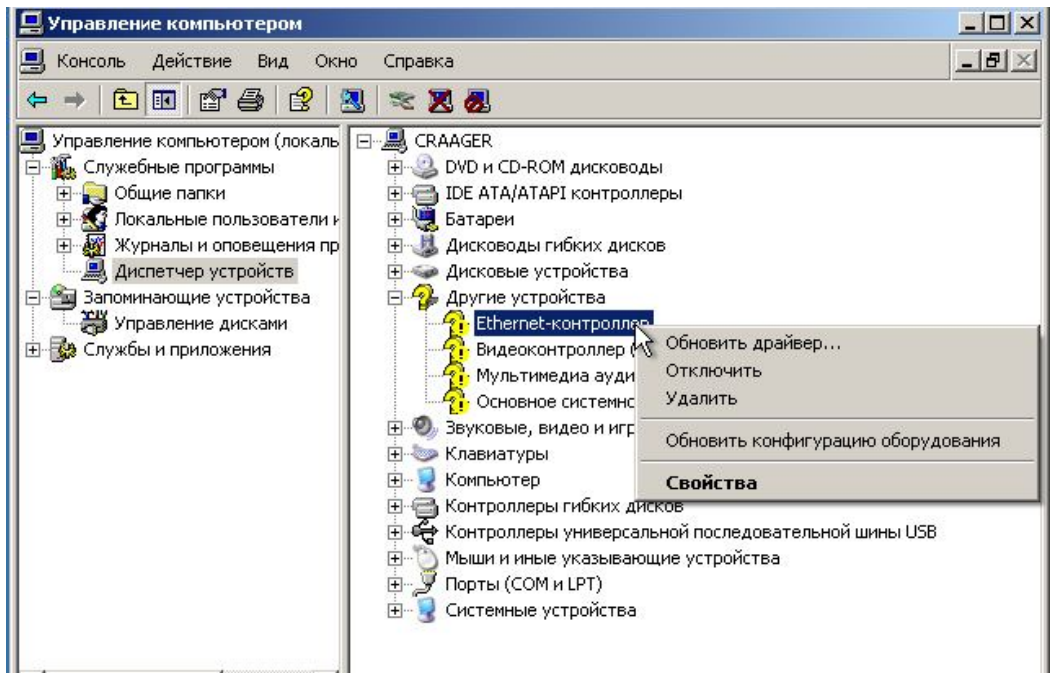


Рисунок 1.11 – Обновление драйвера

Далее необходимо выбрать пункт «Установка из указанного места» и в поле «Включить следующее место для поиска» выбрать папку (может зависеть от версии VirtualBox) «C:\Program Files\Oracle\VirtualBox Guest Additions\Network\AMD» и нажать «Ок» (рисунок 1.12).

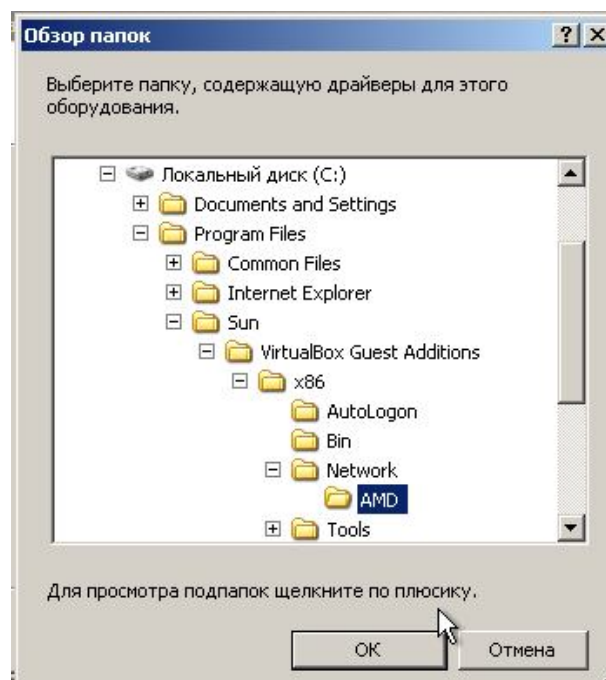


Рисунок 1.12 – Путь к драйверам

После этого необходимо провести настройку IP параметров. В меню «Пуск» выбрать «Панель управления» → «Сеть и подключение к Интернет» → «Сетевые подключения». В появившемся окне на значке сети «Подключение по локальной сети» следует нажать правой кнопкой мыши и из выпадающего меню выбрать «Свойства», затем на пункте «Протокол TCP/IP» кликнуть два раза. Появится окно настройки IP параметров (рисунок 1.13).

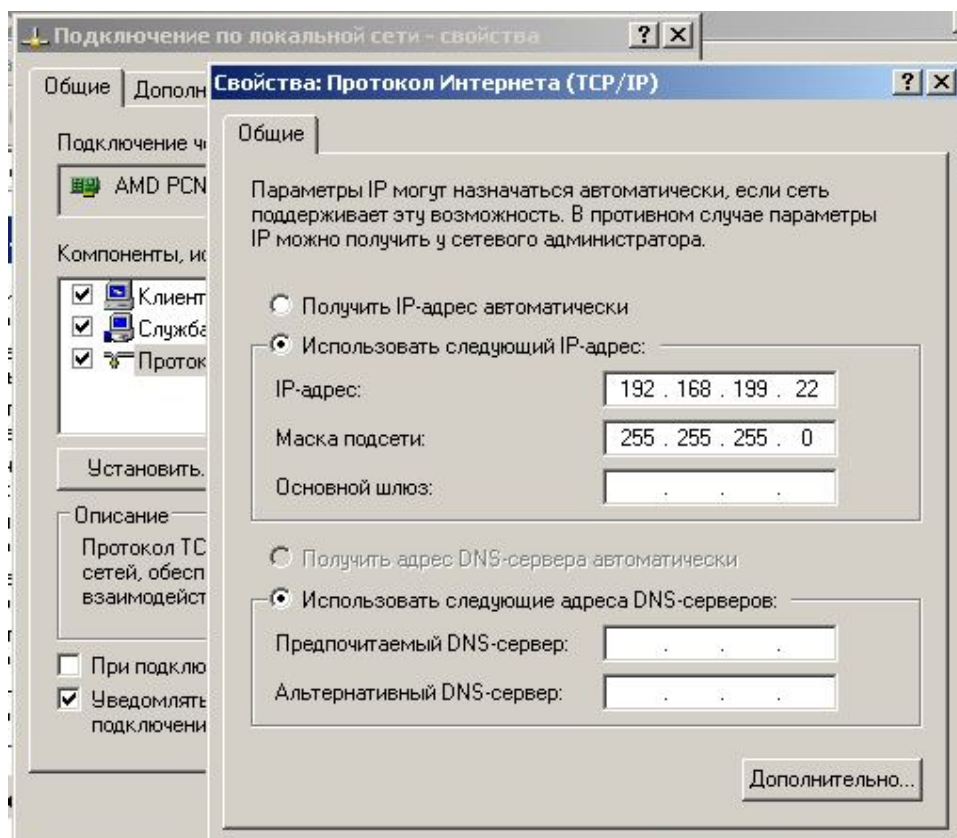


Рисунок 1.13 – параметры IP

В окне необходимо задать требуемый «IP адрес» и «Маску подсети». Для проверки маршрутизации также надо задать «Основной шлюз». Для проверки DNS-серверов задать адрес «Предпочитаемого DNS-сервера». После применения всех изменений (может потребоваться перезагрузка) необходимо проверить работу сети. В меню «Пуск» выберите «Выполнить», в поле «Открыть» наберите «CMD». Откроется командная строка. С помощью команды «IPCONFIG /ALL» проконтролируйте установки IP, затем командой «PING» проверьте связь с соседними компьютерами (для этого необходимо узнать их IP адрес). Пример показан на рисунке 1.14.

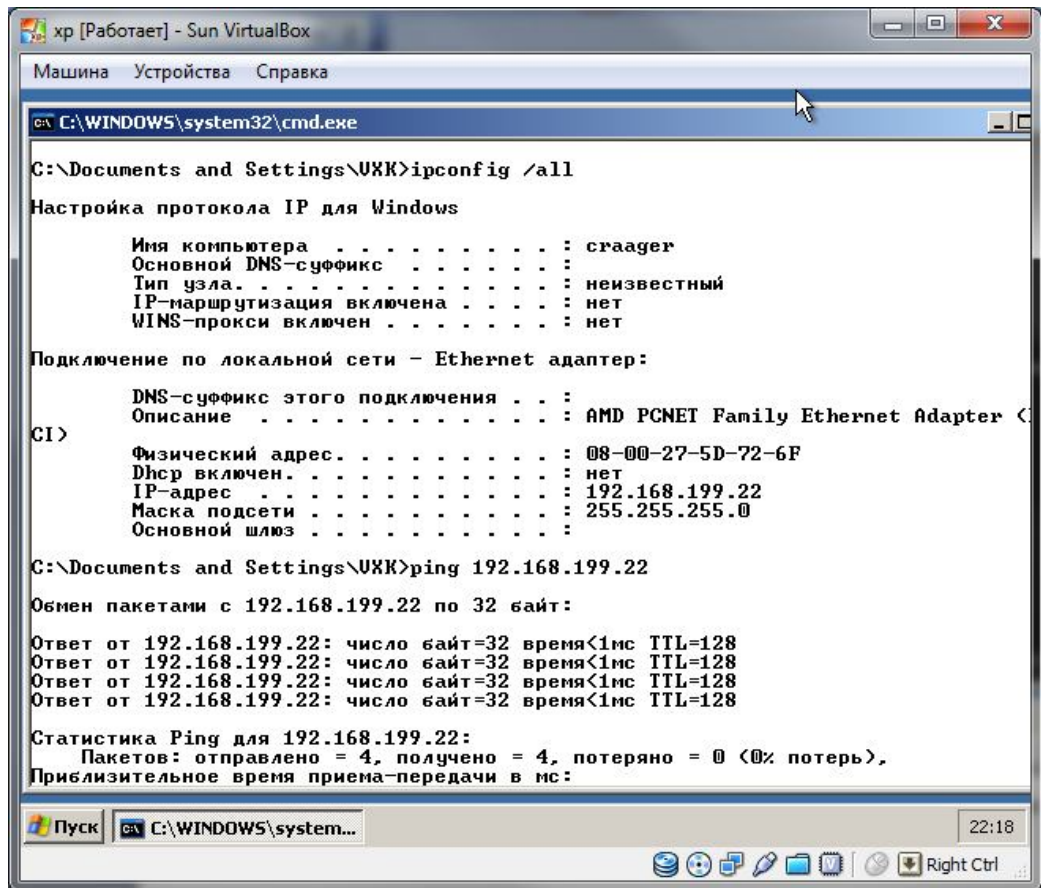


Рисунок 1.14 – Проверка параметров и тестирование сети

Для ОС Unix настройка IP-параметров происходит намного проще. Необходимо командой «ifconfig» вывести на экран список интерфейсов. Затем с помощью той же команды, но с параметрами настроить IP адрес и маску (например, *ifconfig em0 192.168.199.22 netmask 255.255.255.0 up*). Пример показан на рисунке 1.15.

