Министерство образования Красноярского края

Краевое государственное бюджетное профессиональное образовательное

учреждение «Красноярский колледж радиоэлектроники и информационных технологий»



**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ**

По профессиональному модулю \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ОП.07 Основы компьютерные сетей

Курс \_\_\_\_

1

Для специальности (код и наименование)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

09.02.08 Интеллектуальные интегрированные системы

Красноярск, 2025

Методические рекомендации составлены:

Преподавателем высшей категории КГБПОУ СПО «ККРИТ» Е.В. Харитоновой

Преподавателем высшей категории КГБПОУ СПО «ККРИТ» Л.В. Шайхутдиновой

Преподавателем первой категории КГБПОУ СПО «ККРИТ» К.В. Савельевой

РАССМОТРЕНО

на заседании цикловой комиссии преподавателей

профессионального цикла информационно-технического профиля

Протокол №\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2025 г.

Председатель ЦК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е.В. Харитонова

Ответственный редактор: зам. директора по учебной работе М.А. Полютова

Одобрено Методическим советом КГБПОУ СПО «ККРИТ»

протокол № \_\_ от «\_\_\_» \_\_\_\_\_\_ 2025 г.

Председатель методического совета

Зам. директора по УР М.А. Полютова

Содержание

Пояснительная записка

Перечень практических работ

Методические указания для студентов по выполнению практических занятий

## ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические указания по выполнению практических занятий по предмету ОП.07 Основы компьютерных сетей разработаны с целью оказания помощи студентам специальности 09.02.08 Интеллектуальные интегрированные системы и преподавателям по организации практических занятий по изучаемой дисциплине, в соответствии с требованиями федерального государственного стандарта среднего профессионального образования.

Методические разработка включает в себя краткие теоретические сведения, указания по выполнению практических работ, контрольные вопросы, формы контроля.

Программой учебной дисциплины ОП.07 Основы компьютерных сетей предусмотрено проведение практических занятий в количестве **34 часа** по специальности:

09.02.08 Интеллектуальные интегрированные системы.

В результате освоения учебной дисциплины обучающийся **должен уметь:** Организовывать и конфигурировать Основы компьютерных сетей; Строить и анализировать модели компьютерных сетей;

Эффективно использовать аппаратные и программные компоненты компьютерных сетей при решении различных задач;

Выполнять схемы и чертежи по специальности с использованием прикладных программных средств;

Работать с протоколами разных уровней (на примере конкретного стека протоколов: TCP/IP, IPX/SPX);

Устанавливать и настраивать параметры протоколов; Обнаруживать и устранять ошибки при передаче данных;

В результате освоения учебной дисциплины обучающийся **должен знать:**

Основные понятия компьютерных сетей: типы, топологии, методы доступа к среде передачи;

Аппаратные компоненты компьютерных сетей; Принципы пакетной передачи данных; Понятие сетевой модели;

Сетевую модель OSI и другие сетевые модели;

Протоколы: основные понятия, принципы взаимодействия, различия и особенности распространенных протоколов, установка протоколов в операционных системах;

Адресацию в сетях, организацию межсетевого воздействия.

В результате освоения учебной дисциплины ОП.07 «Компьютерные сети» у выпускника должны быть сформированы следующие компетенции:

|  |  |
| --- | --- |
| ОК 01. | Выбирать способы решения задач профессиональной деятельности,  применительно к различным контекстам. |
| ОК 02. | Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач  профессиональной деятельности. |
| ОК 04. | Эффективно взаимодействовать и работать в коллективе и команде |
| ОК 05. | Осуществлять устную и письменную коммуникацию на государственном языке  Российской Федерации с учетом особенностей социального и культурного контекста. |
| ОК 09. | Пользоваться профессиональной документацией на государственном и  иностранном языках. |
| ПК 1.4 | Выполнять работы по вводу в эксплуатацию и сопровождению системы. |
| ПК 2.4 | Консультировать заинтересованных лиц и пользователей по  требованиям и работе с функциями системы. |

Характерная черта практических занятий – индивидуальное выполнение заданий, самостоятельное приобретение знаний. В связи с этим предусмотрены работы по всем основным разделам курса. Перед выполнением практической работы обучающийся получает опережающее теоретическое домашнее задание. На занятии объясняются вопросы, уточняются определения, которые помогают выполнению заданий. Обучающийся может просмотреть запись объяснения любой примерной работы по всем темам. И только после этого обучающийся приступает к выполнению практической работы.

При выполнении работы обучающийся должен самостоятельно изучить методические рекомендации по проведению практической работы, подготовить ответы на контрольные вопросы. Все практические задания выполняются за компьютером, теоретические вопросы сдаются устно или письменно.

|  |  |
| --- | --- |
| **№п.п.** | **НАЗВАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ** |
| 1. | **Практическая работа №1** Построение схемы компьютерной сети. |
| 2. | **Практическая работа №2** Логическое планирование локальной сети. |
| 3. | **Практическая работа №3** Аппаратные средства и оборудование ЛВС |
| 4. | **Практическая работа №4** Установка Cisco Packet Tracer (CPT). Изучение интерфейса. Создание простейшей сети |
| 5. | **Практическая работа №5** Создание и исследование сетей с использованием концентратора и коммутатора в Cisco Packet Tracer |
| 6. | **Практическая работа №6** Подключение к сетевому оборудованию в Cisco Packet Tracer |
| 7. | **Практическая работа №7** Использование технологии VLAN в Cisco Packet Tracer |
| 8. | **Практическая работа №8** Устранение петель - STP в Cisco Packet Tracer |
| 9. | **Практическая работа №9** Агрегация каналов - EtherChannel в Cisco Packet Tracer |
| 10. | **Практическая работа №10** Построение одноранговой сети. Создание общих сетевых ресурсов. |
| 11. | **Практическая работа №11** Организация сетевого шлюза (Настройка программного маршрутизатора) |
| 12. | **Практическая работа №12** Настройка протоколов TCP/IP в операционных системах» (работа с диагностическими утилитами протокола ТСР/IР, решение проблем с TCP/IP). |
| 13. | **Практическая работа № 13** Преобразование форматов IP-адресов. Расчет IP- адреса и маски подсети. |
| 14. | **Практическая работа №14** Настройка удаленного доступа к компьютеру |
| 15. | **Практическая работа №15** Оборудование беспроводных сетей |
| 16. | **Практическая работа №16** Настройка свойств Web-браузера. |

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ СТУДЕНТОВ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ**

**Практическая работа №1** Построение схемы компьютерной сети.

1. Наименование: Построение схемы компьютерной сети.
2. Продолжительность проведения: *2 часа.*
3. **Цель работы:** построение схемы компьютерной сети с помощью специализированной программе
4. **Оборудование:** ПК, ПО специализированной программе

### КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

Программный продукт Visio

Программный продукт Visio является разработкой компании VisioCorporation, которая была куплена в 2000-м году компанией Microsoft, а программа получила название MicrosoftVisio.

* VisioStandard – служит для создания бизнес-диаграмм, в том числе блок-схем, структурных схем, графиков работ, и др.
* VisioProfessional – средство моделирования и документирования бизнес- процессов, проектирования и построения схем сетей, планов помещений, схематических чертежей, предназначенных для IT-специалистов, инженеров, технических руководителей и разработчиков программного обеспечения.

Расширенные средства создания схем сетей выделены в дополнительный продукт – MicrosoftVisioEnterpriseNetworkTools, который предоставляет возможности автоматического создания схем сетей, документирование структур каталогов ActiveDirectory, и др.

Область применения

Программный продукт MicrosoftVisio (в дальнейшем - MS Visio) в последнее время активно завоевывает рынок, выступая в качестве эталона деловой графики.

Для рисования на компьютере существуют десятки различных приложений. Это и простейшие графические редакторы типа Paint, и профессиональные системы типа CorelDraw. Visio не заменяет существующих, особенно сильно развитых систем. Но в этой ситуации появляется много примеров, когда инженер, использующий скажем AutoCAD, начинает дополнительно применять MS Visio. Кроме того, существуют области, для которых нет специализированных продуктов кроме MS Visio, например, рисование химических структурных диаграмм.

Для IT-специалистов и разработчиков программного обеспечения особый интерес представляют такие функции пакета MS Visio:

* построение планов зданий и инженерных коммуникаций;
* разработка схем компьютерных сетей;
* разработка диаграмм баз данных;
* проектирование карт web-сайтов.

### ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Задание 1.

Запустить *MicrosoftVisio* из группы программ *Microsoft Office.*

Запустить и ознакомиться с разделами справочной системы для работы с

*MicrosoftVisio.* Открыть интересующий Вас раздел справки и изучить его.

Просмотреть образцы шаблонов схем, доступных для использования. Изучить интерфейс программы.

Добавить панели инструментов **Формат текста** и **Формат фигуры (**меню **Вид** →

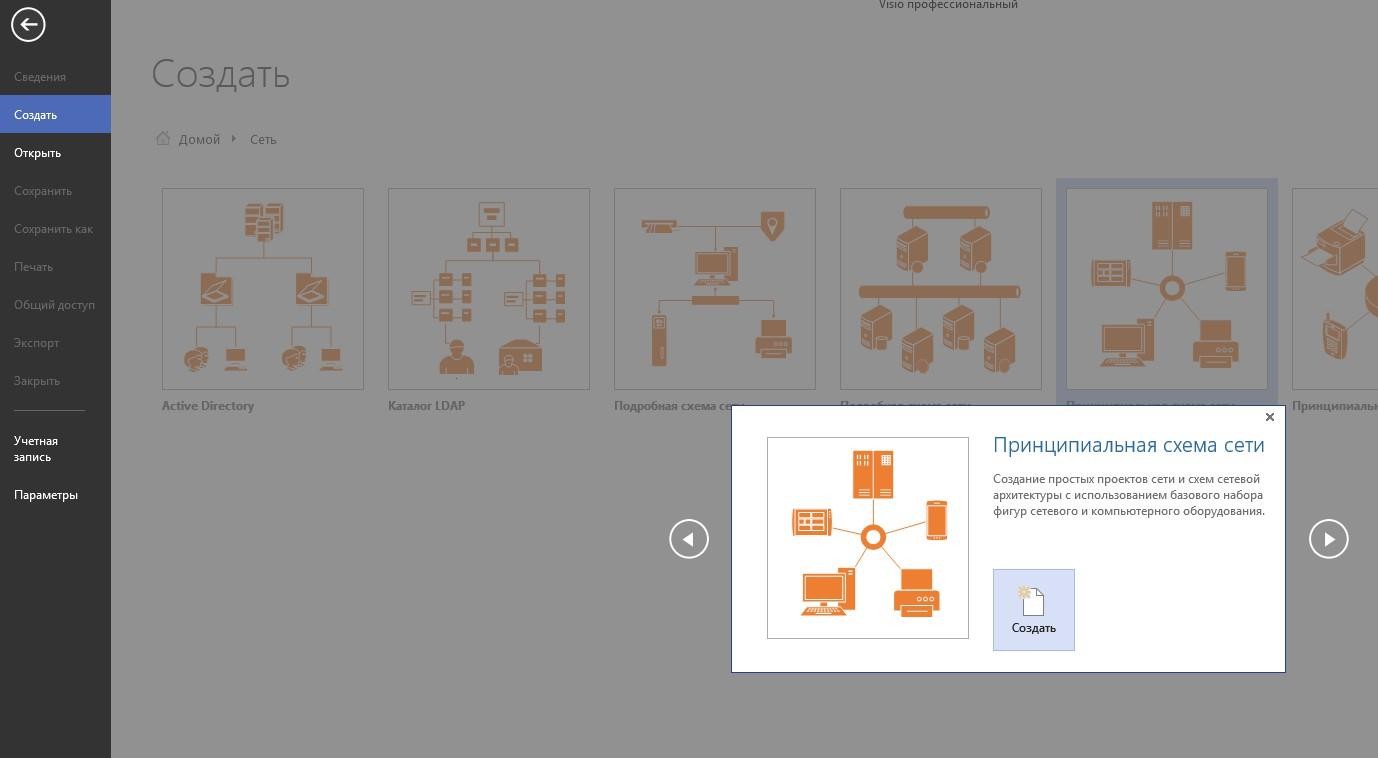
## Панели инструментов).

Для добавления необходимой фигуры следует выбрать меню Файл → Фигуры → группа фигур (дополнительные фигуры).

Задание 2.

Программы Visio 2016 включают шаблон схемы сети, который называется Принципиальная схема сети. На основе этого шаблона можно построить схему простой корпоративной сети, что мы и продемонстрируем на примере.

Для этого щелкнем на вкладке Файл и выберем вкладку Создать. Щелкнем на Категории, затем на Сеть и дважды на миниатюре Принципиальная схема сети.



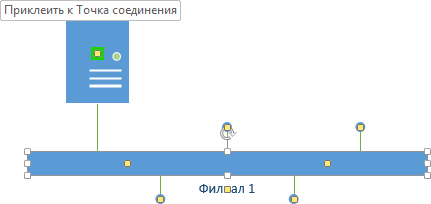
Перетащим фигурку Ethernet из набора элементов Сеть и периферийные устройства на страницу документа и сбросим ее по вертикали по центру чуть правее левого поля страницы.

Перетащим маркер изменения размера с правого края фигуры Ethernet вправо так, чтобы ее ширина стала 100 мм.

Не снимая выделение с фигуры Ethernet, введем Филиал 1 в качестве подписи для сегмента сети, затем щелкнем на любой точке фона страницы.

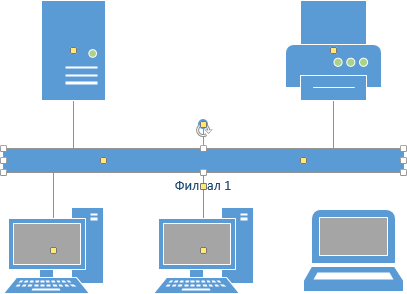
Перетащим фигуру Сервер на страницу и поместим ее над фигурой Ethernet ближе к левому краю последней.

Щелкнем один раз на фигуре Ethernet, чтобы выделить ее, а затем перетащим любой и желтых управляющих маркеров в центр сервера, пока вокруг управляющего маркера не появится зеленый квадрат.



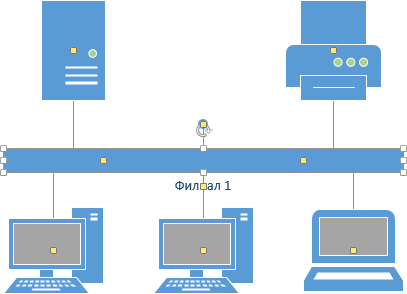
Перетащим фигуру Принтер над фигурой Ethernet ближе к ее правому краю, а затем соединим принтер с сетью, перетащив и приклеив желтый управляющий маркер к принтеру.

Перетащим на страницу две фигуры ПК и одну фигуру Ноутбук из набора Компьютеры и мониторы и сбросим их под фигурой Ethernet.

Перетащим желтый управляющий маркер к каждой из фигур ПК.

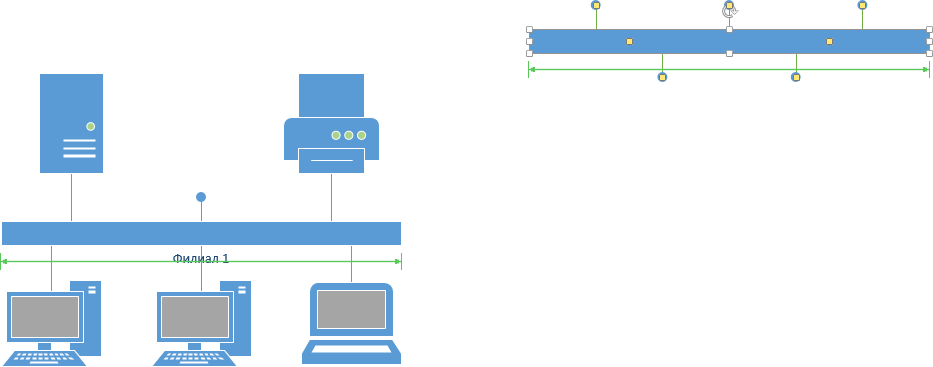
Сейчас только один управляющий маркер остается под фигурой Ethernet, но его назначение – перемещение блока текста. А, следовательно, его нельзя использовать для привязки ноутбука к сети.

Перетащим управляющий маркер из середины фигуры Ethernet и приклеим его к ноутбуку. Теперь ноутбук подключен к сегменту Ethernet, но все еще доступны дополнительные управляющие маркеры, как показано на рисунке.



Перетащим другую фигуру Ethernet в верхний правый угол страницы, оставив достаточно места для того, чтобы над ней можно было разместить другие фигуры.

Перетащим левый маркер изменения размера влево, чтобы сделать сегмент Ethernet шире. Продолжим перетаскивать, пока не появится двунаправленная стрелка, показывая, что новый сегмент сети имеет такую же длину, как и уже существующий на странице.

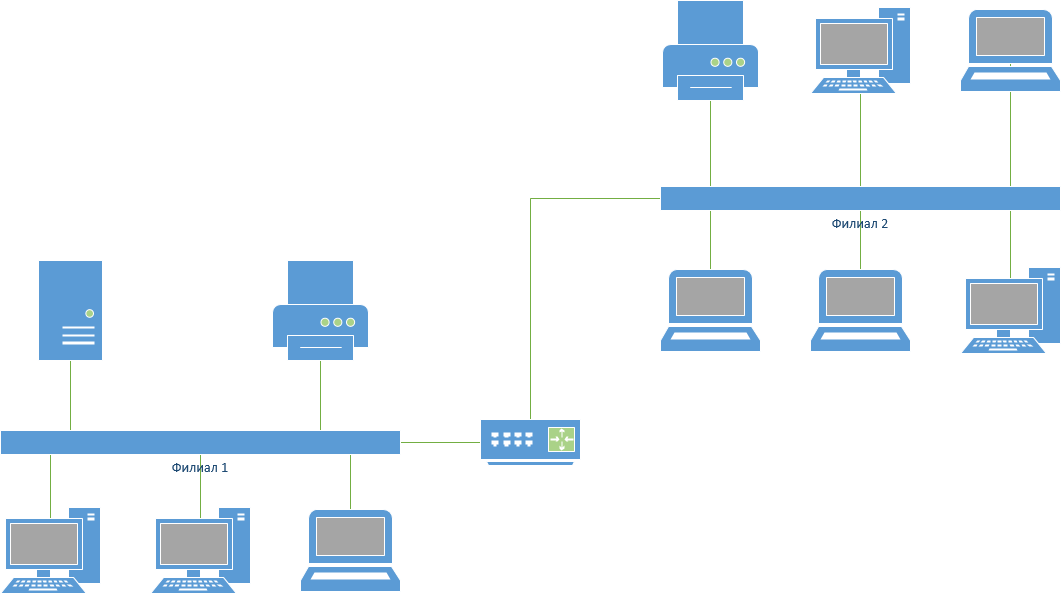


Не снимая выделения с фигуры Ethernet, введем Филиал 2 и щелкнем на пустом месте страницы.

Перетащим фигуру Принтер, две фигуры ПК и три фигуры Ноутбук и соединим их с новым сегментом сети.Перетащим фигуру Маршрутизатор из набора элементов Сеть и переферийные устройства и разместим ее по центру страницы.

Перетащим оставшийся неиспользованный управляющий маркер из фигуры сети Филиал 1 и приклеим его к маршрутизатору.

Перетащим управляющий маркер из сети Филиал 2 и приклеим его к маршрутизатору. Соединительная линия изгибается, когда мы перетаскиваем управляющий маркер к маршрутизатору – она ведет себя как динамическая соединительная, а не как простая линия. Получившаяся схема сети представлена на следующем рисунке.



Контрольные вопросы:

1. Назначение и возможности *Microsoft Office Visio*.
2. Какие способы настройки окна и панели инструментов программы

*MsVisio* вы знаете?

