Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кузбасский государственный технический университет
имени Т. Ф. Горбачева»

Институт профессионального образования

Кафедра информатики и информационных систем

Составитель Е. Б. Зотеев

КОМПЬЮТЕРНЫЕ СЕТИ

Методические материалы

Рекомендовано цикловой методической комиссией
Информационных систем и программирования
в качестве электронного издания
для использования в образовательном процессе

Кемерово 2026

Рецензент:
С. А. Асанов, старший преподаватель кафедры информационных и автоматизированных производственных систем

Зотеев Евгений Борисович

Компьютерные сети : методические материалы для обучающихся специальности СПО 09.02.11 Разработка и управление программным обеспечением / Кузбасский государственный технический университет имени Т. Ф. Горбачева ; кафедра информатики и информационных систем ; составитель Е. Б. Зотеев. – Кемерово : КузГТУ, 2026. – 1 файл (1433 КБ). – Текст : электронный.

Методические материалы по дисциплине «Компьютерные сети» для обучающихся специальности СПО 09.02.11 Разработка и управление программным обеспечением содержат указания для проведения лабораторных работ и самостоятельных работ.

Лабораторная работа №1
Монтаж кабельных сред

Цель работы: ознакомление с конструктивными элементами кабелей связи и соответствующей кабельной арматурой и приобрести практические навыки по разделке кабелей. Результатом лабораторной работы является отчет, в котором должны быть отражены ход работ и результаты проверки работоспособности подготовленного кабеля.

Теоретические положения

Назначение кабельных линий и их основные элементы

Для продуктивной работы организаций компьютеры, телефоны и периферийное оборудование объединяют в единую сеть. Это позволяет совместно использовать данные, принтеры и доступ к другим сетям. Большое влияние на качество, скорость и надежное соединение оказывает сетевое оборудование.

При создании кабельной структуры, необходимо учитывать совместимость всех ее составляющих.

Основными стандартами по кабельным системам являются:

- Международный стандарт ISO/IEC 11801 Generic Cabling for Customer Premises (www.iso.ch, www.iec.ch).
- Европейский стандарт EN 50173 Information technology– Generic cabling systems
- Американский стандарт ANSI/TIA/EIA 568-B Commercial Building Telecommunication Cabling Standard

Стандарты определяют среду передачи, параметры разъемов, линии и канала, в том числе предельно допустимые длины, топологию и характеристики функциональных элементов системы.

Структурированная кабельная система представляет собой иерархическую кабельную среду передачи электрических или оптических сигналов в здании, разделённую на структурные подсистемы и состоящую из элементов – кабелей, разъёмов, панелей, шкафов и вспомогательного оборудования.

Сетевое оборудование не потребляющее электрическую энергию называется пассивным. К пассивному оборудованию относятся розетки, кабель, вилки, патч-панели и т. п.

Основными компонентами являются сетевой кабель и монтируемая на нем вилка.

Сетевой кабель и вилка

При монтаже кабельной системы наиболее часто используют неэкранированную «витую пару» 5 категорий (UTP 5 cat). Он состоит из нескольких пар медных проводов, покрытых пластиковой оболочкой.

Провода, составляющие каждую пару, скручены друг вокруг друга, что обеспечивает защиту от взаимных наводок.

Изоляция каждого провода окрашена в свой цвет (рисунок 1.1):

- бело-зеленый
- зеленый
- бело-оранжевый
- оранжевый
- бело-синий
- синий
- бело-коричневый
- коричневый.

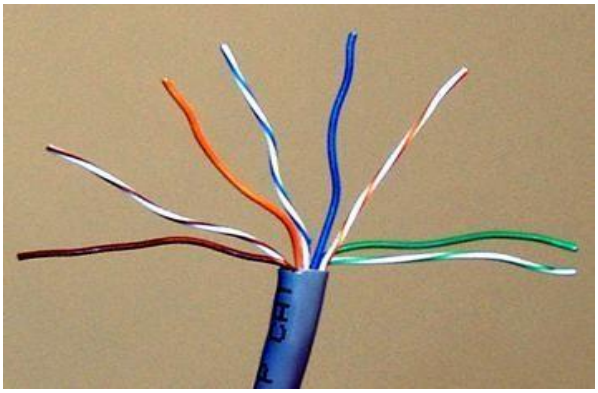

Рис. 1.1. – Изоляция проводов

Провода с одинаковым цветом составляют 4 пары:

- оранжевый / бело-оранжевый,
- зеленый / бело-зеленый,
- синий / бело-синий,
- коричневый / бело-коричневый.

Для подключения кабеля «витая пара» используются вилки RJ45, которые монтируются на концах кабеля. Вилка имеет восемь контактов и монтируется на кабель при помощи специального инструмента.

Коммутационный кабель

Коммутационный кабель или патч-корд (от англ. patching cord — соединительный шнур) представляет собой электрический

кабель для подключения одного электрического устройства к другому.

Может быть любых размеров, на одном или обоих концах кабеля присутствуют разъемы (коннекторы).

Применяются для подключения ПК к розетке, двух коммутационных панелей друг к другу и так далее.

Главное отличие коммутационного кабеля от кабеля внутренней прокладки – использование многожильного провода для каждого из проводников, вместо одножильного. Это снижает передаточные характеристики кабеля, но повышает гибкость и уменьшает радиус безопасного изгиба шнура.

Монтаж вилки RJ-45

Вилка RJ-45 монтируется обжимным способом с помощью специального обжимного инструмента в соответствии с одним из стандартов T568A или T568B.

Правила монтажа определяются типом предполагаемого соединения. Возможны два варианта:

- Компьютер соединяется с сетевым концентратором (hub) или коммутатором (switch) используя «прямую» разводку кабеля (стандарт T568B), рисунок 1.2;

Рис. 1.2. – Правила монтажа

- Соединение между коммутаторами или концентраторами, такие как “hub – hub”, “switch – switch”, “hub – switch” производятся с помощью кабеля с «перевернутой» разводкой (Uplink или Crossover). С одной стороны кабель разводится по стандарту T568A, а с другой по стандарту T568B), рисунок 1.3.

Рис. 1.3. – Правила монтажа

Задания к лабораторной работе №1

1. Прослушать информацию о безопасной работе с инструментом от преподавателя.
2. Получить необходимые инструменты для выполнения работы.
3. Самостоятельно выполнить монтаж вилки RJ-45.

Лабораторная работа №2
Инструменты диагностики кабельной инфраструктуры

Цель работы: изучить работы устройств, предназначенных для диагностики кабельной инфраструктуры. Результатом лабораторной работы является отчет, в котором должно быть приведено описание принципа работы прибора, выданного для выполнения лабораторной работы, и результатов проведенных с его помощью измерений.

Теоретические положения

Оборудование для диагностики и сертификации кабельных систем

К оборудованию данного класса относятся сетевые анализаторы, приборы для сертификации кабелей, кабельные сканеры и тестеры. Основной задачей для их применения является проверка целостности и корректности последовательности расположения проводников в кабельном сегменте.

Сетевые анализаторы

Сетевые анализаторы представляют собой эталонные измерительные инструменты для диагностики и сертификации кабелей и кабельных систем.

Сетевые анализаторы содержат высокоточный частотный генератор и узкополосный приемник. Передавая сигналы различных частот в передающую пару и измеряя сигнал в приемной паре, можно измерить переходное затухание между парами. Сетевые анализаторы – это прецизионные крупногабаритные и дорогие (стоимостью более $20000) приборы, предназначенные для использования в лабораторных условиях специально обученным техническим персоналом. По результатам замеров на данном оборудовании партии кабеля присваивается та или иная категория.

Кабельные сканеры

Данные приборы позволяют определить длину кабеля, переходное затухание между парами, импеданс, последовательность расположения проводников, уровень электрических шумов и провести оценку полученных результатов. Цена на эти приборы варьируется от $1000 до $3000. В отличие от сетевых анализаторов

сканеры могут быть использованы не только специально обученным техническим персоналом, но и рядовыми администраторами сетей.

Для определения местоположения неисправности кабельной системы (обрыва, короткого замыкания, неправильно установленного разъема и т. д.) используется метод "кабельного радара", или Time Domain Reflectometry (TDR). Суть этого метода состоит в том, что сканер излучает в кабель короткий электрический импульс и измеряет время задержки до прихода отраженного сигнала. По полярности отраженного импульса определяется характер повреждения кабеля (короткое замыкание или обрыв). В правильно установленном и подключенном кабеле отраженный импульс совсем отсутствует.

Точность измерения расстояния зависит от того, насколько точно известна скорость распространения электромагнитных волн в кабеле. В различных кабелях она будет разной. Скорость распространения электромагнитных волн в кабеле (обычно задается в процентах к скорости света в вакууме). Современные сканеры содержат в себе электронную таблицу данных для всех основных типов кабелей и позволяют пользователю устанавливать эти параметры самостоятельно после предварительной калибровки.

Тестеры кабельных систем

Тестеры кабельных систем – наиболее простые и дешевые приборы для диагностики кабеля. Они позволяют определить целостность кабельного сегмента, однако, в отличие от кабельных сканеров, не дают ответа на вопрос о том, в каком месте произошел сбой (если таковой имеет место).

Существуют целые классы средств тестирования кабельных систем, появление которых стало возможным благодаря наличию четких стандартов на характеристики компонентов (TIA/EIA568), а также на процедуры и критерии тестирования кабельных линий СКС (TSB-67).

Большинство моделей выпускаемых тестеров СКС предназначено для контроля кабельных линий Категорий 3, 5 и 5E (улучшенная Категория 5) на основе витой пары. Однако до сих пор можно встретить и тестеры для коаксиальных кабелей.

Задания к лабораторной работе №2

1. Изучить теоретический материал.
2. Получить оборудование для тестирования.
3. Используя кабель из прошлой лабораторной работы провести его тестирование.

Лабораторная работа №3
Установка и настройка сетевых адаптеров

Цель работы: изучить разновидности сетевых адаптеров, приобрести навыков их установки и конфигурирования. Результатом лабораторной работы является отчет, в котором должны быть отражены параметры настройки сетевых адаптеров, продемонстрирована работоспособность сети.

Теоретические положения

Сетевые адаптеры

Сетевые адаптеры (СА) или интерфейсные карты (NIC – Network Interface Card), служат для подключения компьютеров к локальной вычислительной сети (ЛВС).

Основные функции СА: организация приема/передачи данных из/в компьютер, согласование скорости приема/передачи информации, формирование пакета данных, накопление пакетов в памяти (буферизация), параллельно-последовательное преобразование (конвертирование), кодирование/декодирование данных, проверка правильности передачи, установление соединения с требуемым абонентом сети, организация собственно обмена данными.

Классификация сетевых адаптеров

Сетевые адаптеры, как сложное устройство, классифицируются по нескольким признакам, в зависимости от того, какой аспект их работы интересует исследователя.

По среде передачи данных:

- проводные (витая пара, коаксиальный кабель, оптоволокно);
- беспроводные (инфракрасная связь, Bluetooth, wireless LAN).