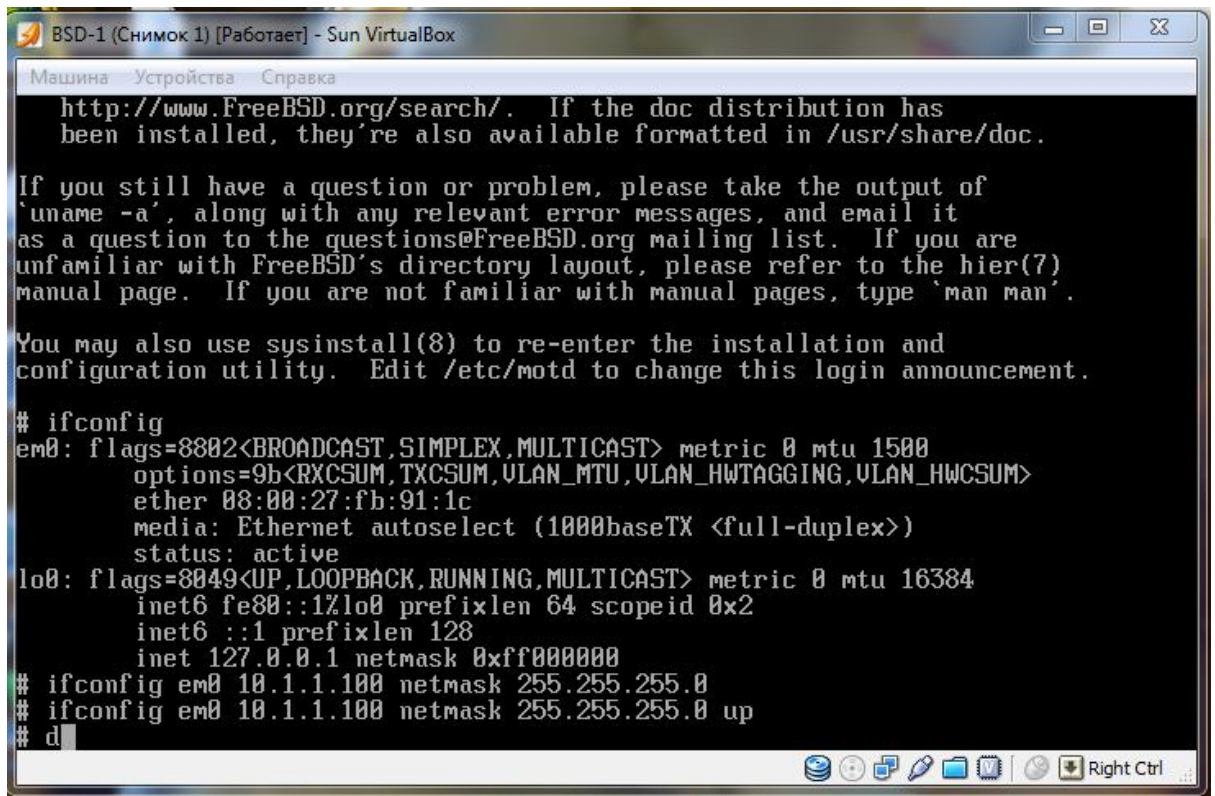


Рисунок 1.15 – Настройка параметров IP в unix

1.2 Рабочее задание

Необходимо настроить IP параметры в системе Windows и FreeBSD. IP-адреса хоста заданы в таблице 1.1 и выбираются в соответствии с номером варианта, указанным преподавателем. Маска принимается равной /24 или 255.255.255.0.

Таблица 1.1 – Варианты заданий

Вариант	IP адрес для Windows	IP адрес для FreeBSD
1	2	3
1	192.168.199.2	192.168.199.102
2	192.168.199.3	192.168.199.103
3	192.168.199.4	192.168.199.104
4	192.168.199.5	192.168.199.105
5	192.168.199.6	192.168.199.106

Продолжение таблицы 1.1

1	2	3
6	192.168.199.7	192.168.199.107
7	192.168.199.8	192.168.199.108
8	192.168.199.9	192.168.199.109
9	192.168.199.10	192.168.199.110
10	192.168.199.11	192.168.199.111

1.3 Контрольные вопросы

- 1) Назначение и основные параметры команды *ifconfig*.
- 2) Назначение и основные параметры команды *route*.
- 3) Назначение и основные параметры команды *netstat*.
- 4) Назначение и основные параметры команд *ping* и *tracert*.
- 5) Опишите этапы создания виртуальной машины.
- 6) Опишите процесс настройки IP- параметров для ОС Windows.
- 7) Опишите процесс настройки IP- параметров для ОС Unix.
- 8) Каким образом можно проверить связь между компьютерами?
- 9) Каким образом можно путь следования пакета между компьютерами?
- 10) Для чего необходима утилита *arp*?

2 Лабораторная работа №2. Проектирование схемы IP адресации корпоративной сети

Цель работы. Изучение процесса формирования IP-пространства крупных сетей, получение навыков вычисления подсетей.

2.1 Общие сведения

Процесс построения сети обычно включает в себя следующие глобальные этапы:

- 1) Анализ задач, для решения которых создается сеть, а также определение объема финансирования проекта.

2) Проектирование физической структуры - этап, на котором анализируются, начальные условия (планировка здания, имеющиеся технические средства и т.п.) и создается детальный проект физической организации сети.

3) Проектирование инфраструктуры – этап, на котором определяются протоколы взаимодействия, используемые службы, политика безопасности и т.п. - т.е. логическая организация сети.

4) Развертывание - этап, связанный с прокладкой линий связи, установкой и настройкой оборудования.

Этап анализа является одним из важнейших, поскольку определяет все остальные решаемые задачи: как физическую структуру сети (например, места расположения компьютеров), так и логическую - используемые протоколы, службы и т.п. На этом этапе необходимо собрать как можно информации, чтобы упростить выполнение следующих этапов.

На этапе планирования IP-сетей необходимо каждому узлу сети назначить IP-адрес. Далее показан один из вариантов планирования сетей:

1) Для узлов создаваемой сети резервируется диапазон уникальных для Интернета IP-адресов (общие адреса). Этот способ наиболее дорогой, поскольку требуется платить за аренду каждого IP-адреса. Кроме того, при подключении сети к Интернету вряд ли удастся получить необходимое количество IP-адресов - в настоящее время наметился их дефицит, поэтому в лучшем случае, можно получить несколько, а зачастую - всего один.

2) Для узлов создаваемой сети адреса назначаются из диапазона так называемых частных сетей. Такие адреса не используются в Интернете, поэтому нет необходимости соблюдать их уникальность. Однако, чтобы узлы, обладающие такими адресами, имели доступ к ресурсам Интернета, на шлюзе, через который сеть подключена к Интернету, необходимо настроить службу трансляции адресов (Network Address Translation, NAT).

Второй подход - наиболее распространенный и простой, с точки зрения администрирования. При планировании IP-адресов необходимо выполнить следующие действия:

1) Определить по числу физических подсетей количество планируемых IP-сетей. Каждая физическая подсеть должна быть представлена хотя бы одной IP-сетью.

2) Определить количество узлов в каждой IP-сети и число адресов, необходимое каждому из них.

3) Определить для каждой сети диапазоны IP-адресов и маски подсети. Если не предполагается, что IP-сетей в сети будет более чем 254, и каждая из них будут содержать более 254 узлов, проще всего закреплять адреса из частного диапазона 192.168.X.0 (где X - уникальное число для каждой IP-сети) и маску 255.255.255.0.

4) Закрепить для каждой сети IP-адреса за интерфейсами маршрутизаторов. Обычно для этого используют начальные номера диапазона адресов IP-сети (например, 192.168.X.1).

5) Закрепить за каждым узлом IP-адрес(а).

6) При использовании статической маршрутизации определить таблицы маршрутизации для каждого маршрутизатора.

7) Определить параметры для настройки службы трансляции адресов.

Так как в базовом IP-адресе фиксированные биты должны располагаться в одной непрерывной группе, начинающейся с самого старшего бита адреса, маска должна содержать непрерывную последовательность единичных битов, соответствующую фиксированной части адреса, за которой следует непрерывная последовательность нулевых битов, обозначающая переменную часть адреса.

Базовый IP-адрес, маска и диапазон адресов связаны друг с другом математической операцией, называемой побитовым логическим «И». При побитовом логическом «И» 32 бита IP-адреса выравниваются с 32 битами маски. Для каждой пары битов выполняется логическое «И». Результат логического «И» равен единице, если оба бита-операнда равны единице; во всех остальных случаях результат операции равен нулю.

Так как переменные биты адреса в маске обозначены нулями, то побитовое логическое «И», выполненное над любым IP-адресом из диапазона (включая базовый IP-адрес) и маской, всегда дает один и тот же результат: базовый IP-адрес.

В последнее время поле номера сети в адресе принято называть сетевым префиксом, так как первая порция каждого IP-адреса идентифицирует номер сети. Все хосты в определенной сети имеют один и тот же сетевой префикс, но при этом они должны иметь уникальные номера хостов. Аналогично, два любых расположенных в разных сетях хоста должны иметь различные сетевые префиксы, но они могут иметь одинаковые номера хостов. Длиной префикса называется количество бит в маске.

Первым шагом в процессе планирования является определение максимального количества требуемых подсетей. Данное число округляется до ближайшей степени двойки. При выполнении этой оценки важно учесть возможное увеличение числа подсетей в будущем.

На втором шаге проверяется факт существования достаточного количества адресов хостов в наибольшей подсети организации.

Предположим, что организация получила сеть 193.1.1.0/24, и ей необходимо сформировать шесть подсетей. Наибольшая подсеть должна поддерживать 25 хостов. На первом шаге определяется число битов, требуемых для определения необходимых шести подсетей ($2^n \geq 6$). В данном примере администратор должен определить восемь подсетей ($2^3 = 8 \geq 6$), т. е. для выделения подсетей будут использованы три бита из выделенного адреса. Полученный после выделения подсетей сетевой префикс будет записан как /27 (24 бита базовой маски + 3 бита на подсети = 27). Это расширенный сетевой префикс и он имеет эквивалентное значение маски подсети 255.255.255.224.

Используемый 27-разрядный расширенный сетевой префикс оставляет 5 бит для задания номеров хостов в каждой из подсетей. Это означает, что в каждой подсети может быть определено до 32 ($2^5 = 32$) индивидуальных адресов хостов. Однако адреса, у которых все биты равны или нулю, или единице, являются зарезервированными, так что общее число адресов хостов в каждой подсети становится равным 30 ($2^5 - 2 = 30$). Пример расчета всех подсетей представлен в таблице 2.1.

Таблица 2.1 - Варианты подсетей для сети 193.1.1.0/24

Сеть	Точечно-десятичная нотация	Двоичное представление адреса
1	2	3
Базовая сеть	193.1.1.0 /24	11000001.00000001.00000001. <u>00000000</u>
Подсеть #0	193.1.1.0 /27	11000001.00000001.00000001. 000 <u>00000</u>
Подсеть #1	193.1.1.32 /27	11000001.00000001.00000001. 001 <u>00000</u>
Подсеть #2	193.1.1.64 /27	11000001.00000001.00000001. 010 <u>00000</u>
Подсеть #3	193.1.1.96 /27	11000001.00000001.00000001. 011 <u>00000</u>
Подсеть #4	193.1.1.128 /27	11000001.00000001.00000001. 100 <u>00000</u>
Подсеть #5	193.1.1.160 /27	11000001.00000001.00000001. 101 <u>00000</u>
Подсеть #6	193.1.1.192 /27	11000001.00000001.00000001. 110 <u>00000</u>
Подсеть #7	193.1.1.224 /27	11000001.00000001.00000001. 111 <u>00000</u>

Выделенные жирным биты определяют номер подсети, выделенные курсивом биты используются для задания конкретных адресов.

2.2 Рабочее задание

1) Разработайте план IP-адресации для корпоративной сети JVI (рисунок 2.1) с учетом таких показателей, как масштабирование, агрегирование и следующих требований заказчика:

- число хостов в каждой сети, исключая филиалы, в будущем может увеличиться в 1,5 раза, но в данный момент нет необходимости создавать сети увеличенного размера. Следует предусмотреть возможность их будущего расширения за счет временно неиспользуемого адресного пространства;

- может быть добавлен третий отдел (15 хостов) или же эти хосты вольтуются в сеть первого отдела (решение будет принято по мере развития бизнеса). Дизайн сети должен быть рассчитан на безболезненное слияние и разделение отделов 1 и 3;

- число филиалов может быть увеличено до 4, размер филиала - 9-12 хостов;

- сеть отделов и серверов включаются в сеть Core каждая через свой маршрутизатор.

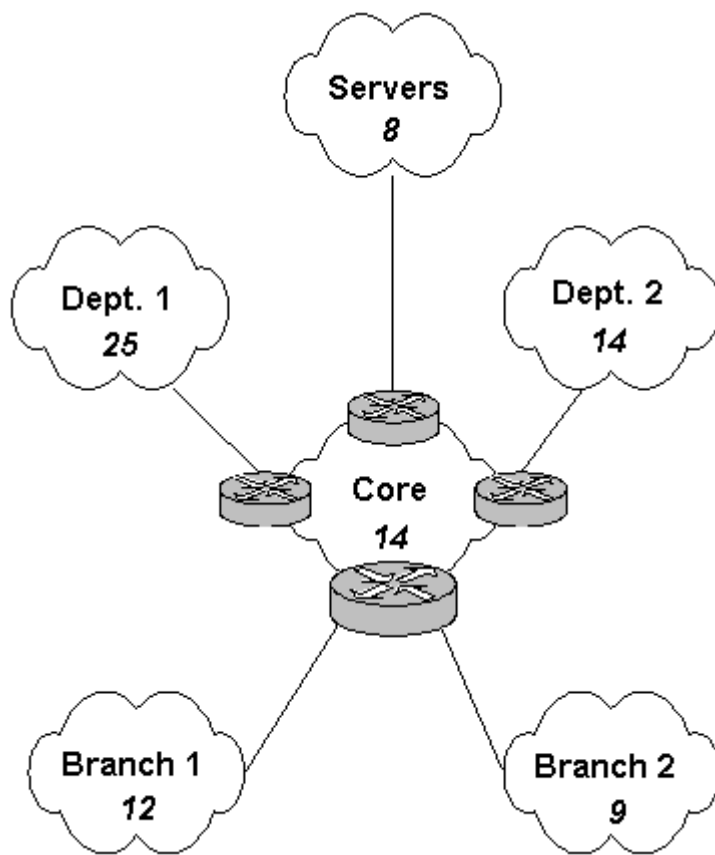


Рисунок 2.1 – Сеть компании

2) По заданным IP-адресу и маске для всей сети компании (таблица 2.1) определите базовый адрес сети, диапазон адресов сети, широковещательный адрес, а также длину префикса.