1. Какие группы фигур программы *MsVisio* используются для создания схем и других графических изображений?
2. Какие инструменты для работы с текстом доступны в программе *MsVisio*?

## Практическое занятие №2

1. Наименование: Логическое планирование локальной сети.
2. **Цель работы:** Изучить структуру сети.
3. **Оборудование:** ПК, интернет.

# КРАТКАЯ ТЕОРИЯ

Под логической структурой сети понимается ее организация на 3-м и выше уровнях модели OSI, т.е. сетевые протоколы, адресация, взаимодействие рабочих станций с серверами. В качестве основного сетевого протокола в вычислительной сети предприятия используется протокол IP. Адреса на сетевом уровне для рабочих станций задаются динамически по протоколу DHCP. Логическая топология представляет собой логическую структуру сети. Такая схема определяет, как элементы сети взаимодействуют между собой, как передается информация в сети, и какой путь она при этом преодолевает

В топологии «логическое кольцо» - неразрывное кольцо, с помощью которого передается информация между ПК, в топологии сети обеспечивается соединением всех узлов каналами связи. Благодаря этому, вся информация движется по кругу в одном направлении. На рис.3.2 представлена логическая топология предприятия.

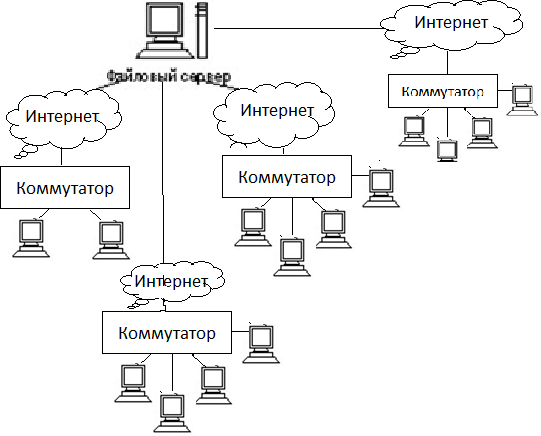


Рис.1- логическая топология предприятия Планирование физической структуры сети

При проектировании локально-вычислительной сети одним из основных моментов является учет факторов, влияющих на выбор кабельной системы. Перечислим некоторые основные факторы:

* + требуемая пропускная способность, скорость передачи в сети
  + размер сети, то есть сколько будет в сети рабочих станций;
  + требуемый набор служб (передача данных, речи, мультимедиа и т.д.), который необходимо организовать;
  + требования к уровню шумов и помехозащищенности;
  + общая стоимость проекта, включающая покупку оборудования, монтаж и последующую эксплуатацию.

Можно выделить несколько основных кабельных средств передачи данных в ЛВС:

* + витая пара;
  + коаксиальный кабель;
  + оптоволокно.

Было принято решение использовать экранированную витую пару, так как она соответствует всем основным, предъявляемым к кабельной системе:

* + гибкость;
  + скорость передачи данных достаточная для ООО «Промагро»
  + простота монтажа и обслуживания;
  + безопасность передачи данных;
  + недорогая себестоимость.

Технико-экономическое обоснование Выбор сетевой операционной системы

При проектирование сети в трёхэтажном здание, где находится управление

ООО

«Промагро» была выбрана сетевая операционная система Windows Server Standard

R2 2012.

Выбранная операционная система Windows Server Standard R2 2012 обладает следующими качествами:

* + позволяет работать с высокими нагрузками;
  + обеспечивает резервное восстановление и бесперебойное функционирование всех служб;
  + обладает высокой надежностью, легкой доступностью и масштабируемостью;
  + предоставляет средства для упрощения управления и администрирования;
  + предоставляет расширенную платформу приложений для быстрого создания решений для обеспечения связей между сотрудниками, партнерами, системами и клиентами путем предоставления встроенного веб-сервера и сервера потоков мультимедиа, обеспечивающих быстрое, простое и надежное создание динамических веб-узлов интрасети Internet
  + возможность получения сотрудниками доступа к информации не зависимо от инфраструктуры, сетей, устройств и приложений с которыми они работают;
  + обеспечивает непрерывный и безопасный доступ к ресурсам компании и корпоративной сети, упростив при этом процесс идентификации пользователей и управление учетными данными на локальных и облачных ресурсах;
  + имеется возможность удаленного доступа к серверу. Выбор сетевого аппаратного обеспечения

Наиболее дешевый вариант сервера базируется на ПК общего назначения с достаточно большим объемом оперативной памяти.

Кроме сервера, необходимо использовать 13 ПК (по количеству рабочих мест). Для оптимального сочетания стоимости (ремонтопригодности) и качества работы (привлечения клиентов) предлагается использовать следующую конфигурацию каждого ПК.

### ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Задание 1.

1. Описать одноранговую локальную сеть с топологией линейная шина.
2. Произвести расчёт стоимости подключения к локальной сети. Расчёт производить согласно ценам на соответствующие товары в магазине (использовать ресурс интернет) и с учётом схемы расположения компьютеров в офисе.
3. Проанализируйте описание локальной сети и сделайте выводы.

|  |  |  |
| --- | --- | --- |
| Схема локальной сети |  | |
| Недостатки |  | |
| Преимущества |  | |
| Количество компьютеров в сети |  | |
| Оборудование, необходимое для создания сети и его стоимость | оборудование | стоимость |
|  |  |

|  |  |
| --- | --- |
| Общая стоимость создания локальной сети |  |
| Выводы: |  |

Задание 2.

1. Описать одноранговую локальную сеть с топологией звезда.
2. Произвести расчёт стоимости подключения к локальной сети. Расчёт производить согласно ценам на соответствующие товары в магазине (использовать ресурс интернет) и с учётом схемы расположения компьютеров в офисе.
3. Проанализируйте описание локальной сети и сделайте выводы.

|  |  |  |
| --- | --- | --- |
| Схема локальной сети |  | |
| Недостатки |  | |
| Преимущества |  | |
| Количество компьютеров в сети |  | |
| Оборудование, необходимое для создания сети и его | оборудование | стоимость |
| стоимость |  |  |
| Общая стоимость создания локальной сети |  | |
| Выводы: |  | |

Задание 3.

1. Описать локальную сеть на основе сервера.
2. Произвести расчёт стоимости подключения к локальной сети. Расчёт производить согласно ценам на соответствующие товары в магазине (использовать ресурс интернет) и с учётом схемы расположения компьютеров в офисе.
3. Проанализируйте описание локальной сети и сделайте выводы.

|  |  |  |
| --- | --- | --- |
| Схема локальной сети |  | |
| Недостатки |  | |
| Преимущества |  | |
| Количество компьютеров в сети |  | |
| Оборудование, необходимое для создания сети и его стоимость | оборудование | стоимость |
|  |  |
| Общая стоимость создания локальной сети |  | |
| Выводы: |  | |

Задание 4.

1. Описать беспроводную локальную сеть для портативных компьютеров (ноутбуков).
2. Произвести расчёт стоимости подключения к локальной сети. Расчёт производить согласно ценам на соответствующие товары в магазине (использовать ресурс интернет) и с учётом схемы расположения компьютеров в офисе.
3. Проанализируйте описание локальной сети и сделайте выводы.

|  |  |  |
| --- | --- | --- |
| Схема локальной сети |  | |
| Недостатки |  | |
| Преимущества |  | |
| Количество компьютеров в сети |  | |
| Оборудование, необходимое для создания сети и его стоимость | оборудование | стоимость |
|  |  |
| Общая стоимость создания локальной сети |  | |
| Выводы: |  | |

Контрольные вопросы:

1. Какие топологии сетей вы знаете?
2. Чем отличается локальная сеть от глобальной?
3. Может ли быть компьютер одновременно клиентом и сервером?
4. По вашему мнению какая из топологий сети наиболее подходит образовательному учреждению? почему?

**Практическая работа №3** Аппаратные средства и оборудование ЛВС

**Цель работы:** ознакомиться с основными аппаратными средствами и оборудованием ЛВС.

## Краткие теоретические сведения

### Локальные вычислительные сети

Под ЛВС(англ. LAN - Lokal Area Network) понимают совместное подключение нескольких отдельных компьютерных рабочих мест (рабочих станций) к единому каналу передачи данных.

ЛВС – аппаратно-программное решение в которомнесколько компьютерных систем связаны друг с другом с помощьюсоответствующих средств коммуникаций.

Преимущества, получаемые при сетевом объединении персональных компьютеров в виде внутрипроизводственной вычислительной сети:

* + *Разделение ресурсов.*

Позволяет экономно использовать ресурсы, например, управлять периферийными устройствами, такими как лазерные печатающие устройства, со всех присоединенных рабочих станций.

* + *Разделение данных.*

Предоставляет возможность доступа и управления базами данных с периферийных рабочих мест, нуждающихся в информации.

* + *Разделение программных средств.*

Разделение программных средств, предоставляет возможность одновременного использования централизованных, ранее установленных программных средств.

* + *Разделение ресурсов процессора.*

Возможно использование вычислительных мощностей для обработки данных другими системами, входящими в сеть. Предоставляемая возможность заключается в том, что на имеющиеся ресурсы не “набрасываются” моментально, а только лишь через специальный процессор, доступный каждой рабочей станции.

* + *Многопользовательский режим.*

Многопользовательские свойства системы содействуют одновременному использованию централизованных прикладных программных средств, ранее установленных и управляемых,например, если пользователь системы работает с другим заданием,то текущая выполняемая работа отодвигается на задний план.

Локальные вычислительные сети подразделяются на два кардинально различающихся класса:

* + Одноранговые (одноуровневые или Peer to Peer).
  + Иерархические (многоуровневые) сети.

### Одноранговая сеть.

Одноранговые, децентрализованные или пиринговые (от англ. peer-to-peer, P2P — один на один, с глазу на глаз) сети - это компьютерные сети, основанные на равноправии участников. В таких сетях отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и сервером. В отличие от архитектуры клиент-сервер, такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов.

Все компьютеры равноправны:

* + Нет иерархии среди компьютеров.
  + Нет выделенного сервера.
  + Как правило, каждый компьютер функционирует и как клиент и как сервер. Одноранговую сеть называют так же рабочей группой.

Рабочая группа – это небольшой коллектив, поэтому в одноранговой сети не более

10 компьютеров. Все пользователи самостоятельно решают, какие данные на своем компьютере сделатьдоступными для всех.

Преимущества:

* Одноранговые сети относительно просты.
* Одноранговые сети дешевле сетей на основе сервера, нотребуют более мощных и дорогих компьютеров.
* Поддержка одноранговых сетей встроена в такие ОС как Windows’95, Windows NT Workstation, OS/2, дополнительного программного обеспечения не требуется

### Иерархическая сеть

Иерархическая сеть, сеть с выделенным сервером (англ. Сlient/Server network) — это локальная вычислительная сеть, в которой сетевые устройства централизованы и управляются одним или несколькими серверами. Индивидуальные рабочие станции или клиенты (такие, как ПК) должны обращаться к ресурсам сети через сервер(ы).

Сервер - специальный компьютер, на котором хранится информация, совместно используемая различными пользователями.Сервер оптимизирован для быстрой обработки запросов от сетевых клиентов и для управления защитой файлов и каталогов. Из-за большого круга выполняемых задач, серверы в больших сетях специализированы (Серверы баз данных, файл-серверы, контроллеры домена и т.д.)

Преимущества:

* Основным аргументом в пользу сети на основе выделенного сервера является защита данных.
* Благодаря тому, что важная информация сосредоточена на одном или нескольких серверах, нетрудно обеспечить ее регулярное резервное копирование
* Сети на основе сервера могут поддерживать тысячи пользователей.
* Для работы в сети компьютеры пользователей могут быть любых конфигураций, даже самых минимальных.

### Архитектура ЛВС

Каждая ЛВС имеет определенную архитектуру, которая в свою очередь определяется топологией, протоколами, интерфейсами, сетевыми техническими и программными средствами.

*Сетевые программные средства* осуществляют управлениеработой компьютерной сети и обеспечивают соответствующий интерфейс пользователям. К сетевым программным средствам относятся сетевые операционные системы и вспомогательные сервисные программы.

Под *сетевыми техническими средствами* подразумевают устройства, обеспечивающие объединение компьютеров в единую компьютерную сеть. К этим устройствам относятся сетевые контроллеры, узлы коммутации и др.

*Интерфейсы* – средства сопряжения функциональных элементов сети. Следует обратить внимание, что в качестве функциональных элементов могут выступать как отдельные устройства, так и программные модули. В соответствии с этим различают аппаратные и программные интерфейсы.

*Протоколы* представляют собой правила взаимодействия функциональных элементов сети.

### Сетевые топологии

Сетевая топология — описание конфигурации сети, схема расположения и соединения сетевых устройств.

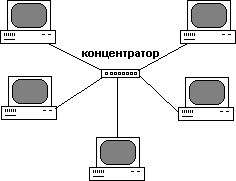
Сетевая топология может быть

* + - * физической — описывает реальное расположение и связимежду узлами сети.
      * логической — описывает хождение сигнала в рамкахфизической топологии.

Существует множество способов соединения сетевых устройств, из них можно выделить пять базовых топологий: шина, кольцо, звезда, ячеистая топология и решётка. Остальные способы являются комбинациями базовых. В общем случае такие топологии называются смешанными или гибридными, но некоторые из них имеют собственные названия, например «Дерево».

### Топология типа звезда

Звезда — базовая топология компьютерной сети, в которой все компьютеры сети присоединены к центральному узлу (обычно сетевой концентратор), образуя физический сегмент сети. Подобный сегмент сети может функционировать как отдельно, так ив составе сложной сетевой топологии (как правило "дерево").



*Рис 1. Топология Звезда*

Рабочая станция, которой нужно послать данные, отсылает их на концентратор, а тот определяет адресата и отдаёт ему информацию. В определённый момент времени только одна машина в сети может пересылать данные, если на концентратор одновременно приходят два пакета, обе посылки оказываются не принятыми и отправителям нужно будет подождать случайный промежуток времени, чтобы возобновить передачу данных.

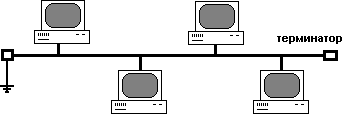
Достоинства:

* + - * выход из строя одной рабочей станции не отражается наработе всей сети в целом;
      * хорошая масштабируемость сети;
      * лёгкий поиск неисправностей и обрывов в сети;
      * высокая производительность сети (при условии правильного проектирования);
      * гибкие возможности администрирования.Недостатки:
      * выход из строя центрального концентратора обернётся неработоспособностью сети (или сегмента сети) в целом;
      * для прокладки сети зачастую требуется больше кабеля, чем для большинства других топологий;
      * конечное число рабочих станций в сети (или сегменте сети) ограничено количеством портов в центральном концентраторе.

Топология Звезда - одна из наиболее распространённых топологий, поскольку проста в обслуживании. В основном используется в сетях, где носителем выступает кабель витая пара. UTP категория 3 или 5.

### Шинная топология.

Топология типа шина, представляет собой общий кабель (называемый шина или магистраль), к которому подсоединены все рабочие станции. На концах кабеля находятся терминаторы, для предотвращения отражения сигнала.

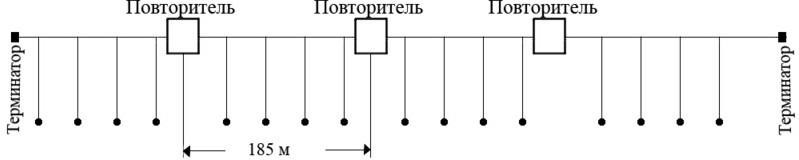


*Рис 2. Топология шина*

Отправляемое рабочей станцией сообщениераспространяется на все компьютеры сети. Каждая машина проверяет — кому адресовано сообщение и если ей, то обрабатывает его. Для того, чтобы исключить одновременную посылку данных, применяется либо

«несущий» сигнал, либо одиниз компьютеров является главным и «даёт слово» остальным станциям.

При построении больших сетей возникает проблема ограничения на длину связи между узлами, в таком случае сеть разбивают на сегменты. Сегменты соединяются

различными устройствами — повторителями, концентраторами или хабами. Например, технология Ethernet позволяет использовать кабельдлиной не более 185 метров.

*Рис. 3. Использование повторителей*

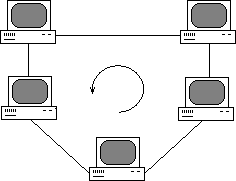
Достоинства:

* + - * Небольшое время установки сети;
      * Дешевизна (требуется меньше кабеля и сетевых устройств);
      * Простота настройки;
      * Выход из строя рабочей станции не отражается на работесети; Недостатки:
      * Любые неполадки в сети, как обрыв кабеля, выход из строятерминатора полностью уничтожают работу всей сети;
      * Сложная локализация неисправностей;
      * С добавлением новых рабочих станций падаетпроизводительность сети. Примером шинной топологии можно считать сегмент компьютерной сети,

использующей коаксиальный кабель в качественосителя и подключенных к этому кабелю рабочих станций. В этом случае шиной будет являться отрезок коаксиального кабеля, к которому подключены компьютеры.

### Кольцевая топология.

Кольцо — базовая топология компьютерной сети, в которой рабочие станции подключены последовательно друг к другу,образуя замкнутую сеть.



*Рис. 4. Кольцевая топология*

В кольце, в отличие от других топологий (звезда, шина), не используется конкурентный метод посылки данных, компьютер в сети получает данные от стоящего предыдущим в списке адресатов и перенаправляет их дальше, если они адресованы не ему. Список адресатов генерируется компьютером, являющимся генератором маркера. Сетевой модуль генерирует маркерный сигнал (обычнопорядка 2-10 байт во избежание затухания) и передает его следующей системе (иногда по возрастанию MAC-адреса). Следующая система, приняв сигнал, не анализирует его, а просто передает дальше. Это так называемый нулевой цикл. Последующий алгоритм работы - пакет данных GRE, передаваемый отправителем адресату начинает следовать по пути, проложенному маркером. если каждая последующая система не является риципиентом то пакет рекурсивно отправляется далее до получателя.

Достоинства:

* + - * Простота установки;
      * Практически полное отсутствие дополнительного оборудования;
      * Возможность устойчивой работы без существенного падения скорости передачи данных при интенсивной загрузке сети, поскольку использование маркера исключаетвозможность возникновения коллизий.

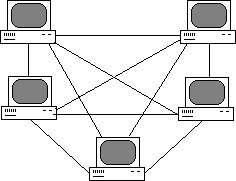
Недостатки:

* + - * Выход из строя одной рабочей станции, и другие неполадки(обрыв кабеля), отражаются на работоспособности всей сети;
      * Сложность конфигурирования и настройки;
      * Сложность поиска неисправностей;

Наиболее широкое применение получила в оптоволоконных сетях. Используется в стандартах FDDI, Token ring.

### Ячеистая топология

Ячеистая топология — соединяет каждую рабочуюстанцию сети со всеми другими рабочими станциями этой же сети. Топология относится к полносвязным, в отличие от других — неполносвязных.



*Рис. 5. Ячеистая топология*

Отправитель сообщения по очереди соединяется с узлами сети, пока не найдёт нужный, который примет у него пакеты данных.

Достоинства:

* + - * надёжность, при обрыве кабеля у компьютера в сети остаётся достаточно путей соединения.Недостатки
      * большая стоимость установки;
      * сложность настройки и эксплуатации;

В проводных сетях данная топология используется редко, поскольку из-за преизбыточного расхода кабеля становится слишком дорогой. Однако, в беспроводных технологиях сети наоснове ячеистой технологии встречаются всё чаще, поскольку затраты на сетевой носитель не увеличиваются и на первый план выходит надёжность сети.

### Древовидная структура ЛВС.

Образуется в основном в виде комбинаций основных топологий вычислительных

сетей.