По выполняемым функциям СА:

- реализующие функции физического и канального уровней. Такие адаптеры, выполняемые в виде интерфейсных плат, отличаются технической простотой и невысокой стоимостью. Они применяются в сетях с простой топологией, где почти отсутствует необходимость выполнения таких функций, как маршрутизация пакетов, формирование из поступающих пакетов сообщений, согласование протоколов различных сетей и др.
- реализующие функции первых четырех уровней базовой

модели взаимодействия открытых систем OSI (Open System Interconnection) – физического, канального, сетевого и транспортного.

Эти адаптеры, кроме функций СА первой группы, могут выполнять функции маршрутизации, ретрансляции данных, формирования пакетов из передаваемого сообщения (при передаче), сборки пакетов в сообщение (при приеме), согласования протоколов передачи данных различных сетей, сокращая таким образом затраты вычислительных ресурсов центрального процессора ЭВМ на организацию сетевого обмена. Технически они могут быть выполнены на базе микропроцессоров.

По топологии ЛВС адаптеры разделяются на группы, поддерживающие различные топологии ЛВС:

- шинную;
- кольцевую;
- звездообразную;
- древовидную;
- комбинированную.

По принадлежности к типу компьютера:

- адаптеры для клиентских компьютеров;
- адаптеры для серверов.

В адаптерах для клиентских компьютеров значительная часть работы по приему и передаче сообщений перекладывается на программное обеспечение (драйвер), выполняемую в ЭВМ. Такой адаптер проще и дешевле, но он дополнительно загружает центральный процессор компьютера. Адаптеры для серверов снабжаются собственными процессорами, выполняющими всю нужную работу.

Основные характеристики СА:

- установленная микросхема контроллера (микрочип);
- разрядность – имеются 8-, 16-, 32- и 64-битные сетевые карты (определяется микрочипом);
- скорость передачи – от 10 до 1000 Мбит/с;
- тип подключаемого кабеля – коаксиальный кабель толстый и тонкий, неэкранированная витая пара, волоконнооптический кабель;
- поддерживаемые стандарты передачи данных – Ethernet, IEEE 802.3, Token Ring, FDDI и т. д.

Сервисные функции сетевых адаптеров

BootRom – специальная микросхема, которая позволяет производить загрузку ЭВМ по сети путём скачивания и запуска с выделенного сервера предварительно подготовленной копии операционной системы. То есть, при соответствующей настройке, компьютер может работать вообще без устройств внешней памяти. Загрузка через сеть настраивается в BIOS ЭВМ, которые поддерживают возможность удалённой загрузки.

Wake-on-Lan – позволяет включать удалённый компьютер путем подачи специально формируемой последовательности пакетов на MAC-адрес сетевого адаптера. При этом материнская плата ЭВМ также должна поддерживать данную функцию (обычно реализуется в виде отдельного порта расширения). Если сетевой адаптер встроен в материнскую плату, то все необходимые коммуникации интегрированы в материнскую плату и порт расширения отсутствует.

Контрольные вопросы

1. Для чего служат сетевые адаптеры?
2. Перечислите основные функции сетевого адаптера.
3. На каких уровнях модели OSI работают сетевые адаптеры?
4. По каким признакам могут различаться сетевые адаптеры?
5. Как определить физический (MAC) адрес адаптера?

Лабораторная работа №4
Построение схемы сети

Цель работы: получить базовые знания и умения, для работы с программой Cisco Packet Tracer и построения в ней схемы сети.

Теоретические положения

Назначение Cisco Packet Tracer

Конфигурирование информационных сетей, их настройка являются сложной задачей. Cisco Packet Tracer (CPT) позволяет имитировать работу различных сетевых устройств: маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров, IP-телефонов и т. д. Работа с интерактивным симулятором дает весьма правдоподобное ощущение настройки реальной сети, состоящей из десятков или даже сотен устройств.

Благодаря возможности визуализации в CPT может отследить перемещение данных по сети, появление и изменение параметров IP-пакетов при прохождении данных через сетевые устройства, скорость и пути перемещения IP-пакетов. Анализ событий, происходящих в сети, позволяет понять механизм ее работы и обнаружить неисправности. С помощью Cisco Packet Tracer можно симулировать построение не только логической, но и физической модели сети и, следовательно, получать навыки проектирования. Схему сети можно наложить на чертеж реально существующего здания или даже города и спроектировать всю его кабельную проводку, разместить устройства в тех или иных зданиях и помещениях с учетом физических ограничений, таких как длина и тип прокладываемого кабеля или радиус зоны покрытия беспроводной сети.

Основы работы в Cisco Packet Tracer

Внешний вид интерфейса программы представлен на рисунке 4.1.

Интерфейс состоит из следующих частей:

1. Область построения логической диаграммы сети
2. Область выбора оборудования
3. Кнопки управления объектами логической схемы

4. Инструмент для визуального моделирования потоков данных.

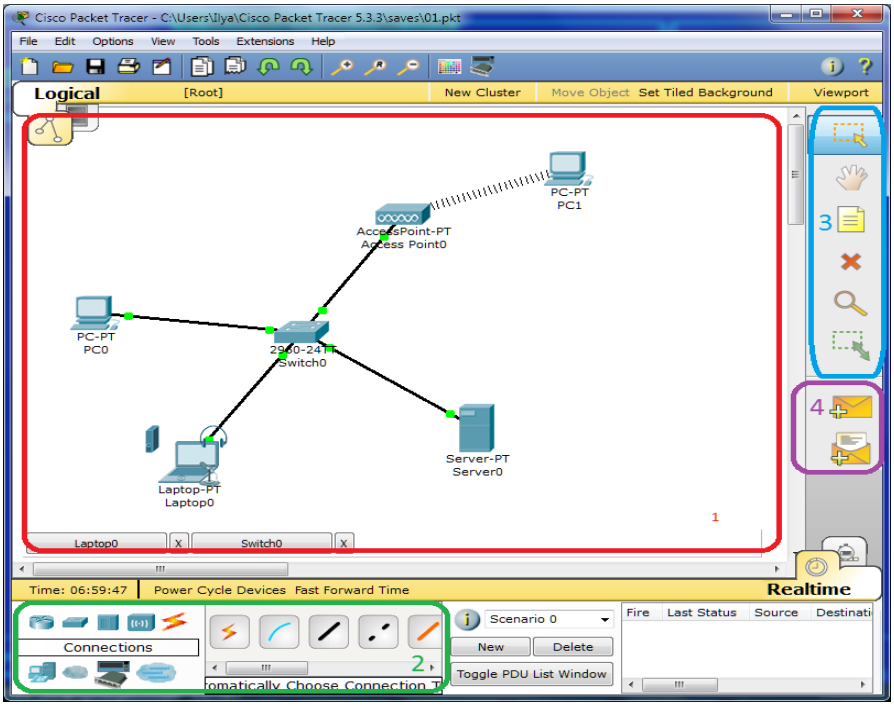

Рис. 4.1. – Интерфейс CPT

Оборудование подразделяется на классы:

1. Роутеры
2. Свитчи
3. Хабы
4. Устройства беспроводной связи
5. Соединители
6. Оконечные устройства

Роутеры, свитчи, хабы предлагают выбор готового оборудования фирмы CISCO.

Соединители подразделяются на:

1. Автоматический
2. Прямой патч-корд
3. Кроссовый патч-корд
4. Консольный кабель
5. Оптический кабель
6. Телефонный

Оконечные устройства делятся на:

1. Обычная рабочая станция (Generic PC)
2. Ноутбук (Generic laptop)

3. Сервер
4. Принтер

Режимы работы Cisco Packet Tracer

Работа с программой ведется в двух режимах. Режим реального времени позволяет размещать оборудование, конфигурировать и коммутировать его. В этом режиме не видно, какие пакеты перемещаются по сети. Режим симуляции позволяет наблюдать за движением сетевых пакетов, наблюдать за их параметрами.

Для того чтобы поместить какое-либо оборудование на логическую схему, достаточно выбрать его тип и щелкнуть мышкой в области логической схемы. При щелчке на пиктограмму оборудования появляется окно, позволяющее редактировать свойства данного объекта. Окно (рисунок 4.2) состоит из нескольких вкладок:

- Physical – конфигурирование оборудования;
- Config – конфигурирование программной части;
- другие вкладки, зависящие от типа оборудования.

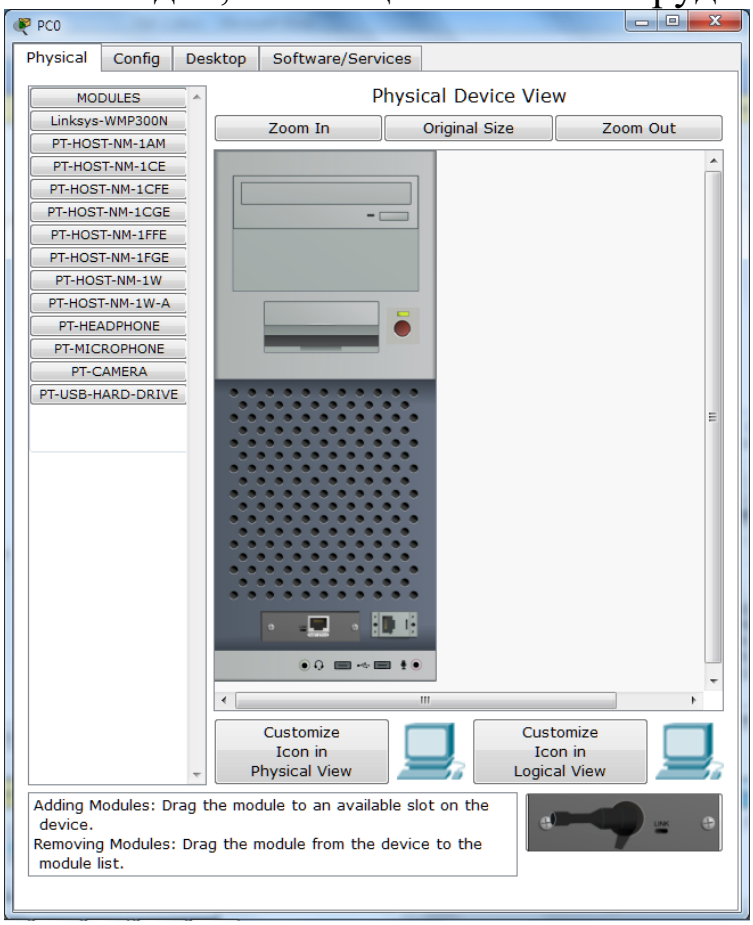

Рис. 4.2. – Конфигурирование рабочей станции

В закладке конфигурирования оборудования можно его включать, выключать, добавлять разные модули (для рабочей станции – сетевые карты, для сетевого оборудования – сетевые модули, в том числе модули оптической связи), подключать дополнительные устройства (наушники, микрофон, и т. д.).

Для рабочей станции, ноутбука и сервера возможна работа с виртуальным рабочим столом данных компьютеров – закладка «Desktop».

Контрольные вопросы

1. Зачем используются среды имитационного моделирования компьютерных сетей?
2. Чем отличается режим рабочей области «Логический» от «Физический»?
3. Какие элементы имеются в основном окне среды Cisco Packet Tracer?
4. Какие виды устройств позволяет использовать Cisco Packet Tracer?
5. Каким образом можно производить конфигурирования устройств в Cisco Packet Tracer?
6. Какие режимы работы предусмотрены в Cisco Packet Tracer? В чем их отличие?