3) По заданному числу хостов (рисунок 2.1) и базовому адресу сети найдите IP-сети для каждого существующего отдела, филиала, и планируемых подразделений, в которых можно разместить указанное число хостов, (сети указывать в виде "адрес сети/длина префикса (маска)").

Таблица 2.1 – Задание для лабораторной работы 2

Вариант	IP адрес	Маска
1	2	3
1	10.129.56.48	255.255.252.0

Продолжение таблицы 2.1

1	2	3
2	172.16.25.58	255.254.0.0
3	192.168.52.14	255.255.248.0
4	10.129.56.38	255.255.224.0
5	172.16.25.28	255.255.192.0
6	192.168.52.19	255.255.128.0
7	10.129.56.52	255.255.254.0
8	172.16.25.75	255.252.0.0
9	192.168.52.21	255.248.0.0
10	11.25.36.54	255.224.0.0

2.3 Контрольные вопросы

- 1) Назовите основные этапы построения сети.
- 2) Как происходит планирование IP-адресов?
- 3) Как по заданному числу хостов в сети и заданному диапазону IP-адресов найти все возможные IP-сети внутри данного диапазона, в которых можно разместить указанное число хостов?
- 4) Как по заданным IP-адресу и маске определить адрес сети, номер хоста, широковещательный адрес, а также длину префикса?
- 5) Как по заданным IP-адресу длине префикса определить адрес сети, номер хоста, широковещательный адрес, а также маску?
- 6) Как рассчитать количество подсетей при известной маске и количестве хостов?
- 7) Как рассчитать количество подсетей при известном количестве хостов?
- 8) Как рассчитать количество хостов при известной маске?
- 9) Как рассчитать количество подсетей при известной базовой маске и маске подсети?
- 10) Как рассчитать маску по известной длине префикса?

3 Лабораторная работа №3. Изучение системы моделирования Cisco Packet Tracer

Цель работы. Изучить систему моделирования корпоративных сетей Cisco Packet Tracer. Получить навыки настройки сетевого оборудования, создания сложных сетевых топологий.

3.1 Общие сведения

Packet Tracer (PT) - бесплатный эмулятор сетевой среды, выпускаемый фирмой Cisco, который:

- позволяет делать работоспособные модели сети, настраивать (командами Cisco IOS и визуально) маршрутизаторы и коммутаторы, взаимодействовать между несколькими пользователями;

- включает в себя серии маршрутизаторов Cisco 1800, 2600, 2800 и коммутаторов 2950, 2960, 3650; серверы DHCP, HTTP, TFTP, FTP, TIME, рабочие станции, различные модули к компьютерам и маршрутизаторам, устройства WiFi, различные кабели;

- успешно позволяет создавать сложные макеты сетей, проверять на работоспособность топологии. Внешний вид рабочего окна Packet Tracer показан на рисунке 3.1.

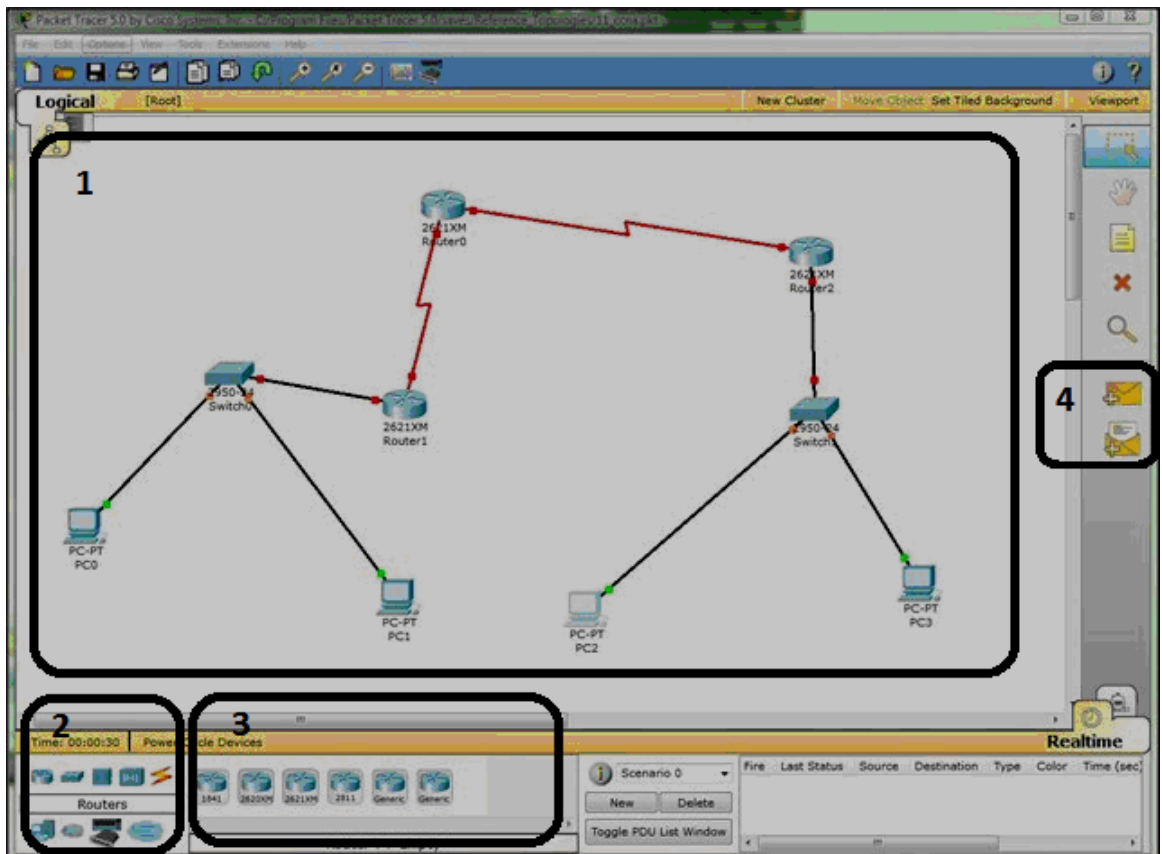


Рисунок 3.1 – Главное окно программы Packet Tracer

Основные области главного окна программы Packet Tracer следующие:

- 1 – рабочая область программы, в этой области можно собирать виртуальные сети, видеть трафик, запускать настройку устройств;
- 2 – область, используемая для выбора типа устройств, которые будут добавляться в рабочую область;
- 3 – область для выбора конкретного устройства для добавления;
- 4 – область, необходимая для визуального запуска сетевого пакета с одного устройства на другое.

В рабочей области отображается *логическая диаграмма сети*. Работа с объектами на логической диаграмме происходит мышью. Чтобы войти в режим настройки оборудования надо кликнуть на нужной картинке оборудования. Откроется окно настройки (рисунок 3.2).

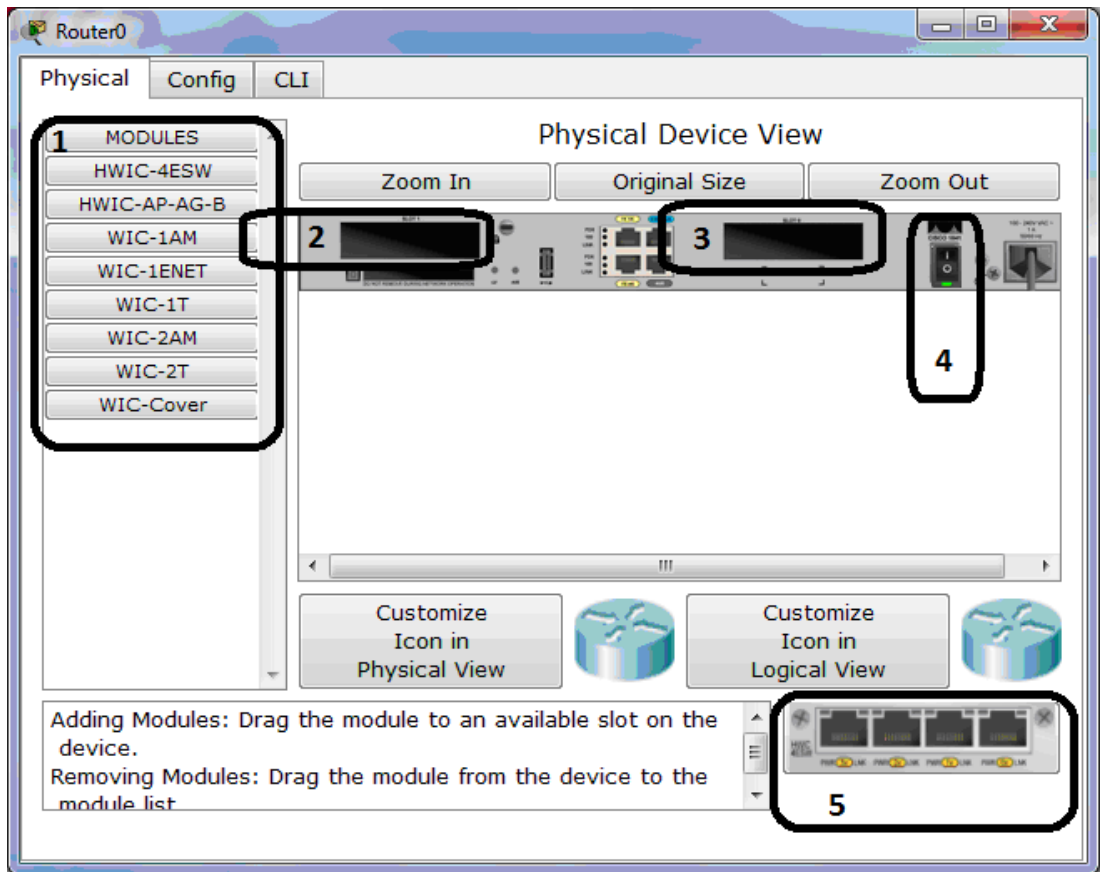


Рисунок 3.2 – Окно настройки

В первой вкладке окна настройки есть следующие элементы:

1) Модули, которые можно вставить в роутер. Чтобы вставить модуль, необходимо сначала выключить устройство (элемент 4), выбрать в списке нужный модуль, он появится в элементе 5. Перетащить мышью изображение модуля в пустой слот для модулей (элемент 2 или 3).

- 2) Слот для модуля 1.
- 3) Слот для модуля 2.
- 4) Кнопка выключения питания.
- 5) Изображение выбранного модуля.

В маршрутизаторах представлены следующие модули:

- HWIC-4ESW – модуль-коммутатор с 4 портами Ethernet;
- HWIC-AP-AG-B – модуль точки доступа 802.11B/G;
- WIC-1AM – 1 аналоговый порт модема V.90;
- WIC-1ENET – 1 маршрутизируемый порт Ethernet;

- WIC-2AM – 1 аналоговых порта модема V.90;
- WIC-2T – 2 последовательных порта serial;
- WIC-Cover – заглушка.

В каждом маршрутизаторе есть, как минимум, 2 порта Ethernet – как правило, для модульных маршрутизаторов они называются FastEthernet 0/0 и FastEthernet 0/1. Для немодульных устройств это будет FastEthernet0 и FastEthernet1.

Если в пустой слот вставлена карта расширения, например WIC-1ENET с 1 портом Ethernet в слоте №1, порт в маршрутизаторе будет обозначаться Ethernet0/0/0, где первая цифра 1 – это номер слота. Если карта будет вставлена в слот №2, то порт будет обозначаться Ethernet0/1/0. Последовательные (serial) порты обозначаются в маршрутизаторе аналогично, например, Serial0/0/0. Лучший способ проверить названия интерфейсов – зайти на вкладку «Config» окна настройки (рисунок 3.3).