Основание дерева вычислительной сети располагается в точке (корень), в которой

собираются коммуникационные линии информации (ветви дерева).

Применяются там, где невозможно непосредственное применение базовых сетевых структур в чистом виде.



Рис. 6. Топология дерево

### Физическая передающая среда ЛВС

Физическая передающая среда обеспечивает перенос информации между абонентами вычислительной сети. Для ЛВС она, как правило, представлена тремя типами кабелей: витая пара проводов, коаксиальный кабель, оптоволоконный кабель.

### Витая пара.

Витая пара (англ. twisted pair) — вид кабеля связи,представляет собой одну или несколько пар изолированныхпроводников, скрученных между собой (с небольшим числом витков на единицу длины), покрытых пластиковой оболочкой. Свивание

проводников производится с целью повышения связи проводников одной пары (электромагнитная помеха одинаково влияет на оба провода пары) и последующего уменьшения электромагнитных помех от внешних источников, а так же взаимных наводок при передаче дифференциальных сигналов.

Витая пара — один из компонентов современных структурированных кабельных систем. В настоящее время,благодаря своей дешевизне и лёгкости в установке, является самым распространённым для построения локальных сетей.

Кабель подключается к сетевым устройствам при помощи соединителя RJ45, немного большим, чем телефонный соединитель RJ11.



*Рис. 7. Витая пара.*

В зависимости от наличия защиты — электрически заземлённой медной оплетки или алюминиевой фольги вокруг скрученных пар, определяют разновидности данной технологии.

Незащищенная витая пара:

* неэкранированная витая пара (UTP — Unscreened twisted pair) — экранирование полностью отсутствует;
* фольгированная витая пара (FTP — Foiled twisted pair) — также известна как S/UTP[1] присутствует один общий внешний экран;
* фольгированная экранированная витая пара (SFTP — Shielded Foiled twisted pair) — отличается от FTP наличиемдополнительного внешнего экрана из медной оплетки; Защищенная витая пара:
* защищенная витая пара (STP — Shielded twisted pair) — присутствет экран для каждой пары;
* защищенная экранированная витая пара (S/STP — Screened shielded twisted pair) — отличается от STP наличием дополнительного общего внешнего экрана.

Экранирование обеспечивает защиту от электромагнитных наводок как внешних, так и внутренних.

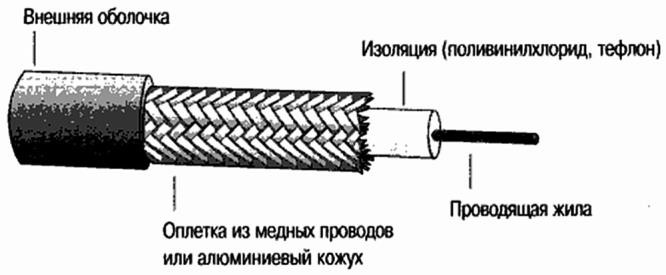
При использовании 100 мегабитного соединения используются только 2 из 4-х пар.

### Коаксиальный кабель

Коаксиальный кабель (от лат. co — совместно и axis — ось,то есть «соосный») — вид электрического кабеля. Состоит из двух цилиндрических проводников, соосно вставленых один в другой. Чаще всего используется центральный медный проводник, покрытый пластиковым изолирующим материалом, поверх которогоидёт второй проводник

— медная оплётка или алюминиевая фольга с оплёткой из медных луженых проволок.

Основной характеристикой кабеля является волновое сопротивление. В зависимости от этой величины и толщины коаксиальный кабель делится на несколько категорий. Компьютерные сети на основе этого кабеля обычно требуют наличия терминаторов на оконечных точках.



*Рис. 8. Коаксиальный кабель*

Тонкий Ethernet

Был наиболее распространённым кабелем для построения локальных сетей. Диаметр примерно 6 миллиметров и значительная гибкость позволяли ему быть проложенным практически в любых местах. Кабели соединялись друг с другом и с сетевой платой в компьютере при помощи Т-коннектора BNC (British Naval Connector). Между собой кабели могли соединяться с помощью I- коннектора BNC (прямое соединение). На обоих концах сегмента должны быть установлены терминаторы. Поддерживает передачуданных до 10 Мб/с на расстояние до 185 метров.

Толстый Ethernet

Более толстый, по сравнению с предыдущим кабель — около 12 миллиметров в диаметре, имел более толстый центральный проводник. Плохо гнулся и имел значительную стоимость. Кроме того в присоединении к компьютеру были некоторые сложности — использовались трансиверы AUI (Attachment Unit Interface), присоединённые к сетевой карте с помощью ответвления, пронизывающего кабель, т. н.

«вампирчики». За счёт более толстого проводника передачу данных можно было осуществлять на расстояние до 500 метров со скоростью 10 Мб/с.

### Оптоволоконный кабель.

Оптоволоконный кабель – идеальная передающая среда. Онне подвержен действию электромагнитных полей и сам практически не имеет излучения. Последнее свойство позволяет использоватьего в сетях, требующих повышенной секретности информации.

Скорость передачи информации по оптоволоконному кабелю может достигать несколько Гбит/с. Большое распространение получил 30-волоконный кабель. Толщина оптического волокна 50-100 мкм. Основным стандартным соотношением номинальных диаметров сердцевины иокружающего его слоя считается соотношение 62.5/125 мкм. По сравнению с предыдущими типами передающей среды он болеедорог, менее технологичен в эксплуатации.

Помимо кабелей необходимо применение и другихустройств для создания ЛВС.

### Сетевая плата

Сетевая плата (также известная как сетевая карта, сетевой адаптер, Ethernet-адаптер, NIC (англ. network interface card)) — периферийное устройство, позволяющее компьютеру взаимодействовать с другими устройствами сети.

На сетевой плате для подключения к локальной сети имеются разъёмы для подключения кабеля витой пары и/или BNC- коннектор для коаксиального кабеля, а также несколько информационных светодиодов, сообщающих о наличии подключения и передаче информации.



*Рис. 9. Сетевые адаптеры*

Плата сетевого адаптера принимает последовательность электрических сигналов из сетевого кабеля и переводит в форму, понятную центральному процессору компьютера.

### Повторитель

Повторитель (англ. Repeater) предназначен для увеличения расстояния сетевого соединения путем повторения электрического сигнала «один в один». Бывают однопортовые повторители и многопортовые. В терминах модели OSI работает на физическом уровне.

Первоначально в Ethernet использовался коаксиальныйкабель с топологией "шина", и нужно было соединять между собой всего несколько протяженных сегментов. Для этого обычно использовались повторители (repeater), имевшие два порта. Несколько позже появились многопортовые устройства, называемые концентраторами (concentrator). Их физический смысл был точно такой же, но восстановленный сигнал транслировался на все активные порты, кроме того, с которого пришел сигнал.

С появлением протокола 10baseT (витой пары) для избежания терминологической путаницы многопортовые повторители для витой пары стали называться сетевыми концентраторами (хабами), а коаксиальные - повторителями (репитерами).

### Мост

Мост (с англ. Bridge) — сетевое оборудование для объединения сегментов локальной сети. Сетевой мост работает на втором уровне модели OSI, обеспечивая ограничение доменаколлизий (в случае сети Ethernet).

Мост принимает кадр, буферизует его, анализирует адрес назначения кадра и только в том случае, когда адресуемый узел действительно принадлежит другой сети, он передает его туда.

Мост, изолирует трафик одного сегмента от трафика другого сегмента, фильтруя кадры. Так как в каждый из сегментов теперь направляется трафик от меньшего числа узлов, то коэффициент загрузки сегментов уменьшается.

### Маршрутизатор

Маршрутизатор или роутер (от англ. router) — сетевое устройство, на основании информации о топологии сети и определённых правил принимающее решения о пересылке пакетов сетевого уровня (уровень 3 модели OSI) между различнымисегментами сети.

Маршрутизаторы помогают уменьшить загрузку сети, благодаря её разделению на домены коллизий и широковещательные домены, а также благодаря фильтрации пакетов. В основном их применяют для объединения сетей разных типов, зачастую несовместимых по архитектуре и протоколам, например для объединения локальных сетей Ethernet и WAN- соединений, использующих протоколы xDSL, PPP, ATM, Frame relay и т. д. Нередко маршрутизатор используется для обеспечения доступа из локальной сети в глобальную сеть Интернет,осуществляя функции трансляции адресов и межсетевого экрана.

### Задания к лабораторной работе

1. Ознакомится с средствами и оборудованием ЛВС.
2. Составить паспорт локальной сети лаборатории (топология сети, использованное оборудование, кабельные системы).
3. Определить параметры сети (IP-адреса узлов, способ их назначения , MAC-

адреса узлов, тип сиволического имени) с помощью команды **ipconfig /all**.

1. Исследовать достижимость узлов сети и маршрутов к ним с помощью команд **ping** IP-адрес-узла (или **ping** имя-узла), **tracert** IP-адрес-узла (или **tracert** имя-узла). *В качестве примеров использовать следующие адреса: имя компьютера, IP-адрес компьютера, имя и адрес другого компьютера лаборатории, 192.168.0.1, 10.70.0.3, 10.70.1.1, kampi.ru,* [*www.yandex.ru.*](http://www.yandex.ru/)Исследовать ресурсы домена с помощью команд: net view /DOMAIN:PIUnet view \\ имя\_станции

### Содержание отчета:

1. Теоретическая справка.
2. Паспорт сети.
3. Информация об основных командах и утилитах,применяемых при настройке и изучении сети (ping, tracert, net, ipconfig, …) и их основных параметрах.

Параметры узла и сети, полученные с помощью команд, указанных в заданиях.

1. Параметры узла и сети, полученные с помощью команд, указанных в задании

### Контрольные вопросы:

1. Отличие сетей одноранговой и иерархической структуры.
2. Основные сетевые топологии. Достоинства и недостатки.
3. Основные типы кабелей, применяемых при построениекомпьютерных сетей.
4. Основные сетевые устрйоства и их назначение.

**Практическая работа №4** Установка Cisco Packet Tracer (CPT). Изучение интерфейса.

Создание простейшей сети

**Цель занятия:** Установить Cisco Packet Tracer (CPT). Изучить интерфейс Cisco Packet Tracer (CPT)

***Оборудование, приборы, аппаратура, материалы:*** ПК, Cisco Packet Tracer (CPT)

### Краткие теоретические сведения

Cisco Packet Tracer - это эмулятор сети, созданный компанией Cisco.

Данное приложение позволяет строить сети на разнообразном оборудовании в произвольных топологиях с поддержкой разных протоколов.

Программное решение Cisco Packet Tracer 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 ощущение настройки реальной сети, состоящей из десятков или даже сотен устройств.

Настройки, в свою очередь, зависят от характера устройств: одни можно настроить с помощью команд операционной системы Cisco IOS, другие – за счет графического веб-интерфейса, третьи – через командную строку операционной системы или графические меню.

Благодаря такому свойству Cisco Packet Tracer, как режим визуализации, пользователь 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 обнаружитьнеисправности.

Cisco Packet Tracer может быть использован не только как симулятор, нои как сетевое приложение для симулирования виртуальной сети через реальнуюсеть, в том числе Интернет. Пользователи разных компьютеров, независимо от их местоположения, могут работать над одной сетевой топологией, производяее настройку или устраняя проблемы. Эта функция многопользовательского режима Cisco Packet Tracer может применяется для организации командной работы.

В Cisco Packet Tracer пользователь может 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.

Симуляция, визуализация, многопользовательский режим и возможность проектирования делают Cisco Packet Tracer уникальным инструментом для обучения сетевым технологиям.

Раздел 1. Интерфейс Cisco Packet Tracer

* 1. Главное окно Cisco Packet Tracer

На рис.1.1. представлен интерфейс программы, разделенный на области.

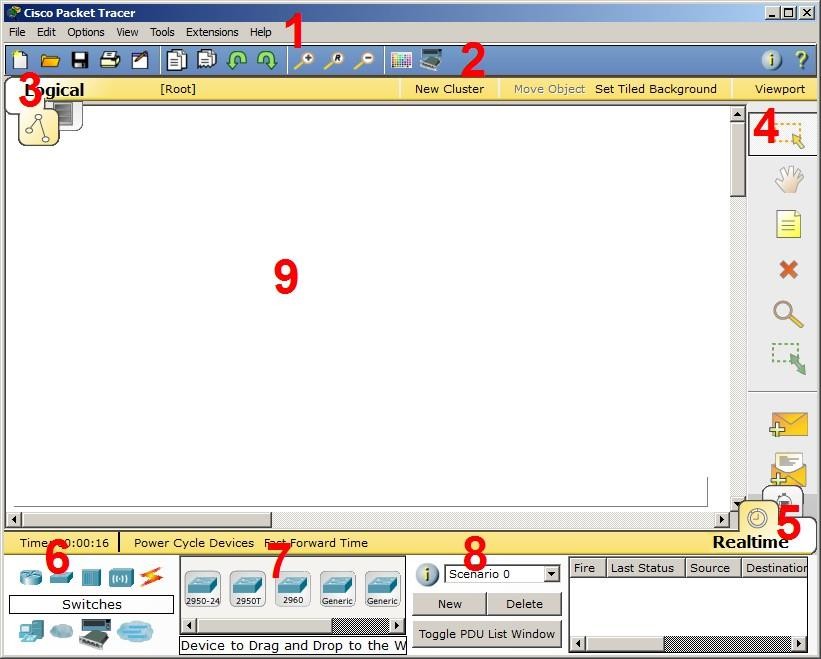


Рис.1.1. Интерфейс программы Cisco Packet Tracer.

* + 1. Главное меню программы со следующим содержимым:
       - Файл - содержит операции открытия/сохранения документов;
       - Правка - стандартные операции "копировать/вырезать, отменить/повторить";
       - Настройки - говорит само за себя;
       - Вид - масштаб рабочей области и панели инструментов;
       - Инструменты - цветовая палитра и кастомизация конечных устройств;
       - Расширения - мастер проектов, многопользовательский режим и несколько приблуд, которые из CPT (так я иногда буду ласково называть Cisco Packet Tracer) могут сделать целую лабораторию;
       - Помощь - ни за что не угадаете, что там содержится;
    2. Панель инструментов, часть которых просто дублирует пункты меню;
    3. Переключаетль между логической и физической организацией;
    4. Ещё одна панель инструментов, содержит инструменты выделения, удаления, перемещения, масштабирования объектов, а так же формирование произвольных пакетов;
    5. Переключатель между реальным режимом (Real-Time) и режимом симуляции;
    6. Панель с группами конечных устройств и линий связи;
    7. Сами конечные устройства, здесь содержатся всевозможные коммутаторы,узлы, точки доступа, проводники.
    8. Панель создания пользовательских сценариев;
    9. Рабочее пространство.

Пример размещения цветовых областей (рис.1.2), позволяющий, например,отделять визуально одну подсеть от другой.

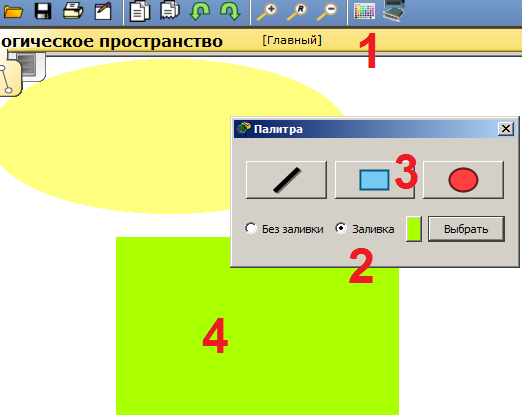


Рис.1.2. Пример размещения цветовых областей.

Для установки цветных областей выполните следующие действия:1 - На панели инструментов выбираем соответствующий значок;

2 - Выбираем режим области "Заливка", например;3 - Выбираем цвет и форму;

4 - Рисуем область на рабочем пространстве.

Можно также добавить подпись и перемещать/масштабировать эту область.

**2.2.** Оборудование и линии связи в Cisco Packet Tracer

Маршрутизаторы

Маршрутизаторы в Cisco Packet Tracer

Маршрутизаторы используется для поиска оптимального маршрута передачи данных на основании специальных алгоритмов маршрутизации, например выбор маршрута (пути) с наименьшим числом транзитных узлов.

Внешний вид маршрутизатора в Cisco Packet Tracer

Работают на сетевом уровне модели OSI.

Коммутаторы

Коммутаторы в Cisco Packet Tracer

Коммутатор CiscoКоммутаторы - это устройства, работающие на канальном уровне модели OSI и предназначенные для объединения нескольких узлов в пределах одного или нескольких сегментов сети. Передаёт пакеты коммутатор на основании внутренней таблицы - таблицы коммутации, следовательно трафик идёт только на тот MAC-адрес, которому он предназначается, а не повторяется на всех портах (как на концентраторе).

Концентраторы

Концентраторы в cisco packet tracer

Концентратор повторяет пакет, принятый на одном порту на всех остальныхпортах. Беспроводные устройства

Беспроводные устройства в Cisco Packet Tracer

Беспроводные технологии Wi-Fi и сети на их основе. Включает в себя точкидоступа. Линии связи

Линии связи в Cisco Packet Tracer

С помощью этих компонентов создаются соединения узлов в единую схему. Packet Tracer поддерживает широкий диапазон сетевых соединений (см. табл.1.1).

Каждый тип кабеля может быть соединен лишь с определенными типамиинтерфейсов. Таблица 1.1. Типы кабелей.

|  |  |
| --- | --- |
| Тип кабеля | Описание |

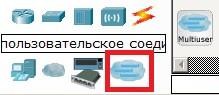
|  |  |
| --- | --- |
| Консоль  консоль.jpg | Консольное соединение может быть выполнено между ПК и маршрутизаторами или коммутаторами. Должны быть выполнены некоторые требования для работы консольного сеанса с ПК: скорость соединения с обеих сторон должна быть одинаковая, должно быть 7 бит данных (или 8 бит) для обеих сторон, контроль четности должен быть одинаковый, должно быть 1 или 2 стоповых бита (но они не обязательно должны быть одинаковыми), а поток данных может быть чем  угодно для обеих сторон. |
| Медный прямой  медный прямой.jpg | Этот тип кабеля является стандартной средой передачиEthernet для соединения устройств, который функционирует на разных уровнях OSI. Он должен быть соединен со следующими типами портов: медный  10 Мбит/с (Ethernet), медный 100 Мбит/с (Fast Ethernet)и медный 1000 Мбит/с (Gigabit Ethernet). |
| Медный кроссовер  медный кроссовер.jpg | Этот тип кабеля является средой передачи Ethernet для соединения устройств, которые функционируют на одинаковых уровнях OSI. Он может быть соединен со следующими типами портов: медный 10 Мбит/с(Ethernet), медный 100 Мбит/с (Fast Ethernet) и медный  1000 Мбит/с (Gigabit Ethernet) |
| Оптика | Оптоволоконная среда используется для соединения |
| оптика.jpg | между оптическими портами (100 Мбит/с или 1000 Мбит/с). |
| Телефонный  телефонный.jpg | Соединение через телефонную линию может быть осуществлено только между устройствами, имеющими модемные порты. Стандартное представление модемного соединения - это конечное устройство  (например, ПК), дозванивающееся в сетевое облако. |
| Коаксильный  коаксильный.jpg | Коаксиальная среда используется для соединения между коаксиальными портами, такие как кабельныймодем, соединенный с облаком Packet Tracer. |
| Серийный DCE Серийный DTE | Соединения через последовательные порты, часто используются для связей WAN. Для настройки таких соединений необходимо установить синхронизацию на стороне DCE-устройства. Синхронизация DTE выполняется по выбору. Сторону DCE можно определить по маленькой иконке “часов” рядом с портом. При выборе типа соединения Serial DCE, первое устройство, к которому применяется соединение, становиться DCE- устройством, а второе - автоматически станет стороной DTE.  Возможно и  обратное расположение сторон, если выбран тип соединения Serial DTE. |

Конечные устройства



Здесь представлены конечные узлы, хосты, сервера, принтеры, телефоны и т.д. Эмуляция Интернета

Пример эмуляция глобальной сети. Модем DSL, "облако" и т.д. Пользовательские устройства и облако для многопользовательскойработы



Устройства можно комплектовать самостоятельно. Можно создаватьпроизвольные подключения.