Лабораторная работа №5
Расчёт IP-адресов

Цель работы:

Научиться определять адрес сети, широковещательный адрес, диапазон допустимых адресов и количество компьютеров в сети по заданному IP-адресу и маске.

Теоретические положения

Типы адресов стека TCP/IP

В стеке TCP/IP используются три типа адресов: локальные, IP-адреса и символьные доменные имена.

Под *локальным адресом* понимается такой тип адреса, который используется средствами базовой технологии для доставки данных в пределах подсети, являющейся элементом составной интерсети. В разных подсетях допустимы разные сетевые технологии, разные стеки протоколов, поэтому при создании стека TCP/IP предполагалось наличие разных типов локальных адресов. Если подсетью интерсети является локальная сеть, то локальный адрес - это MAC-адрес. MAC-адрес назначается сетевым адаптерам и сетевым интерфейсам маршрутизаторов, MAC-адреса назначаются производителями оборудования и являются уникальными. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байт, например 11-AO-17-3D-BC-01.

IP-адреса представляют собой основной тип адресов, на основании которых сетевой уровень передает пакеты между сетями. Эти адреса состоят из 4 байт, например 109.26.17.100. IP-адрес назначается администратором во время конфигурирования компьютеров и маршрутизаторов.

IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (Internet Network Information Center, InterNIC), если сеть должна работать как составная часть Internet. Обычно поставщики услуг Internet получают диапазоны адресов у подразделений InterNIC, а затем распределяют их между своими абонентами. Номер узла в протоколе IP назначается независимо от локального

адреса узла. Маршрутизатор по определению входит сразу в несколько сетей. Поэтому каждый порт маршрутизатора имеет собственный IP-адрес. Конечный узел также может входить в несколько IP-сетей. В этом случае компьютер должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

Символьные доменные имена. Символьные имена в IP-сетях называются доменными и строятся по иерархическому признаку. Составляющие полного символьного имени в IP-сетях разделяются точкой и перечисляются в следующем порядке: сначала простое имя конечного узла, затем имя группы узлов (например, имя организации), затем имя более крупной группы (поддомена) и так до имени домена самого высокого уровня (например, домена объединяющего организации по географическому принципу: RU - Россия, UK - Великобритания, US - США). Между доменным именем и IP-адресом узла нет никакого алгоритмического соответствия, поэтому необходимо использовать какие-то дополнительные таблицы или службы, чтобы узел сети однозначно определялся как по доменному имени, так и по IP-адресу. В сетях TCP/IP используется специальная распределенная служба Domain Name System (DNS), которая устанавливает это соответствие на основании создаваемых администраторам сети таблиц соответствия. Поэтому доменные имена называют также DNS-именам

Классы IP-адресов

IP-адрес состоит из двух логических частей - номера сети и номера узла в сети. Какая часть адреса относится к номеру сети, а какая - к номеру узла, определяется значениями первых бит адреса. Значения этих бит являются также признакам того, к какому классу относится тот или иной IP-адрес.

Для идентификации сетей и сетевого оборудования протокол IPv4 использует 32-разрядную схему адресации.

Существуют 5 классов IP-адресов, отличающиеся количеством бит в сетевом номере и хост-номере. Класс адреса определяется значением его первого октета.

В таблице 5.1 приведено соответствие классов адресов значениям первого октета и указано количество возможных IP-адресов каждого класса.

Таблица 5.1. – Характеристики классов адресов

Класс	**Диапазон значений первого октета**	**Возможное кол-во сетей**	**Возможное кол-во узлов**
A	1 - 126	126	16777214
B	128-191	16382	65534
C	192-223	2097150	254
D	224-239	-	2**28
E	240-247	-	2**27

Адреса класса A предназначены для использования в больших сетях общего пользования. Они допускают большое количество номеров узлов. Адреса класса B используются в сетях среднего размера, например, сетях университетов и крупных компаний. Адреса класса C используются в сетях с небольшим числом компьютеров. Адреса класса D используются при обращениях к группам машин, а адреса класса E зарезервированы на будущее.

Некоторые IP-адреса являются выделенными и трактуются по-особому:

• Если весь IP-адрес состоит только из двоичных нулей, то он обозначает адрес того узла, который сгенерировал этот пакет

• Если в поле номера сети стоят только нули, то по умолчанию считается, что узел назначения принадлежит той же самой сети, что и узел, который отправил пакет.

• Если все двоичные разряды IP-адреса равны 1, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такая рассылка называется *ограниченным широковещательным сообщением (limited broadcast).*

• Если в поле номера узла назначения стоят только единицы, то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером сети. Например пакет с адресом 192.190.21.255 доставляется всем узлам сети 192.190.21.0. Такая рассылка называется *широковещательным сообщением (broadcast).*

При адресации необходимо учитывать те ограничения, которые вносятся особым назначением некоторых IP-адресов. Так, ни номер сети, ни номер узла может состоять только из одних двоичных единиц или только из одних двоичных нулей.

Особый смысл имеет IP-адрес, первый октет которого равен 127. Он используется для тестирования программ и взаимодействия процессов в пределах одной машины. Когда программа посылает данные по IP-адресу 127.0.0.1, то образуется как бы «петля». Данные не передаются по сети, а возвращаются модулям верхнего уровня как только что принятые. Поэтому в IP-сети запрещается присваивать машинам IP-адреса, начинающиеся со 127. Этот адрес имеет название *loopback.*

Форма группового IP-адреса - *multicast* - означает, что данный пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса. Узлы сами идентифицируют себя, есть определяют, к какой из групп они относятся. Один и тот же узел может входить в несколько групп. Члены какой-либо группы multicast не обязательно должны принадлежать одной сети. В общем случае они могут распределяться по совершенно различным сетям, находящимся друг от друга на произвольном количестве хопов. Групповой адрес не делится на поля номера сети и узла и обрабатывается маршрутизатором особым образом. Основное назначение multicast-адресов – распространение информации по схеме «один-ко-многим». Хост, который хочет передавать одну и ту же информацию многим абонентам, с помощью специального протокола IGMP (Internet Group Manageme Protocol) сообщает о создании в сети новой мультивещательной группы с определенным адресом. Машрутизаторы, поддерживающие мультивещательность, распространяют информацию о создании новой группы в сетях, подключенных к портам этого маршрутизатора. Хосты, которые хотят присоединиться к вновь создаваемой мультивещательной группе, сообщают об этом своим локальным маршрутизаторам и те передают эту информацию хосту, инициатору создания новой группы. Групповая адресация предназначена для экономичного распространения в Internet или большой корпоративной сети аудио- или видеопрограмм,

предназначенных сразу большой аудитории слушателей или зрителей.

Новый протокол Ipv6 использует 128-разрядные адреса для идентификации устройств и применяет другую схему адресации. Ipv6 поддерживает множество других функциональных возможностей:

- передачу критичного трафика в реальном времени;
- мобильность хостов;
- сквозное шифрование и аутентификацию на сетевом уровне;
- фвтонастройку.

В новой схеме адресации Ipv6 появилась концепция общего адреса, которая позволяет присваивать один и тот же адрес разным устройствам. Посланный по общему адресу пакет доставляется единственному устройству, которое является ближайшим по определению маршрутизатора устройством среди всех имеющих данный адрес. Например, Web-узел может быть зеркалирован на несколько серверов, а соединение будет устанавливаться с ближайшим к пользователю сервером. Новая схема адресации позволяет формировать группы адресов и осуществлять многоадресную рассылку. Причем групповой адрес может быть ограничен отдельным доменом, связан с определенным сетевым соединением или даже распределен по глобальной сети. Важно, что появление групповых адресов позволяет отказаться от широковещательной передачи.

Как назначать номера сетей и подсетей

Одно из важнейших решений, которое необходимо принять при установке сети, заключается в выборе способа присвоения IP-адресов вашим машинам. Этот выбор должен учитывать перспективу роста сети. Иначе в дальнейшем вам придется менять адреса. Когда к сети подключено несколько сотен машин, изменение адресов становится почти невозможным.

Организации, имеющие небольшие сети с числом узлов до 126, должны запрашивать сетевые номера класса С. Организации с большим числом машин могут получить несколько номеров класса С или номер класса В. Удобным средством структуризации сетей в рамках одной организации являются подсети, когда все адресное пространство сети internet может быть разделено на непересекающиеся подпространства – "подсети", с каждой

из которых можно работать как с обычной сетью TCP/IP. Таким образом единая IP-сеть организации может строиться как объединение подсетей. При этом ваша организация должна получить один сетевой номер, например, номер класса B. Для IP-адресов класса B первые два октета являются номером сети. Оставшаяся часть IP-адреса может использоваться как угодно. Например, вы можете решить, что третий октет будет определять номер подсети, а четвертый октет - номер узла в ней. После того, как решено использовать подсети или множество IP-сетей, вы должны решить, как назначать им номера. Обычно это довольно просто. Каждой физической сети, например, Ethernet или Token Ring, назначается отдельный номер подсети или номер сети.

Вы также должны выбрать "маску подсети". Маска подсети (subnet mask) – число, которое служит для выделения частей IP-адреса, чтобы TCP/IP мог отличать номер сети от номера хоста. Используя маску подсети, TCP/lP-хосты могут связаться и определить, где находится хост назначения: в локальной или удаленной сети. Вот пример корректной маски подсети: 255.255.255.0.

Биты IP-адреса, определяющие номер IP-сети, в маске подсети должны быть равны 1, а биты, определяющие номер узла, в маске подсети должны быть равны 0. Чтобы разобраться, как работает маска подсети, нужно иметь представление о логических операциях. Так, оператор AND (логическое И) в логических вычислениях дает результат TRUE (истинно) в том случае, если значение обоих аргументов TRUE.

Обычно TRUE выражается значением – 1, а FALSE (ложно) - значением 0. Чтобы определить, какая часть IP-адреса указывает на сеть, а какая идентифицирует компьютер, выполняется простая логическая операция с полученным адресом и маской подсети. Пример такого вычисления показан в таблице 5.2.

Таблица 5.2. – Характеристики классов адресов

Значение IP-адреса	**Значение маски**	**Результат**
1	1	1
1	0	0
0	1	0
0	0	0

Таким образом, когда маска подсети 255.0.0.0 применяется по отношению к адресу класса С, только часть IP-адреса, содержащаяся в первом байте, определяется как адрес сети. Отсюда несложно рассчитать маски подсети для адресов класса В – 255.255.0.0 и класса С – 255.255.255.0.

Маски подсетей могут использоваться для маскирования тех частей адреса, которые согласно структуре класса определяются как адреса сети. На практике разделение на подсети применяется в случае, когда конкретное сетевое адресное пространство разбивается дальше на отдельные подсети.

Например, маска подсети 255.255.255.128 может использоваться для разделения адресного пространства класса С на две подсети. Если эту маску применить к сети с IP-адресом 192.113.255, в результате получается одна подсеть с диапазоном адресов от 192.113.255.1 до 192.113.255.128 и вторая подсеть - от 192 .113. 255 .129 д 192.113.255.254. Обратите внимание, что адреса, которые содержали бы в последнем байте все нули или все единицы, были исключены. Они являются адресами специального использования и, как правило, не присваиваются компьютерам (например, 192.113.255.0).

