

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

Сергей Александрович Асанов  
Юрий Сергеевич Гладышев

## **КОМПЬЮТЕРНЫЕ СЕТИ**

Методические материалы к практическим занятиям  
и самостоятельной работе

Рекомендовано ЦМК специальности 09.02.07 Информационные  
системы и программирования в качестве электронного издания  
для использования в образовательном процессе

Кемерово 2024

Рецензенты: Семенова О. С. – канд., тех. наук, доцент кафедры эксплуатации автомобилей, заведующий кафедрой информатики и информационных систем ИПО ФГБОУ ВО «Кузбасский государственный технический университет имени Т. Ф. Горбачева»»

**Асанов, С.А., Гладышев, Ю.С. Компьютерные сети:** методические материалы к практическим занятиям и самостоятельной работе для студентов специальности СПО «09.02.07 Информационные системы и программирование» очной формы обучения / сост. Асанов С. А., Гладышев Ю.С.; Кузбасский государственный технический университет имени Т. Ф. Горбачева. – Кемерово, 2024. – Текст: электронный.

Приведены методические материалы к практическим занятиям и самостоятельной работам по дисциплине «Компьютерные сети», позволяющие закрепить знания, полученные в ходе аудиторных занятий; способствующие закреплению теоретических положений; развитию навыков по их практическому применению.

© Кузбасский государственный  
технический университет  
имени Т. Ф. Горбачева, 2024  
© Асанов С. А.,  
Гладышев Ю.С.;  
составление, 2024

## СОДЕРЖАНИЕ

Общие положения.....	3
Практическое занятие № 1. Монтаж кабельных сред .....	4
Практическое занятие № 2. Инструменты диагностики кабельной инфраструктуры.....	8
Практическое занятие № 3. Установка и настройка сетевых адаптеров .....	12
Практическое занятие № 4. Построение схемы сети.....	15
Практическое занятие № 5. Расчет IP сетей .....	19
Практическое занятие № 6. Преобразование адресов .....	28
Практическое занятие № 7. Маршрутизация в сетях TCP/IP .....	39
Практическое занятие № 8. Протоколы динамической маршрутизации .....	43
Самостоятельная работа .....	45
Список литературы.....	46

## **Общие положения**

Целью освоения дисциплины «Компьютерные сети» является приобретение обучающимися знаний в области теоретических основ построения и функционирования компьютерных сетей, приобретение практических навыков монтажа и настройки активного и пассивного сетевого оборудования.

Основными задачами изучения дисциплины «Компьютерные сети», являются:

- изучение моделей взаимодействия информационных систем через сеть;
- ознакомление студентов с технологиями интеграции локальных сетей в глобальную сеть Интернет и передачи данных в глобальной сети;
- изучение функциональных возможностей коммуникационного оборудования и технологий их реализации;
- овладение средствами анализа трафика в сетях и методами его минимизации;
- овладение основами проектирования и моделирования локальных сетей.

Изучение дисциплины «Компьютерные сети» предусматривает проведение лекционных занятий, практических занятий и самостоятельной работы обучающимися очной формы обучения.

## **Практическое занятие № 1. Монтаж кабельных сред**

**Цель работы** – Ознакомление с конструктивными элементами кабелей связи и соответствующей кабельной арматурой и приобрести практические навыки по разделке кабелей.

### **Теоретические положения**

Кабельная среда – это совокупность кабелей и соединительных устройств, используемых для передачи данных между компьютерами, сетевыми устройствами и другими электронными устройствами. Кабельная среда обеспечивает физическое соединение между устройствами и обеспечивает передачу информации в виде электрических сигналов или световых волн.

В кабельной среде могут использоваться различные типы кабелей, такие как витая пара, оптоволокно, коаксиальный кабель и другие. Каждый тип кабеля имеет свои особенности и применяется в зависимости от конкретных потребностей сети.

Монтаж кабельных средств является процессом установки, подключения и организации кабельной инфраструктуры для передачи данных в сети. Эта процедура включает множество этапов, которые следует выполнить для корректной установки кабельной среды.

### **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](http://www.iso.ch), [www.iec.ch](http://www.iec.ch)).
- Европейский стандарт EN 50173 Information technology–Generic cabling systems.
- Американский стандарт ANSI/TIA/EIA 568-B Commercial Building Telecommunication Cabling Standard ([www.tiaonline.org](http://www.tiaonline.org), [www.eia.org](http://www.eia.org)).

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, разъемов, 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: бело-зеленый; зеленый; бело-оранжевый; оранжевый; бело-синий; синий; бело-коричневый; коричневый.

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 RJ-45, 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:

1. Компьютер соединяется с сетевым концентратором (hub) или коммутатором (switch) используя «прямую» разводку кабеля (стандарт T568B);

1		бело-оранжевый	бело-оранжевый		1
2		оранжевый	оранжевый		2
3		бело-зелёный	бело-зелёный		3
4		синий	синий		4
5		бело-синий	бело-синий		5
6		зелёный	зелёный		6
7		бело-коричневый	бело-коричневый		7
8		коричневый	коричневый		8

Рисунок 1 – Прямая разводка кабеля

2. 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.


1		бело-оранжевый	бело-зелёный		1
2		оранжевый	зелёный		2
3		бело-зелёный	бело-оранжевый		3
4		синий	синий		4
5		бело-синий	бело-синий		5
6		зелёный	оранжевый		6
7		бело-коричневый	бело-коричневый		7
8		коричневый	коричневый		8

Рисунок 2 – Перевернутая разводка

### Задания для практического занятия:

Первоначально следует изучить теоретический материал практической работы 1. Затем выполнить следующие действия:

1. Нарисовать схему кабельной среды с элементами подключения и отобразить стандарт использования и расположения проводов.

Варианты:

- 1) Подключение двух компьютеров.
- 2) Подключение коммутатора с концентратором.
- 3) Подключение компьютера и свитча.
- 4) Подключение концентратора с концентратором.
- 5) Подключение компьютера и коммутатора.

2. Описать получившиеся структуры и сделать вывод про использование стандартов T568A и T568B.

3. Получить у преподавателя коннекторы RJ-45, кусок витой пары и определить схему монтажа.



Рисунок 3 – Коннектор RJ-45

4. Прослушать инструктаж по использованию обжимного инструмента.



Рисунок 4 – Вариант обжимного инструмента.

5. Произвести монтаж кабельной среды по определенному стандарту и выбранной схеме.
6. Результаты занести в отчет с добавлений фотографий добавив в отчет.
7. Ответить на контрольные вопросы

#### **Контрольные вопросы**

1. Что такое структурированная кабельная система, и каково ее назначение?
2. Какие элементы относятся к классу пассивного сетевого оборудования.
3. Какие типы кабельных сред могут использоваться для передачи данных в ЛВС?
4. Что определяют стандарты T568A и T568B?
5. Каково назначение патч-корда и в чем его отличие от кабеля внутренней прокладки?

## **Практическое занятие № 2.**

### **Инструменты диагностики кабельной инфраструктуры**

**Цель работы** – Изучение работы устройств, предназначенных для диагностики кабельной инфраструктуры.

#### **Теоретические положения**

Диагностика кабельной инфраструктуры играет ключевую роль в обеспечении надежности и эффективности сетевых коммуникаций. Кабельная инфраструктура является основой для передачи данных в сети, и ее правильное функционирование критически важно для бесперебойной работы информационных систем и оборудования.