**2.3.** Физическая комплектация оборудования Установите в рабочем поле роутер Cisco 1841 В настройках на роутереоткрываем его **физическую конфигурацию** (рис.1.3).

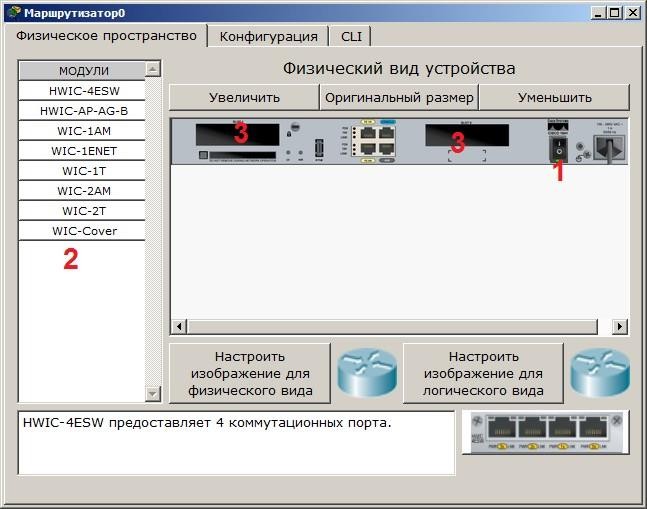


Рис.1.3. Физическая конфигурация устройства.

Слева, как мы видим, список модулей (цифра 2), которыми можно укомплектовать данный роутер. Сейчас в нем 2 пустоты (цифра 3). В них можно вложить эти модули. Разумеется, эту операцию нужно производить при выключенном питании (цифра 1).

Модули WIC (HWIC, VWIC) это платы расширения, увеличивающиефункционал устройства:

:

1. **WIC** - WAN interface card. the first original models.
2. **HWIC**- high-speed wan interface card- the evolution of wic that is now in use on theISR routers.
3. **VIC** - voice interface card, support voice only.
4. **VIC2** - evolution of the above
5. **VWIC** - voice and wan interface card. An E1/T1 card that can be user for voice ordata.
6. **VWIC2** - evolution of the above

Например для компьютера есть платы, подключаемые к PCI-шине (TV-тюнеры,звуковые карты, USB-разветвители, сетевые карты), так и здесь. Вообще, устройство Cisco - это тот же системный блок со своей операционкой и многими сетевыми картами, который может делать что-то только с сетью.

Ниже предствалена информация о каждом модуле:

* **HWIC - 4ESW** - высокопроизводительный модуль с 4-мя коммутационными портами Ethernet под разъем RJ-45. Позволяет сочетать в маршрутизаторе

возможности коммутатора.

* **HWIC-AP-AG-B** - это высокоскоростная WAN-карта, обеспечивающая функционал встроенной точки доступа для роутеров линейки Cisco 1800 (модульных), Cisco 2800 и Cisco 3800. Данный модуль поддерживает радиоканалы Single Band 802.11b/g или Dual Band 802.11a/b/g.
* **WIC-1AM** включает в себя два разъема RJ-11 (телефоннка), используемых для подключения к базовой телефонной службе. Карта использует один порт для соединения с телефонной линией, другой может быть подключен к аналоговому телефону для звонков во время простоя модема.
* **WIC-1ENET** - это однопортовая 10 Мб/с Ethernet карта для 10BASE-T Ethernet LAN.
* **WIC-1T** предоставляет однопортовое последовательное подключение к удаленным офисам или устаревшим серийным сетевым устройствам, например SDLC концентраторам, системам сигнализации и устройствам packet over SONET (POS).
* **WIC-2AM** содержит два разъема RJ-11, используемых для подключения к базовой телефонной службе. В WIC-2AM два модемных порта, что позволяет использовать оба канала для соединения одновременно.
* **WIC-2T** - 2-портовый синхронный/асинхронный серийный сетевой модуль предоставляет гибкую поддержку многих протоколов с индивидуальной настройкой каждого порта в синхронный или асинхронный режим. Применения для синхронной/асинхронной поддержки представляют:
* низкоскоростную агрегацию (до 128 Кб/с);
* поддержку dial-up модемов;
* синхронные или асинхронные соединения с портами управления другого оборудования и передачу устаревших протоколов типа Bi-sync и SDLC.
* **WIC-Cover** - стенка для WIC слота, необходима для защиты электронных компонентов и для улучшения циркуляции охлаждающего воздушного потока.

Для изменения комплектации оборудования необходимо:

отключить питание, кликнув мышью на кнопке питания, перетащить мышью модуль **4ESW** в свободный слот и включить питание. Подождать окончания загрузки роутера. В конфигурации GUI можем увидеть появившиеся 4 новых интерфейса (рис.1.4).

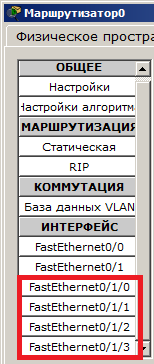


Рис.1.4. Конфигурация интерфейсов устройства.

Остальные устройства комплектуются аналогично. Добавляются новые модули Ethernet (10/100/1000), оптоволоконные разъемы нескольких типов, адаптеры беспроводной сети. На рабочий компьютер есть возможность добавить например микрофон с наушниками, жесткий диск для хранения данных.

## Контрольные вопросы

1. Какая плата расширения обеспечивает функционал встроенной точкидоступа?
2. Какая плата расширения предоставляет однопортовое последовательное подключение к удаленным офисам или устаревшим серийным сетевым устройствам?
3. Как называется высокопроизводительный модуль с 4-мя коммутационными портами Ethernet под разъем RJ-45?
4. Перечислите сетевые карты, позволяющие подключаться к WAN сетям?
5. Какой тип интерфейса следует выбрать при создании кластера?
6. Назовите модели коммутаторов третьего уровня?
7. Какой тип кабеля следует использовать при соединении роутеров между собой?
8. Укажите серии магистральных маршрутизаторов.
9. В каких случаях используется интерфейс SERIAL?
10. Как организовать связь двух магистральных маршрутизаторов?
11. Перечислите все возможные режимы работы программы Cisco Paket Tracer?
12. Назовите модели коммутаторов второго уровня?
13. Перечислите все типы связей, используемых в Cisco Paket Tracer и укажитеих назначение.

**Практическая работа №5** Создание и исследование сетей с использованием концентратора и коммутатора в Cisco Packet Tracer

**Цель занятия:** Изучить принцип построения структурированной кабельной системы (СКС), с использованием концентратора и коммутатора в Cisco Packet Tracer.

***Оборудование, приборы, аппаратура, материалы:*** ПК Cisco Packet Tracer

### Краткие теоретические сведения

Состав сети: 4 узла, сервер, принтер и два концентратора. Концентраторы межсобой соединяются кроссоверным кабелем (рис.2.1).

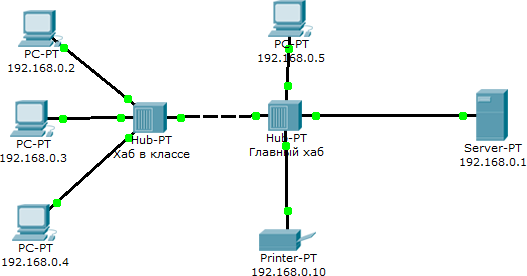


Рис.2.1. Схема сети.

Нужно перейти в режим симуляции (Shift+S), либо кликнув на иконку симуляции в правом нижнем углу рабочего пространства. Здесь мы видим окно событий, кнопка сброса (очищает список событий), управление воспроизведением и фильтр протоколов. Предложено много протоколов, но отфильтруем пока только ICMP, это исключит случайный трафик между узлами.

Для перехода к следующему событию используем кнопку "Вперёд", либо автоматика (рис.2.2).

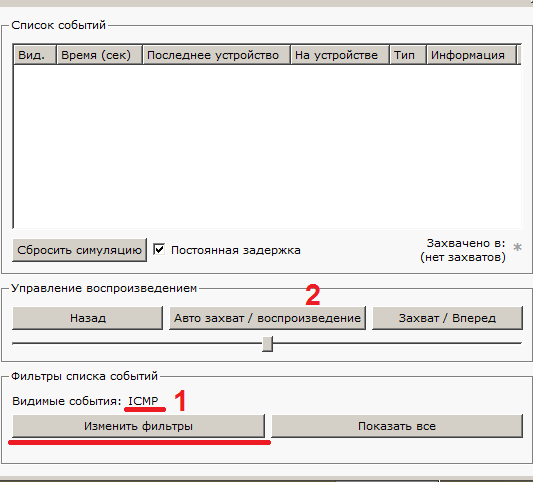


Рис.2.2. Интерфейс симулятора. Посылаем PING-запрос.

С одного из узлов попробуем пропинговать другой узел. Выбираем далеко расположенные узлы, чтобы наглядней увидеть, как будут проходить пакеты по сети в режиме симуляции. Итак, входим на узел .4 и пошлём пинг- запрос на узел .5.

С розового узла пингуем зелёный. На розовом узле образовался пакет (конвертик), который ждёт (иконка паузы на нём). Запустить пакет в сеть можно нажав кнопку "Вперёд" в окне симуляции (рис.2.3).

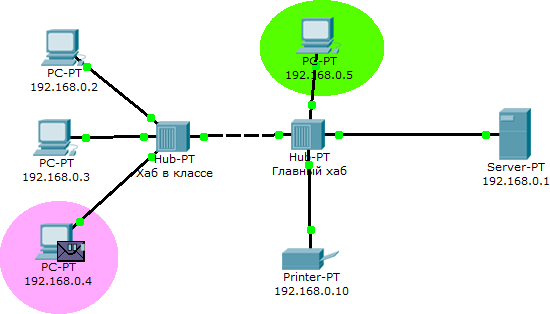
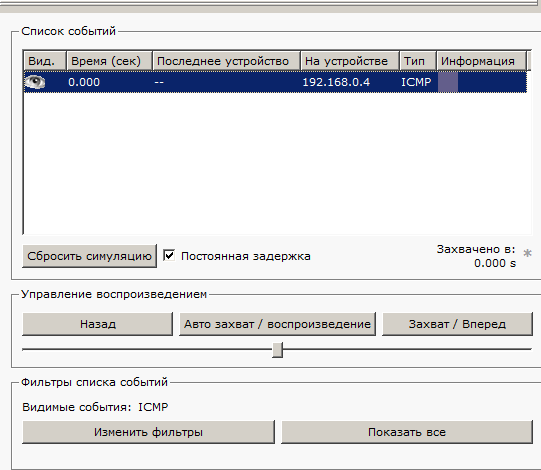


Рис.2.3. Демонстрация работы симулятора.

Так же в окне симуляции мы увидим этот пакет, отметив его тип (ICMP) иисточник (192.168.0.4) – рис.2.4.

Рис.2.4. Мониторинг работы протоколов.

Клик на пакете покажет нам подробную информацию. При этом мы увидим модель OSI.

Сразу видно, что на 3-ем уровне (сетевой) возник пакет на исходящем направлении, который пойдёт до второго уровня, затем до первого, на физическую среду и передастся на следующий узел (рис.2.5).

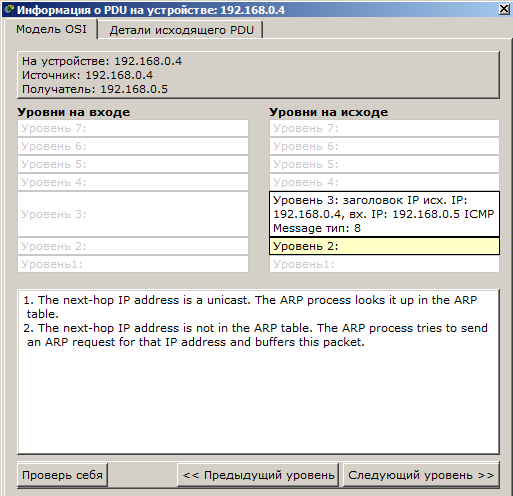


Рис.2.5. Мониторинг работы на модели OSI.

А на другой вкладке можно посмотреть структуру пакета (рис.2.6).

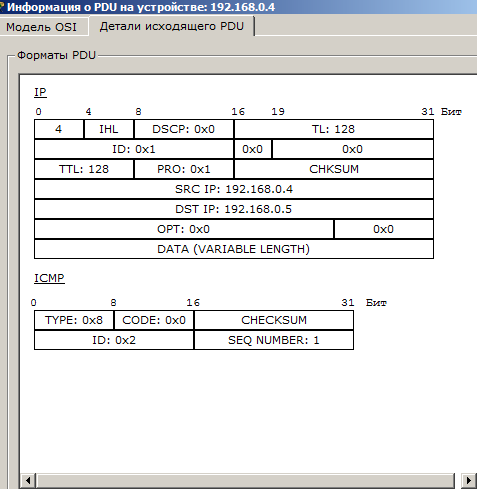


Рис.2.6. Структура пакета.

Нажмём кнопку "Вперёд". И пакет тут же двинется к концентратору. Этоединственное сетевое подключение с этой стороны (2.7).

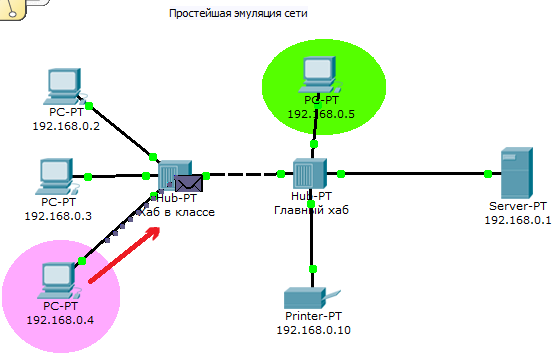


Рис.2.7. Прохождение пакета. Первый этап.

Концентратор повторяет пакет на всех остальных портах в надежде, что наодном из них есть адресат (рис.2.8)

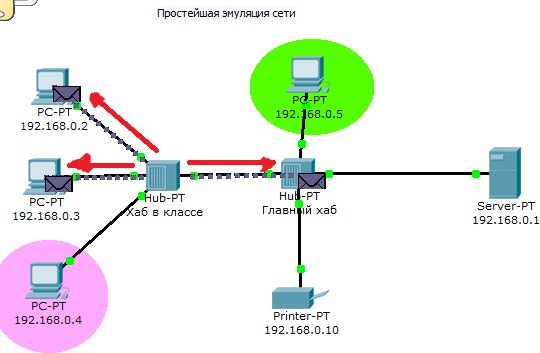


Рис.2.8. Прохождение пакета. Второй этап.

Если пакеты каким-то узлам не предназначенны, они просто игнорируют их(рис.2.9).

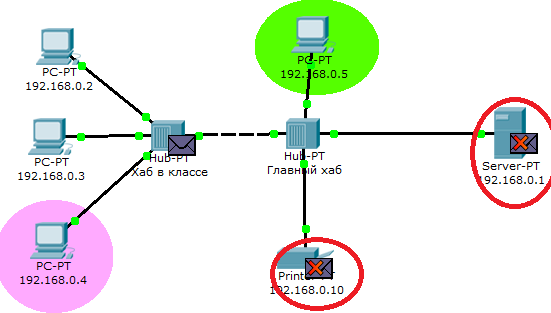


Рис.2.9. Прохождение пакета. Третий этап.

Когда пакет вернётся обратно, то увидим подтверждение соединения:

## Контрольные вопросы.

1. Для чего используется режим симуляции?
2. Как просмотреть прохождение пакета по уровням модели OSI?
3. Можно ли определить причину того, что посланный в режиме симуляции пакет не дошел до адресата и на каком этапе произошел сбой работы сети?
4. Укажите в составе пакета IP адреса отправителя и получателя.
5. Как изменить фильтры списка событий?
6. Как в режиме симуляции определить, какие протоколы были задействованыв работе сети?
7. Как в режиме симуляции проследить изменение содержимого пакета при прохождении его по сети?
8. Перечислите основные возможности режима симуляции.

**Практическая работа №6** Подключение к сетевому оборудованию в Cisco Packet Tracer

**Цель занятия:** Изучить принцип подключения к сетевому оборудованию в Cisco Packet Tracer.

***Оборудование, приборы, аппаратура, материалы:*** ПК, Cisco Packet Tracer

### Краткие теоретические сведения

Эмулятор Cisco Packet Tracer позволяет проводить настройку таких сетевых сервисов, как: HTTP, DHCP, TFTP, DNS, NTP, EMAIL, FTP в составе сервера сети. Рассмотрим настойку некоторых из них.

## Задание.

Создайте следующую схему сети, представленную на рис. 3.1:

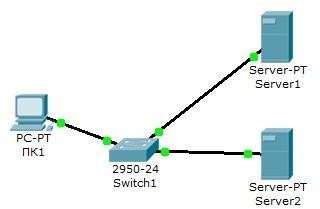


Рис.3.1. Схема сети.

Задача:

Настроить сеть следующим образом:

1. - Server1 – DNS и Web сервер;
2. - Server2 – DHCP сервер;
3. - Компьютер ПК1 получает параметры протокола TCP/IP c DHCP сервера иоткрывает сайт [www.rambler.ru](http://www.rambler.ru/) на Server1.

Этап 1.

Задайте параметры протокола TCP/IP на ПК1 и серверах.

Войдите в конфигурацию ПК1 и установите настройку IP через DHCP серверрис.3.2.

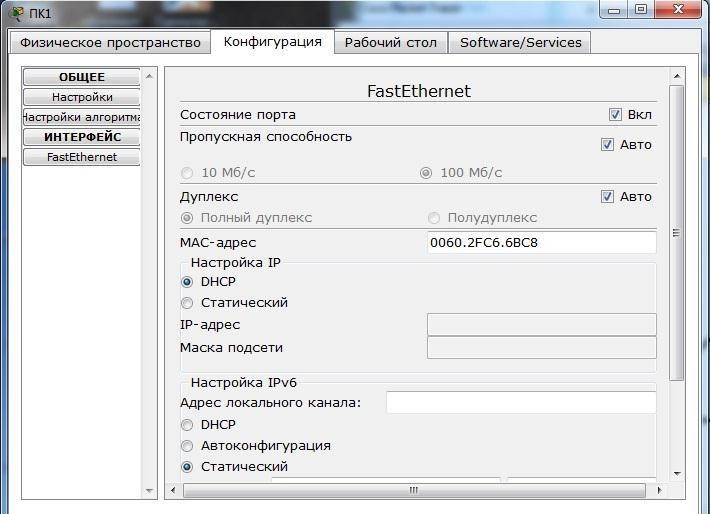


Рис. 3.2. Настройка IP на ПК1.

Задайте в конфигурации серверов следующие настройки IP: Server1: IP адрес – 10.0.0.1, маска подсети – 255.0.0.0 Server2: IP адрес – 10.0.0.2, маска подсети – 255.0.0.0

Этап 2. Настройте службу DNS на Server1.