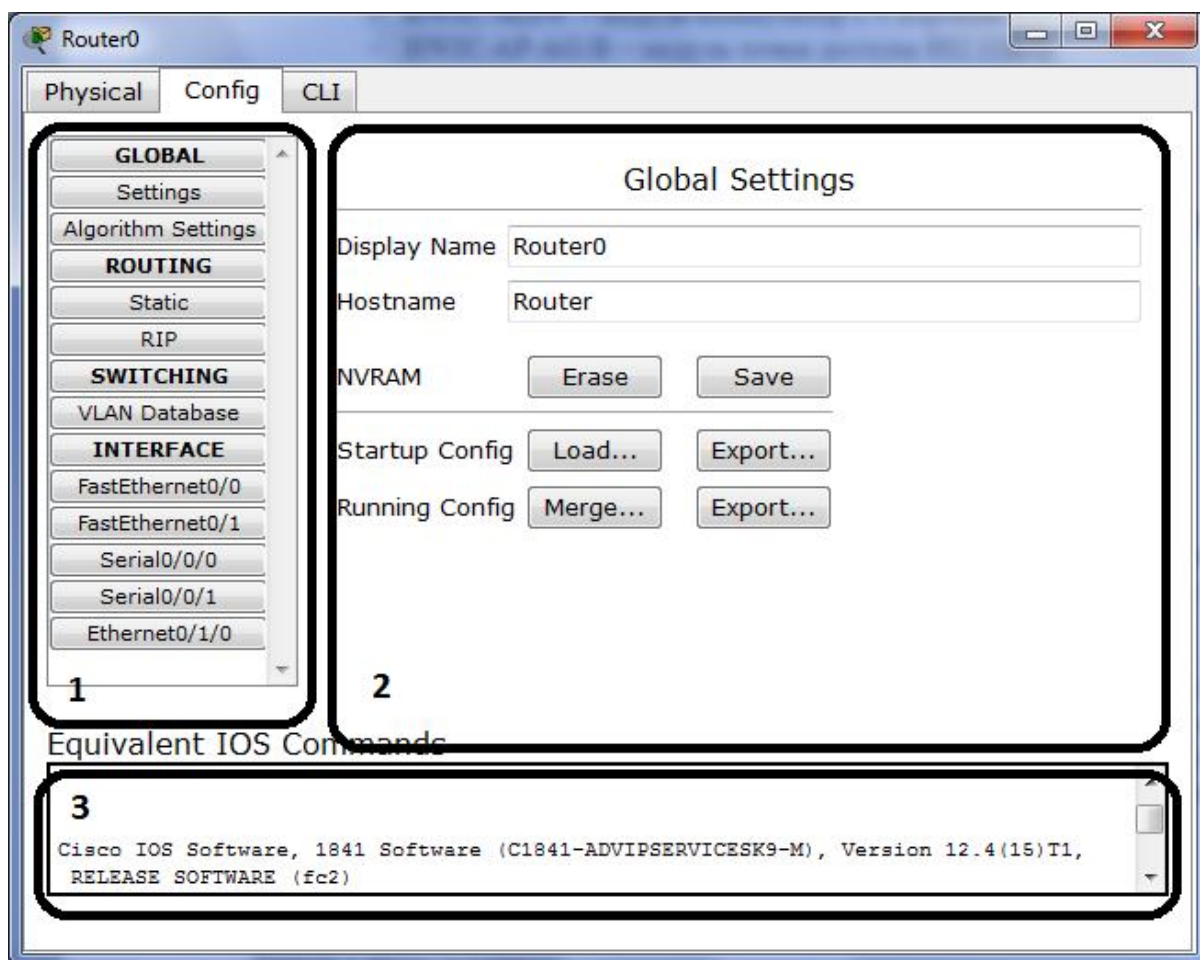


Рисунок 3.3 – Вкладка «Config» окна настройки

В окне настройки маршрутизатора есть следующие **элементы**:

1) Выбор типа настройки, имеет четыре вкладки, выделенные жирным шрифтом:
ТОМ:

а) GLOBAL - для общих настроек (рисунок 3.4).

б) ROUTING - для статической и динамической маршрутизации.

в) SWITCHING – для внутренней коммутации между виртуальными подсетями VLAN.

г) INTERFACE – настройка конкретных интерфейсов.

2) Область «2» предназначена для задания настроек.

3) В области «3» показываются эквиваленты команд для настройки маршрутизатора через командную строку (CLI, command line interface). На рисунке 3.4 показана настройка интерфейса.

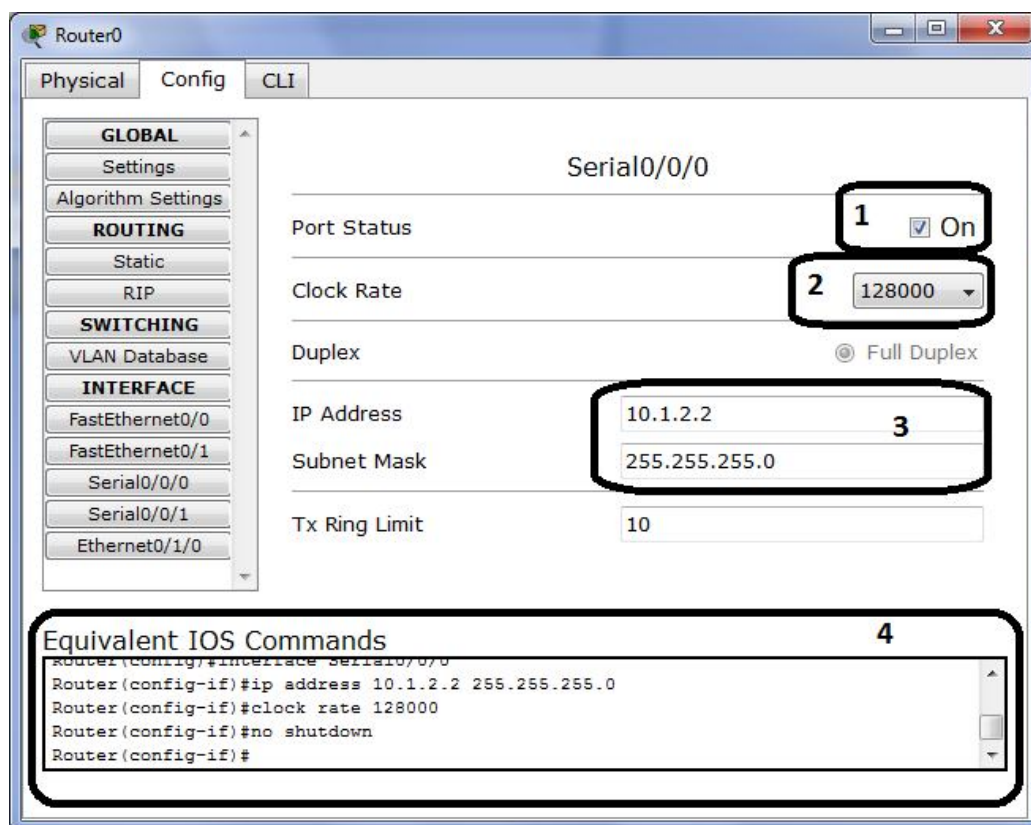


Рисунок 3.4 – Настройка интерфейса

Первое, что необходимо сделать – включить интерфейс (элемент 1). Затем можно задать IP адрес и маску (элемент 3). Для Serial интерфейсов необходимо за-

полнить еще скорость передачи данных Clock rate (элемент 2). В нижней части окна (элемент 4) будет показано, как сделать то же самое, только без использования графических инструментов, в командной строке.

Для конечных устройств, таких как компьютер, ноутбук, сервер, используется третья вкладка “Desktop”, которая выглядит, как показано на рисунке 3.5.

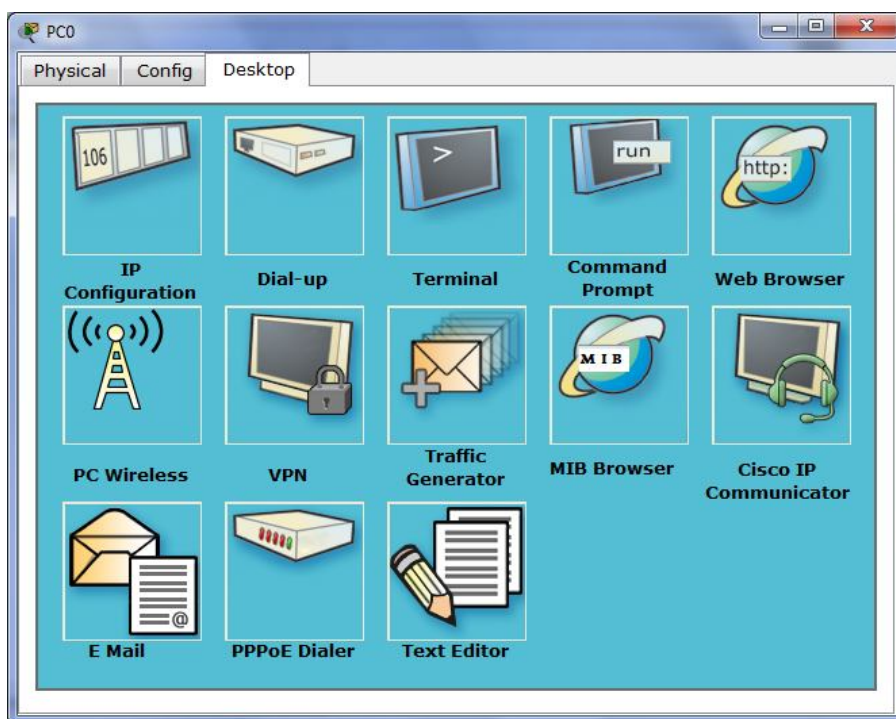


Рисунок 3.5 – Вкладка “Desktop” компьютера

Для настройки IP адреса, маски, шлюза по умолчанию и DNS лучше всего воспользоваться пунктом IP Configuration (рисунок 3.6).

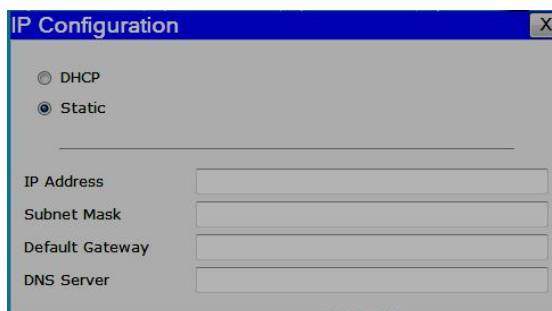


Рисунок 3.6 – Настройка IP параметров компьютера и сервера

Также часто используется пункт Command Prompt (рисунок 3.7). Командная строка поддерживает основные команды для тестирования сети – *ping*, *tracert*, *arp*, *telnet*.

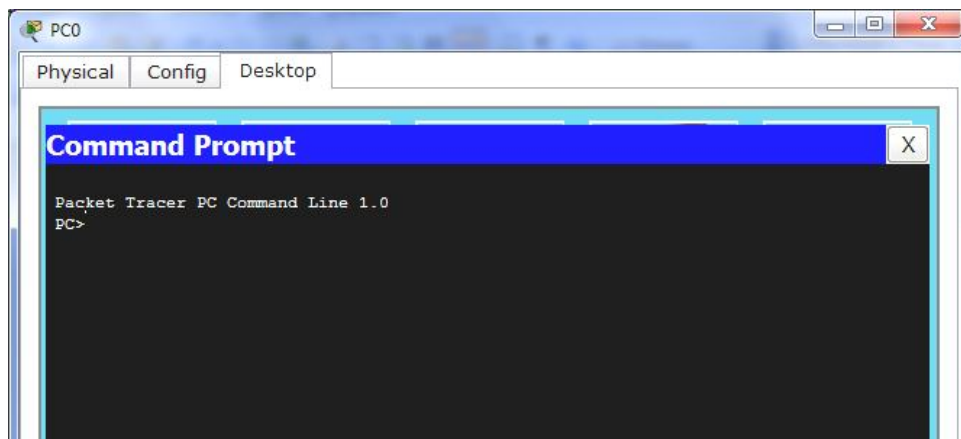


Рисунок 3.7 – Командная строка компьютера

Для проверки Web-серверов можно использовать браузер из пункта Web Browser (рисунок 3.8).