Понимание принципов работы устройств для диагностики кабельной инфраструктуры, а также умение проводить тестирование и анализ результатов, позволяет обеспечить высокую производительность сети, выявить возможные проблемы и оперативно реагировать на них. Овладение навыками диагностики кабельной среды позволяет специалистам эффективно управлять и поддерживать сетевую инфраструктуру, обеспечивая ее стабильную работу и минимизируя риски сбоев и простоев.

В данной практической работе мы рассмотрим основные аспекты диагностики кабельной инфраструктуры, включая инструменты и методики, необходимые для проведения тестирования, интерпретации результатов и обеспечения надежности сетевых соединений.

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.

1) 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.



Рисунок 5 – Портативный сетевой анализатор

## 2) Кабельные сканеры.

Данные приборы позволяют определить длину кабеля, переходное затухание между парами, импеданс, последовательность расположения проводников, уровень электрических шумов и провести оценку полученных результатов. 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.



Рисунок 6 – Сетевой кабельный трекер NOYafa NF-8209S

### **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 так – же 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.



Рисунок 7 – Вариант кабельного тестера

### **Задания для практического занятия:**

Результатом практической работы является отчет, в котором должно быть приведено описание принципа работы прибора, выданного для выполнения практической работы, и результатов

проведенных с его помощью измерений.

Для выполнения практической работы № 2 студент должен изучить приведенный теоретический материал. Отчет сдается в распечатанном и электронном видах (файл Word).

Для выполнения работы вам потребуется обжатый с первой практической работы провод витой пары.

Вам нужно прослушать инструктаж по работе с кабельным тестером, после чего произвести в отчете пометки по принципам его работы.

Затем следует выполнить тестирование своего провода витой пары, в соответствии с инструктажем, проведенным ранее, в кабельном тестере и описать результат тестирования. В случае если результаты тестирования отрицательные, нужно описать причину неполадки и предложить варианты решения проблемы.

Данные занести в отчет, ответить на контрольные вопросы.

#### **Контрольные вопросы**

1. Какие типы кабелей вы знаете?
2. Максимальная длина кабеля UTP. Объясните причину ограничения длины кабеля?
3. Чем отличается прямой кабель от перекрещенного?
4. Каким стандартом определяется порядок разводки проводов для разъемов RJ-45?
5. Какие виды оборудования диагностики кабельной инфраструктуры Вы знаете?
6. В чём отличие кабельного тестера от кабельного сканера?
7. Для чего применяются сетевые анализаторы?

### **Практическое занятие № 3.**

#### **Установка и настройка сетевых адаптеров**

**Цель работы** – изучение разновидностей сетевых адаптеров, приобретения навыков их установки и конфигурирования.

#### **Теоретические положения:**

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.

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

1) По среде передачи данных:

а проводные (витая пара, коаксиальный кабель, оптоволокно);

б беспроводные (инфракрасная связь, Bluetooth, wireless LAN).

2) По выполняемым функциям СА:

а 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.

б 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.

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

- а шинную;
- б кольцевую;
- с звездообразную;
- д древовидную;
- е комбинированную.

4) По принадлежности к типу компьютера:

- а адаптеры для клиентских компьютеров;
- б 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.

Основные характеристики СА:

- 1) установленная микросхема контроллера (микрочип);
- 2) разрядность – имеются 8-, 16-, 32- и 64-битные сетевые карты;
- 3) (определяется микрочипом);
- 4) скорость передачи – от 10 до 1000 Мбит/с;
- 5) тип подключаемого кабеля – коаксиальный кабель толстый и тонкий, неэкранированная витая пара, волоконно-оптический кабель;
- 6) 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).

### **Задания для практического занятия:**

Результатом практической работы является отчет, в котором должны быть отражены параметры настройки сетевых адаптеров, продемонстрирована работоспособность сети.

Для выполнения практической работы № 3 студент должен изучить приведенный ниже теоретический материал. Отчет сдается в распечатанном и электронном (файл Word) видах.

1) Составить таблицу по сетевым адаптерам, которая будет включать вид адаптера, особенности, и главный функционал.

2) Определить принадлежность сетевого адаптера по теоретическому материалу, предоставленному выше.

3) Установить сетевой адаптер в среду

4) Составить отчет по проделанной работе

### **Контрольные вопросы:**

1. Для чего служат сетевые адаптеры?

2. Перечислите основные функции сетевого адаптера.

3. На каких уровнях модели OSI есть сетевые адаптеры?

4. По каким признакам могут различаться сетевые адаптеры?

5. Как определить физический (MAC) адрес адаптера?

## **Практическое занятие № 4. Построение схемы сети**

**Цель работы** – Получение базовые знаний и умений для работы с программой Cisco Packet Tracer и построения в ней схемы сети.

### **Теоретические положения**

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 отслеживать перемещение данных по сети, появление и изменение пара-

метров 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 8.

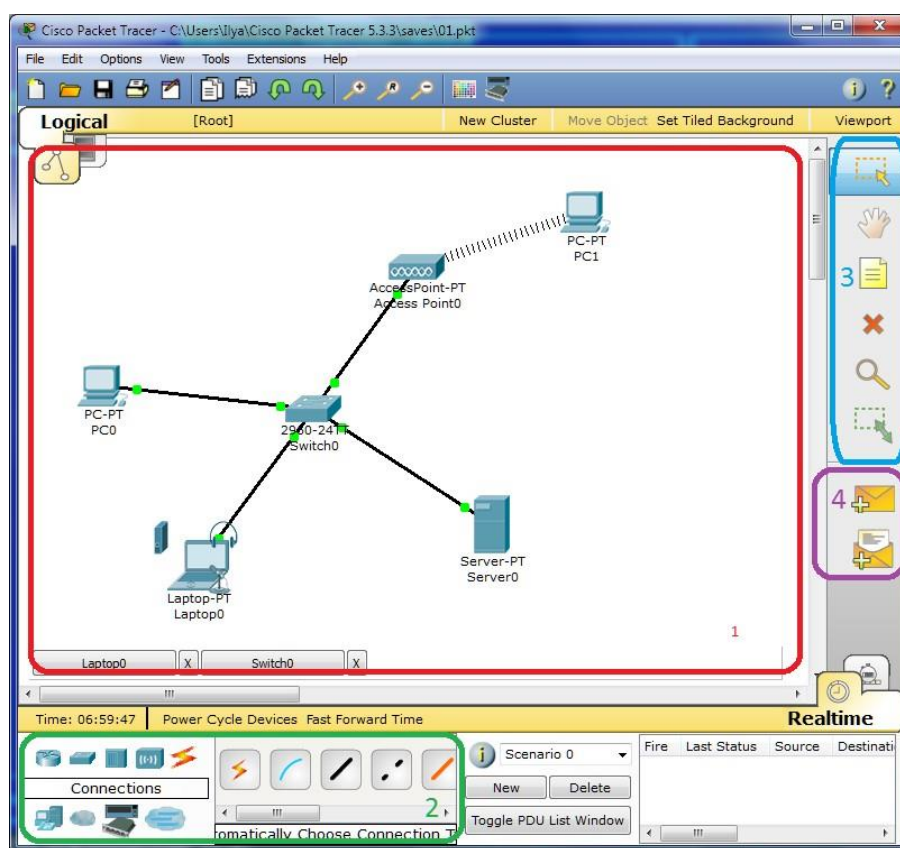


Рисунок 8 – Интерфейс СРТ

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.