Маска подсети 255.255.255.192 разделила бы адресное пространство класса С на четыре подсети с доступными 62 адресами узлов в каждой. В двоичном формате значение 190 имеет вид 11000000. Таким образом, остается только шесть битов, которые могут быть использованы для определения адреса узла. Наибольшая величина, которая может быть записана шестью битами, - 63, а поскольку нельзя использовать адреса узлов со всеми нулями или единицами, остается только 62 доступные комбинации.

Расчеты подсетей. Если вы решили разделить ваше адресное пространство на подсети, определитесь с количеством компьютеров, которые вам необходимо иметь в каждой подсети, и выразите это количество двоичной величиной. Это покажет вам, сколько битов займет адрес компьютера. Вычтите это значение из общего количества битов (из восьми, если разбивается адресное пространство класса С). Затем вычислите десятичный эквивалент двоичной величины, которая в первых битовых позициях имеет столько единиц, сколько показала вышеописанная операция вычитания.

Например, каждая из подсетей должна содержать 30 компьютеров с отдельными адресами. В двоичном формате 30 (11110) занимает пять битов. Остается три битовых позиции (8 – 5 = 3), которые необходимо выделить с помощью маски из общего адресного пространства. Тогда двоичная запись требуемой маски будет 11100000, что эквивалентно 224 в десятичном формате.

Поскольку для маски подсети выделено только три бита, наибольшее значение, которое можно записать в этом случае, равно семи (111 в двоичном формате соответствует 7 в десятичном). С учетом нулевого значения можно создать восемь адресов подсетей.

Это означает, что в случае использования маски 255.255.255.224 для разделения адресного пространства класса С на подсети можно создать восемь подсетей с 30 узлами в каждой.

Произведем подсчеты: адрес первой подсети 000. Так как IP-адрес записывается в десятичном формате с разделительными точками, вычислим, сколько адресов можно определить 8-битовой двоичной величиной. которая всегда начинается с 000, а затем преобразуем этот диапазон в десятичную величину. Например, диапазон от 00000001 до 00011110 будет соответствовать значениям от 1 до 30. Адреса 00000000 и 0001111 не действительны, так как адрес узла в них представлен всеми единицами или нулями, что недопустимо. Если эту маску применить к адресу сети класса С 192.113.255.0, узлы первой подсети будут представлены адресами от 192.113.255.1 до 192.113.255.30.

Адрес второй подсети 001. Диапазон адресов, которые могут быть созданы в этой подсети – от 00100001 до 00111110, что соответствует значениям 33-62 в десятичном формате. Применительно к адресу сети 192.113.255.0 узлы второй подсети будут адресоваться от 192.113.255.65 до 192.113.255.94.

Адрес третьей подсети 010. Диапазон адресов узлов – от 01000001 до 01011110 или 65-94 в десятичном формате. Это соответствует диапазону адресов от 192.113.255.65 до 192.113.255.94.

Если вы продолжите вычисления для оставшихся подсетей (от 011 до 111), то обнаружите, что получилось восемь подсетей с 30 доступными адресами узлов в каждой.

Задание к лабораторной работе №5

Определите для своего варианта (таблица 5.3):

1. Адрес сети и класс сети
2. Широковещательный адрес
3. Первый доступный адрес для компьютера
4. Последний доступный адрес для компьютера
5. Сколько всего компьютеров можно подключить к этой сети

Таблица 5.3. – Варианты заданий

Номер варианта	**Характеристики**
Вариант 1	IP-адрес: 192.168.10.25, маска: 255.255.255.0
Вариант 2	IP-адрес: 10.0.0.50, маска: 255.0.0.0
Вариант 3	IP-адрес: 172.16.5.100, маска: 255.255.0.0
Вариант 4	IP-адрес: 192.168.1.150, маска: 255.255.255.0
Вариант 5	IP-адрес: 10.10.10.10, маска: 255.0.0.0
Вариант 6	IP-адрес: 172.20.15.30, маска: 255.255.0.0
Вариант 7	IP-адрес: 192.168.50.200, маска: 255.255.255.0
Вариант 8	IP-адрес: 10.100.50.5, маска: 255.0.0.0
Вариант 9	IP-адрес: 172.30.1.75, маска: 255.255.0.0
Вариант 10	IP-адрес: 192.168.77.130, маска: 255.255.255.0

Лабораторная работа №6
Создание и настройка серверов: WEB, DNS, DHCP, MAIL

Цель работы: изучить принципы настройки 4 типов серверов и включение их в состав локальной не маршрутизируемой сети.

Работа выполняется в среде Cisco Packet Tracer. В качестве аппаратного обеспечения серверов используется один и тот же элемент из набора программы, но каждый из них настроен определенным образом.

Задание к лабораторной работе №6

1. Создайте новый проект сети, в котором изначально будет следующее оборудование:

- в качестве клиентских машин Generic PC-PT или Generic Laptop-PT – всего 2 штуки;
- в качестве первого сервера будем настраивать WEB-сервер, для этой цели используем Generic – Server-PT;
- в качестве коммутатора используем Generic Switch-PT, причем в него нужно добавить 2 дополнительных сетевых интерфейса PTSwitch-NM-1CFE и не забыть включить его и каждый из портов (если не включены по умолчанию).

Для соединения использовать сплошной черный (не пунктирный) кабель. Убедиться, что все точки на кабелях стали зелеными.

2. Присвоить клиентским ПК IP-адреса, например, 192.168.1.2 и 192.168.1.3 соответственно.

Здесь и далее вы можете везде присваивать свои адреса, а также имена сетевых устройств и серверов.

3. Настроим WEB-сервер, который уже должен быть соединен кабелем с коммутатором. Открываем свойства сервера и переходим сначала на вкладку Config и настраиваем статический IP-адрес 192.168.1.1.

Все эти настройки также можно выполнить и через вкладку Desktop / IP Configuration.

Затем переходим на вкладку Services. Нас интересует сейчас раздел HTTP. Справой стороны выключаем безопасный HTTP-сервер, чтобы не вводить пароль при входе на сайт. Обычный HTTP-сервер должен быть включен.

Далее щелкаем по надписи (edit) в строке № 5, при этом откроется редактор файла index.html. Делаем изменения содержимого файла, как показано на рисунке 6.1.

Текст может быть произвольным, но должен содержать вашу Фамилию и инициалы. Сохранить изменения и закрыть свойства WEB-сервера.

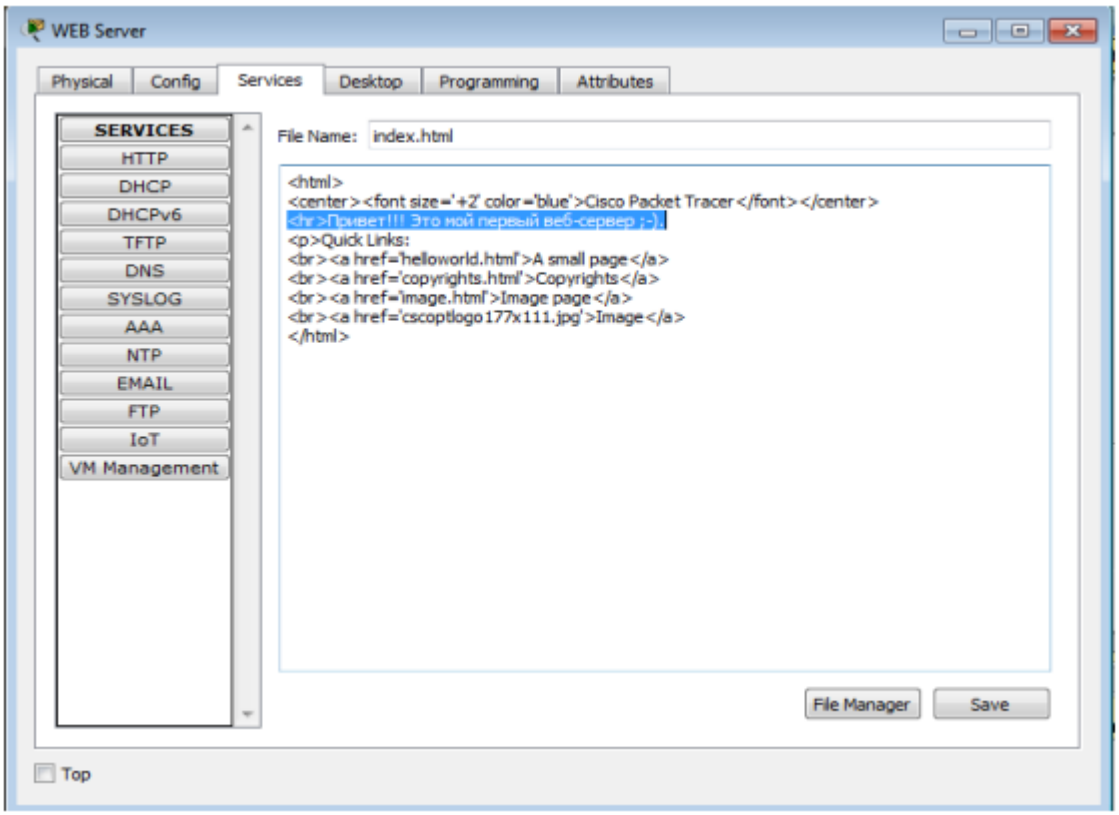

Рис. 6.1. – Настройка свойств WEB-сервера

4. Проверим работу WEB-сервера.

Для этого с одного из клиентских ПК через вкладку Desktop открываем приложение Web Browser и вводим в строке адреса IP-адрес вашего созданного web-сервера и нажимаем Go. Если все настроено верно, то вы должны увидеть вашу измененную веб-страницу с вашим произвольным текстом и фамилией.

Данный скриншот обязательно поместить в отчет. Если веб-страница недоступна, то проверить доступность веб-сервера командой Ping.

5. Настроим DNS-сервер, который позволит нам обращаться к нашему веб-сайту не только по IP-адресу, но по доменному имени, как это мы обычно делаем в повседневной жизни.

Сначала необходимо добавить на нашу схему второй аналогичный сервер и присвоить ему нужный IP-адрес

и присоединить его к коммутатору.

Затем на вкладке Services в разделе DNS убедимся, что этот сервис включен и добавим в таблицу строку доменного имени для нашего WEB-сервера (строку доменного имени для нашего EMAIL-сервера можно будет добавить позже, либо сделать это сразу).

В данном примере на рисунке 6.2. веб-сервер назвали, например, MyServer.ru (произвольно) и указали для него существующий IP-адрес. Не забудьте сохранить добавленную запись. Если в данном окне изначально уже будет какая-то запись, то ее можно изменить в соответствии с вашими предпочтениями. Другие ненужные сервисы – Web (HTTP), DHCP рекомендуется отключить.