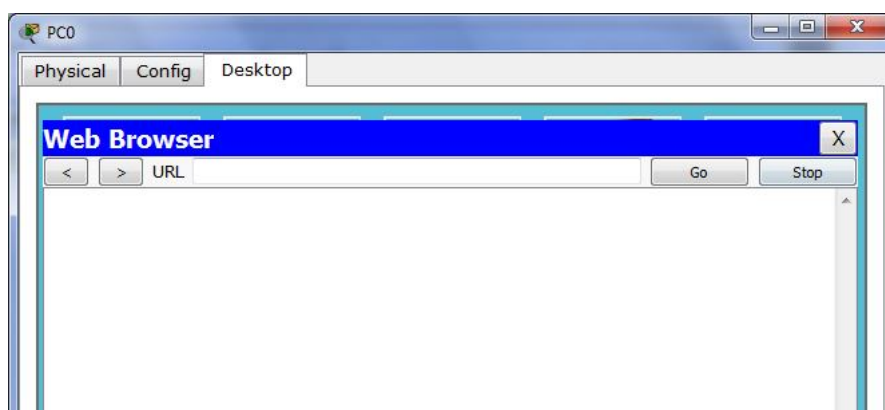


Рисунок 3.8 – Браузер компьютера

Сервер в Packet Tracer имеет почти такую же вкладку «Desktop», но вкладка «Config» значительно отличается (рисунок 3.9)

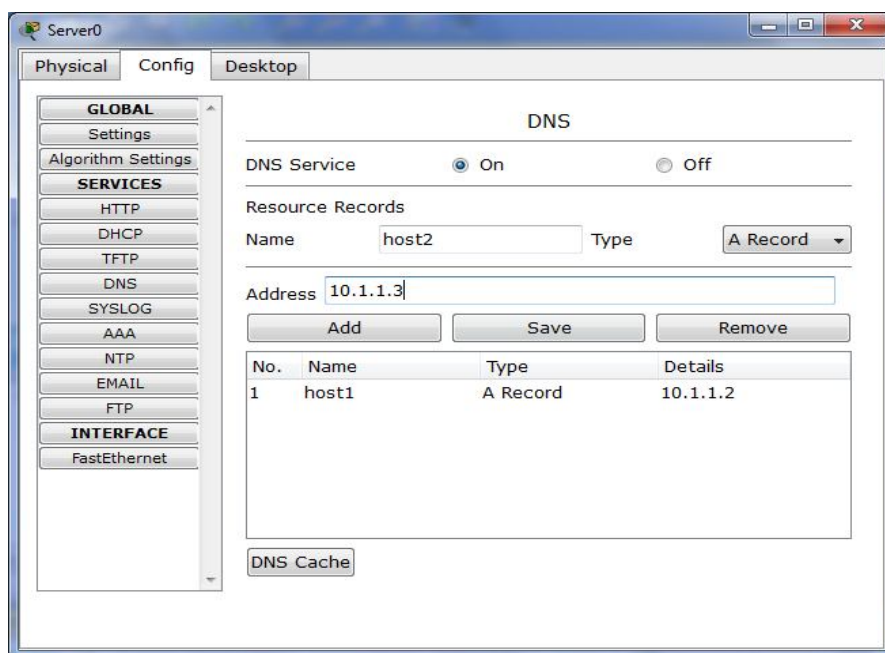


Рисунок 3.9 - Настройка сервисов в сервере

На этой вкладке расположены элементы настройки для сервисов, например DNS. Каждый сервис имеет переключатель On/Off и настройки. Например, в DNS сервере можно вручную задать соответствие IP адреса и доменного имени.

При настройке второго по популярности сервиса – DHCP – необходимо задать такие параметры, как шлюз по умолчанию (default gateway), DNS сервер (обычно это адрес текущего сервера), начальный адрес для раздачи адресов (Start IP address), маску для всех раздаваемых адресов (Subnet mask), количество адресов для резервирования (Maximum number of Users) и имя пула (Pool Name). Пример можно увидеть на рисунке 3.10.

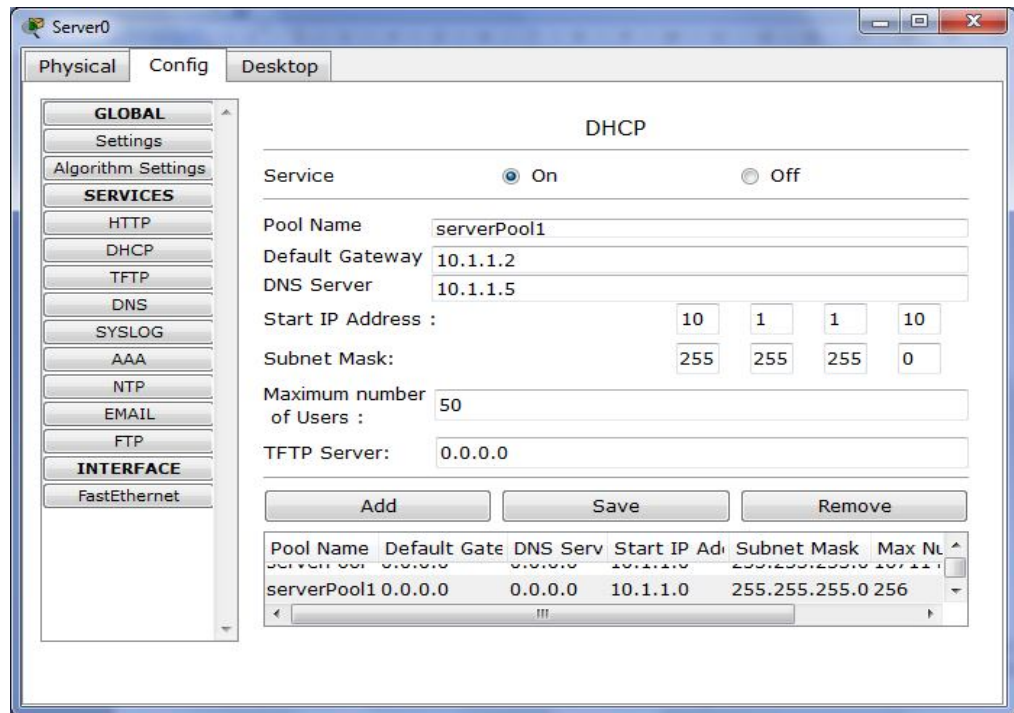


Рисунок 3.10 – Настройка DHCP сервера

В Packet Tracer дополнительно есть множество различных устройств. Символическое изображение показано на рисунке 3.11.

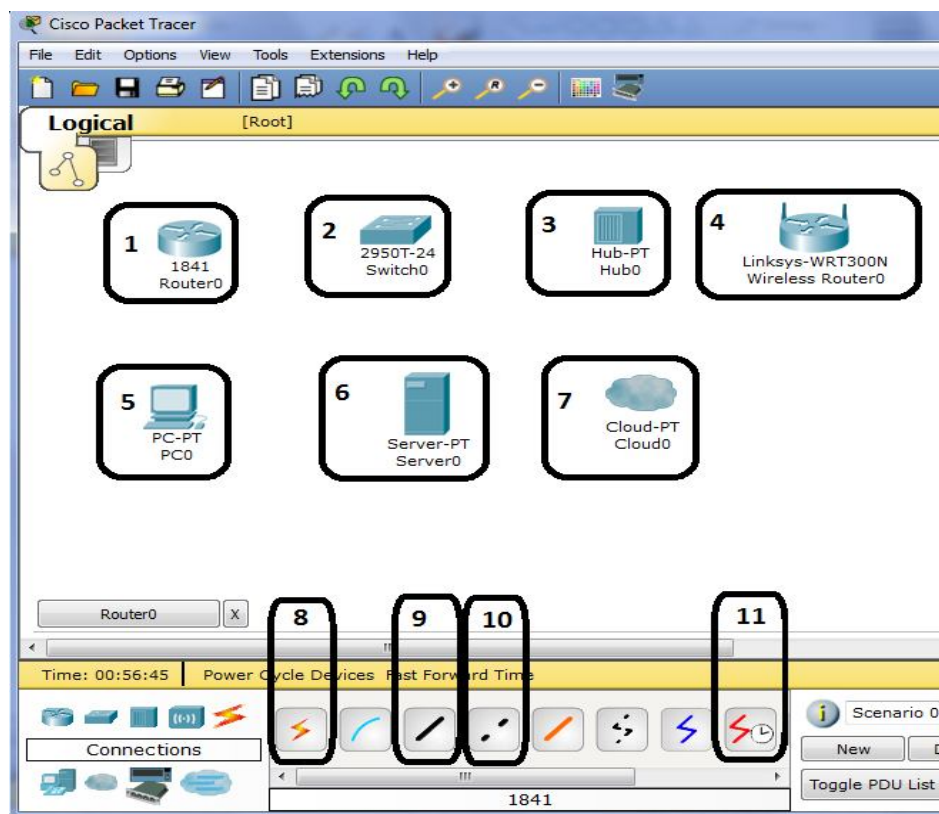


Рисунок 3.11 – Устройства и связи в Packet Tracer

Устройства обозначаются следующим образом:

1 – маршрутизатор, он же «роутер». Используется для передачи данных между сетями;

2 – коммутатор, он же «свич». Используется для объединения компьютеров в одну сеть;

3 – концентратор, он же «хаб». Используется с той же целью, что и коммутатор, но менее интеллектуален, поэтому уже несколько лет не выпускается;

4 – беспроводной маршрутизатор. Обычный маршрутизатор, оснащенный беспроводным модулем. Изображенный на рисунке маршрутизатор относится к серии домашних, поэтому имеет только Веб-интерфейс для настройки;

5 – персональный компьютер;

6 – сервер;

7 – облако, изображает провайдера Интернет;

Кроме устройств сеть состоит еще из соединительных носителей, например, из кабелей. На рисунке они обозначены как:

8 – автоматический определитель типа кабеля. Используется для быстрого соединения устройств. Имеет существенный недостаток: нельзя проконтролировать, в какой порт устройства будет присоединен кабель. Это очень неудобно, когда надо знать интерфейс, например, при соединении двух маршрутизаторов;

9 – прямой кабель, он же «патч-корд». Используется для соединения разных классов устройств, например компьютер-коммутатор, коммутатор-маршрутизатор;

10 – обратный кабель, он же «кроссовер». Используется для соединения одинакового класса устройств, например компьютер-компьютер, коммутатор-коммутатор, компьютер-маршрутизатор;

11 – последовательный кабель, он же «серийный». Используется исключительно для соединения портов типа Serial между маршрутизаторами.

3.2 Рабочее задание

1) Создайте в Packet Tracer простейшую сеть, состоящую из двух компьютеров. Соедините их подходящим кабелем. Настройте IP адресацию и проведите тестирование соединения.

2) Создайте в Packet Tracer топологию, состоящую из двух компьютеров, коммутатора и сервера. Настройте на сервере DHCP сервис и IP параметры. Обновите на компьютерах IP параметры для проверки работы DHCP. Протестируйте связь от компьютеров к серверу.

3) Создайте в Packet Tracer топологию, состоящую из двух компьютеров и маршрутизатора cisco 1841. Соедините компьютеры с маршрутизатором соответствующим кабелем. Настройте параметры IP на маршрутизаторе, затем на компьютерах. Протестируйте соединений с помощью утилиты *tracert*.

IP параметры необходимо взять из таблиц 3.1 – 3.2.

Таблица 3.1 – Параметры IP для заданий 1 и 2

Вариант	IP сеть для компьютеров
1	2
1	192.168.100.128/26
2	192.168.100.64/27
3	10.14.2.192/26
4	10.18.22.16/28
5	172.16.32.32/27
6	192.168.100.128/26
7	192.168.100.64/27
8	10.14.2.192/26
9	10.18.22.16/28
10	172.16.32.32/27

Таблица 3.3 – Параметры IP для задания 3

Вариант	IP сеть для компьютера 1	IP сеть для компьютера 2
1	2	3
1	172.16.32.32/27	10.14.2.192/26
2	10.18.22.16/28	192.168.100.128/26
3	192.168.100.64/27	10.18.22.16/28
4	10.14.2.192/26	172.16.32.32/27
5	192.168.100.128/26	192.168.100.64/27
6	172.16.32.32/27	10.14.2.192/26
7	10.18.22.16/28	192.168.100.128/26
8	192.168.100.64/27	10.18.22.16/28
9	10.14.2.192/26	172.16.32.32/27
10	192.168.100.128/26	192.168.100.64/27

3.3 Контрольные вопросы

- 1) Каким типом кабеля соединяется маршрутизатор и компьютер?
- 2) Чем отличается настройка Serial интерфейса от остальных?
- 3) Какие данные требуются для настройки DHCP сервера?
- 4) Назовите основные сетевые устройства.
- 5) Назовите основные типы интерфейсов на маршрутизаторе.
- 6) Опишите процесс настройки IP адресации на маршрутизаторе.
- 7) Опишите процесс проверки соединений между устройствами.
- 8) Чем кроссовер отличается от прямого кабеля?
- 9) Чем отличается концентратор от коммутатора?
- 10) Какие существуют дополнительные инструменты на конечных устройствах?

4 Лабораторная работа №4. Создание логической схемы сети в Cisco Packet Tracer

Цель работы. Изучить принципы построения сложных сетей. Изучить работу динамической маршрутизации. Получить навыки тестирования сложных сетей.

4.1 Общие сведения

Работа будет проводиться в эмуляторе сетей Cisco Packet Tracer. Логическая схема сети показана на рисунке 13.