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: автоматический; прямой патч-корд; кроссовый патч-корд; консольный кабель; оптический кабель; 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 состоит из нескольких вкладок:

- \* Physical – конфигурирование оборудования
- \* Config – конфигурирование программной части
- \* другие закладки, зависящие от типа оборудования.

В закладке конфигурирования оборудования можно его включать, выключать, добавлять разные модули (для рабочей станции – сетевые карты, для сетевого оборудования – сетевые

модули, в т.ч. 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».

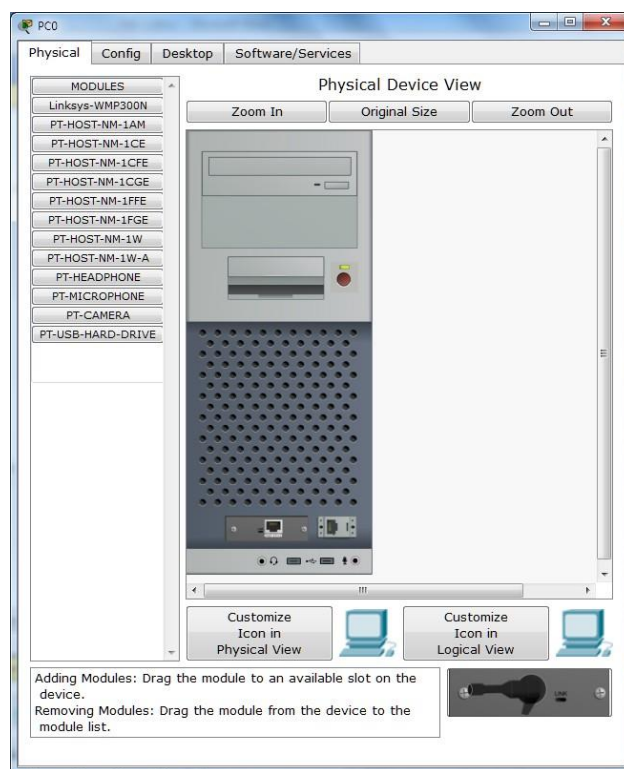


Рисунок 9 – Конфигурирование рабочей станции

### **Задания для практического занятия:**

Результатом практической работы является отчет, в котором должны быть приведена созданная схема сети и продемонстрированы результаты проверки её работоспособности.

Для выполнения работы следует выполнить следующие шаги:

- 1) Изучить теоретическое положение;
- 2) Ответить на контрольные вопросы, прикладывая скриншоты из Cisco Packet Tracer.
- 3) Пройти собеседование с преподавателем и определить вариант компьютерной сети, представленных ниже:
  - 3 компьютера, сервер, роутер. Один компьютер соединен беспроводной связью с роутером, остальные проводным подключением,

- 2 компьютера, 1 ноутбук, роутер. Все устройства подключены по кабельной среде.

- 1 ноутбук, 2 компьютера, роутер, почтовый сервер. Все подключены через кабельную среду.

- 1 ноутбук, 2 компьютера, свитч, сервер. Один компьютер подключен беспроводным способом, остальные устройства проводным.

4) Составить отчет, содержащий этапы создания компьютерной сети.

5) Добавить в отчет скриншоты, отображающие результаты проверки её работоспособности

### **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 PacketTracer?

4. Какие виды устройств позволяет использовать Cisco PacketTracer?

5. Каким образом можно производить конфигурирование устройств в Cisco Packet Tracer?

6. Какие режимы работы предусмотрены в Cisco Packet Tracer? В чем их отличие?

## **Практическое занятие № 5. Расчет IP сетей**

**Цель работы** – Получение практических навыков в работе по анализу и настройке конфигурации вычислительной сети, использующей семейство протоколов TCP/IP.

### **Теоретические положения**

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. Если подсетью интерсети является локальная сеть, то локальный адрес – это МАС-адрес. *МАС-адрес* назначается сетевым адаптерам и сетевым интерфейсам маршрутизаторов, МАС-адреса назначаются производителями оборудования и являются уникальными. Для всех существующих технологий локальных сетей МАС-адрес имеет формат 6 байт, например 11-АО- 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 прин-

ципу: RU – Россия, 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 ниже приведено соответствие классов адресов значениям первого октета и указано количество возможных IP-адресов каждого класса.

Таблица 1. Характеристики классов адресов

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

Адреса класса А предназначены для использования в больших сетях общего пользования. Они допускают большое количество номеров узлов. Адреса класса В используются в сетях среднего размера, например, сетях университетов и крупных компа-

ний. Адреса класса С 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 не 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 с 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. Маршрутизаторы, 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.

#### 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 объедине-

ние подсетей. При этом ваша организация должна получить один сетевой номер, например, номер класса В. Для IP-адресов класса В 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 будет 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/IP-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.

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 до 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 192 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 00011111 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.

### **Задания для практического занятия:**

Выполнение работ по данному практическому занятию включает в себя изучение кратких теоретических сведений, выполнение практического задания, оформление отчета и ответы на контрольные вопросы.

1. Произвести расчет подсетей, получив доступные диапазоны IP-адресов для компьютеров в каждой подсети, согласно данных индивидуального варианта. Номера вариантов приведены в таблице 2.

Таблица 2 – Варианты исходных заданий

Вариант	Начальный адрес сети (адрес первой подсети)	Количество компьютеров в подсети	Вариант	Начальный адрес сети (адрес первой подсети)	Количество компьютеров в подсети
1	194.57.253.0	20	9	196.192.176.10	34
2	199.117.13.0	22	10	182.141.255.0	36
3	207.133.254.0	24	11	193.254.15.10	38
4	220.115.46.10	25	12	185.110.255.0	40
5	217.155.31.20	26	13	191.118.255.0	42
6	193.110.255.0	28	14	192.18.155.0	45
7	210.99.130.0	30	15	200.200.200.0	50
8	132.18.255.0	32	<b>16</b>	194.57.253.0	<b>50</b>

### Контрольные вопросы

1. Какую долю всего множества IP-адресов составляют адреса класса А? Класа В? Класа С?

2. Какие из ниже приведенных адресов не могут быть использованы в качестве IP-адреса конечного узла сети, подключенной к Internet? Для синтаксически правильных адресов определите их класс: А, В, С, D или Е.

(А) 127.0.0.1 (Е) 10.234.17.25 (I) 193.256.1.16

(В) 201.13.123.245 (F) 154.12.255.255 (J) 194.87.45.0

(С) 226.4.37.105 (G) 13.13.13.13 (K) 195.34.116.255

(D) 103.24.254.0 (H) 204.0.3.1 (L) 161.23.45.305

3. Пусть IP-адрес некоторого узла подсети равен 198.65.12.67, а значение маски для этой подсети — 255.255.255.240. Определите IP-адрес подсети. Какое максимальное число узлов (IP-адресов для компьютеров) может быть в этой подсети?

4. Пусть поставщик услуг Internet имеет в своем распоряжении адрес сети класса В. Для адресации узлов своей собственной сети он использует 254 адреса. Определите максимально возможное число абонентов этого поставщика услуг, если размеры требуемых для них сетей соответствуют классу С? Какая маска должна быть установлена на маршрутизаторе поставщика услуг, соединяющем его сеть с сетями абонентов?