Для этого в в конфигурации Server1 войдите на вкладку DNS и задайте две ресурсные записи в прямой зоне DNS:

* 1. – в ресурсной записи типа А свяжите доменное имя компьютера с его IPадресом рис.3.3 и нажмите кнопку ДОБАВИТЬ:

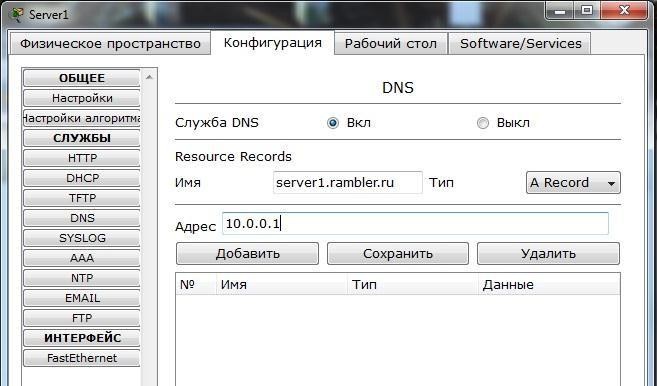


Рис.3.3. Ввод ресурсной записи типа А.

* 1. – в ресурсной записи типа CNAME свяжите псевдоним сайта с компьютером(рис.3.4):

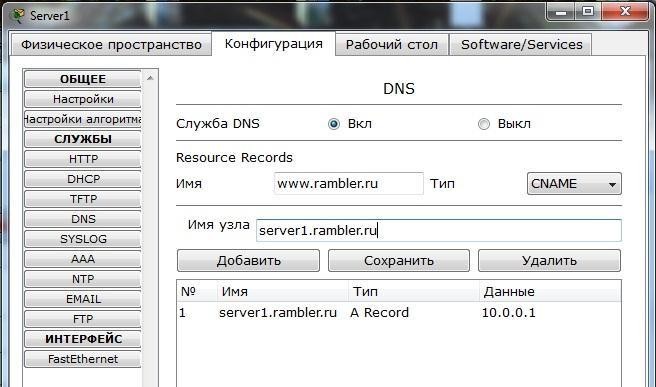


Рис.3.4. Ввод ресурсной записи типа CNAME.

В конфигурации Server1 войдите на вкладку HTTP и задайте стартовуюстраницу сайта [WWW.RAMBLER.RU](http://www.rambler.ru/) (рис.3.5):

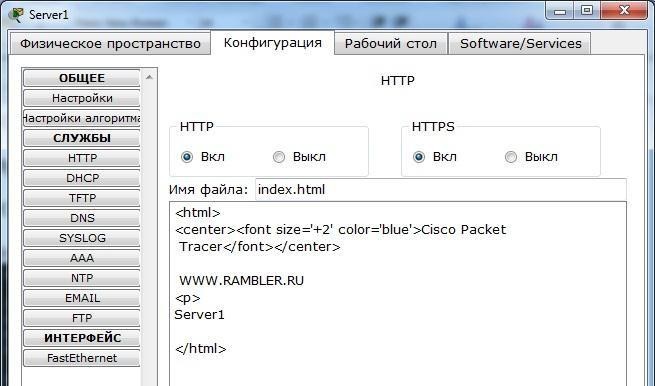


Рис.3.5. Стартовая страница сайта.

Включите командную строку на Server1 и проверьте работу службы DNS. Дляпроверки прямой зоны DNS сервера введите команду

SERVER>**nslookup** [**www.rambler.ru**](http://www.rambler.ru/)

Если все правильно, то вы получите отклик, представленный на рис.3.6, суказанием полного доменного имени DNS сервера в сети и его IP адрес.

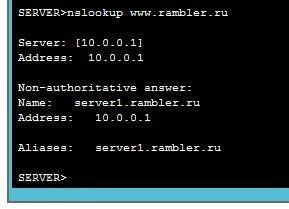


Рис. 3.6. Проверка прямой зоны DNS.

Этап 3. Настройте DHCP службу на Server2.

Для этого войдите в конфигурацию Server2 и на вкладке DHCP настройтеслужбу (рис.3.7):

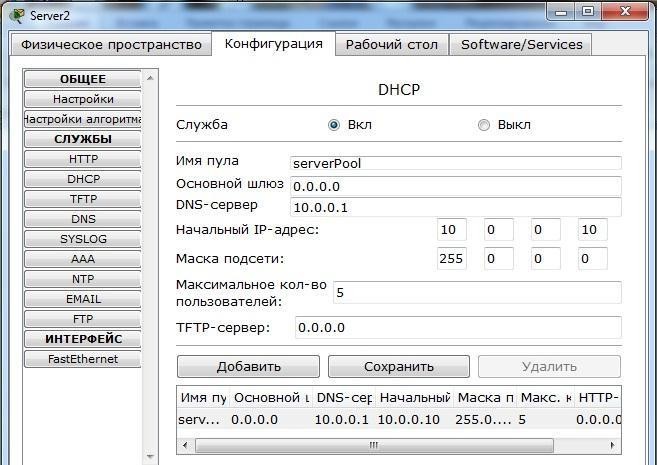


Рис. 3.7. Настройка DHCP сервера. Этап 3. Проверка работы клиента.

Войдите в конфигурации хоста ПК1 на рабочий стол и в командной строке сконфигурируйте протокол TCP/IP.

Командой PC>ipconfig /release

сбросьте старые параметры IP адреса, а командой:

PC>ipconfig /renew

получите новые параметры с DHCP сервера (рис.3.8):

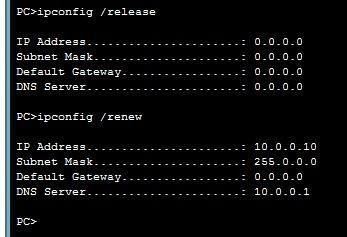


Рис.3.8. Конфигурация протокол TCP/IP клиента.

Откройте сайт [WWW.RAMBLER.RU](http://www.rambler.ru/) в браузере на клиенте (рис.3.9):

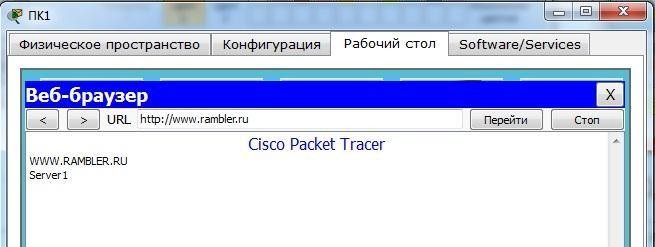


Рис.3.9. Проверка работы клиента.

## Контрольные вопросы.

1. Что такое рекурсивный запрос DNS и какова схема его работы?
2. Укажите назначение типов ресурсных записей в прямой и обратной зонах DNS.
3. Как на DNS сервере настраивается пересылка пакетов на другие DNSсервера?
4. Опишите работу службы DHCP.
5. Как настраивается клиент DHCP?
6. Укажите местоположения папки с контентом Web узла и FTP сервера.
7. Как определяется состав обратных зон DNS сервера в корпоративной сети.
8. Продемонстрируйте настройку служба DNS в Cisco Paket Tracer?
9. Продемонстрируйте настройку служба DHCP в Cisco Paket Tracer?
10. Продемонстрируйте настройку служба FTP в Cisco Paket Tracer?
11. Продемонстрируйте настройку аивается WEB сервер в Cisco Paket Tracer?

**Практическая работа №7** Использование технологии VLAN в Cisco Packet Tracer

**Цель занятия:** Изучить принцип использование технологии VLAN в Cisco Packet

Tracer

***Оборудование, приборы, аппаратура, материалы:*** ПК Cisco Packet Tracer

### Краткие теоретические сведения

VLAN (аббр. от англ. Virtual Local Area Network) — логическая("виртуальная")

локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети.

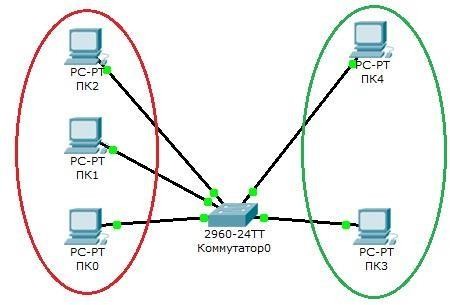
VLAN'ы могут быть настроены на коммутаторах, маршрутизаторах, других сетевых устройствах.

Преимущества:

1. - Облегчается перемещение, добавление устройств и изменение их соединений друг с другом.
2. - Достигается большая степень административного контроля вследствие наличия устройства, осуществляющего между сетями VLAN маршрутизацию на 3-м уровне. 3 - Уменьшается потребление полосы пропускания по сравнению с ситуацией одного широковещательного домена.
3. - Сокращается непроизводственное использование CPU за счет сокращения пересылки широковещательных сообщений.
4. - Предотвращение широковещательных штормов и предотвращение петель.

В данной работе рассматривается настройка VLAN на коммутаторе фирмы Сisco на его портах доступа. Создайте сеть, логическая топология которой представлена на рис.9.1. Компьютеры соединены коммутатором Cisco 2960-24ТТ. В таблице 9.1 приведены адреса компьютеров.

Задача данной работы – сделать две независимые группы компьютеров: ПК0, ПК1 и ПК2 должны быть доступны только друг для друга, вторая независимая группа - компьютеры ПК3 и ПК4. Для этого создадим два отдельных VLAN (рис.8.1)



VLAN 2

VLAN 3

Рис. 8.1. Схема сети с одним коммутатором. Таблица 8.1.

|  |  |  |
| --- | --- | --- |
| Компьютер | IP адрес | Порт коммутатора |
| ПК0 | 10.0.0.1/8 | 1 |
| ПК1 | 10.0.0.2/8 | 2 |
| ПК2 | 10.0.0.3/8 | 3 |
| ПК3 | 10.0.0.4/8 | 4 |
| ПК4 | 10.0.0.5/8 | 5 |

Далее будем считать, что ПК0, ПК1 и ПК2 находятся в VLAN 2, а ПК3 и ПК4 находятся в VLAN 3.

Для проверки конфигурации хоста ПК0 выполним команду ipconfig. Результат выполнения команды на рисунке 8.2. При желании можно выполнить аналогичную проверку на остальных хостах.

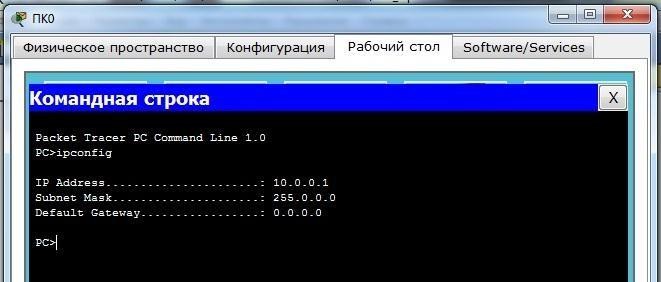


Рис.8.2. Проверка конфигурации хоста

Используя команду PING проверим связь между всеми компьютерами. Сейчас они в одной сети и все доступны друг для друга

Теперь займемся настройкой VLAN 2 и VLAN3, чтобы структурировать сети на коммутаторе и навести в них порядок.

Далее перейдем к настройке коммутатора. Откроем его консоль. Для того чтобы это выполнить в Packet Tracer дважды щелкните левой кнопкой мыши покоммутатору в рабочей области.

В открывшемся окне перейдите на вкладку CLI. Вы увидите окно консоли. Нажмите Enter, чтобы приступить к вводу команд. Информация, которая в данный момент отражена на консоли, свидетельствует о том что интерфейсы FasteEthernet0/1 – FasteEthernet0/5 находятся в рабочем состоянии.

Перейдем в привилегированный режим выполнив команду **enable**:

Switch

>**en** Switch #

Просмотрим информацию о существующих на коммутаторе VLAN-ах (рис.8.3).Для этого выполним следующую команду:

Switch#**sh vl br**

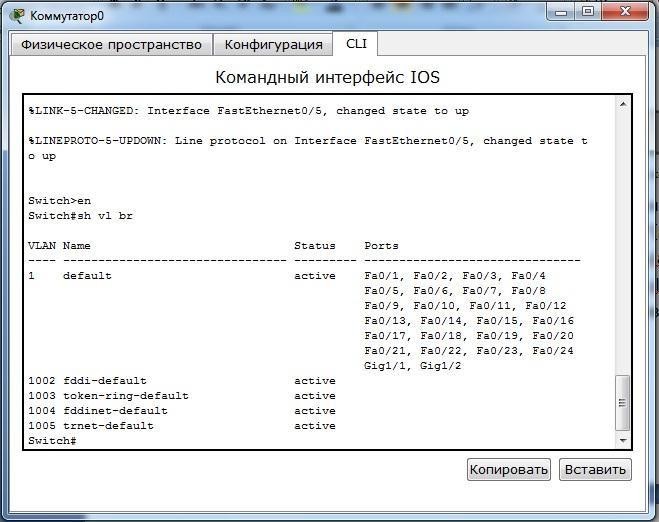


Рис.8.3. Просмотр информации о VLAN на коммутаторе.

В результате выполнения команды на экране появится: номера VLAN – первый столбец, название VLAN - второй столбец, состояние VLAN (работает он в данный момент или нет) – третий столбец, порты принадлежащие к данному VLAN – четвертый столбец. Как мы видим по умолчанию на коммутаторе существует пятьVLAN-ов. Все порты коммутатора по умолчанию принадлежат VLAN 1. Остальные четыре VLAN являются служебными и используются не очень часто.

Для реализации сети, которую мы запланировали сделать, создадим накоммутаторе еще два VLAN. Для этого в привилегированном режиме выполните следующую команду:

Switch#**conf t**

Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#

для перехода в режим конфигурации. Вводим команду VLAN 2. Данной командой вы

создадите на коммутаторе VLAN с номером 2. Указатель ввода Switch(config)# изменится на Switch(config-vlan)# это свидетельствует о том,что вы конфигурируете уже не весь коммутатор в целом, а только отдельный VLAN, в данном случае VLAN номер 2. Если вы используете команду «vlan x», где x номер VLAN, когда VLAN x еще не создан на коммутаторе, то он будет автоматически создан и вы перейдете к его конфигурированию. Когда вы находитесь в режиме конфигурирования VLAN, возможно изменение параметров выбранной виртуальной сети, например можно изменить ее имя с помощью команды name.

Для достижения поставленной в данном посте задачи, сконфигурируем VLAN 2 следующим образом:

Switch(config)#**vlan 2** Switch(config-vlan)#**name subnet\_10** Switch(config)#**interface range fastEthernet 0/1-3** Switch(config-if-

range)#**switchport mode access** Switch(config-if-range)#**switchport access vlan 2**

Разберем данную конфигурацию. Как уже говорилось ранее командой VLAN 2, мы создаем на коммутаторе новый VLAN с номером 2. Команда **name subnet\_10** присваивает имя subnet\_10 виртуальной сети номер 2. Выполняякоманду **interface range fastEthernet 0/1-3** мы переходим к конфигурированию интерфейсов fastEthernet0/1, fastEthernet0/2 и fastEthernet0/3 коммутатора. Ключевое слово **range** в данной команде, указывает на то, что мы будем конфигурировать не один единственный порт, а целый диапазон портов, в принципе ее можно не использовать, но тогда последние три строки придется заменить на:

Switch(config)#**interface fastEthernet 0/1** Switch(config- if)#**switchport mode access** Switch(config-if)#**switchport access vlan 2** Switch(config)#**interface fastEthernet 0/2** Switch(config- if)#**switchport mode access** Switch(config-if)#**switchport access vlan 2** Switch(config)#**interface fastEthernet 0/3** Switch(config- if)#**switchport mode access** Switch(config-if)#**switchport access vlan 2**

Команда **switchport mode access** конфигурирует выбранный порт коммутатора,как порт доступа (аксесс порт).

Команда **switchport access vlan 2** указывает, что данный порт является портомдоступа для VLAN номер 2.

Выйдите из режима конфигурирования, дважды набрав команду **exit** и просмотрите результат конфигурирования (рис.8.4), выполнив уже знакомую нам команду **sh vl br** еще раз:

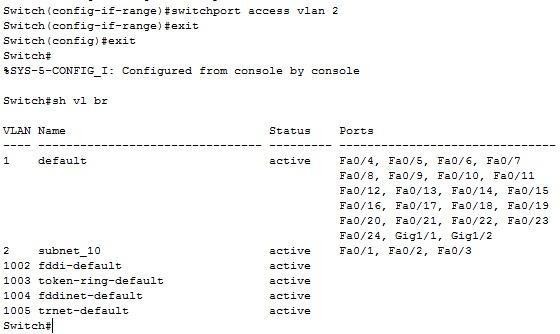


Рис.8.4. Распределение портов на VLAN.

На коммутаторе появился еще один VLAN с номером 2 и именем subnet\_10, портами доступа которого являются fastEthernet0/1, fastEthernet0/2 и fastEthernet0/3.Далее аналогичным образом создадим VLAN 3 с именем subnet\_192 и сделаем его портами доступа интерфейсы fastEthernet0/4 и fastEthernet0/5. Результат должен получиться следующим (рис.8.5):

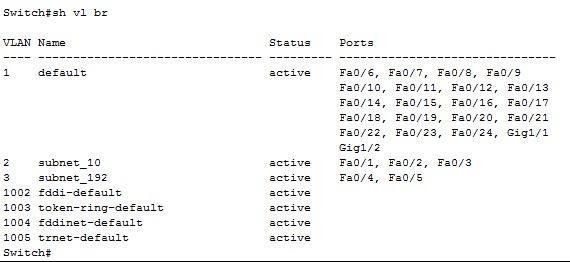
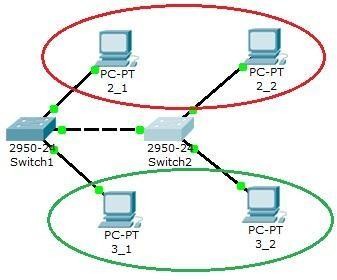


Рис.8.5. Распределение портов на VLAN.

В принципе уже все готово и наша сеть настроена. Осталось лишь ее немного протестировать. Перейдите в консоль компьютера ПК0. Пропингуйте с него остальные компьютеры сети. Компьютеры ПК1 и ПК2 доступны, а компьютеры ПК3 и ПК4 не доступны. Все пять компьютеров теоретически должны находится в одной подсети 10.0.0.0/8 и видеть друг друга, на практике они находятся в разных виртуальных локальных сетях и поэтому не могут взаимодействовать между собой.

Создайте сеть, логическая топология которой представлена на рис.8.6. Компьютеры соединены коммутатором Cisco 2950-24. В таблице 8.2 приведеныадреса компьютеров.



VLAN 20

VLAN 30

Рис.8.6. Схема сети.

Таблица 8.2.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Компьютер | IP адрес | Коммутатор | Порт  коммутатора | Вилан |
| 2\_1 | 10.0.0.1/8 | Switch1 | 1 | VLAN 20 |
| 2\_2 | 10.0.0.3/8 | Switch2 | 1 | VLAN 20 |
| 3\_1 | 10.0.0.2/8 | Switch1 | 2 | VLAN 30 |
| 3\_2 | 10.0.0.4/8 | Switch2 | 2 | VLAN 30 |

Далее будем считать, что 2\_1 и 2\_2 находятся в VLAN 20, а 3\_1 и 3\_2 находятсяв VLAN 30.

Проверим связность получившейся сети. Для этого [пропингуем](http://www.netza.ru/2012/10/ping-tracert.html) с 2\_1 все остальные компьютеры. Поскольку пока в сети нет разделения на VLAN, то всекомпьютеры должны быть доступны.

Теперь займемся настройкой VLAN 20 и VLAN30, чтобы структурировать сети на коммутаторах.

Перейдите к настройке коммутатора Switch1. Откройте его консоль. В открывшемся окне перейдите на вкладку CLI, войдите в привилегированный режим и настройте VLAN 20 и VLAN30 согласно таблице 2.

Создайте на коммутаторе VLAN 20. Для этого в привилегированном режиме выполните следующую команду:

Switch1#**conf t**

Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#

для перехода в режим конфигурации и настройте VLAN 20 и VLAN 30 следующим образом:

Switch1(config)#**vlan 20** Switch1(config)#**interface fastEthernet 0/1** Switch1(config-if-range)#**switchport mode access** Switch1(config-if- range)#**switchport access vlan 20** Switch1(config-if-range)#**exit** Switch1(config)#**vlan 30** Switch1(config)#**interface fastEthernet 0/2** Switch1(config-if-range)#**switchport mode access** Switch1(config-if- range)#**switchport access vlan 30**

Просмотрите информацию о существующих на коммутаторе VLAN-ах командой:Switch1#**sh vl br**

У вас должен получится результат, показанный на рис.8.7.