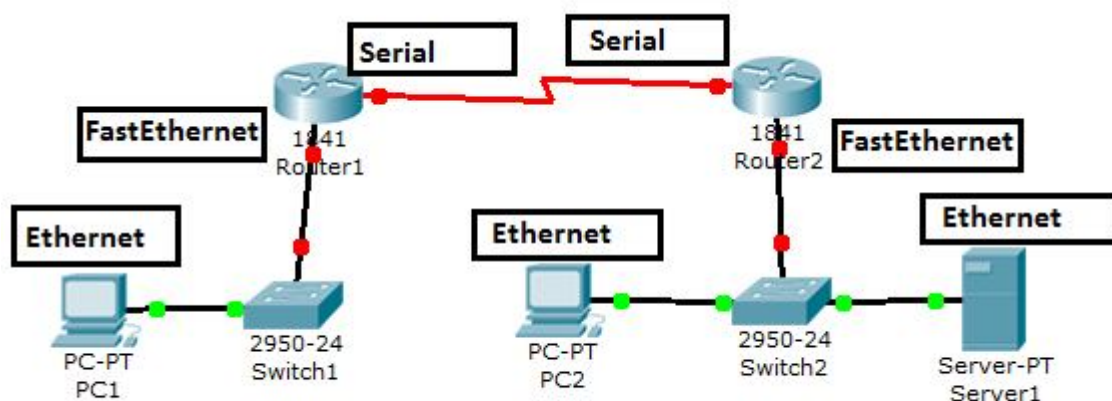


Рисунок 4.1 – Схема сети

Для реализации корректной работы сети необходимо, во-первых, рассчитать IP адреса для каждой из сетей. Для сети 1 (слева) возьмем адрес 10.1.1.0/24, для сети 2 (справа) – адрес 10.1.3.0/24, для связи между маршрутизаторами адрес 10.2.1.0/30.

Возьмем первый адрес сети 1 и 2 в качестве адреса интерфейса маршрутизатора, второй адрес – в качестве адреса конечных устройств. Общая адресация показана в таблице 4.1.

Таблица 4.1 – Конечные адреса для сети

Устройство	Адрес/маска	Шлюз	DNS
1	2	3	4
PC1	10.1.1.2/255.255.255.0	10.1.1.1	10.1.3.2
Router1 - FastEthernet0/0	10.1.1.1/255.255.255.0	-	-
Router1 – Serial0/0/0	10.1.2.1/255.255.255.252	-	-
Router2 - FastEthernet0/0	10.1.3.1/255.255.255.0	-	-
Router2 – Serial0/0/0	10.1.2.2/255.255.255.252	-	-
PC2	10.1.3.3/255.255.255.0	10.1.3.1	10.1.3.2
Server1	10.1.3.2/255.255.255.0	10.1.3.1	10.1.3.2

Затем необходимо настроить IP адреса на компьютерах и сервере (рисунок 4.2). Шлюзом указывается ближайший интерфейс ближайшего маршрутизатора, DNS-сервер находится на сервере в сети 2.

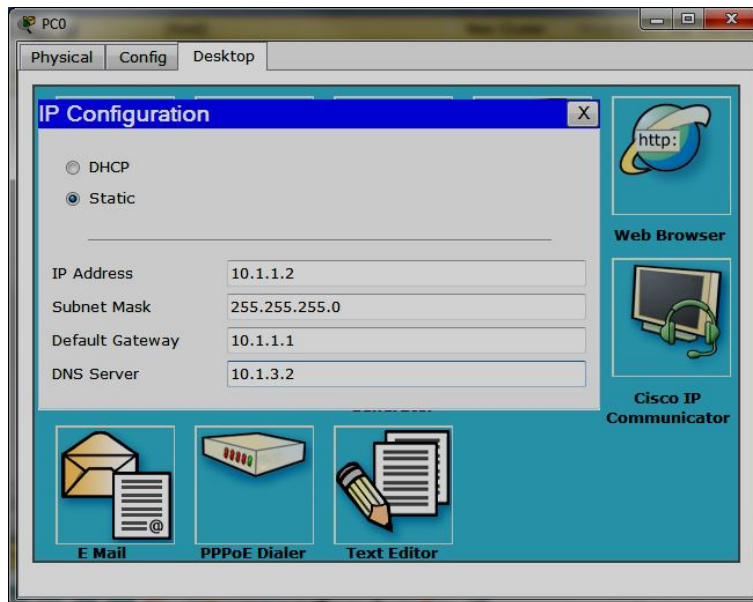


Рисунок 4.2 – Настройка параметров IP конечных устройств

Настройка IP адреса на интерфейсе маршрутизатора ничем не отличается от настройки компьютера, кроме того, что указывать шлюз и DNS сервер не надо (рисунок 4.3).

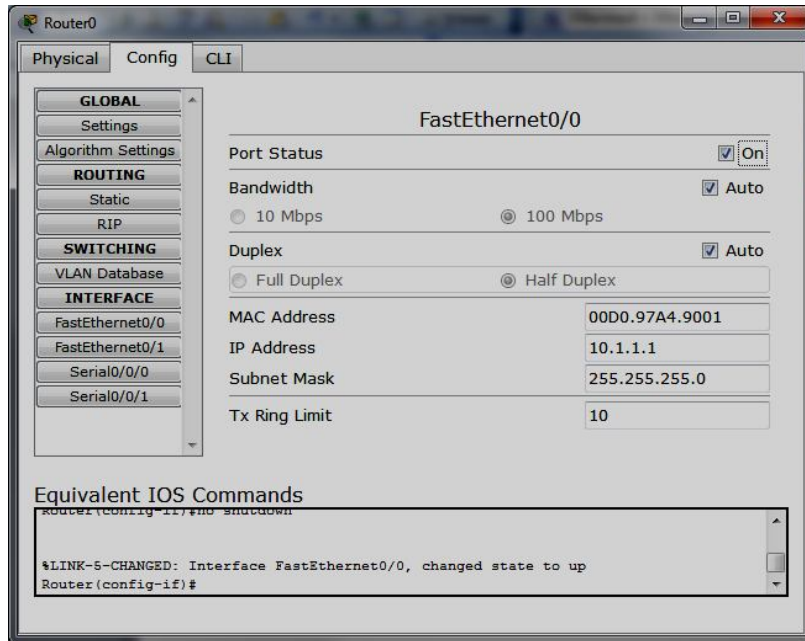


Рисунок 4.3 – Настройка FastEthernet на маршрутизаторах

Настройка интерфейса Serial отличается тем, что дополнительно необходимо указать скорость интерфейса «Clock Rate» (рисунок 4.4).

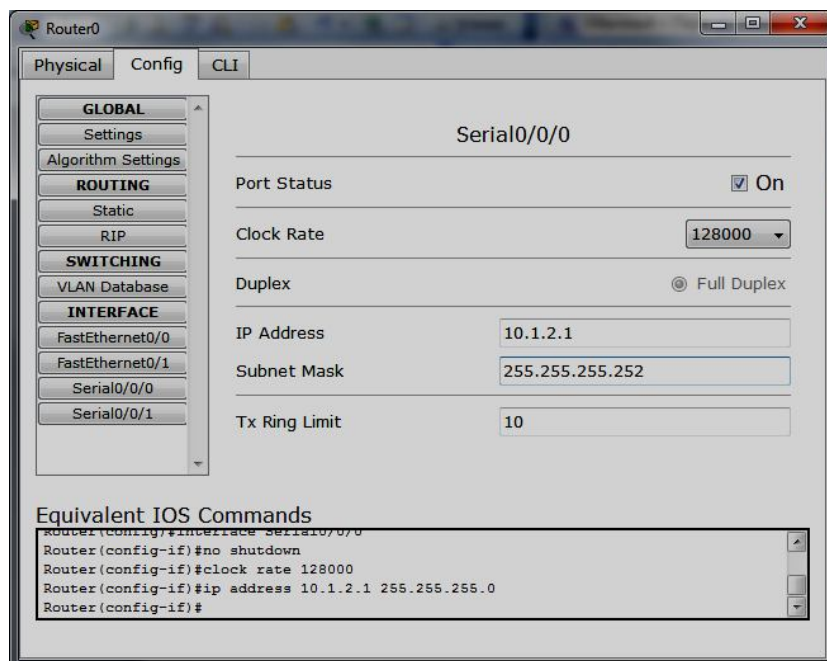


Рисунок 4.4 – Настройка Serial на маршрутизаторах

Затем необходимо настроить динамическую маршрутизацию на маршрутизаторе. В качестве протокола был выбран RIPv2 (Routing Internet Protocol Version 2) как самый простой в настройке (рисунок 4.5). Необходимо на вкладке RIP задать адрес всех сетей, которые есть на данном маршрутизаторе (ни в коем случае не на соседнем). При добавлении сетей (кнопка «ADD») они могут агрегироваться из-за недостатков протокола.

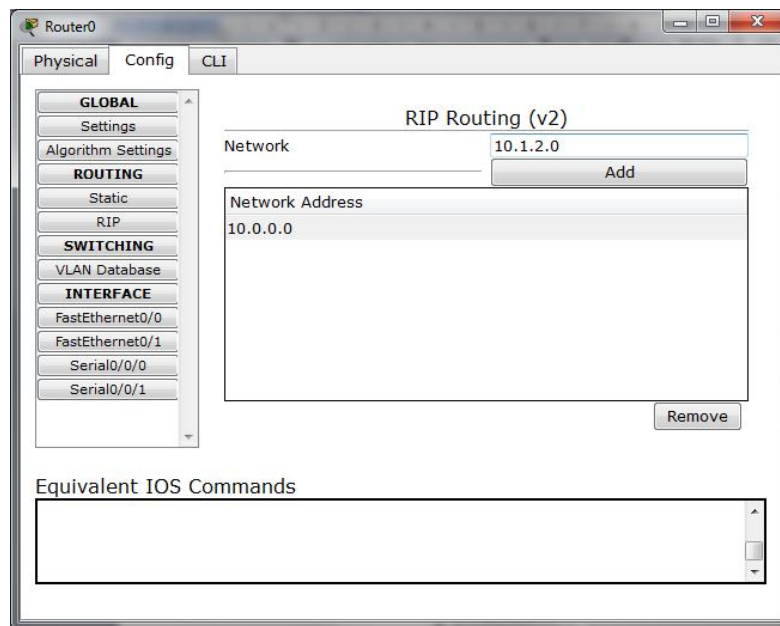


Рисунок 4.5 – Настройка RIP на маршрутизаторе

После добавления сетей необходимо переключить RIP на вторую версию протокола. Для этого необходимо сразу после добавления сетей переключиться на вкладку «CLI» и набрать команду «*version 2*», после чего нажать Ctrl-Z (рисунок 4.6).

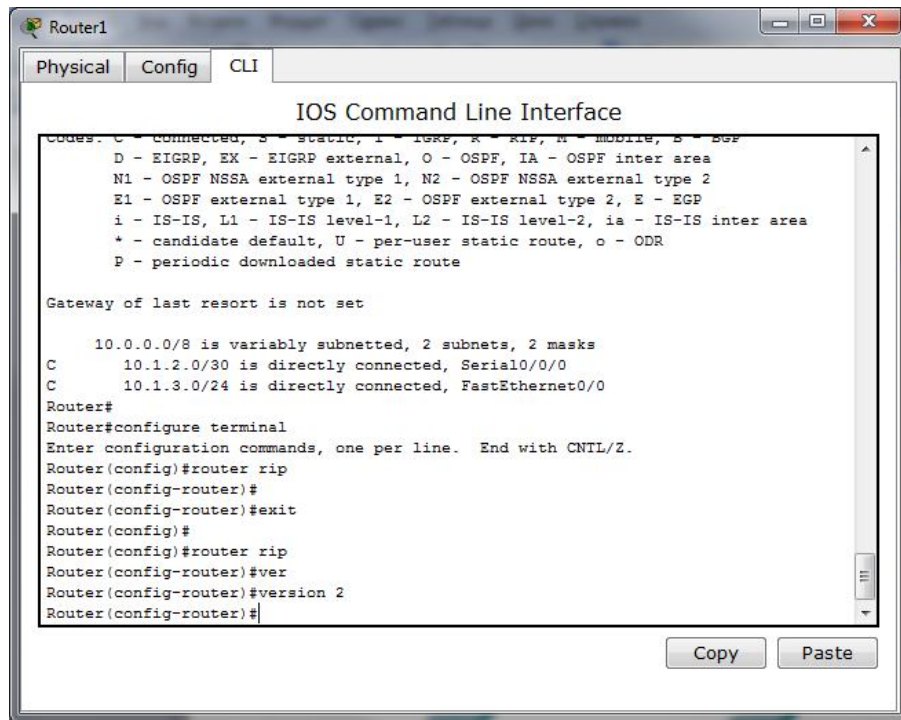


Рисунок 4.6 – Настройка версии RIP на маршрутизаторе

После настройки обоих маршрутизаторов необходимо проверить корректность работы. Для этого необходимо набрать в командной строке команду «*show ip route*» и нажать «Enter». В выводе команды должна быть строка, начинающаяся буквой «*R*», что значит RIP (рисунок 4.7). Если такой строки нет, значит, неправильно произведена настройка.