5. Какое максимальное количество подсетей теоретически возможно организовать, если в вашем распоряжении имеется сеть класса С? Какое значение должна при этом иметь маска?

## **Практическое занятие № 6. Преобразование адресов**

**Цель работы** – Изучение принципов настройки четырех типов серверов и включение их в состав локальной не маршрутизируемой сети.

### **Теоретические положения**

Сервер – это компьютер или система, которая предоставляет другим компьютерам, называемым клиентами, доступ к своим ресурсам. Эти ресурсы могут включать в себя файлы и папки, приложения, интернет соединение и другое.

Серверы могут быть разных типов, в зависимости от того, какие услуги они предоставляют. Например, веб-серверы хранят веб-страницы и делают их доступными для пользователей интернета. Файловые серверы хранят файлы и позволяют пользователям получать доступ к ним и скачивать их.

Серверы обычно мощнее обычных персональных компьютеров, поскольку они должны обрабатывать большое количество запросов от множества клиентов одновременно. Они также обычно имеют специальное программное обеспечение, которое помогает им управлять этими запросами и обеспечивать безопасность и стабильность.

Серверы можно классифицировать по различным критериям, включая их функциональное назначение, тип программного обеспечения и аппаратного обеспечения.

Вот некоторые основные типы серверов:

1) Веб-сервер – это программное обеспечение, которое обрабатывает запросы от клиентов через протокол HTTP (Hypertext Transfer Protocol) и отвечает им, обычно предоставляя веб-страницы и другие ресурсы. Он играет ключевую роль в обеспечении работы веб-сайтов и веб-приложений. Веб-серверы могут обслуживать статические и динамические контенты, включая HTML-страницы, изображения, видео, аудио, файлы и многое другое.

Существует множество различных веб-серверов, таких как Apache, Nginx, Microsoft IIS, LiteSpeed и другие. Каждый из них имеет свои особенности, преимущества и недостатки. Например, Apache является одним из самых популярных веб-серверов из-за

своей гибкости и расширяемости, в то время как Nginx известен своей высокой производительностью и эффективным управлением ресурсами.

Веб-серверы работают на определенном порту (обычно порт 80 для HTTP и порт 443 для HTTPS) и могут быть настроены для обработки различных типов запросов и обеспечения безопасности передачи данных. Они являются неотъемлемой частью инфраструктуры веб-сайтов и обеспечивают их доступность и производительность.

2) DNS-сервер – это специализированное программное обеспечение или устройство, которое отвечает за обработку запросов на разрешение доменных имен в IP-адреса и наоборот. Они играют важную роль в работе DNS и обеспечивают правильное функционирование системы и доступность ресурсов в Интернете.

DNS-серверы могут выполнять разные функции в зависимости от их ролей:

1. Они отвечают на запросы клиентов, запрашивая информацию у других DNS-серверов, пока не найдут искомую запись.

2. Авторитетные DNS-серверы: Они содержат авторитетные записи для конкретных доменов и отвечают непосредственно за предоставление информации о доменных именах и их соответствующих IP-адресах.

3. Кэширующие DNS-серверы: Они временно хранят информацию о разрешенных доменных именах, чтобы ускорить процесс разрешения запросов и снизить нагрузку на другие DNS-серверы.

DNS-серверы работают с использованием различных протоколов, таких как UDP (User Datagram Protocol) и TCP (Transmission Control Protocol), для обмена информацией между собой и клиентами. Они также поддерживают различные типы записей, такие как A (IPv4-адрес), AAAA (IPv6-адрес), CNAME (каноническое имя), MX (почтовый сервер) и другие, для обеспечения разнообразных функций и возможностей DNS.

3) DHCP-сервер – это специализированное программное обеспечение или устройство, которое выполняет функции по назначению IP-адресов и других сетевых параметров клиентам в

сети с использованием протокола DHCP (Dynamic Host Configuration Protocol). DHCP-серверы обеспечивают автоматическую настройку сетевых параметров для устройств, подключенных к сети, что значительно упрощает процесс управления сетевой инфраструктурой.

Функции DHCP-сервера включают:

1. Назначение IP-адресов: DHCP-сервер выделяет свободные IP-адреса из пула адресов и назначает их клиентам на определенное время.

2. Настройка других параметров: Кроме IP-адреса, DHCP-сервер также предоставляет другие сетевые параметры, такие как шлюз по умолчанию, DNS-серверы, субнет-маску и другие, для правильной работы клиентских устройств.

3. Управление арендой IP-адресов: DHCP-сервер отслеживает аренду IP-адресов клиентам и управляет их продлением или освобождением по истечении срока аренды.

4. Мониторинг и журналирование: DHCP-серверы могут вести журналы событий, отслеживать использование IP-адресов и предоставлять администраторам информацию о состоянии сети.

5. Безопасность: DHCP-серверы могут поддерживать механизмы аутентификации клиентов, фильтрацию доступа и другие меры безопасности для защиты сети от несанкционированного доступа.

DHCP-серверы могут быть настроены для работы в различных сетевых средах, от небольших домашних сетей до крупных корпоративных сетей. Они играют важную роль в автоматизации процесса настройки сетевых параметров и обеспечивают гибкость и эффективность управления сетью.

- 4) Почтовый сервер (Mail Server) – это серверное программное обеспечение, которое отвечает за отправку, прием, хранение и доставку электронной почты. Почтовые сервера играют ключевую роль в обмене электронными сообщениями в сети Интернет и внутри корпоративных сетей. Почтовые серверы работают с использованием протоколов SMTP (Simple Mail Transfer Protocol) для отправки почты, POP3 (Post Office Protocol) или IMAP (Internet Message Access Protocol) для получения почты, а также других протоколов для обеспечения безопасности и эффек-

тивности обмена сообщениями.

### **Задания для практического занятия:**

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. По окончании работы должен быть составлен отчет со скриншотами и краткими текстовыми пояснениями, на основе которых будет понятен ход и результат ваших действий.

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 будем использовать Generic Switch-PT, причем в него нужно добавить два дополнительных сетевых интерфейса PT- Switch-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, а далее на этой же вкладке в разделе Global / Setting указываем IP-адрес будущего DNS-сервера, например 192.168.1.4. Все эти настройки можно выполнить и через вкладку Desktop / IP Configuration.

Затем переходим на вкладку Services. Нас интересует сейчас раздел HTTP. С правой 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. Текст может быть произвольным, но должен содержать вашу Фамилию и инициалы. Сохранить изменения и закрыть свойства WEB-сервера.