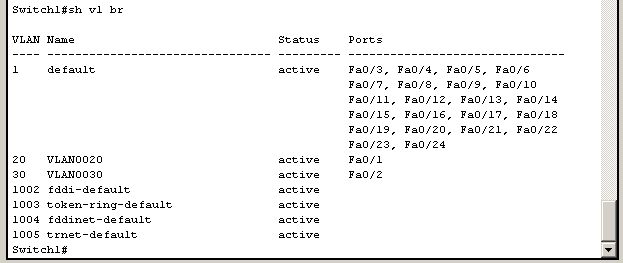


Рис. 8.7. Конфигурация Switch1.

Аналогичным образом сконфигурируйте Switch2 (рис. 8.8).

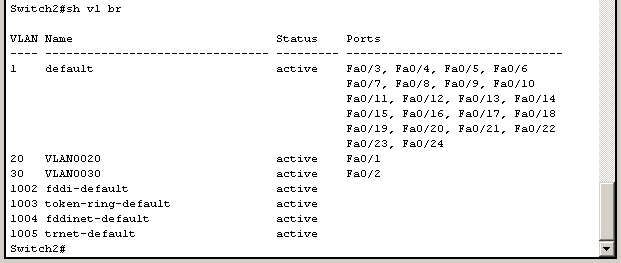


Рис. 8.7. Конфигурация Switch2.

Поскольку в данный момент нет обмена информации о вилланах, токомпьютеры будут пинговать только себя.

Теперь организуем магистраль обмена между коммутаторами. Для этогонастроим третий порт на каждом коммутаторе как транковый.

Войдите в консоль коммутатора Switch1 и задайте транковый порт:Switch1>**en**

Switch1#**conf t** Switch1(config)#**interface fastEthernet 0/3** Switch1(config)#**switchport mode trunk** Switch1(config)#**no shutdown** Switch1(config)#**exit**

Откройте конфигурацию коммутатора на интерфейсе FastEthernet0/3 и убедитесь, что порт транковый (рис.8.8).

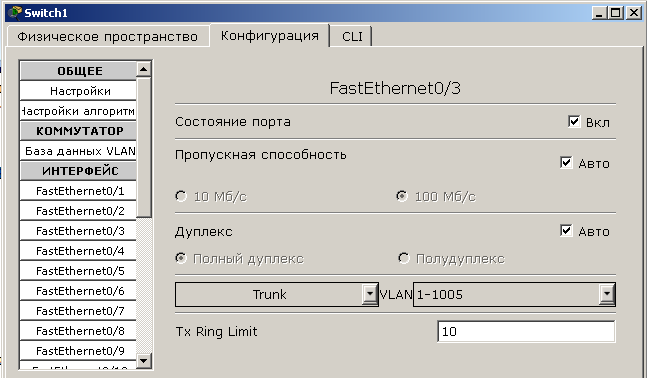


Рис.8.8. Конфигурация интерфейса FastEthernet0/3.

На коммутаторе Switch2 интерфейс FastEthernet0/3 автоматически настроится как транковый.

Теперь компьютеры, входящие в один виллан должны пинговаться. У вас должна появиться связь между компьютерами 2\_1 и 2\_2, а так же между 3\_1 и 3\_2. Но компьютеры в другом виллане будут недоступны.

Сохраните схему сети.

Теперь объединим две виртуальные сети с помощью маршрутизатора.

Добавьте в схему сети маршрутизатор, как показано на рис.8.9. Маршрутизаторсоединен с интерфейсами **fastEthernet 0/4** коммутаторов.

Разобьем нашу сеть 10.0.0.0 на две подсети: 10.2.0.0 и 10.3.0.0. Для этого поменяйте IP адреса и маску подсети на 255.255.0.0, как указано в таблице 8.3.

Таблица 8.3.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Компьютер | IP адрес | Коммутатор | Порт коммутатора | Вилан |
| 2\_1 | 10.2.0.1/16 | Switch1 | 1 | VLAN 20 |
| 2\_2 | 10.2.0.3/16 | Switch2 | 1 | VLAN 20 |
| 3\_1 | 10.3.0.2/16 | Switch1 | 2 | VLAN 30 |
| 3\_2 | 10.3.0.4/16 | Switch2 | 2 | VLAN 30 |

Компьютеры должны пинговаться в пределах одного виллана и одной подсети.

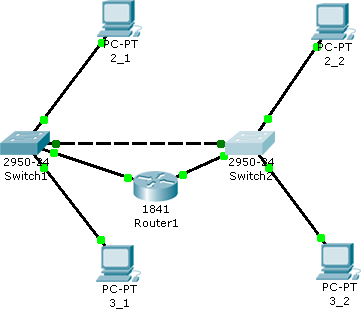


Рис. 8.9. Схема сети.

Обозначим на коммутаторах интерфейсы, подсоединенные к маршрутизатору в виртуальные сети.

Войдите в конфигурацию первого коммутатора Switch1 и задайте параметры четвертого порта:

Switch1(config)#**interface fastEthernet 0/4**

Switch1(config-if)#**switchport access vlan 20**

Проверьте настройки первого коммутатора Switch1 (рис.8.10):

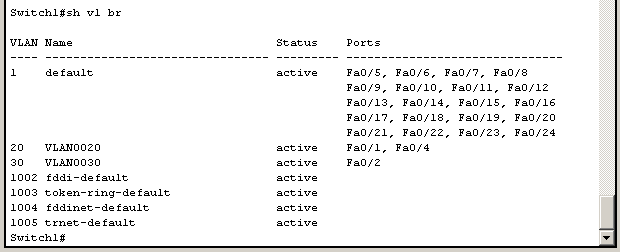


Рис.8.10. Настройки коммутатора Switch1.

Войдите в конфигурацию второго коммутатора Switch2 и задайте параметры четвертого порта:

Switch2(config)#**interface fastEthernet 0/4**

Switch2(config-if)#**switchport access vlan 30**

Проверьте настройки второго коммутатора Switch2 (рис.8.11):

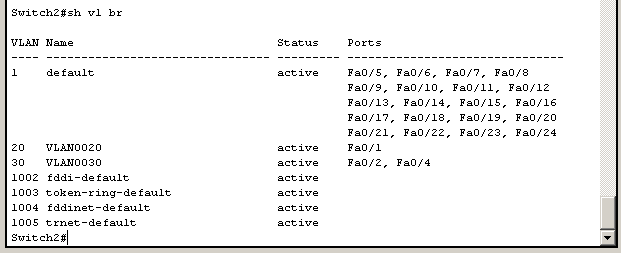


Рис.8.11. Настройки коммутатора Switch2.

Войдите в конфигурацию маршрутизатора и настройте IP адреса намаршрутизаторе:

Router1(config-if)#**interface fa0/0** Router1(config-if)#**ip address 10.2.0.254 255.255.0.0**Router1(config-if)#**no shutdown** Router1(config-if)#**interface fa0/1** Router1(config-if)#**ip address 10.3.0.254 255.255.0.0** Router1(config-if)#**no shutdown**

С этого момента мы установили маршрутизацию между двумя подсетями.Осталось установить шлюзы на компьютерах (таблица 8.4).

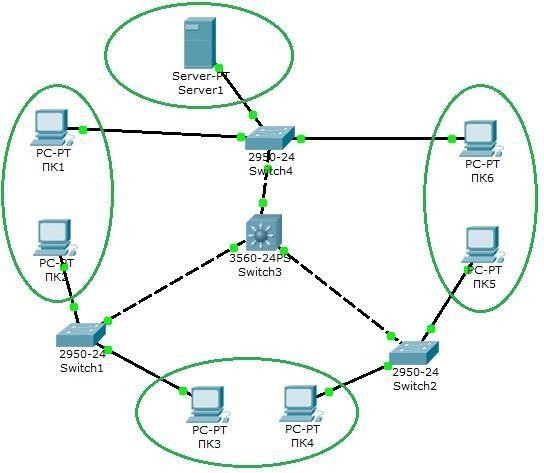
Таблица 8.4.

|  |  |
| --- | --- |
| Компьютер | Gataway |
| 2\_1 | 10.2.0.254 |
| 2\_2 | 10.2.0.254 |
| 3\_1 | 10.3.0.254 |
| 3\_2 | 10.3.0.254 |

Проверьте доступность компьютеров в сети. Теперь все компьютеры должныбыть доступны и все адреса должны пинговаться.

Создайте следующую схему сети (рис.8.12):

VLAN 10



VLAN 13

VLAN 12

VLAN 11

Рис.8.12. Схема корпоративной сети.

Состав сети:

* три коммутатора второго уровня распределения 2950-24 (Switch1, Switch2,Switch4);
* центральный коммутатор третьего уровня 3560-24PS (Switch3), выполняющийроль роутера;
* сервер (Server1);
* три подсети по два узла в каждой

Задача:

Для любого вилана могут быть доступны только узлы этого же вилана и серверServer1.

В таблице 8.5 и 8.6 приведены данные для установки параметров компьютерови коммутаторов.

Таблица 8.5. Конфигурация компьютеров.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Компьютер | IP адрес | Коммутатор | Порт коммутатора | VLAN |
| ПК1 | 10.11.0.11/16 | Switch4 | 4 | VLAN 11 |
| ПК2 | 10.11.0.2/16 | Switch1 | 1 | VLAN 11 |
| ПК3 | 10.13.0.3/16 | Switch1 | 2 | VLAN 13 |
| ПК4 | 10.13.0.4/16 | Switch2 | 1 | VLAN 13 |
| ПК5 | 10.12.0.5/16 | Switch2 | 2 | VLAN 12 |
| ПК6 | 10.12.0.6/16 | Switch4 | 2 | VLAN 12 |
| Server1 | 10.10.0.7/16 | Switch4 | 1 | VLAN 10 |

Таблица 8.6. Связь коммутаторов по портам.

|  |  |
| --- | --- |
| Порт центрального коммутатора Switch3 | Порт коммутатора второго уровня распределения |
| 1 | Switch1 – 3 порт |
| 2 | Switch4 – 3 порт |
| 3 | Switch2 – 3 порт |

После настройки всех коммутаторов установите самостоятельно шлюзы на всех компьютерах и сервере.

Сконфигурируйте центральный коммутатор:

Этап 1.

Перейдите к конфигурации центрального коммутатора Switch3 и создайте нанем базу VLAN.

1. Создайте VLAN 10:

Switch3>**en** Switch3#**conf t** Switch3(config) #**vlan 10**

Switch3(config-vlan)#**exit**

1. Создайте VLAN 11, VLAN 12 и VLAN 13.
2. Настройте протокол VTP в режиме сервера:

Switch3(config)#**vtp domain HOME** Switch3(config)#**vtp password HOME** Switch3(config)#**vtp mode server**

1. Просмотрите информацию о конфигурации VTP:

Switch#**sh vtp status**

1. Настройте все интерфейсы на транк:

Switch3(config)#**int fa0/1** Switch3(config-if)#**switchport mode trunk**Switch3(config- if)#**exit**

и повторите эти настройки для второго и третьего интерфейсов.Этап 2.

Перейдите к конфигурации коммутатора Switch4 и переведите его в режим client:

1. Создайте на коммутаторе VLAN 10 и задайте в нем порт 1 как access порт:

Switch4>**en** Switch4#**conf t** Switch4(config) #**vlan 10** Switch4(config- vlan)#**exit** Switch4(config)#**in t fa0/1**

Switch4(config-if)#**switchport access vlan 10**Switch4(config- if)#**switchport mode access** Switch4(config-if)#**no shut**

1. Создайте на коммутаторе VLAN 11 и задайте в нем порт 4 как access порт.
2. Создайте на коммутаторе VLAN 12 и задайте в нем порт 2 как access порт.
3. Переведите коммутатор в режим clint:

Switch4(config)#**vtp domain HOME** Switch4(config)#**vtp password HOME** Switch4(config)#**vtp mode client**

**ВАЖНО!** При вводе имени домена и пароля соблюдайте нужный регистр.Этап 4. Перейдите к конфигурации коммутатора Switch1 и выподните следующие настройки:

.

1. Создайте на коммутаторе VLAN 11 и задайте в нем порт 1 как access порт.
2. Создайте на коммутаторе VLAN 13 и задайте в нем порт 2 как access порт.
3. Переведите коммутатор в режим client.Этап 5.

Перейдите к конфигурации коммутатора Switch2.

1. Создайте на коммутаторе VLAN 12 и задайте в нем порт 2 как access

порт.

1. Создайте на коммутаторе VLAN 13 и задайте в нем порт 1 как access порт.
2. Переведите коммутатор в режим client.

Этап 6.

Проверьте работоспособность сети на канальном уровне модели OSI.

После установки всех настроек таблица VLAN разойдется по коммутаторам с помощью протокола VTP.

В результате компьютеры, расположенные в одном виллане, будут доступны друг для друга, а другие компьютеры недоступны. Проверьте связь командой PING между следующими парами компьютеров:

* ПК1 – ПК2;
* ПК3 – ПК4;
* ПК5 – ПК6.

Если Вы все сделали правильно, то ping между парами пройдет, если нет – проверьте следующие установки:

* транковыми портами являются: на Switch3 все порты, на Switch1, Switch2 иSwitch4 – третий порт;
* соединения интерфейсов на коммутаторах;
* названия и пароли доменов на каждом коммутаторе (команда sh vtp status);
* привязку интерфейсов к вилланам на коммутаторах (команда sh vl br).

Этап 7.

Настройка маршрутизации на центральном коммутаторе. Создадим интерфейсы для каждого VLAN.

Настройка интерфейса для vlan 10 (шлюз по умолчанию):

Switch3(config)#**int vlan 10**

Switch3(config-if)#**ip address 10.10.0.1 255.255.0.0**

Switch3(config-if)#**no shut**

Switch3(config-if)#**exit**

Повторите эти настройки для каждого VLAN, задавая адрес IP: 10.[VLAN].0.1и маску

/16.

После этого зайдите в настройки каждого компьютера и установите нужныйшлюз по умолчанию. Например для ПК1 – 10.11.0.1.

Включите маршрутизацию командой:

Switch3(config)#**ip routing**

Этап 8.

Проверьте работоспособность сети на сетевом уровне модели OSI.

После включения маршрутизации все компьютеры будут доступны с любогохоста. Этап 9.

Выполним основную задачу работы: для любого вилана могут быть доступнытолько узлы этого же вилана и сервер Server1.

Для этого введем следующие ограничения на трафик сети:1 - Разрешить пакеты от любого хоста к серверу.

1. - Разрешить пакеты от сервера до любого хоста.
2. – Трафик от одной подсети к этой же подсети

разрешить.4 – Правило по умолчанию: запретить всё остальное.

Ограничения на трафик сети задаются с помощью команды фильтрации **access- list**. Данная команда задает критерии фильтрации в списке опций разрешения и запрета, называемом списком доступа. Списки доступа имеют два правила:**permit** – разрешить и **deny** – запретить. Данные правила либо пропускают пакет дальше по сети, либо блокируют его доступ.

Открываем центральный коммутатор (Switch3) и меняем его конфигурацию спомощью команды фильтрации **access-list**:

Switch3(config)#**ip access-list extended 100**

(создается расширенный список доступа под номером 100)

Switch3(config-ext-nacl)#**permit ip any 10.10.0.0 0.0.0.255**

Switch3(config-ext-nacl)#**permit ip 10.10.0.0 0.0.0.255 any**

(разрешается доступ к сети 10.10.0.0/24)

Switch3(config-ext-nacl)#**permit ip 10.11.0.0 0.0.0.255**

**10.11.0.0**

|  |  |  |  |
| --- | --- | --- | --- |
| 0.0.0.255Switch3(config-ext- nacl)#**permit**  **0.0.0.255** | **ip** | **10.12.0.0 0.0.0.255** | **10.12.0.0** |
| Switch3(config-ext-  nacl)#**permit0.0.0.255** | **ip** | **10.13.0.0 0.0.0.255** | **10.13.0.0** |

(разрешается: доступ из сети 10.11.0.0/24 в эту же сеть;

доступ из сети 10.12.0.0/24 в эту же сеть; доступ из сети 10.13.0.0/24 в эту же сеть).

Switch3(config-ext-nacl)#**exit**

Теперь этот access-list наложим на конкретный интерфейс и применим ко всем VLAN-ам на входящий трафик (опция **in –** на входящий трафик, **out –** на исходящий трафик):

Switch3(config)#**int vlan 10** Switch3(config-if)#**ip access- group 100 in**Этот шаг повторяем для каждого из VLAN-ов.

В результате получим:

для любого вилана могут быть доступны только узлы этого же вилана и серверServer1.

## Самостоятельная работа .

На предприятии имеется два отдела, схема сетей которых представлена на рис.8.13.

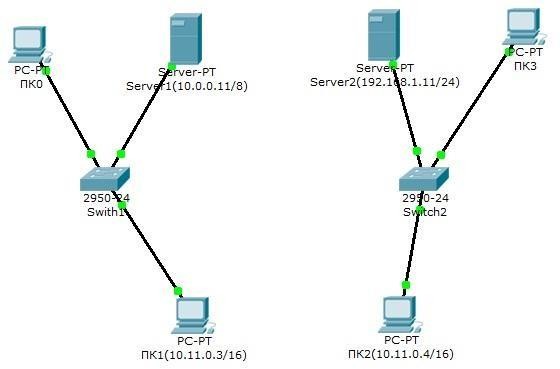


Рис.8.13. Схема сетей отделов предприятия. Отдел 1 – Switch1, отдел 2 – Switch2.

В каждой сети имеется сервер со службами DHCP, DNS и HTTP (на серверахServer1 и Server2 расположены интернет-сайты отделов).

Компьютеры ПК0 и ПК3 с DHCP серверов своих сетей получают параметры IPадреса и шлюз.

Компьютеры ПК1 и ПК2 находятся в отдельной сети в одном VLAN. Задание:

Дополните схему сети маршрутизатором или коммутатором третьего уровня,чтобы обеспечить работу корпоративной сети в следующих режимах:

1. - компьютеры ПК0 и ПК3 должны открывать сайты каждого отдела;
2. – компьютеры ПК1 и ПК2 должны быть доступны только друг для друга.

## Контрольные вопросы.

* 1. Для чего создаются виртуальные локальные сети? Каковы их достоинства?
  2. Как связываются между собой VLAN и порты коммутатора?
  3. Как обеспечивается общение между узлами разных виртуальных сетей?
  4. Как обеспечивается управление виртуальными локальными сетями?
  5. Можно ли построить VLAN на нескольких коммутаторах? Как это сделать?
  6. Для чего служит идентификатор кадра (tag)? Где он размещается?
  7. Что такое транк? Как он создается на коммутаторе и маршрутизаторе?
  8. Какие команды используются для назначения VLAN на интерфейсы?
  9. Какие команды используются для создания транковых соединений?
  10. Какие команды используются для верификации VLAN?

**Практическая работа №8** Устранение петель - STP в Cisco Packet Tracer

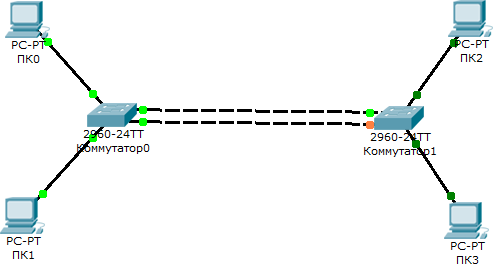
**Цель:** Изучение протокола STP в сети с избыточной топологией. Используя эмулятор сети Cisco Packet Tracer, изучить работу протокола STP по устранению коммутационных петель в сети с избыточной топологией связей.