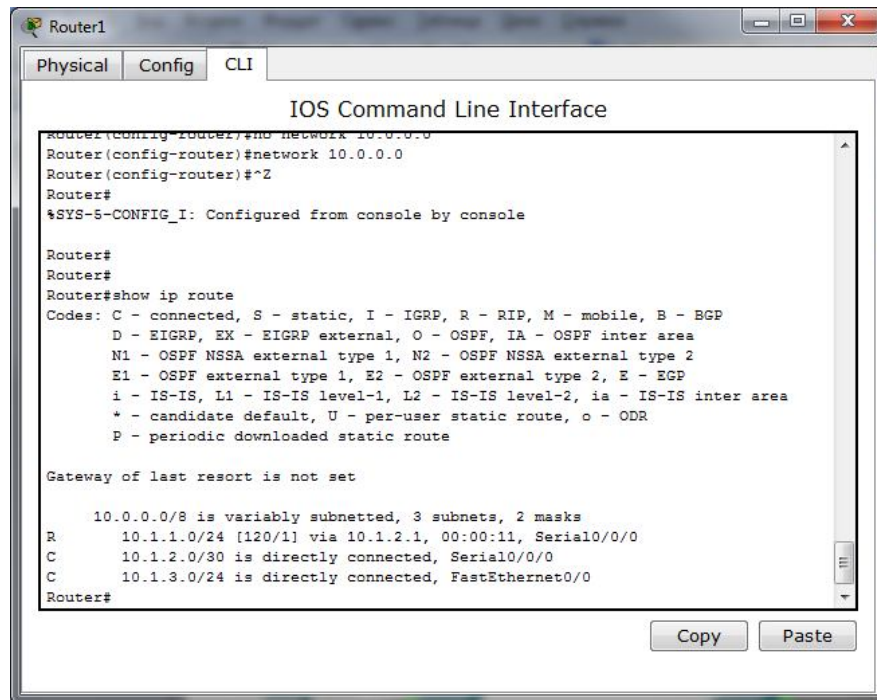


Рисунок 4.7 – Проверка работы RIP на маршрутизаторах

Затем необходимо настроить DNS сервер. Для этого, на вкладке «DNS» сервера Server1 нужно добавить имя будущего сервера (например server или yandex.ru) и добавить IP адрес текущего сервера и нажать кнопку «Add».

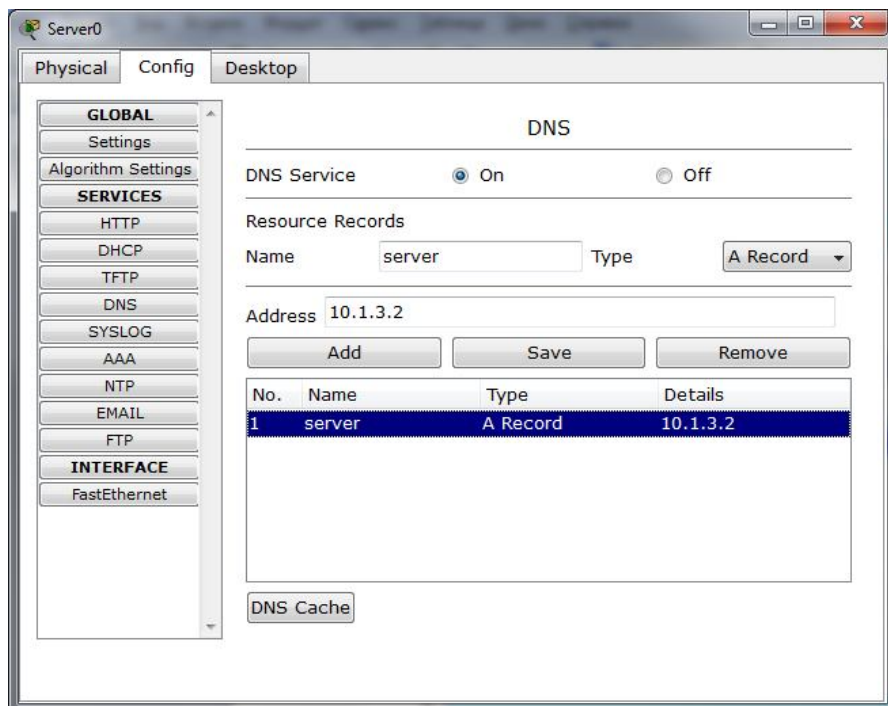
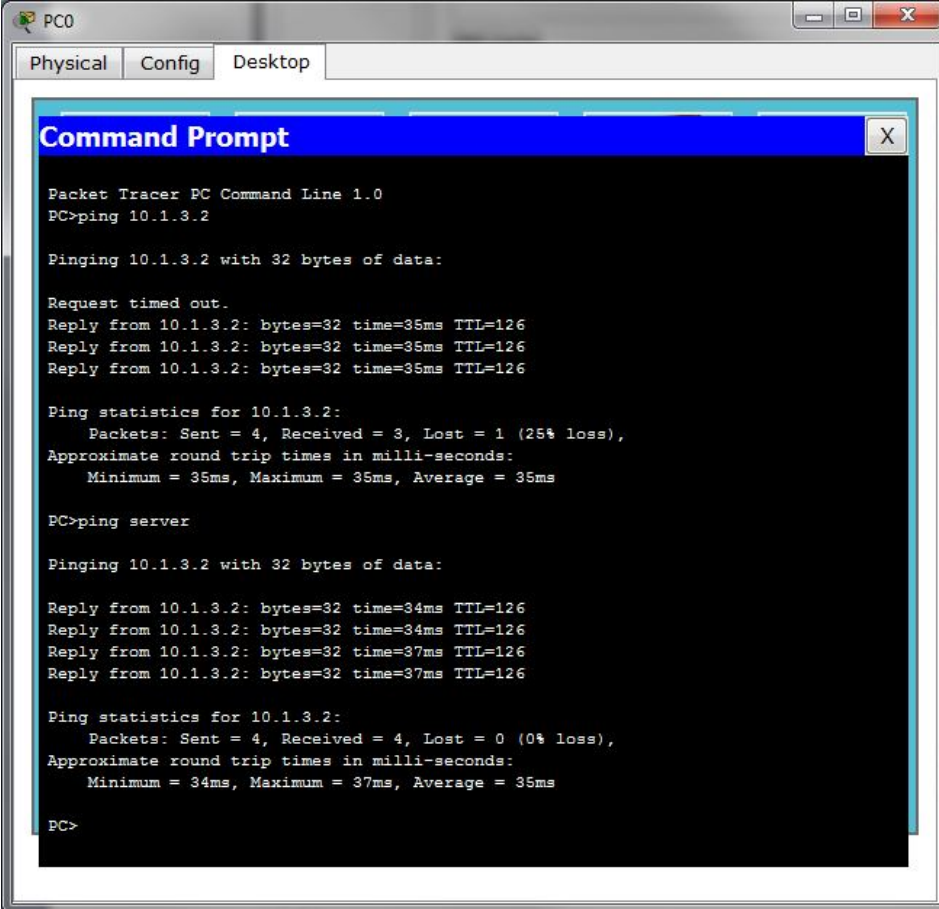


Рисунок 4.7 – Настройка DNS службы на сервере

После окончания всех настроек необходимо проверить работу сети командой *ping*. Сначала проверим связь по IP протоколу. Для этого используем IP адрес сервера в команде *Ping* на компьютере PC1. Если связь работает (первый пакет может потеряться, это нормально), будет выведена информация о задержках пакетов и статистическая информация. После этого необходимо проверить работу DNS службы командой *ping ИМЯ*, где *ИМЯ* – это доменное имя, заданное в DNS сервере.



```
Packet Tracer PC Command Line 1.0
PC>ping 10.1.3.2

Pinging 10.1.3.2 with 32 bytes of data:

Request timed out.
Reply from 10.1.3.2: bytes=32 time=35ms TTL=126
Reply from 10.1.3.2: bytes=32 time=35ms TTL=126
Reply from 10.1.3.2: bytes=32 time=35ms TTL=126

Ping statistics for 10.1.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 35ms, Maximum = 35ms, Average = 35ms

PC>ping server

Pinging 10.1.3.2 with 32 bytes of data:

Reply from 10.1.3.2: bytes=32 time=34ms TTL=126
Reply from 10.1.3.2: bytes=32 time=34ms TTL=126
Reply from 10.1.3.2: bytes=32 time=37ms TTL=126
Reply from 10.1.3.2: bytes=32 time=37ms TTL=126

Ping statistics for 10.1.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 34ms, Maximum = 37ms, Average = 35ms

PC>
```

Рисунок 4.8 – Проверка с помощью PING по IP адресу и доменному имени

Если проверка Ping завершилась успешно, необходимо проверить работу Web-сервера. Для этого на компьютере PC1 нужно на вкладке «Desktop» выбрать «Web Browser» и в строке адреса набрать доменное имя сервера (рисунок 4.9).

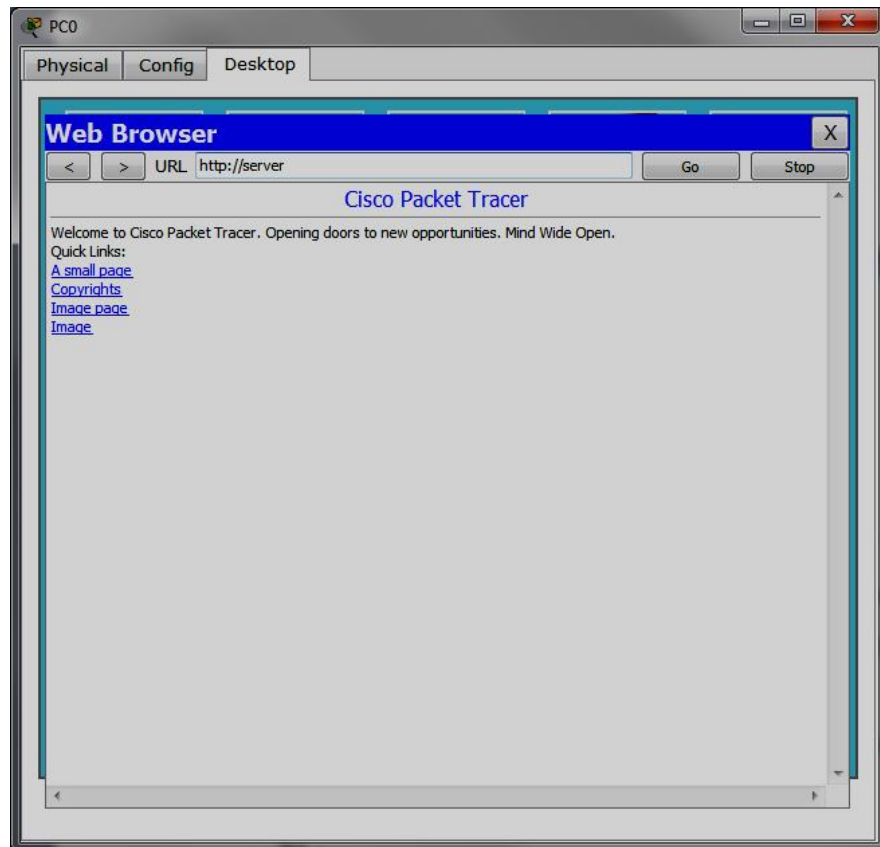


Рисунок 4.9 – Проверка через Веб-браузер

Если все тесты пройдены успешно, значит сеть работает корректно.

4.2 Рабочее задание

- 1) Собрать схему сети (рисунок 4.1) в программе Packet Tracer. После сборки сети, следует перерисовать (или распечатать) эту схему и подписать ВСЕ интерфейсы ВСЕХ устройств, в том числе интерфейсы присоединения кабелей.
- 2) Провести проектирование IP адресации, подписать все IP адреса всех интерфейсов оборудования.
- 3) Настроить компьютеры и сервер. Задать им IP адреса и маски в соответствии с п.2. Подписать эти адреса и маски в схеме. Настроить DNS службу.
- 4) Сконфигурировать маршрутизаторы. В настройках включить нужные интерфейсы (по схеме), задать IP адрес, маску для каждого из интерфейсов.
- 5) Использовать *ping*-запросы из командной строки для проверки доступности или недоступности связи.

- 6) Настроить динамическую маршрутизацию в настройках маршрутизаторов.
 - 7) Использовать *ping*-запросы из командной строки для проверки связи.
 - 8) Использовать трассировку маршрута (*tracroute, tracert*) для проверки пути следования пакетов.
 - 9) Использовать Веб-браузер для проверки работы сервера.
- Варианты заданий показаны в таблице 4.1

Таблица 4.1 – Параметры IP

Вариант	IP сеть для сети 1	IP сеть для сети 2	IP сеть для связи между маршрутизаторами
1	2	3	4
1	172.16.32.32/27	10.14.2.192/26	10.18.22.16/30
2	10.18.22.16/28	192.168.100.128/26	172.16.32.32/30
3	192.168.100.64/27	10.18.22.16/28	10.14.2.192/30
4	10.14.2.192/26	172.16.32.32/27	192.168.100.128/30
5	192.168.100.128/26	192.168.100.64/27	10.0.0.0/30
6	172.16.32.32/27	10.14.2.192/26	10.18.22.16/30
7	10.18.22.16/28	192.168.100.128/26	172.16.32.32/30
8	192.168.100.64/27	10.18.22.16/28	10.14.2.192/30
9	10.14.2.192/26	172.16.32.32/27	192.168.100.128/30
10	192.168.100.128/26	192.168.100.64/27	10.0.0.0/30

4.3 Контрольные вопросы

- 1) Что такое RIP?
- 2) Как настроить RIP на поддержку двух сетей?
- 3) Опишите настройку маршрутизации с помощью командной строки.
- 4) На каком уровне модели OSI происходит проверка связи с помощью протокола HTTP?