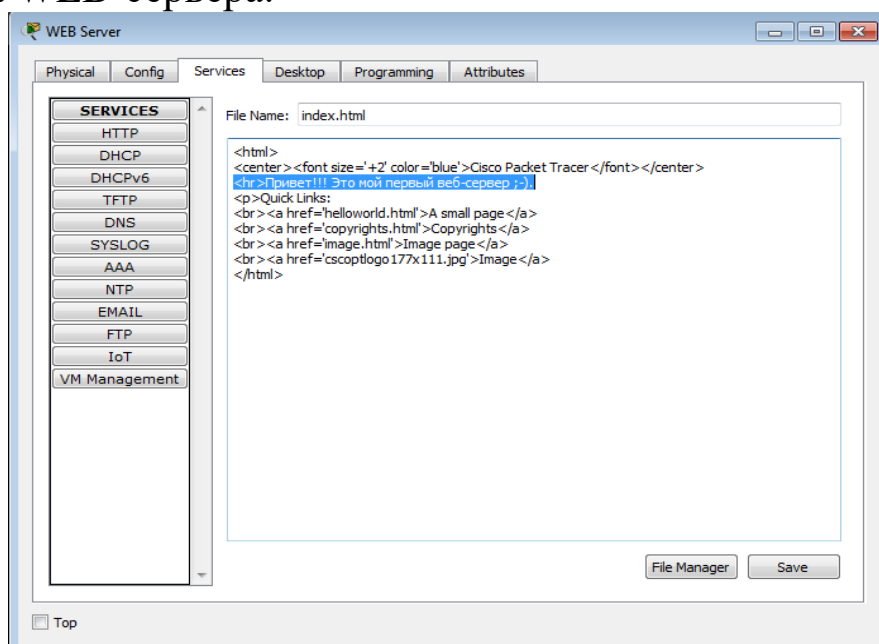


Рисунок 10 – Интерфейс программы

#### 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 всё 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 до-

менного 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 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.

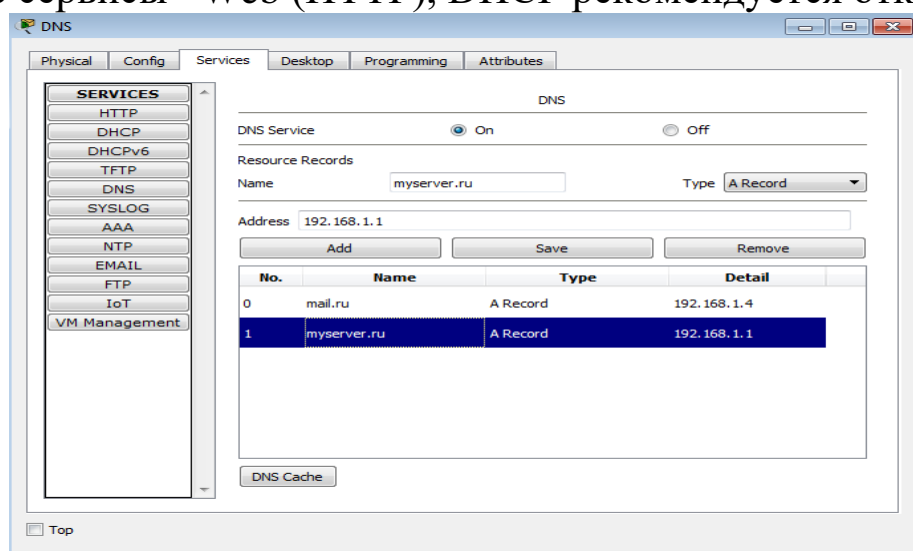


Рисунок 11 – Работа приложения

## 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, 192.168.1.5.

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 12.

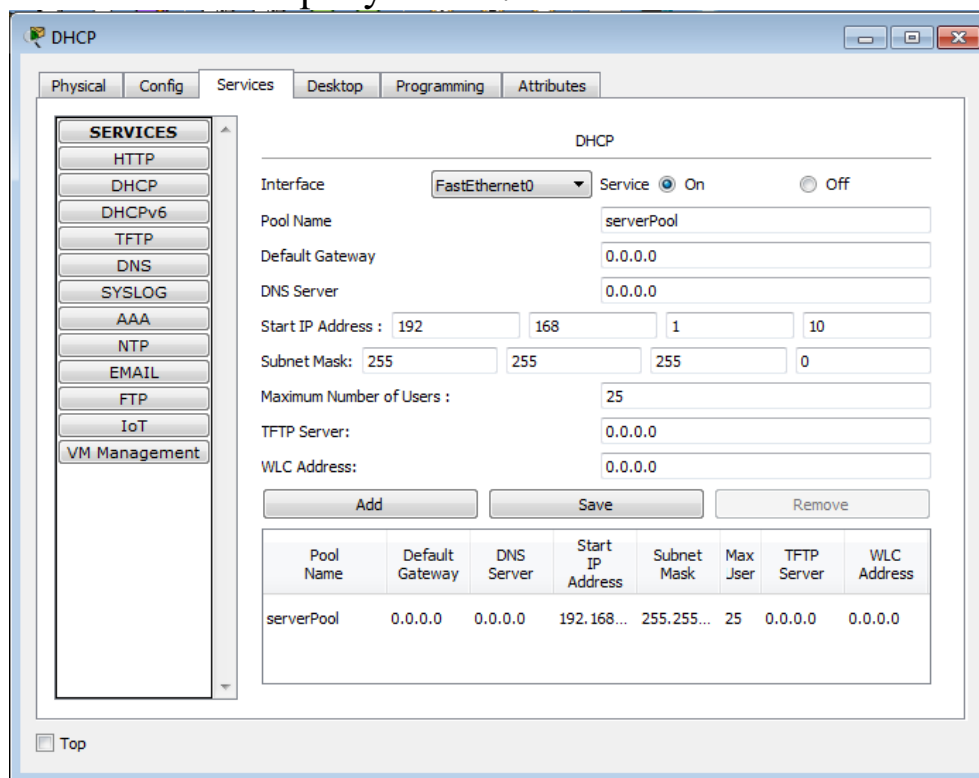
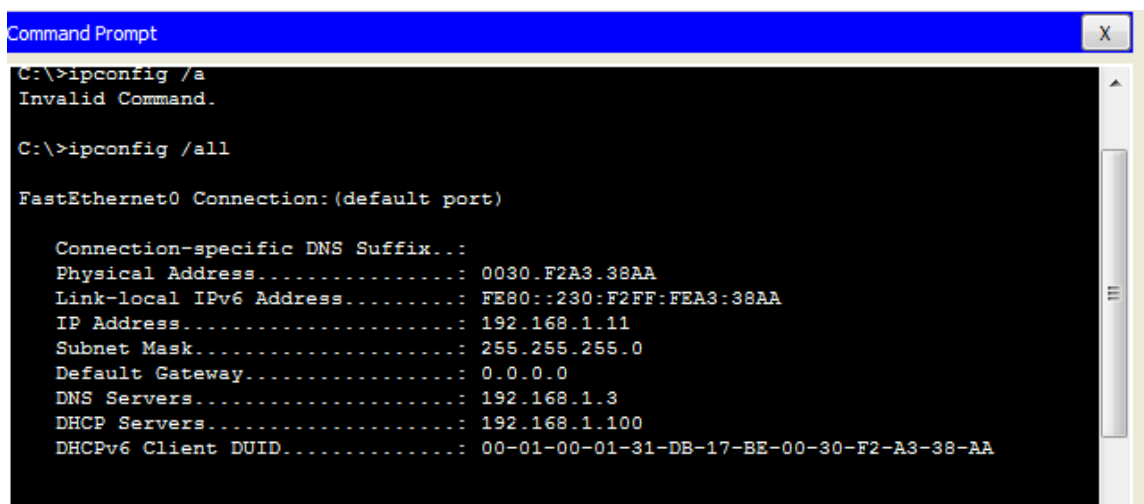


Рисунок 12 – Пример настройки

## 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 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` (рисунок 13)



```
Command Prompt
C:\>ipconfig /a
Invalid Command.

C:\>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0030.F2A3.38AA
Link-local IPv6 Address.....: FE80::230:F2FF:FEA3:38AA
IP Address.....: 192.168.1.11
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 0.0.0.0
DNS Servers.....: 192.168.1.3
DHCP Servers.....: 192.168.1.100
DHCPv6 Client DUID.....: 00-01-00-01-31-DB-17-BE-00-30-F2-A3-38-AA
```

Рисунок 13 – Получение информации через командную строку

Значение всех параметров кроме Default Gateway не должны быть равны 0.