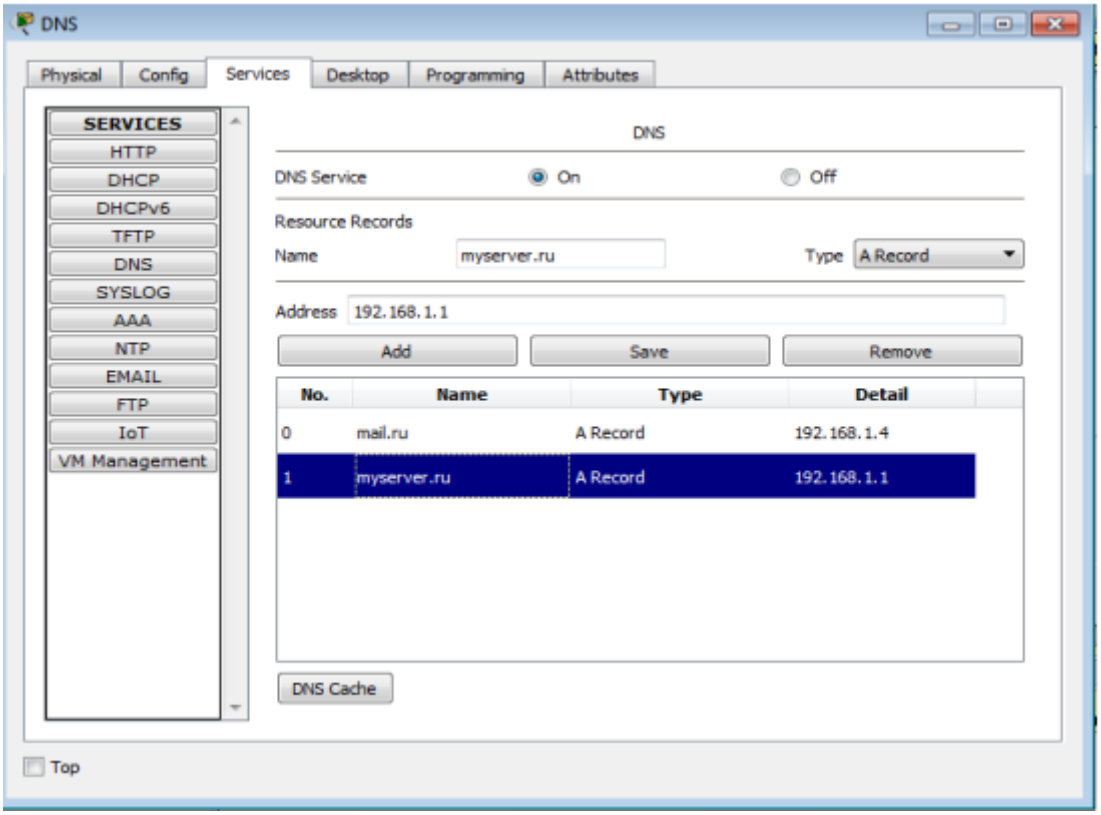

Рис. 6.2. – Вкладка Services

6. Проверим работу DNS-сервера.

Прежде всего необходимо дописать в сетевые настройки клиентских ПК IP-адрес созданного DNS-сервера.

Затем на любом клиентском ПК открываем веб-браузер и в строке адреса вводим уже не IP, а URL-адрес с именем сервера (в данном примере – myserver.ru). Должна открыться ваша

веб-страница. При наличии проблем проверить доступность DNS-сервера и в том, что его IP-адрес прописан в настройках веб-сервера.

7. Создадим DHCP-сервер, который будет раздавать клиентским ПК автоматически IP-адреса (для серверов обычно используют статические IP-адреса). Для этого помещаем на схему третий сервер, соединяем его коммутатором и уже привычным образом назначаем ему IP-адрес, например, 192.168.1.4.

Затем на вкладке Services в разделе DHCP убедимся, что этот сервис включен. Настройка DHCP-сервера сводится к созданию именованного пула (диапазона IP-адресов) для сетевых клиентов. При этом указывается начальный IP-адрес и количество адресов. Не забудьте сохранить созданную запись. Пример настройки показан на рисунке 6.3.

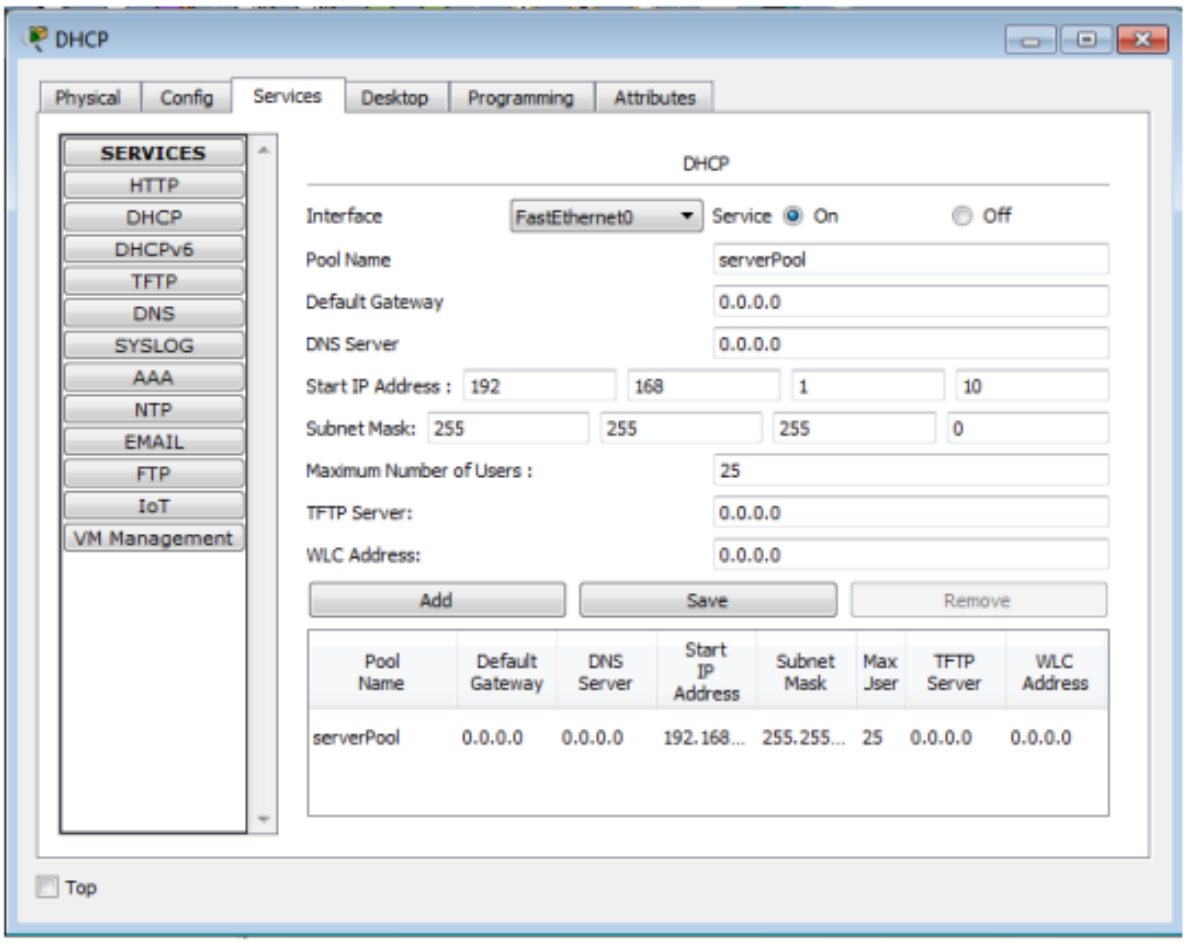

Рис. 6.3. – Настройка DHCP-сервера

8. Проверим работу DHCP-сервера.

Для этого в сетевых настройках обоих клиентских ПК вместо

режима Static включаем режим DHCP. Далее нужно подождать секунд 10-15 пока сервер присвоит клиентам IP-адреса. Если все сделано правильно, то на вкладке Desktop в окне IP-Configuration мы увидим назначенные сервером IP-адреса бледным цветом. Если друг сразу вы не увидели изменения, то нужно закрыть это окно и через несколько секунд открыть его снова.

Другим способом получить подробную информацию о сетевом соединении можно через командную строку, используя команду Ipconfig /all.

9. Создадим почтовый (EMAIL) – сервер и заведем на нем 2 аккаунта для наших клиентов с логинами, например, user1 и user2. Имя нашего почтового сервера пусть будет, например, Mail.ru.

Прежде всего, как обычно, добавляем аппаратный сервер и выставляем на нем сетевые параметры: IP-адрес, маска, DNS-сервер, шлюз не нужен, т. к. у нас сеть не маршрутизируемая (либо при полной настройке DHCP-сервера, с указанием нашего DNS-сервера, автоматически выдаём EMAIL-серверу IP-адрес)

Также необходимо в самом DNS-сервере добавить строку доменного имени для почтового сервера так же, как это было сделано ранее для WEB-сервера (см. п.5 и соответствующий рисунок).

10. Настроим почтовый сервис и создадим 2 почтовых ящика (аккаунта).

На вкладке Services переходим в раздел EMAIL и включаем службы SMTP и POP3. Затем придумываем доменное имя почтового сервера и создаем 2 пользовательских аккаунта с произвольными именами и паролями. В результате должно получится примерно так, как показано на рисунке.

По окончании настроек закрыть окно свойств сервера.

11. Настроим клиентскую часть почтового сервиса на каждом из ПК.

Для этого открываем в свойствах ПК вкладку Desktop, находим и открываем программный инструмент Email.

В открывшемся окне MAIL BROWSER нажимаем кнопку Configure Mail и заполняем окно свойств для данного аккаунта, используя логины и пароли как на сервере и не забыв сохранить настройки.

Данную процедуру затем повторить и на втором ПК. Пример настройки показан на рисунке 6.5.

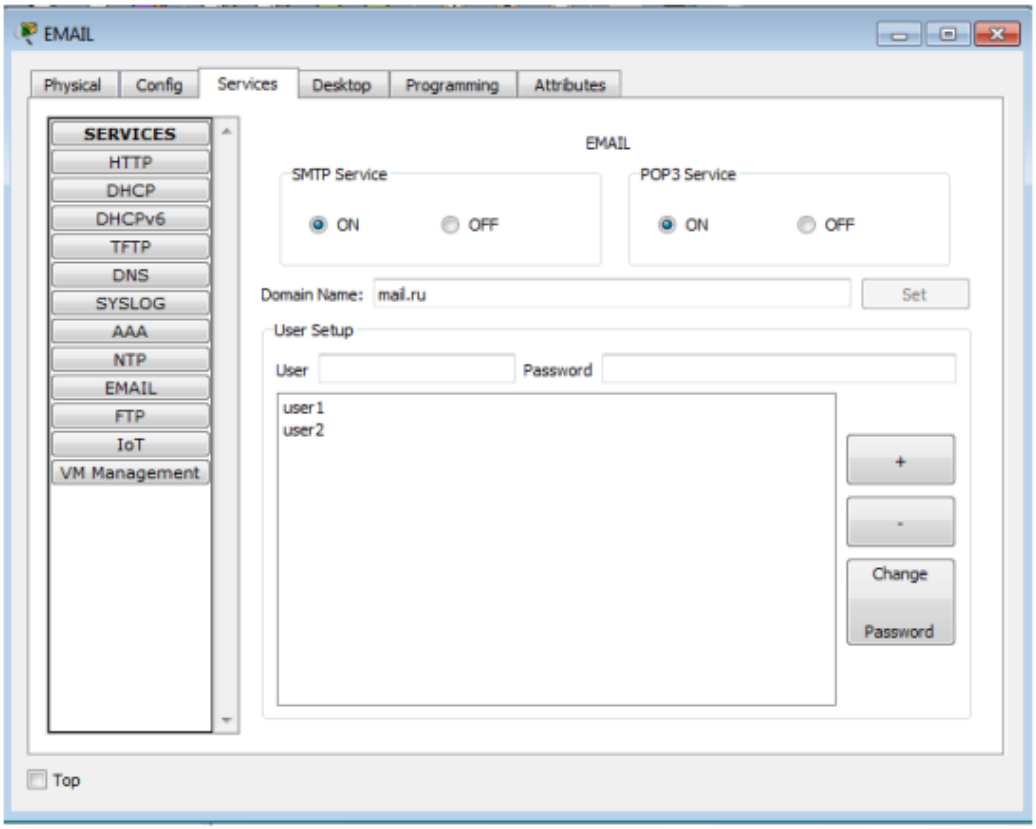

Рис. 6.4. – Создание почтового сервера

12. Проверим работу почтового сервера.