Материально-техническое обеспечение:

* + 1. Рабочее место обучающегося – ПК, Windows 10
    2. Эмулятор построения сетей Cisco Packet Tracer 5.3.2
    3. Презентация «Lesson6.pdf» из папки «Видеоуроки Cisco Packet Tracer (Курс молодого бойца)\Презентации»
    4. Видео «6.STP.mp4» [19:07] из папки «Видеоуроки Cisco Packet Tracer (Курс молодого бойца)\Видео»

Задание:

* + - 1. Создать в Cisco Packet Tracer простейшую сеть, содержащую конфигурационную петлю, изображённую следующей схеме:



* + - 1. Выставить на ПК IP-адреса и маски из класса C так, чтобы все компьютеры оказались в одной подсети.
      2. Войти в конфигурацию каждого из двух коммутаторов и просмотреть настройки протокола STP (#show spanning-tree)
      3. Определить какой из коммутаторов назначен корневым. В комментарии к скриншотам указать почему именно данный коммутатор назначен корневым.
      4. Перечислить в столбец порты 0-го и 1-го коммутаторов и указать их роли статус в протоколе STP.
      5. Выключить работающий порт на одном из коммутаторов и пронаблюдать за работой протокола STP, как он будет переключать заблокированный ранее порт в рабочий режим. Включить выключенный на 6-м шаге порт. Дождаться окончания работы STP. Открыть командную строку на одном из ПК 1-го коммутатора и запустить там

«бесконечный пинг» (PC>ping 192.168.1.xx -t). Снова выключить порт. По количеству «потерянных» пинг-пакетов определить время сходимости (срабатывания) протокола STP.

* + - 1. Переключить оба коммутатора на более быстрый протокол RSTP (#spanning-tree mode rapid-pvst).
      2. Включит порт (#shutdown), отключённый на шаге 5, и пронаблюдать за работой протокола RSTP.
      3. Определить время сходимости протокола RSTP по аналогии с шагом 7.

**Отчёт о проделанной работе** необходимо оформить в MS Word. Он должен содержать: дату, тему и цель работы, описание всех шагов задания со скриншотами и подробными комментариями, вывод о проделанной работе и ответы на контрольные вопросы.

## Контрольные вопросы:

1. Что такое избыточная топология сети и резервирование соединений? Для чего оно используется?
2. В чём состоит суть метода агрегирования каналов?
3. Что такое коммутационная петля и к каким проблемам в сетях передачи данных она может приводить?
4. Для чего предназначен протокол связующего дерева – STP? Какие проблемы он решает?
5. Что такое время сходимости протокола?
6. Какие более современные аналоги протокола STP используются в настоящее время? Какое они имеют преимущество?
7. Какая запись в конфигурации коммутатора свидетельствует от том, что он является корневым?
8. Какая роль может быть назначена каждому порту по протоколу STP?
9. В каких состояниях может находиться порт в соответствии с протоколом STP?
10. На основании каких соображений коммутаторы Cisco рассчитывают BID порта?
11. На основании каких соображений коммутаторы Cisco выбирают назначенные порты на некорневых коммутаторах?

**Практическая работа №9** Агрегация каналов - EtherChannel в Cisco Packet Tracer

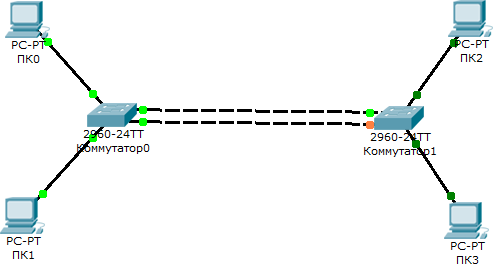
**Цель:** Используя эмулятор сети Cisco Packet Tracer, изучить работу протокола STP по устранению коммутационных петель в сети с избыточной топологией связей.

Материально-техническое обеспечение:

1. Рабочее место обучающегося – ПК, Windows 10
2. Эмулятор построения сетей Cisco Packet Tracer 5.3.2
3. Презентация «Lesson6.pdf» из папки «Видеоуроки Cisco Packet Tracer (Курс молодого бойца)\Презентации»
4. Видео «6.STP.mp4» [19:07] из папки «Видеоуроки Cisco Packet Tracer (Курс молодого бойца)\Видео»

Задание:

* 1. Создать в Cisco Packet Tracer простейшую сеть, содержащую конфигурационнуюпетлю, изображённую следующей схеме:



* 1. Выставить на ПК IP-адреса и маски из класса C так, чтобы все компьютеры оказались в одной подсети.
  2. Войти в конфигурацию каждого из двух коммутаторов и просмотреть настройкипротокола STP (*#show spanning-tree*)
  3. Определить какой из коммутаторов назначен корневым. В комментарии к скриншотам указать почему именно данный коммутатор назначен корневым.
  4. Перечислить в столбец порты 0-го и 1-го коммутаторов и указать их роли статусв протоколе STP.
  5. Выключить работающий порт на одном из коммутаторов и пронаблюдать за работой протокола STP, как он будет переключать заблокированный ранее портв рабочий режим.
  6. Включить выключенный на 6-м шаге порт. Дождаться окончания работы STP. Открыть командную строку на одном из ПК 1-го коммутатора и запустить там

«бесконечный пинг» (*PC>ping 192.168.1.xx -t*). Снова выключить порт. По количеству «потерянных» пинг-пакетов определить время сходимости (срабатывания) протокола STP.

* 1. Переключить оба коммутатора на более быстрый протокол RSTP

*(#spanning-tree mode rapid-pvst).*

* 1. Включит порт (*#shutdown*), отключённый на шаге 5, и пронаблюдать за работойпротокола RSTP.
  2. Определить время сходимости протокола RSTP по аналогии с шагом 7.

**Отчёт о проделанной работе** необходимо оформить в MS Word. Он должен

содержать: дату, тему и цель работы, описание всех шагов задания со скриншотами иподробными комментариями, вывод о проделанной работе и ответы на контрольные вопросы.

Контрольные вопросы:

1. Что такое избыточная топология сети и резервирование соединений? Для чего оно используется?
2. В чём состоит суть метода агрегирования каналов?
3. Что такое коммутационная петля и к каким проблемам в сетях передачи данныхона может приводить?
4. Для чего предназначен протокол связующего дерева – STP? Какие проблемы онрешает?
5. Что такое время сходимости протокола?
6. Какие более современные аналоги протокола STP используются в настоящее время? Какое они имеют преимущество?
7. Какая запись в конфигурации коммутатора свидетельствует от том, что он является корневым?
8. Какая роль может быть назначена каждому порту по протоколу STP?
9. В каких состояниях может находиться порт в соответствии с протоколом STP?
10. На основании каких соображений коммутаторы Cisco рассчитывают BID

порта?

1. На основании каких соображений коммутаторы Cisco выбирают назначенные

порты на некорневых коммутаторах?

**Практическая работа №10** Построение одноранговой сети. Создание общих сетевых ресурсов.

## Цель:

* закрепить умение осуществлять оконцовку витой пары с использованиемконнекторов 8P8C;
* закрепить умение осуществлять первичную настройку сетевых параметров в ОС Windows для первичной настройки одноранговой сети.

Материально-технические средства:

* 1. Ноутбуки с установленной ОС MS Windows.
  2. Витая пара UTP5 – 3 метра.
  3. Коннекторы 8P8C (RJ-45) – 4 шт.
  4. Кримпер 8P8C (RJ-45).
  5. Тестер витой пары. Первая часть работы

Для выполнения работы необходимо изготовить патч-корд с разъёмами RJ-45 в соответствии с расстоянием от вашего ноутбука до центрального

коммуникационного устройства – коммутатора (Switch). В среднем это расстояние будет составлять около 3-х метров, у кого-то меньше.

Патч-корд необходим для подключения компьютера к коммутатору, т.е. соединяемые устройства принадлежат к разным уровням модели OSI, а потому используем прямой провод обжатый по схеме:



После изготовления паnч-корда его необходимо протестировать с помощью тестера витой пары. При подключении провода к порту коммутатора на его панели должен светиться зелёным или жёлтым светом соответствующий индикатор.

Аналогичный индикатор должен загореться при подключении патч-корда к сетевой карте ноутбука.

Если тестер витой пары показал правильное обжатие и при включении патч- корда в ноутбук и в коммутатор световые индикаторы работают в нормальном

режиме, то можно перейти к настройке первичных сетевых параметров. К ним относятся: IP-адрес (ip), маска сети (net mask), сетевой шлюз (gateway), DNS-сервера(dns).

IP-адрес однозначно идентифицирует данный компьютер в сети и должен быть уникальным, т.е. не допускается использование одинаковых сетевых адресов впределах одного сетевого сегмента.

IP-адрес состоит из 4-х байт. Каждый байт записывается в виде отдельного десятичного числа через точку. Например: 192.168.1.1. Т.к. в одном байте можно записать числа от 0000 00002 до 1111 11112, то это соответствует десятичным

числам от 0 до 255.

Для частных сетей рекомендуется несколько диапазонов IP-адресов. Вам надо будет настроить адреса в подсети 192.168.1.0.

Маска сети предназначена для указания того, какая часть IP-адреса относитсяк адресу сети, а какая к адресу узла. В двоичном виде маска сети имеет вид: 1111 1111.1111 1111.1111 1111.0000 0000. В этой записи каждому байту IP-адреса сопоставляется соответствующий байт маски сети. Единичные биты в маске сети показывают на те биты IP-адреса, которые соответствуют адресу сети. Нулевые биты

«показывают» на номер (адрес) узла в подсети.

Для первичной настройки сети вам достаточно будет задать всего лишь два сетевых параметра:

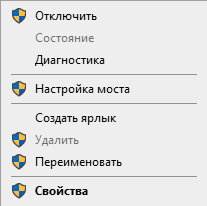
IP-адрес: 192.168.1.???

Маска: 255.255.255.0

Вместо знаков вопроса вы должны поставить свой собственный IP-адрес, который соответствует вашему порядковому номеру в списке группы.

В Windows 10 данные настройки можно найтизапустив «Панель управления» и выбрав там опцию «Сеть и Интернет».

Затем надо перейти в «Центр управления сетями иобщим доступом»



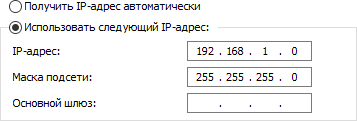
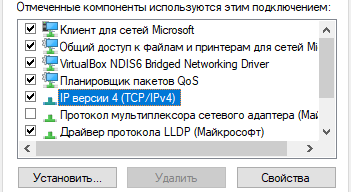
После этого нажимаем на ссылку в левом меню

«Изменениепараметров адаптера». Выбираем нужное сетевое

подключение Ethernet. Нажимаем на него правой кнопкоймыши и выбираем в контекстном меню пункт свойства.

После выбора данного пункта меню должно появиться окносетевых настроек вида:

Т.к. мы будем настраивать протокол TCP/IPверсии 4, то необходимо выбрать соответствующий пункт «IP версии 4 (TCP/IPv4)»и нажать кнопку свойства, которая после выбора настраиваемого пункта станет доступной.

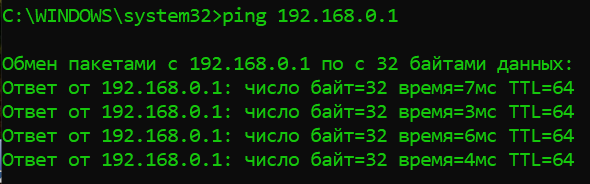


Далее мы должны увидеть окно сетевых настроек, где необходимо будет ввести свой IP-адрес 192.168.1.??? и маску сети 255.255.255.0. После чего последовательно двараза нажать кнопку «Ok».

В данной работе выставлять адреса DNS-серверов не нужно!

На следующем этапе требуется запустить со своего ноутбука командную строку нажав Win+R, а затем набрав cmd.exe. Из командной строки необходимо пропинговать компьютер преподавателя, имеющий IP-адрес 192.168.1.0, и

убедиться, что данный компьютер доступен по сети. В командной строке набираемping 192.168.1.0. При этом мы должны получить ответ вида:

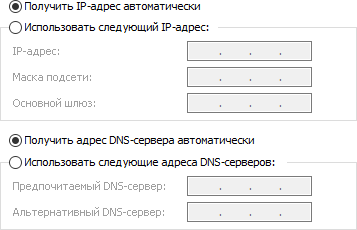


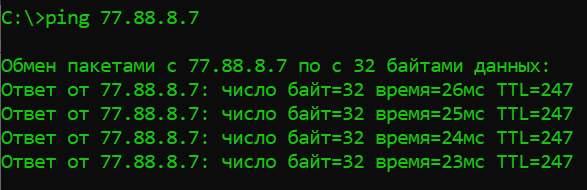
Положительный тест команды ping надо показать преподавателю!

Вторая часть работы

Вторая часть работы состоит в том, чтобы настроитьсвои компьютеры на сеть Интернет, выставив на

сетевых настройках автоматическое получение адресов «Получить IP-адрес автоматически» и на автоматическое получение адресов DNS- серверов,установив переключатель «Получать адреса DNS-сервера автоматически».

После этого необходимо проверить значок сетевого соединения в системном трее, он должен показывать «Доступ к Интернету». А также для проверки работоспособности сети Интернет надо запустить командную строку и пропинговать DNS-адреса поисковой системы Яндекс: ping 77.88.8.7 и ping 77.88.8.3.



Положительный тест команды ping надо показать преподавателю! Письменный отчёт о проделанной работе должен содержать:

1. Тему работы.
2. Цель работы.
3. Используемые материально-технические средства.
4. Ход работы (подробное описание всех шагов работы).
5. Вывод

* что нужно, чтобы настроить компьютеры для работы в одноранговой сети;
* как можно настроить компьютер сети на работу с DHCP при подключении к Интернету.

1. Ответы на контрольные вопросы.

## Контрольные вопросы:

1. В каких случаях при монтаже сети необходимо применять прямой обжимвитой пары?
2. При соединении каких устройств используется обжим «кроссовер»?
3. Какие первичные сетевые настройки необходимо выставить для того, чтобыкомпьютеры в сети могли «видеть» друг друга?
4. Для чего нужен IP-адрес в сетях TCP/IP?
5. Что показывает маска сети в сетевых настройках?
6. Как с помощью утилиты ping можно проверить доступность другогокомпьютера в сети?
7. Как с помощью утилиты ping можно проверить наличие Интернета накомпьютере?

**Практическая работа №11** Организация сетевого шлюза (Настройка программного маршрутизатора)

**Цель:** *Закрепить знания и навыки настройки виртуальных сетей VLAN. Научиться выполнять настройку маршрутизации между виртуальными сетями в*

*маршрутизаторах.*

Материально-техническое обеспечение:

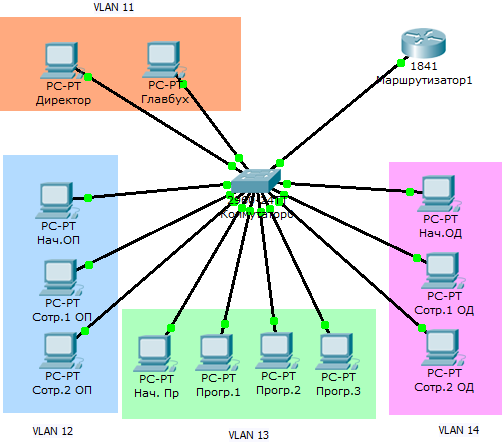
1. Рабочее место обучающегося – ПК, Windows 10
2. Эмулятор построения сетей Cisco Packet Tracer 5.3.2
3. Презентация «Lesson9.pdf» из папки «Видеоуроки Cisco Packet Tracer (Курсмолодого бойца)\Презентации»
4. Видео «9.Маршрутизатор.mp4» [24:20] из папки «Видеоуроки Cisco PacketTracer (Курс молодого бойца)\Видео» - до момента 15:10.

Что нужно сделать (задача)

Необходимо построить сеть небольшой организации, занимающейся разработкой ПО, в которой работают следующие сотрудники: директор, главный бухгалтер, начальник отдела проектирования с двумя сотрудниками, начальник отдела дизайна с двумя сотрудниками и начальник отдела разработки с тремя программистами:

Алгоритм выполнения сетевых настроек

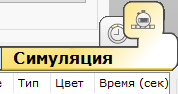
VLAN 11 - руководство VLAN 12 -

ОП (отдел проектиров ания) VLAN 13 -

Пр. (отдел программи рования)

VLAN 14 – ОД (отдел дизайна)

Рис.1

1. Построить в Cisco Packet Tracer сеть по приведенному на Рис. 1 образцу.
2. Подключить все ПК поочерёдно к свободным портам fastEthernet коммутатора- 0(2960).
3. Подключить очередной свободный порт fastEthernet коммутатора 2960 кпервому свободному порту маршрутизатора 1841.
4. Войти в настройки коммутатора-0 (2960) и создать там четыре виртуальных сетис номерами 11, 12, 13 и 14. Имена виртуальным сетям присвоить VLAN11, VLAN12, VLAN13 и VLAN14 соответственно. Смотри п. I.
5. Включить на коммутаторе 2960 в каждый порт, подключённый к ПК,соответствующую виртуальную сеть vlan. Смотри п. II.
6. Настроить на коммутаторе 2960 trunk-порт, соединяющий его с маршрутизатором 1841, разрешив для этого порта все виртуальные сети 11, 12,13 и 14. Смотри п. III.
7. Войти на роутере 1841 в конфигурирование в режиме настроек (без диалога).Смотри п. IV.
8. Включить на роутере 1841 необходимый для связи с коммутатором 2960 порт.Смотри п. V.
9. Настройка на роутере (1841) sub-интерфейсов и подключение на них всехсоответствующих vlan. Смотри п. VI.
10. Сделать сетевые настройки для всех ПК в локальной сети. Смотри п. VII.
11. Выполнить тестирование сети с помощью команды ping в командной строке компьютера. При этом должны пинговаться шлюзы sub-интерфейсов роутера ивсе другие компьютеры во всех виртуальных сетях.
12. Проверить прохождение пакетов в сети из режима симуляции:

Как выполнить настройки (основные команды)

## Настройка vlan на коммутаторе 2-го уровня (2960):

*Замечание: На маршрутизаторах vlan не настраивают, т.к. vlan работаетна 2-м уровне OSI.*

* 1. enable;
  2. configure terminal;
  3. vlan 100 – создание на коммутаторе vlan с номером 100;
  4. name VLAN100 – задание настраиваемой vlan имени VLAN100;
  5. exit.

1. Включение созданных vlan в соответствующий порт доступа

коммутатора:

1. interface fa0/1 – войти в конфигурирование интерфейса fa0/1;
2. switchport mode access – переключить порт в режим доступа;
3. switchport access vlan 100 – подключить к порту доступа vlan с номером 100;
4. exit.
5. Включение всех созданных vlan в соответствующий trunk-порт:
6. interface fa0/1 – войти в конфигурирование транкового порта fa0/1;
7. switchport mode trunk – задать для порта режим транка;
8. switchport trunk allowed vlan x1,x2,x3 – разрешить пропускать черезтранковый порт виртуальные сети с номерами x1, x2 и x3;
9. exit.
10. Входим на роутере (1841) в конфигурирование в режиме настроек (бездиалога):

Continue with configuration dialog? [yes/no]: no

1. Включение необходимых портов на роутере:
   1. interface fa0/1 – войти в настройки порта fa0/1;
   2. no shutdown – включить порт;
   3. exit.
2. Настройка на роутере (1841) sub-интерфейсов и подключение на них

соответствующей vlan:

*Замечание 1: Для каждой vlan надо создать свой sub-интерфейс на роутере.*

*Замечание 2: На маршрутизаторах и межсетевых экранах все порты поумолчанию выключены. Поэтому для того, чтобы можно было их*

*использовать, необходимо их включить.*

* 1. enable;
  2. configure terminal;
  3. **interface fa0/0.2** – начать конфигурирование sub-interface (под-интерфейса) сномером 2 на интерфейсе с номером 0, к которому подключён коммутатор;
  4. **encapsulation dot1q 100** – подключить к sub-интерфейсу vlan с номером 100 врежиме инкапсуляции dot1q;
  5. ip address 192.168.100.1 255.255.255.0 – задать sub-интерфейсу ip- адрес,который будет шлюзом vlan;
  6. no shutdown – включить порт sub-интерфейса, который по умолчанию нароутере тоже выключен;
  7. exit.
  8. Настройка ПК:Выставить на каждом ПК ip-адрес вида 192.168.XX.YY, где XX – номер соответствующей vlan, YY – уникальный адрес ПК в подсети, начиная со 2- го;
  9. Задать на каждом ПК маску 255.255.255.0;
  10. Указать на каждом ПК шлюз вида 192.168.YY.1, где YY – номер соответствующей данному ПК vlan.