9. Создадим почтовый (EMAIL) – сервер и заведем на нем два 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. 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 рисунок 11).

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

На вкладке Services переходим в раздел EMAIL и включаем службы SMTP и POP3. Затем придумываем доменное имя почтового сервера и создаем два пользовательских аккаунта с произвольными именами и паролями. В результате должно получиться примерно так, как показано на рисунке. По окончании настроек закрыть окно свойств сервера ПК.

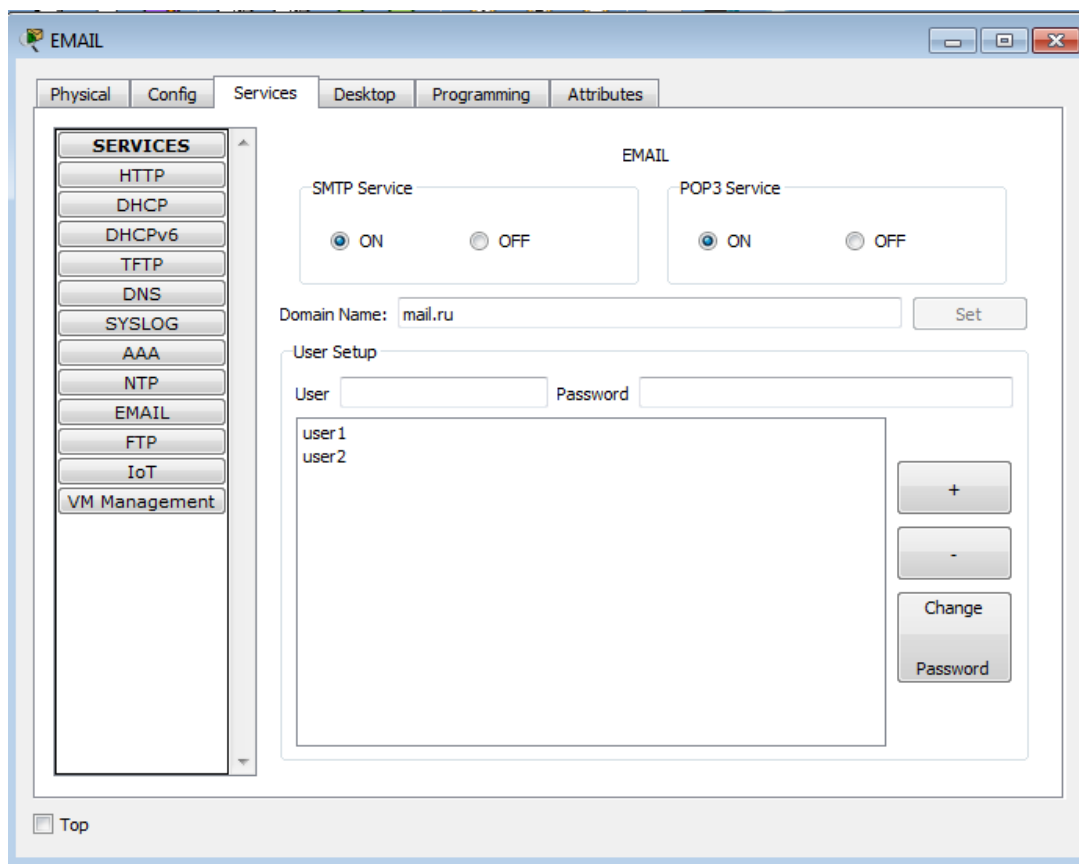


Рисунок 14 – Настройка почтового сервиса

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 15.

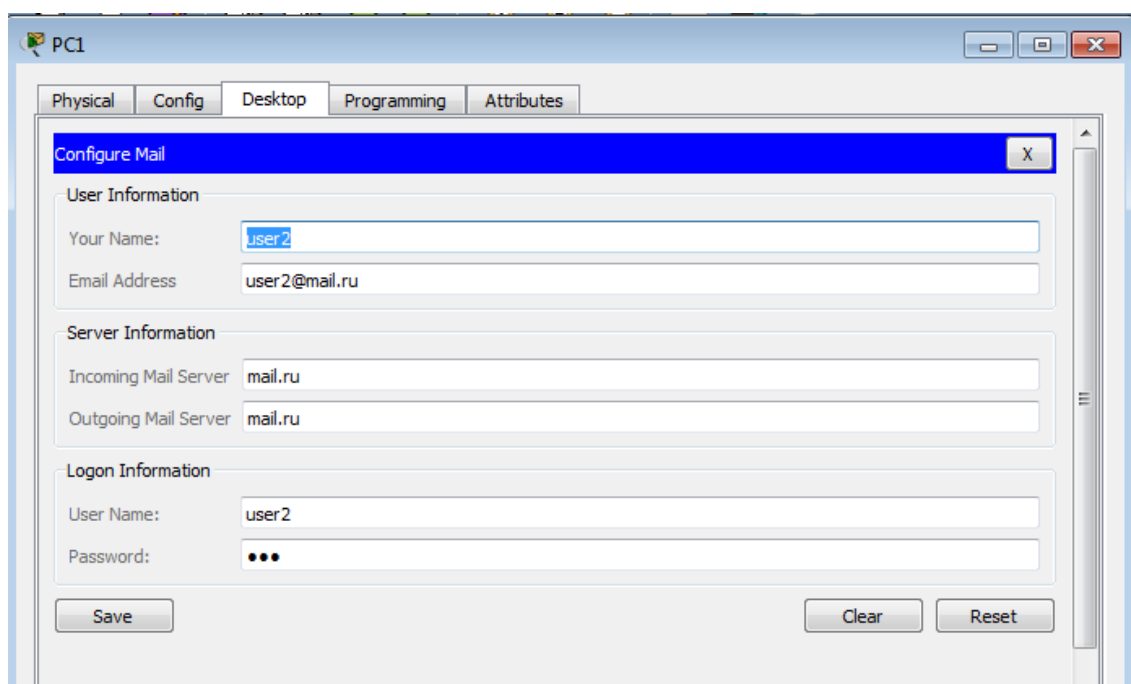


Рисунок 15 – Настройка клиентской части

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*.

Затем перейти на второй ПК, открыть на нем MAIL BROWSER и принять почту. Фактом получения почты служит таблица входящих писем, как на рисунке 16.