- 5) На каком уровне модели OSI происходит проверка связи с помощью команды ping?
- 6) Каким образом работает команда *ping ИМЯ*?
- 7) Что необходимо настроить для поддержки второй версии RIP?
- 8) IP адреса на последовательных интерфейсах маршрутизатора должны располагаться в разных подсетях или в одной?
- 9) IP адреса на Ethernet интерфейсах маршрутизатора должны располагаться в разных подсетях или в одной?
- 10) При проверке Web-браузером, какие уровни модели OSI проверяются?

5 Лабораторная работа №5. Проектирование физической схемы сети, расчет комплектующих и расходных материалов

Цель работы. Изучить принципы проектирования физической схемы сети. Получить навыки выбора оборудования для проектируемой сети.

5.1 Общие сведения

Создание рабочего проекта сети очень трудоемко и требует значительных временных затрат. На этапе проектирования решаются следующие задачи:

- 1) На основе определенных целевых требований к сети определяется необходимый состав оборудования и, прежде всего, компьютеров: количество, характеристики и т.д.
- 2) Определяется физическое расположение рабочих мест. Если речь идет о создании сети в одном здании, то определяются этажи и комнаты, которые должны охватываться сетью. При решении этой задачи должна учитываться принципиальная возможность прокладки линий связи к рабочим местам/помещениям.
- 3) Исходя из решаемых задач, стоимости и расположения, определяется тип физических линий связи, соединяющих рабочие места, а также состав и расположение коммуникационного оборудования (например, концентраторов).

4) Определяется способ подключения к Интернету, выбирается провайдер - организация, обеспечивающая подключение организации к сети Интернет.

5) Исходя из технических требований, определяется узел проектируемой сети, который будет являться шлюзом для подключения к Интернету и определяется место его расположения. При этом учитывается удобство физического соединения шлюза с проектируемой сетью и удобство подведения физических линий для подключения к Интернету.

Проектирование инфраструктуры является самой трудоемкой задачей в проекте. Оно решает следующие задачи:

1) Определяются протоколы, которые будут использоваться в сети. Основными протоколами для сетей Windows являются протоколы стека TCP/IP. Они же используются для подключения к Интернету. Если в сети используются компьютеры под управлением других ОС, необходимо выбирать протоколы, поддерживаемые всем используемым оборудованием (например, IP телефония).

2) Осуществляется планирование IP-сетей - сетям назначаются диапазоны IP-адресов, планируется топология маршрутизации.

3) Определяется, будет ли планируемая сеть одноранговой (все компьютеры такой сети равноправны) или в ней предполагается разместить выделенные серверы для поддержки определенных функций.

4) Определяется, будут ли компьютеры планируемой сети объединяться в рабочие группы или в домены.

5) Определяется, какие службы будут развертываться в сети.

6) Определяются группы пользователей сети, и планируется политика безопасности в сети.

Исходя из плана какого-либо помещения, необходимо выполнить проектирование сети. При создании новой сети желательно учитывать следующие факторы:

– требуемый размер сети (в настоящее время, в ближайшем будущем и по прогнозу на перспективу);

– структура, иерархия и основные части сети (по подразделениям предприятия, а также по комнатам, этажам и зданиям предприятия);

- основные направления и интенсивность информационных потоков в сети (в настоящее время, в ближайшем будущем и в дальнейшей перспективе);
- характер передаваемой по сети информации;
- технические характеристики оборудования (компьютеров, адаптеров, кабелей, репитеров, концентраторов, коммутаторов);
- возможности прокладки кабельной системы в помещениях и между ними, а также меры обеспечения целостности кабеля;
- обслуживание сети и контроль ее безотказности и безопасности;
- требования к программным средствам по допустимому размеру сети, скорости, гибкости, разграничению прав доступа, стоимости, по возможностям контроля обмена информацией и т.д. (например, если предполагается использование одного ресурса многими пользователями, то следует использовать серверную ОС);
- необходимость подключения к другим сетям (например, глобальным);
- имеющиеся компьютеры и их программное обеспечение, а также периферийные устройства (принтеры, сканеры и т.д.).

В настоящее время для организации локальных сетей в подавляющем большинстве случаев используется неэкранированная витая пара UTP. Более дорогие варианты на основе экранированной витой пары, оптоволоконного кабеля или беспроводных соединений применяются на предприятиях, где в этом существует действительно острая необходимость. Например, оптоволокно может использоваться для связи между удаленными сегментами сети без потери скорости.

Для физического проектирования сетей применяют метод пятидесятиметровой окружности. Метод пятидесятиметровой окружности заключается в следующем. Необходимо на плане сети нарисовать несколько окружностей радиусом 50м. Затем выбрать то количество и расположение окружностей, которые оптимально покрывают все компьютеры. Например, в длинном помещении оптимально будет две-три окружности (рисунок 5.1). Все окружности должны пересекаться минимум на 20%. Центр каждой окружности – оптимальное место для установки коммутатора. Однако надо учитывать и особенности помещения, так как шкаф с оборудованием может висеть только на стене (за редким исключением).

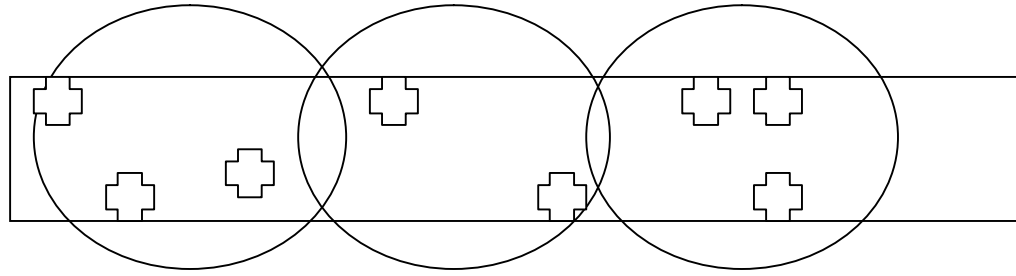


Рисунок 5.1 – Пример оптимального изображения пятидесятиметровых окружностей в длинном здании.

Длина кабеля рассчитывается для каждого помещения отдельно методом средней длины. При этом:

- 1) Кабель делится на два отрезка: от коммутатора до ввода в помещение (эту длину обозначим $L1$) и от ввода в помещение до компьютеров (эту длину обозначим $L2$).
- 2) Длина каждого отрезка кабеля измеряется по плану здания.
- 3) Общая длина кабеля, необходимая для подключения n компьютеров в помещении рассчитывается по формуле (5.1):

$$L = n * (L1 + L2 * 0.7) \quad (5.1)$$

где n – количество компьютеров.

Затем рассчитывается общее число портов каждого коммутатора суммированием всех подведенных к нему кабелей. Реальное количество портов коммутатора должно превышать требуемое количество не менее чем на 20% или на 5шт. Это делается для обеспечения масштабируемости.

5.2 Рабочее задание

В соответствии с вариантами заданий (таблица 5.1) и планом помещений (рисунок 5.2):

- 1) Определить количество компьютеров и комнаты, в которых они будут стоять, выбрать комнату - центральную серверную.
- 2) Разместить компьютеры по помещениям.
- 3) Исходя из расположения компьютеров, методом пятидесятиметровой окружности выбрать оптимальные места расположения коммутаторов.
- 4) Визуально провести кабель до коммутаторов, рассчитать требуемое количество портов коммутаторов.
- 5) Рассчитать длину требуемого кабеля для каждого помещения.
- 6) Рассчитать длину кабеля от коммутаторов до центральной серверной.
- 7) Рассчитать количество портов центрального коммутатора.
- 8) Составить список требуемого оборудования (серверы, коммутаторы, маршрутизаторы, беспроводные точки, модемы, ИБП, стойки, шкафы, патч-панели, патч-корды, кабель, кабель-каналы, коннекторы, дюбель-гвозди, подвесы, лотки и.т.д.).
- 9) Выбрать конкретные модели оборудования и материалов, вставить в спецификацию модели и цены.
- 10) Оформить схему сети и спецификацию оборудования.

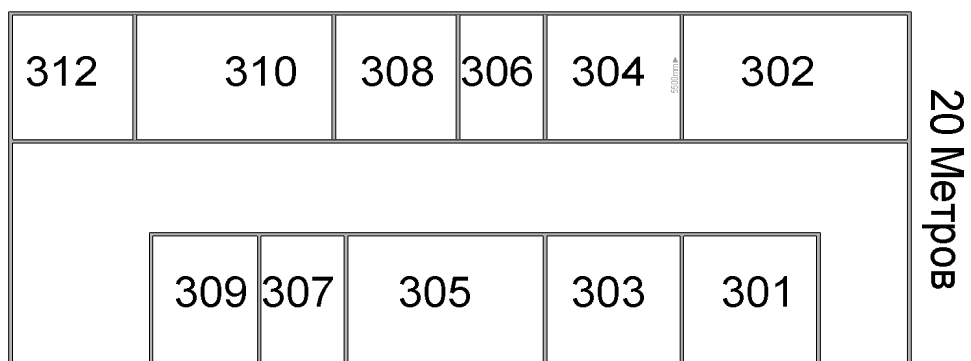
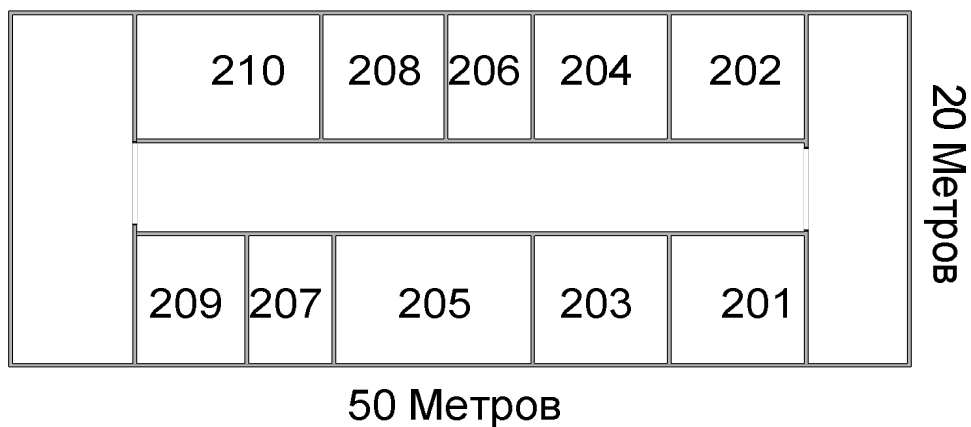


Рисунок 5.2 – План помещений 2 и 3 этажей

Таблица 5.1 – Варианты заданий

Вариант	Номера помещений с компьютерами	Общее количество компьютеров
1	2	3
1	210 206 201 310 305 302	30
2	207 208 203 301 303 309	40
3	208 206 203 201 312 302	25
4	209 207 203 308 304 303	32
5	205 203 312 306 301 302	36
6	205 206 207 307 308 312	28
7	210 205 202 301 308 309	29
8	209 207 205 309 307 310	31
9	208 204 202 303 307 310	52
10	202 206 210 308 304 303	45

5.3 Контрольные вопросы

- 1) Описать процесс проектирования сети.
- 2) Какие задачи решаются на этапе проектирования сети?
- 3) Какие факторы необходимо учитывать при проектировании новой сети?

- 4) В чем суть метода пятидесятиметровой окружности?
- 5) Описать алгоритм расчета длины кабеля при создании новой сети.
- 6) Как учитывается требование масштабируемости при проектировании сети?
- 7) Когда применяется метод пятидесятиметровой окружности?
- 8) Что включает в себя проектирование инфраструктуры?
- 9) Что должно учитываться при проектировании линий связи до конечных пользователей?
- 10) Что необходимо предусмотреть при выборе серверной комнаты?

Список использованных источников

- 1) Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учеб. пособие для вузов / В. Г. Олифер, Н. А. Олифер .- 3-е изд. - СПб. [и др.] : Питер, 2008. - 960 с. : ил.. - (Учебник для вузов)
- 2) Немет, Э. Руководство администратора Linux = Linux Administration Handbook [Текст] : пер. с англ. / Э. Немет, Г. Снайдер, Т. Р. Хейн .- 2-е изд. - М. : Вильямс, 2008. - 1072 с. : ил.
- 3) Максимов, Н. В. Компьютерные сети [Текст] : учеб. пособие / Н. В. Максимов, И. И. Попов .- 3-е изд., перераб. и доп. - М. : Форум, 2008. - 447 с. : ил.