Проверка работы почтовой службы сводится к написанию и отправке почтового сообщения от одного клиентского ПК к другому.

Открываем окно MAIL BROWSER.

Назначение кнопок очень простое:

Compose – написать письмо

Reply – ответить на входящее письмо

Receive – принять почту (автоматического приема писем здесь нет)

После написания текста письма выполнить его отправку с помощью кнопки Send.

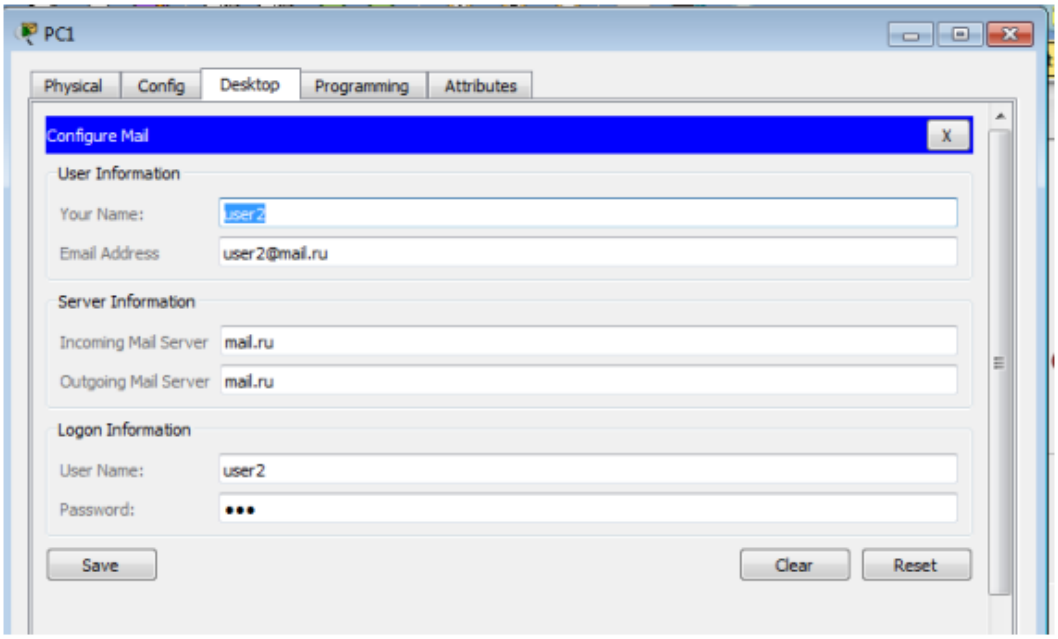

Рис. 6.5. – Пример настройки Configure Mail

Затем перейти на второй ПК, открыть на нем MAIL BROWSER и принять почту. Фактом получения почты служит таблица входящих писем, как на рисунке 6.6.

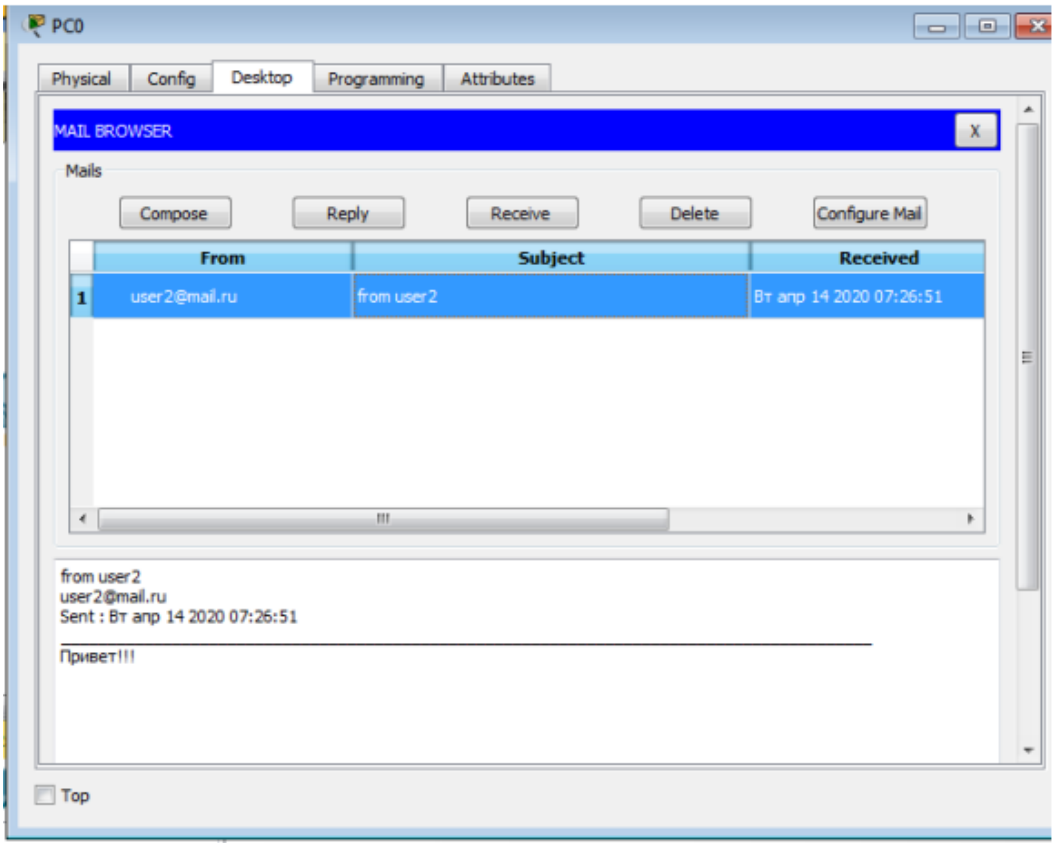

Рис. 6.6. – Таблица входящих писем

Если письма доходят в обе стороны от одного клиента к

другому, значит почтовый сервис работает нормально. Если при отправке программа не может найти ваш почтовый сервер, то возможно проблема с настройками DNS либо на почтовом, либо на DNS-сервере.

Лабораторная работа №7
Маршрутизация в сетях TCP/IP

Цель работы: изучить процесс передачи пакетов между различными IP сетями. Результатом лабораторной работы является отчет, в котором должны быть приведены примеры успешного прохождения пакетов через несколько смежных IP-сетей в сетевом эмуляторе Cisco Packet Tracer.

Теоретические положения

Маршрутизация – задача передачи пакетов информации из одной сети в другую. Как правило, компьютеры, относящиеся к одной сети, подключены к одному коммутатору или к совокупности нескольких коммутаторов. На рисунке 7.1 виден пример топологии локальной сети с двумя подсетями 172.20.2.0 и 172.20.3.0. Между компьютерами одной подсети пакеты передаются при помощи коммутаторов. Между отдельными подсетями пакеты не передаются вообще. Для передачи пакетов между отдельными подсетями необходимо использовать оборудование третьего уровня – роутер. Пример сети с роутером приведен на рисунке 7.2.

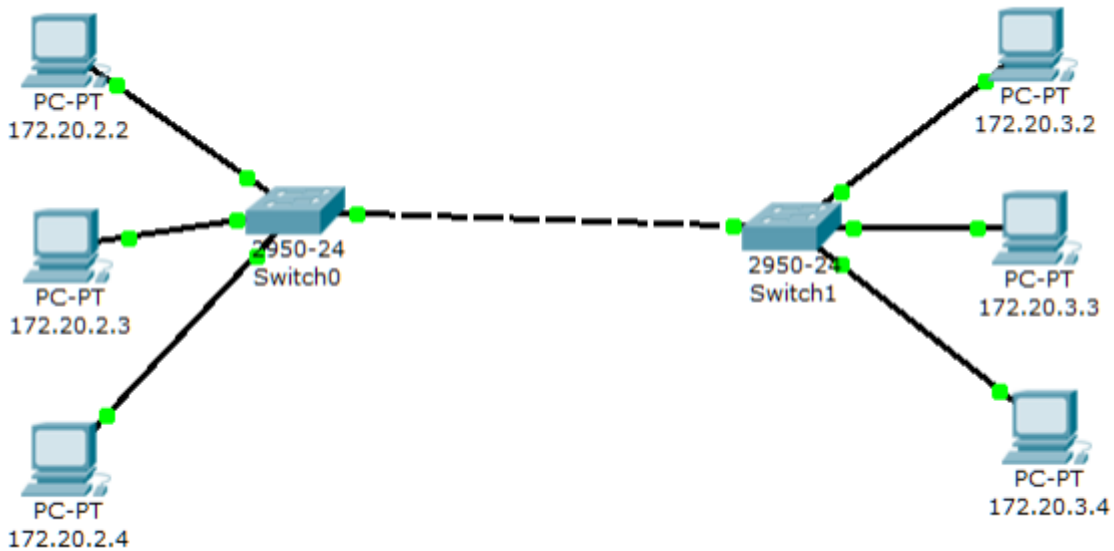

Рис. 7.1. – Пример сети с одним маршрутизатором

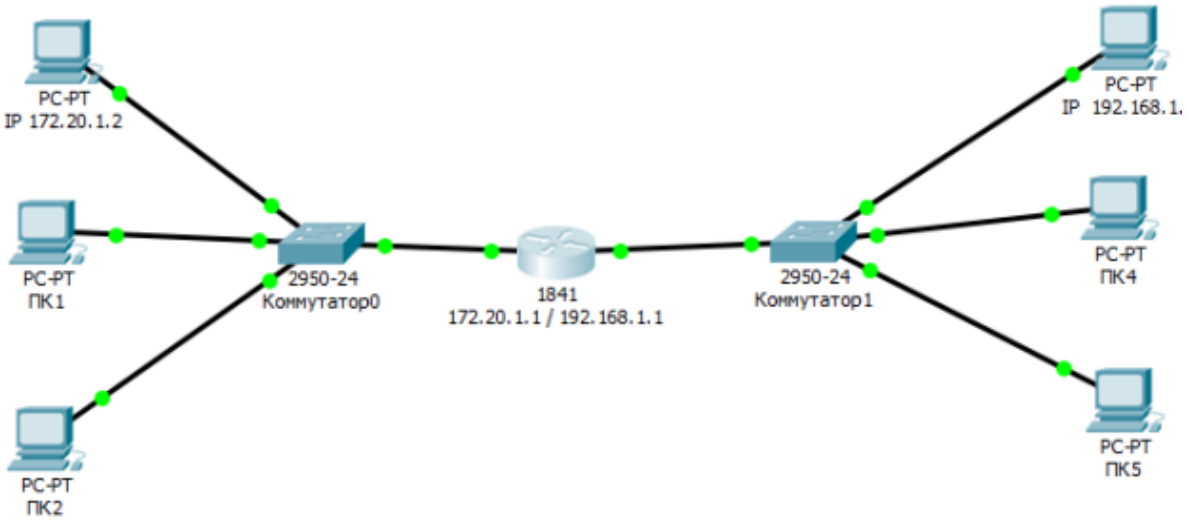

Рис. 7.2. – Пример сети с роутером

Просто поместить роутер между двумя коммутаторами недостаточно для того, чтобы сеть заработала в полном объеме. Необходимо настроить роутер на передачу данных между отдельными подсетями. Существует два способа настройки роутеров.