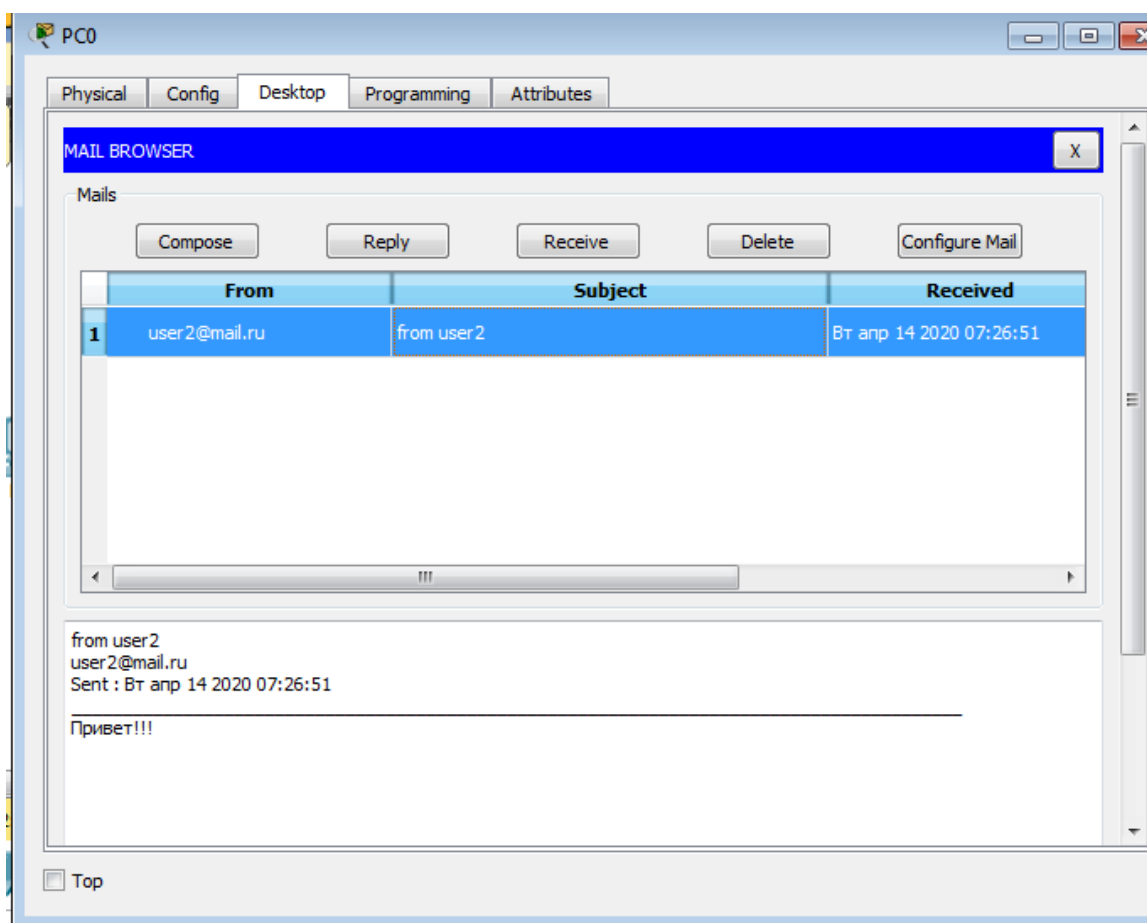


Рисунок 16 – Таблица входящих писем

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.

Содержание отчета:

1. Окончательная построенная схема сети с четырьмя серверами, причем каждый сервер должен иметь название (например, WEB, DNS, MAIL и т.п.), а также IP-адрес. На клиентских ПК в названии IP-адреса указывать не нужно, т.к. они присваиваются автоматически.
2. Скрины работы приложения с результатами проверки работы каждого сервера.
3. Скрин, подтверждающий факт приема сообщения через почтовый инструмент.

4. При наличии нерешенных проблем – дополнительные скрины по ситуации

5. Абсолютно все скрины должны быть прокомментированы, безымянные не будут учитываться.

6. Ответы на контрольные вопросы

### **Контрольные вопросы**

1. Можно ли в среде Cisco Packet Tracer симитировать сетевой шлюз, выполняющий функцию межсетевого экрана между двумя разными сетями?

2. Какие из рассмотренных серверов можно совмещать на одной аппаратной платформе, а какие нежелательно?

3. Можно ли в среде Cisco Packet Tracer симитировать домен-контроллер локальной сети?

4. Какие типы серверов можно реализовать на базе Windows Server 2012 Standard?

## **Практическое занятие № 7. Маршрутизация в сетях TCP/IP**

Цель работы – Изучение процесса передачи пакетов между различными IP сетями.

### **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 не скольких коммутаторов.

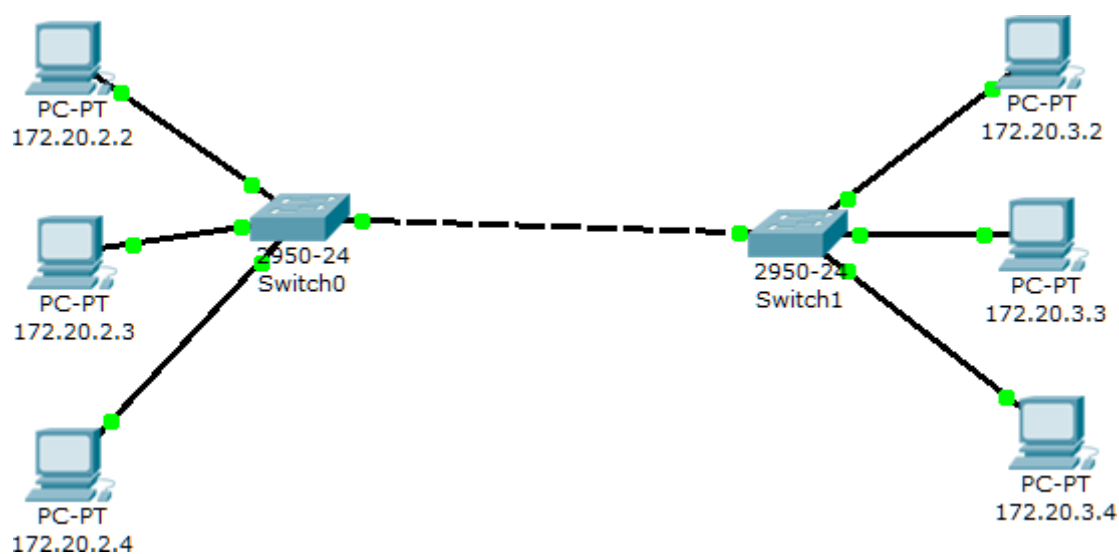


Рисунок 17 – Пример сети без маршрутизатора

На рисунке 17 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 18.

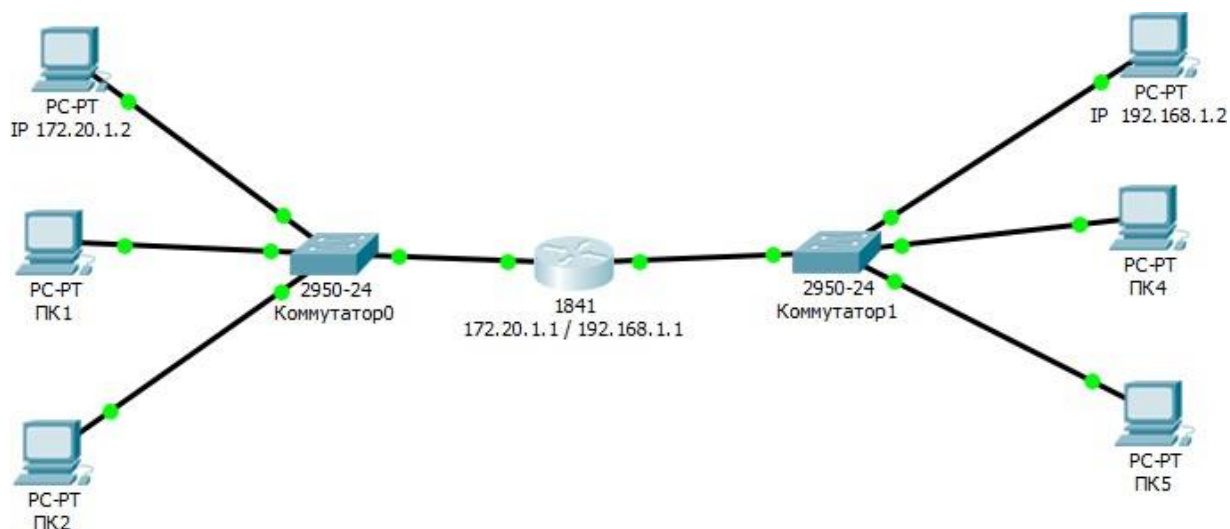


Рисунок 18 – Пример сети с роутером

Просто поместить роутер между двумя коммутаторами недостаточно для того, чтобы сеть заработала в полном объеме. Необхо-

можно 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.

### **Задания для практического занятия:**

Для выполнения работы следует изучить теоретический материал по маршрутизации, после перейти к реализации следующих структур, указанных ниже. Каждый этап нужно отобразить в отчете с комментариями.

#### *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. Настроить таблицу маршрутизации, в которой будет указано, в какой роутер нужно направить пакет, чтобы он добрался до заданной сети.

3. 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. Пример настройки портов роутеров приведен на рисунке 19.



## Практическое занятие № 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 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 20.

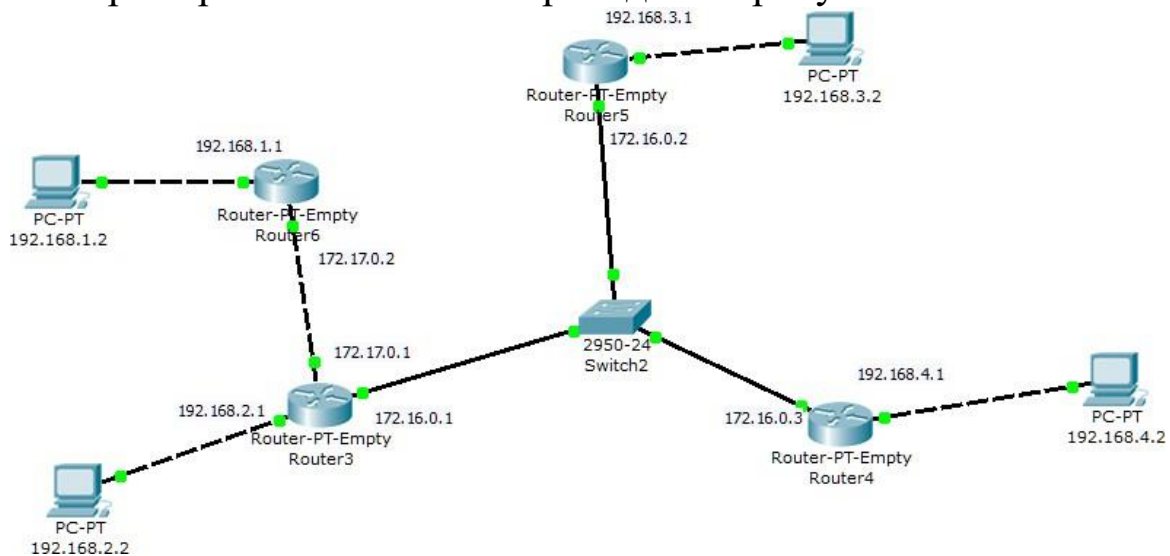


Рисунок 20 – Топология сети

Для задания настройки протокола RIP необходимо лишь указать, адреса подсетей, к которым подключен роутер. Т.е. 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 обмениваются нуж-

ными данными. В результате этого обмена на всех роутерах в таблице маршрутизации появляются данные обо всех подсетях, доступных в существующей сети.

### **Задания по практической работе:**

Результатом практической работы является отчет, в котором должны быть приведены таблицы маршрутизации, сформированные маршрутизаторами без участия администратора.

Для выполнения практической работы студент должен изучить приведенный ниже теоретический материал. Отчет сдается в распечатанном и электронном (файл Word) видах.

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

2. Описать принципиальные различия сети из практической работы 7 с изменённой (динамической) в виде таблицы.

3. Ответить на контрольные вопросы.

### **Контрольные вопросы**

1. Что такое динамическая маршрутизация
2. Чем отличаются векторные алгоритмы маршрутизации от алгоритмов на основе состояний каналов связей?
3. Что такое метрика маршрута? Зачем она используется?
4. Может ли в таблице маршрутизации быть несколько строк, описывающих путь до одной и той же сети?
5. Зачем в протоколе RIP используются триггерные обновления?

## Самостоятельная работа

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.

Виды самостоятельной работы обучающихся указаны в таблице 3

Таблица 3 – Виды самостоятельной работы

Наименование тем	Виды самостоятельной работы
Аппаратные компоненты компьютерных сетей	Структура стандартов IEEE
	Стандарты в сфере структурированных кабельных систем
Передача данных по сети	Система DNS
	Классовая и бесклассовая IP-адресация
Сетевые архитектуры	Протоколы внешней маршрутизации
	Автономные системы

## Список литературы

1. Компьютерные сети : учебник для среднего профессионального образования по специальностям 09.02.06 "Сетевое и системное администрирование", 09.02.07 "Информационные системы и программирование" / В. В. Баринов, И. В. Баринов, А. В. Пролетарский, А. Н. Пылькин ; В. В. Баринов, И. В. Баринов, А. В. Пролетарский, А. Н. Пылькин. – 4-е изд. испр. и доп. – Москва : Академия, 2021. – 192 с. с. – URL: <https://academia-moscow.ru/reader/?id=551458> (дата обращения: 05.04.2024). – Текст : электронный.
2. Максимов, Н. В. Компьютерные сети : Учебное пособие / Н. В. Максимов, И. И. Попов. – Москва : НИЦ ИНФРА - М, 2023 . – 464 с . – ISBN 978-5-00091-454-0 . – URL : <https://znanium.com/catalog/document?id=428554> (дата обращения: 05.04.2024). – Текст : электронный.
3. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры : Учебник / А. В. Назаров, А. Н. Мельников В. П. Енгальчев. – Москва : НИЦ ИНФРА-М, 2023. – 360 с. – ISBN 978-5-906923-06-6. – URL: <https://znanium.com/catalog/document?id=428836> (дата обращения: 05.04.2024). – Текст : электронный.
4. Кистрин, А. В. Технологии физического уровня передачи данных : Учебник / А. В. Кистрин, Б. В. Ефимов А. И. Устюков Д. И. Костров. – Москва : НИЦ ИНФРА-М, 2023. – 208 с. – ISBN 978-5-906818-37-9. – URL: <https://znanium.com/catalog/document?id=428837> (дата обращения: 05.04.2024). – Текст : электронный.