1. Статический
2. Динамический

В обоих случаях в роутере настраивается таблица маршрутизации. Каждая запись в этой таблице показывает, через какой роутер необходимо направлять пакеты в заданные подсети.

Этапы настройки маршрутизации

1. Для каждого порта роутера необходимо задать IP адрес. Этот адрес должен принадлежать той же подсети, к которой он подключается этим портом. В рассматриваемом примере «левый» порт должен иметь адрес из подсети 172.20.2.0, «правый» - из подсети 192.168.1.0. Как правило, IP адрес порта роутера, предназначенного для подключения к существующей подсети, выбирают равным 1 или 254. (172.20.2.1 или 172.20.2.254). Эта рекомендация нужна для того, чтобы в дальнейшей при развитии каждой подсети у администратора не возникало проблем при выборе новых IP адресов компьютеров – он будет знать, что роутер в этой сети имеет адрес 1, и все адреса, что больше единицы, свободны для назначения их новым компьютерам. Если роутеры соединяются между собой непосредственно или через коммутаторы, то порты роутеров, предназначенных для соединения

с другими роутерами должны иметь адреса из одной подсети.

2. После настройки роутера в сети необходимо настроить компьютеры. В настройках компьютеров необходимо указать адрес шлюза (Gateway), это делается в разделе Global / Setting. Адрес должен совпадать с адресом порта роутера, обращенного к подсети, включающей настраиваемый компьютер.

3. Проверьте передачу ICMP-пакетов с помощью команды Ping из своей сети в другую сеть, находящуюся за роутером. В отчете приведите подтверждающие скрины.

Пример сети с четырьмя маршрутизаторами.

Для данной сети необходимо настроить таблицы маршрутизации в каждом роутере, в которых будет указано, в какой роутер нужно направить пакет, чтобы он добрался до заданной сети. Нужный роутер находится в списке перед «1841».

После настройки роутеров в сети необходимо настроить компьютеры. В настройках компьютеров необходимо указать адрес шлюза (Gateway). Адрес должен совпадать с адресом порта роутера, обращенного к подсети, включающей настраиваемый компьютер. Пример настройки портов роутеров приведен на рисунке 7.3.

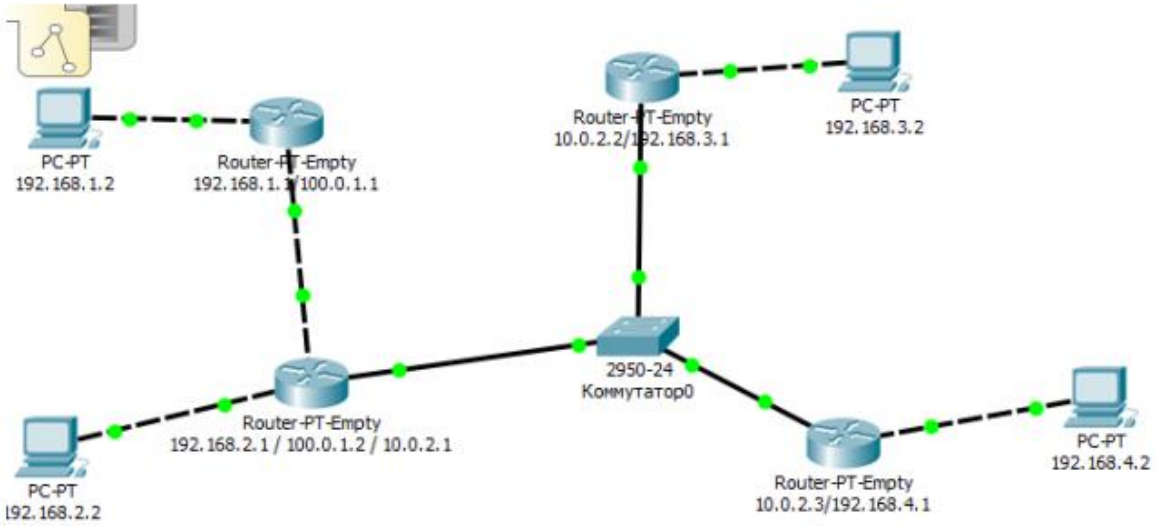

Рис. 7.3. – Сложная сеть

Обратите внимание на адреса портов роутеров, предназначенных для соединения с другими роутерами. Связь между роутерами Router3 и Router6 осуществляется через подсеть 10.0.1.0, а между Router3, Router5, Router4 – через подсеть 10.0.2.0 (рисунок 7.4).

Network Address
192.168.4.0/24 via 10.0.2.3
192.168.1.0/24 via 10.0.1.1
192.168.3.0/24 via 10.0.2.2

Рис. 7.4. – Таблица маршрутизации Router 3

Для каждой сети необходим маршрут через отдельный роутер.

Примечание:

1. Для добавления нужных Ethernet-портов в пустой роутер нужно открыть его свойства, затем отключить питание роутера, кликнув по кнопке питания (на рисунке 7.5 показано цифрой 1).

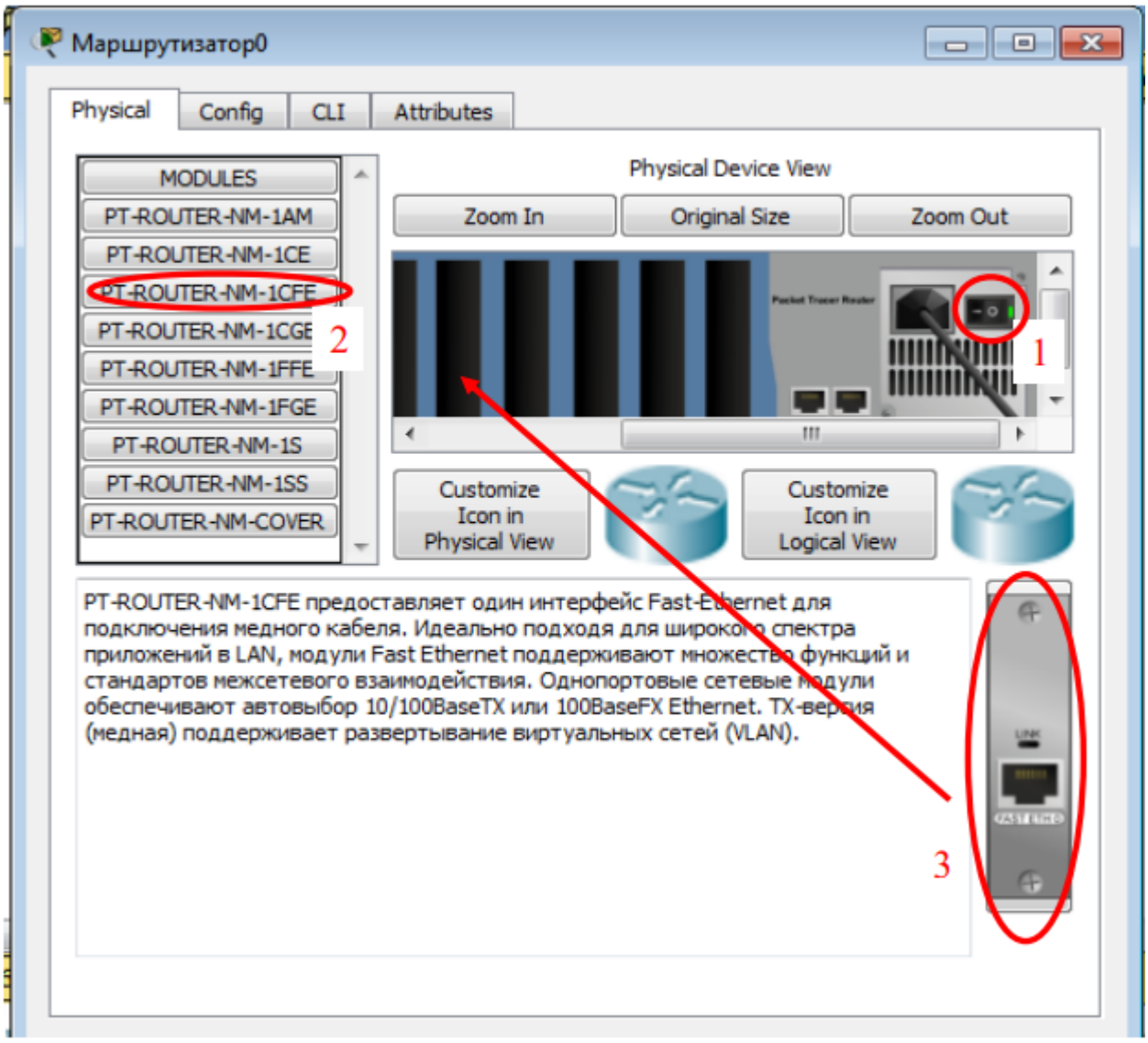

Рис. 7.5. – Свойства маршрутизатора

2. В списке модулей выбрать модуль, показанный на рисунке 7.5 цифрой 2.

3. Перетащить выбранные модули поочередно в свободные гнезда роутера, как показано на рисунке 7.5. цифрой 3.

4. Таблица маршрутизации для роутеров настраивается на вкладке Config / Маршрутизация / Статическая…. Количество записей в каждом роутере должно быть = 3 по количеству соседних подсетей.

Принцип прописывания статических маршрутов следующий:

- указываем IP подсети в которой находится удаленный (пингуемый вами) ПК
- маску подсети вводим вручную
- в поле «Следующий переход» указываем IP следующего (второго) роутера от вашего ближайшего. При этом указывается тот интерфейс, который ближе к вашему ПК.

Задание к лабораторной работе

1. Создать рассмотренные в теоретическом материале примеры сетей.
2. Настроить созданные сети и посмотреть их работу.
3. Ответить на контрольные вопросы.

Контрольные вопросы

1. Что такое маршрутизация?
2. Что такое маршрутизатор?
3. Что такое маска подсети?
4. Что такое маршрут (роут) и таблица маршрутизации?
5. Как просмотреть или очистить таблицу маршрутов, добавить новый маршрут?
6. Что такое шлюз по умолчанию?
7. Что такое трассировка маршрута? Как она выполняется?

Лабораторная работа №8
Протоколы динамической маршрутизации

Цель работы: исследование возможностей формирования таблиц маршрутизации в автоматическом режиме.

Теоретические положения

Протокол RIP

Для настройки маршрутизации в маленькой сети допустима ручная настройка таблицы маршрутизации. В этом случае таблица будет статической.

В случае развитой сети, содержащей большое количество роутеров, подсетей, ручная настройка становится затруднительной – на каждом роутере нужно указывать маршруты до всех сетей, при этом 43 количество записей в таблице маршрутизации может достигать нескольких десятков. Для упрощения создания таблиц маршрутизации автоматически существует несколько протоколов динамической маршрутизации. Самым простым из них является протокол RIP (Route Internet Protocol)

Пример топологии сети приведен на рисунке 8.1.

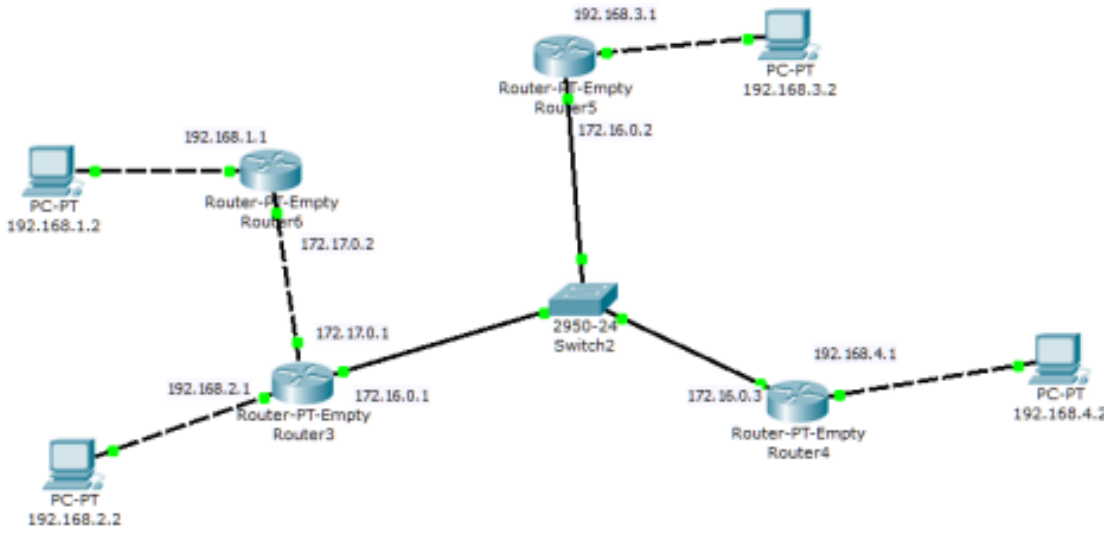

Рис. 8.1. – Пример топологии сети

Для задания настройки протокола RIP необходимо лишь указать, адреса подсетей, к которым подключен роутер. То есть для роутера Router6 нужно указать сети 192.168.1.0 и 172.17.0.0. Для Router3 – 192.168.2.0, 172.17.0.0, 172.16.0.0 и т. д. Когда на все

роутерах в сети будут настроены подсети, они обменяются нужными данными. В результате этого обмена на всех роутерах в таблице маршрутизации появляются данные обо всех подсетях, доступных в существующей сети.

Задание к лабораторной работе №8

Для созданной ранее сети изменить в свойствах роутера тип маршрутизации – вместо «Статическая» настроить RIP и проверить во всех направлениях передачу Ping. Показать результаты преподавателю.

Лабораторная работа №9
Настройка статической маршрутизации (через консоль)

Цель работы: Научиться настраивать статические маршруты на маршрутизаторах Cisco для обеспечения связи между разными сетями, с помощью консольных команд.

Теоретические положения

На всем оборудовании фирмы Cisco установлена операционная система IOS (Internetwork Operating System – Межсетевая Операционная Система). Вся работа по настройке оборудования проводится через командную строку.

Cisco поддерживают два способа подключения к интерфейсу IOS для настройки: последовательный порт, установленный непосредственно на коммутаторе или маршрутизаторе и удаленный доступ по протоколам Telnet и SSH (шифрованный канал доступа).

Вся работа по настройке ведется в режиме диалога – в консоли отображается приглашение, пользователь вводит команды, система выводит результаты работы.

Пользовательские режимы IOS

В IOS предусмотрено два основных режима работы: пользовательский (user mode) и привилегированный (privileged mode). При первом подключении устройство работает в пользовательском режиме. В документации Cisco он упоминается как пользовательский режим исполнения (user exec mode). Его можно узнать по приглашению подобного вида: **Router>**

В любом режиме и в любом месте командного интерфейса можно ввести команду **«?»** и увидеть доступные команды/параметры с кратким пояснением. В пользовательском режиме доступно относительно мало команд, в основном для просмотра каких-либо данных. Например, команда **show**, предназначенная для просмотра статуса протекающих процессов.

Для перевода из пользовательского в привилегированный режим служит команда **enable**. Из привилегированного режима доступен переход к настройкам системы командой **configure terminal**. Пример получения привилегированного доступа и перехода в режим настроек:

Switch>enable

Switch#configure terminal
Switch(config)#

Основные команды для настройки системы приведены на рисунке 9.1.

Команда	Назначение
banner {login|motd} <приглашение>	Настройка приветствия после входа в систему (login) или «сообщения дня» (motd)
hostname <имя хоста>	Настройка имени устройства, выводимого в приглашении, например hostname Sw приведет к тому, что приглашение будет выглядеть так: Sw#
interface <имя интерфейса>	Переход в режим настройки заданного сетевого интерфейса
username <имя пользователя> password <пароль>	Включение аутентификации пользователя по паролю при входе в систему
enable password <пароль>	Задание пароля для команды смены режима (enable), пароль сохраняется в незашифрованном виде. Применимо только на старом оборудовании, не поддерживающем шифрование
enable secret <секрет>	Задание пароля для команды смены режима, пароль сохраняется в зашифрованном виде.
line <тип> <номер>	Настройка терминалов типа console или vty с заданными номерами.

Рис. 9.1. – Основные команды для настройки системы

Доступ к настройкам оборудования может быть произведен при помощи разных методов – непосредственно через последовательный порт (**console**) или через удаленный доступ по протоколу telnet (**vty**). Поддерживается 5 одновременных TELNET соединений с номерами 0 – 4. Таким образом команда

sw(config)# line console 0

приведет к настройке доступа через консоль (последовательный порт), а команда

sw(config)# line vty 0 4

приведет к настройке доступа через TELNET соединения.

В каждом из этих случаев доступны команды password <пароль> и login. Команда для добавления статического маршрута:

ip route [сеть_назначения] [маска] [следующий_маршрутизатор].

Задание к лабораторной работе №9

1. Разместите устройства:

- 2 маршрутизатора (Router → 2911)
- 2 коммутатора (Switches → 2950-24)
- 4 компьютера (End Devices → PC)

2. Выполните соединения:

- ПК1 и ПК2 подключите к коммутатору S1 (прямым кабелем)
- ПК3 и ПК4 подключите к коммутатору S2 (прямым кабелем)
- S1 подключите к R1 (прямым кабелем, порт FastEthernet0/0)
- S2 подключите к R2 (прямым кабелем, порт FastEthernet0/0)
- R1 и R2 соедините между собой (кроссовым кабелем, порты FastEthernet0/1)

3. Настройте IP-адреса на ПК:

Сеть 1 (слева):

- ПК1: 192.168.1.10/24, шлюз 192.168.1.1
- ПК2: 192.168.1.11/24, шлюз 192.168.1.1

Сеть 2 (справа):

- ПК3: 192.168.2.10/24, шлюз 192.168.2.1
- ПК4: 192.168.2.11/24, шлюз 192.168.2.1

4. Настройте интерфейсы маршрутизаторов:

На Router1:

```
enable
configure terminal
hostname R1
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
exit
interface FastEthernet0/1
ip address 10.0.0.1 255.255.255.252
no shutdown
exit
```

На Router2:

```
enable
configure terminal
hostname R2
interface FastEthernet0/0
ip address 192.168.2.1 255.255.255.0
no shutdown
exit
interface FastEthernet0/1
ip address 10.0.0.2 255.255.255.252
no shutdown
exit
```

5. Настройте статические маршруты:
На R1:

```
ip route 192.168.2.0 255.255.255.0 10.0.0.2
```

На R2:

```
ip route 192.168.1.0 255.255.255.0 10.0.0.1
```

6. Проверьте связь, выполнив команду Ping.

Содержание самостоятельной работы

Цель самостоятельной работы обучающихся – получить новые знания по дисциплине «Компьютерные сети».

Самостоятельная работа необходима для формирования у обучающихся способности самостоятельно решать задачи профессиональной деятельности, формирования умения и навыков планирования времени, формирования стремления развиваться и совершенствоваться.

Самостоятельная работа обучающихся состоит в изучении литературы и Интернет-ресурсов по темам:

1. Структура стандартов IEEE
2. Стандарты в сфере структурированных кабельных систем
3. Система DNS
4. Классовая и бесклассовая IP-адресация
5. Протоколы внешней маршрутизации
6. Автономные системы

Список литературы

1. Урбанович, П. П. Компьютерные сети : учебное пособие / П. П. Урбанович, Д. М. Романенко. – Москва, Вологда : Инфра-Инженерия, 2022. – 460 с.
2. Максимов, Н. В. Компьютерные сети : учебное пособие / Н. В. Максимов, И. И. Попов. – 6-е изд., перераб. и доп. – Москва : ИНФРА-М, 2026. – 464 с.
3. Кузин, А. В. Компьютерные сети : учебное пособие / А. В. Кузин, Д. А. Кузин. – 4-е изд., перераб. и доп. – Москва : ФОРУМ : ИНФРА-М, 2025. – 190 с.
4. Андриянов, А. М. Компьютерные сети и сетевые технологии : учебное пособие / А. М. Андриянов. – Тюмень : Тюменский индустриальный университет, 2023. – 80 с.
5. Рабчевский, А. Н. Компьютерные сети и системы связи. вводный курс : учебное пособие для СПО / А. Н. Рабчевский. – Москва : Юрайт, 2025. – 207 с.
6. Ибе, О. Компьютерные сети и службы удаленного доступа / О. Ибе ; перевод И. В. Синицын. – 3-е изд. – Саратов : Профобразование, 2024. – 335 с.
7. Артюшенко, В. В. Компьютерные сети и телекоммуникации : учебно-методическое пособие / В. В. Артюшенко, А. В. Никулин. – Новосибирск : Новосибирский государственный технический университет, 2020. – 72 с.
8. Компьютерные сети : учебник и практикум для СПО / под науч. ред. А. М. Нечаева, А. Е. Трубина, А.Ю. Анисимова. – Москва : Юрайт, 2025. – 515 с.
9. Уймин, А. Г. Компьютерные сети. L2-технологии : практикум для СПО / А. Г. Уймин. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2024. – 190 с.

СОДЕРЖАНИЕ