Отчёт о проделанной работе:

Отчёт необходимо оформить в MS Word. Он должен содержать: дату, тему и цель работы, описание всех шагов задания со скриншотами и подробными комментариями, вывод о проделанной работе и ответы на контрольные вопросы.

## Контрольные вопросы:

1. В каких сетях более целесообразно использовать L3-коммутаторы вместомаршрутизаторов и почему?
2. Назовите основные преимущества маршрутизаторов, которые отсутствуют в L3-коммутуторах.
3. На каком уровне модели OSI работают устройства:
   1. L2-коммутаторы,
   2. L3-коммутаторы,
   3. маршрутизаторы?
4. Возможна ли настройка в маршрутизаторах виртуальных сетей vlan и почему?
5. Почему на коммутаторах все порты по умолчанию являются активными, а намаршрутизаторах наоборот – выключены?

**Практическая работа №12** Настройка протоколов TCP/IP в операционных системах» (работа с диагностическими утилитами протокола ТСР/IР, решение проблем с TCP/IP).

**Цель работы:** обобщение и систематизация знаний по теме

«Межсетевое взаимодействие»

Целью устранения неисправностей в настройке TCP/IP является восстановление нормальной работы сети. Для поиска неисправностей можно использовать специальные диагностические утилиты, предназначенные для проверки конфигурации стека TCP/IP и тестирования сетевого соединения

Практическое задание Задание 1. Получение справочной информации по командам. Выведите на экран справочную информацию по всем рассмотренным утилитам (см. таблицу п.1). Для этого в командной строке (значок Windows + R, затем ввести cmd, затем

Enter) введите имя утилиты без параметров и дополните /?

|  |  |
| --- | --- |
| **arp** | *Выводит для просмотра и изменения таблицу трансляции адресов, используемую*  *протоколом разрешения адресов ARP (Address Resolution Protocol - определяет локальныйадрес по IP-адресу)* |
| **hostname** | *Выводит имя локального хоста. Используется без параметров.* |
| **ipconfig** | *Выводит значения для текущей конфигурации стека TCP/IP: IP-адрес, маску подсети,*  *адрес шлюза по умолчанию, адреса WINS (Windows Internet Naming Service) и DNS(Domain Name System)* |
| **nbtstat** | *Выводит статистику и текущую информацию по NetBIOS, установленному поверх*  *TCP/IP. Используется для проверки состояния текущих соединений NetBIOS.* |
| **netstat** | *Выводит статистику и текущую информацию по соединению TCP/IP.* |
| **nslookup** | *Осуществляет проверку записей и доменных псевдонимов хостов, доменных сервисов*  *хостов, а также информации операционной системы, путем запросов к серверам DNS.* |
| **ping** | *Осуществляет проверку правильности конфигурирования TCP/IP и проверку связи с*  *удаленным хостом.* |
| **route** | *Модифицирует таблицы маршрутизации IP. Отображает содержимое таблицы,*  *добавляет и удаляет маршруты IP.* |
| **tracert** | *Осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-*  *пакетов протокола ICMP (Internet Control Message Protocol). Выводит маршрутпрохождения пакетов на удаленный компьютер.* |

1. Сохраните справочную информацию в отдельном файле.
2. Изучите ключи, используемые при запуске утилит. Задание 2. Получение имени хоста.
3. Выведите на экран имя локального хоста с помощью команды hostname.
4. Сохраните результат в отдельном файле. Задание 3. Изучение утилиты ipconfig.

1. Проверьте конфигурацию TCP/IP с помощью утилиты ***ipconfig***. Заполните таблицу:

|  |  |
| --- | --- |
| Имя хоста |  |
| IP-адрес |  |
| Маска подсети |  |

|  |  |
| --- | --- |
| Основной шлюз |  |
| Используется ли DHCP (адрес DHCP-сервера) |  |
| Описание адаптера |  |
| Физический адрес сетевого адаптера |  |
| Адрес DNS-сервера |  |
| Адрес WINS-сервера |  |

**Задание 4.** Тестирование связи с помощью утилиты ping.

Утилита ping (Packet Internet Grouper) используется для проверки конфигурирования TCP/IP и диагностики ошибок соединения. Она определяет доступность и функционирование указанного узла и позволяет измерить время прохождения пакетов от данного узла до любого другого узла сети. Использование ping лучший способ проверки того, что между локальным компьютером и сетевым хостом существует маршрут. (Хостом называется любое сетевое устройство (компьютер, маршрутизатор), обменивающееся информацией с другими сетевыми устройствами по TCP/IP.)

Команда ping проверяет соединение с удаленным хостом, посылая к этому хосту несколько IP-пакетов и ожидая ответы на них. При этом она измеряет интервал времени, в течение которого пакет вернулся, а также показывает соотношение количества отосланных пакетов к количеству принятых, то может служить субъективной оценкой

«качества связи» между узлами. Если связь между хостами плохая, из сообщений ping станет ясно, сколько пакетов потеряно.

Утилита использует протокол ICMP. Посылаемые и получаемые IP-пакеты – это эхо-запросы и эхо-ответы протокола ICMP.

По умолчанию передается 4 эхо-пакета длиной 32 байта (периодическая последовательность символов алфавита в верхнем регистре). Ping позволяет изменить размер и количество пакетов, указать, следует ли записывать маршрут, который она использует, какую величину времени жизни (ttl) устанавливать, можно ли фрагментировать пакет и т.д.. При получении ответа в поле time указывается, за какое время (в миллисекундах) посланный пакет доходит до удаленного хоста и возвращается назад. Так как значение по умолчанию для ожидания отклика равно 1 секунде, то все значения данного поля будут меньше 1000 миллисекунд. Если вы получаете сообщение

«Request time out» (Превышен интервал ожидания), то, возможно, если увеличить время ожидания отклика, пакет дойдет до удаленного хоста. Это можно сделать с помощью ключа –w.

Ping можно использовать для тестирования как имени хоста (DNS или NetBIOS), так и его IP-адреса. Если pingс IP-адресом выполнилась успешно, а с именем – неудачно, это значит, что проблема заключается в распознавании соответствия адреса и имени, а не в сетевом соединении.

* 1. Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.
  2. Проверьте возможность установления соединения с удаленным хостом.
  3. С помощью команды ping проверьте адреса (взять из списка локальных ресурсов на сайте aspu.ru)и для каждого из них отметьте время отклика.

1) Для проверки того, что TCP/IP установлен и правильно сконфигурирован на локальном компьютере,в команде ping задается адрес петли обратной связи (loopback address): ping 127.0.0.1

Если тест успешно пройден, то вы получите следующий ответ: Reply from 127.0.0.1

Reply from 127.0.0.1

Reply from 127.0.0.1

Reply from 127.0.0.1

Чтобы убедиться в том, что компьютер правильно добавлен в сеть и IP-адрес не дублируется, используется IP-адрес локального компьютера:

ping IP-адрес\_локального\_хоста

Чтобы проверить, что шлюз по умолчанию функционирует и что можно установить соединение с любым локальным хостом в локальной сети, задается IP-адрес шлюза по умолчанию:

ping IP-адрес\_шлюза

Для проверки возможности установления соединения через маршрутизатор в команде ping задается IP-адрес удаленного хоста:

ping IP-адрес\_удаленного хоста Синтаксис утилиты ping:

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [ [-j host-list] | [- k host-list] ] [-w timeout] destination-list

Параметры:

-t выполняет команду ping до прерывания. Control-Break - посмотреть статистику и продолжить.

Control-C - прервать выполнение команды;

-a позволяет определить доменное имя удаленного компьютера по его IP-адресу;

-n count посылает количество пакетов ECHO, указанное параметром count;

-l length посылает пакеты длиной length байт (максимальная длина 8192 байта);

-f посылает пакет с установленным флагом «не фрагментировать». Этот пакет не будет фрагментироваться на маршрутизаторах по пути своего следования;

-i ttl устанавливает время жизни пакета в величину ttl (каждый маршрутизатор уменьшает ttl на единицу);

-v tos устанавливает тип поля «сервис» в величину tos;

-r count записывает путь выходящего пакета и возвращающегося пакета в поле записи пути. Count - от 1 до 9 хостов;

-s count позволяет ограничить количество переходов из одной подсети в другую (хопов). Count задает максимально возможное количество хопов;

-j host-list направляет пакеты с помощью списка хостов, определенного параметром host-list. Последовательные хосты могут быть отделены промежуточными маршрутизаторами (гибкая статическая маршрутизация). Максимальное количество хостов в списке, позволенное IP, равно 9;

-k host-list направляет пакеты через список хостов, определенный в host-list.

Последовательные хосты не могут быть разделены промежуточными маршрутизаторами (жесткая статическая маршрутизация). Максимальное количество хостов – 9;

-w timeout указывает время ожидания (timeout) ответа от удаленного хоста в миллисекундах (по умолчанию – 1сек);

destination-list указывает удаленный хост, к которому надо направить пакеты ping.

Пример использования утилиты ping. C:\WINDOWS>ping –n 10

Обмен пакетами с [205.188.247.65] по 32 байт:

Ответ от 205.188.247.65: число байт=32 время=194мс TTL=48 Ответ от 205.188.247.65: число байт=32 время=240мс TTL=48 Ответ от 205.188.247.65: число байт=32 время=173мс TTL=48 Ответ от 205.188.247.65: число байт=32 время=250мс TTL=48 Ответ от 205.188.247.65: число байт=32 время=187мс TTL=48 Ответ от 205.188.247.65: число байт=32 время=239мс TTL=48 Ответ от 205.188.247.65: число байт=32 время=263мс TTL=48 Ответ от 205.188.247.65: число байт=32 время=230мс TTL=48 Ответ от 205.188.247.65: число байт=32 время=185мс TTL=48 Ответ от 205.188.247.65: число байт=32 время=406мс TTL=48 Статистика Ping для 205.188.247.65:

Пакетов: послано = 10, получено = 10, потеряно = 0 (0% потерь) Приблизительное время передачи и приема:

Наименьшее = 173мс, наибольшее = 406мс, среднее =236мс Задание 5. Определение пути IP-пакета.

**Tracert** - это утилита трассировки маршрута. Она позволяет проследить путь от данного узла до любого другого узла сети Internet. Хост за хостом показывается прохождение IP-пакетов, при этом выводится название и IP-адрес каждого пройденного хота, а также значение интервала времени, в течение которого был получен ответ.

Утилита использует поле TTL (time-to-live, время жизни) из заголовка IP-пакета и сообщения об ошибках протокола ICMP для определения маршрута от одного хоста до другого.

Утилита tracert может быть более содержательной и удобной, чем ping, особенно в тех случаях, когда удаленный хост недостижим. С помощью нее можно определить район проблем со связью (у Internet-провайдера, в опорной сети, в сети удаленного хоста) по тому, насколько далеко будет отслежен маршрут. Если возникли проблемы, то утилита выводит на экран звездочки (\*), либо сообщения типа «Destination net unreachable»,

«Destination host unreachable», «Request time out», «Time Exeeded».

Утилита tracert работает следующим образом: посылается по 3 пробных эхо-пакета на каждый хост, через который проходит маршрут до удаленного хоста. На экран при этом выводится время ожидания ответа на каждый пакет (Его можно изменить с помощью параметра -w). Пакеты посылаются с различными величинами времени жизни. Каждый маршрутизатор, встречающийся по пути, перед перенаправлением пакета уменьшает величину TTL на единицу. Таким образом, время жизни является счетчиком точек промежуточной доставки (хопов). Когда время жизни пакета достигнет нуля, предполагается, что маршрутизатор пошлет в компьютер-источник сообщение ICMP “Time Exeeded” (Время истекло). Маршрут исследуется путем посылки первого эхо- пакета с TTL=1. Затем TTL увеличивается на 1 в каждом последующем пакете до тех пор, пока пакет не достигнет удаленного хоста, либо будетдостигнута максимально возможная величина TTL (по умолчанию 30, задается с помощью параметра -h).

С помощью команды tracert проверьте для адреса yarus.aspu.ru, через какие промежуточные узлы идет сигнал. Изучите ключи команды.

Маршрут определяется путем изучения сообщений ICMP, которые присылаются обратно промежуточными маршрутизаторами.

Примечание: некоторые маршрутизаторы просто молча уничтожают пакеты с истекшим TTL и не будут видны утилите tracert.

Синтаксис:

tracert [-d] [-h maximum\_hops] [-j host-list] [-w timeout] имя\_целевого\_хоста Параметры:

-d указывает, что не нужно распознавать адреса для имен хостов;

-h maximum\_hops указывает максимальное число хопов для того, чтобы искать

цель;

-j host-list указывает нежесткую статическую маршрутизацию в соответствии с

host-list;

-w timeout указывает, что нужно ожидать ответ на каждый эхо-пакет заданное число мсек.

**Задание 6.** Просмотр ARP-кэша.

Основная задача протокола ARP – трансляция IP-адресов в соответствующие локальные адреса. Для этого ARP-протокол использует информацию из ARP-таблицы (ARP-кэша). Если необходимая запись в таблице не найдена, то протокол ARP отправляет широковещательный запрос ко всем компьютерам локальной подсети, пытаясь найти владельца данного IP-адреса. В кэше могут содержаться два типа записей: статические и динамические. Статические записи вводятся вручную и хранятся в кэше постоянно.

Динамические записи помещаются в кэш в результате выполнения широковещательных запросов. Для них существует понятие времени жизни. Если в течение определенного времени (по умолчанию 2 мин.) запись не была востребована, то она удаляется из кэша.

* 1. С помощью утилиты arp просмотрите ARP-таблицу локального компьютера.
  2. Внести в кэш локального компьютера любую статическую запись. Утилита arp выводит для просмотра и изменения таблицу трансляции адресов.

Синтаксис:

arp [-s inet\_addr eth\_addr] | [-d inet\_addr] | [-a] Параметры:

-s занесение в кэш статических записей;

-d удаление из кэша записи для определенного IP-адреса;

-a просмотр содержимого кэша для всех сетевых адаптеров локального компьютера;inet\_addr - IP-адрес;

eth\_addr - MAC-адрес.

**Задание 7.** Просмотр локальной таблицы маршрутизации.

С помощью утилиты route просмотреть локальную таблицу маршрутизации.

**Задание 8.** Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.

Утилита netstat позволяет получить статическую информацию по некоторым из протоколов стека (TCP, UDP,IP, ICMP), а также выводит сведения о текущих сетевых соединениях. Особенно она полезна на брандмауэрах, с ее помощью можно обнаружить нарушения безопасности периметра сети.

С помощью утилиты netstat выведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.

Синтаксис:

netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] Параметры:

-a выводит перечень всех сетевых соединений и прослушивающихся портов локального компьютера;

-e выводит статистику для Ethernet-интерфейсов (например, количество полученных и отправленных

байт);

-n выводит информацию по всем активным соединениям (например, TCP) для всех сетевых

интерфейсов локального компьютера. Для каждого соединения выводится информация об IP-адресах локального и удаленного интерфейсов вместе с номерами используемых портов;

-s выводит статистическую информацию для протоколов UDP, TCP, ICMP, IP. Ключ «/more» позволяет просмотреть информацию постранично;

-r выводит содержимое таблицы маршрутизации. Контрольные вопросы

1. Раскрыть термины: хост, шлюз, хоп, время жизни пакета, маршрут,маска сети, порт TCP, петля обратной связи, время отклика.
2. Какие утилиты можно использовать для проверки правильностиконфигурирования TCP/IP?
3. Каким образом команда ping проверяет соединение с удаленнымхостом?
4. Каково назначение протокола ARP?
5. Как утилита ping разрешает имена узлов в ip-адреса (и наоборот)?
6. Какие могут быть причины неудачного завершения ping и tracert? (превышен интервал ожидания для запроса, сеть недоступна, превышен срок жизнипри передаче пакета).

Содержание отчета

1. Наименование и цель лабораторной работы
2. Таблицу с полученными результатами задания 3.
3. Скриншоты выполнения лабораторной работы.
4. Выводы по лабораторной работе.
5. Ответы на контрольные вопросы.

**Практическая работа № 13** Преобразование форматов IP-адресов. Расчет IP-адреса и маски подсети.

**Цель работы:** Изучение особенностей адресации в IP – сетях. Изучение настроек подсети и маски подсети

Средства для выполнения работы:

* аппаратные: ПК;
* программные: установленная ОС Windows 7, Windows 10;
* информационные: IP-адрес; маска подсети; основной шлюз; предпочитаемый DNS.

1. Теоретические сведения

**IP-адреса** используются для идентификации устройств в сети. Для взаимодействия c другими устройствами по сети IP-адрес должен быть назначен каждому сетевому устройству — компьютерам, серверам, маршрутизаторам, принтерам и т.д. С помощью маски подсети определяется максимально возможное число хостов в конкретной сети.

Одна часть IP-адреса представляет собой адрес сети, другая — адрес хоста внутри этой сети. Адрес сети используется маршрутизаторами (роутерами) для передачи пакетов в нужные сети, тогда как адрес хоста определяет конкретное устройство в этой сети, которому должны быть доставлены пакеты.

Структура IP-адреса

IP-адрес состоит из четырех частей, записанных в виде десятичных чисел с точками (например, 192.168.1.2). Каждую из этих четырех частей называют октетом. Октет представляет собой восемь двоичных цифр (например, 11000000, или 192 в десятичном виде). Таким образом, каждый октет может принимать в двоичном виде значения от 00000000 до 11111111, или от 0 до 255 в десятичном виде.

Количество двоичных цифр в IP-адресе, которые приходятся на адрес сети, и количество цифр в IP- адресе, приходящееся на адрес хоста, могут быть различными в зависимости от маски подсети.

Частные IP-адреса

У каждого хоста в сети Интернет должен быть уникальный адрес. Если сеть изолирована от Интернета (например, связывают два филиала компании), для хостов можно использовать любые IP-адреса. Однако, уполномоченной организацией по распределению нумерации в сети Интернет (IANA) специально для частных сетей зарезервированы следующие три блока IP-адресов:

10.0.0.0 — 10.255.255.255

172.16.0.0 — 172.31.255.255

192.168.0.0 — 192.168.255.255

*IP-адреса указанных частный подсетей иногда называют «****серыми****».*

Маска подсети используется для определения того, какие биты являются частью адреса сети, а какие — частью адреса хоста (для этого применяется логическая операция

«И»). Маска подсети включает в себя 32 бита. Если бит в маске подсети равен 1, то соответствующий бит IP-адреса является частью адреса сети. Если бит в маске подсети равен 0, то соответствующий бит IP-адреса является частью адреса хоста.



Маски подсети всегда состоят из **серии последовательных единиц**, начиная с самого левого бита маски, за которой следует серия последовательных нулей, составляющих в общей сложности 32 бита.



Размер сети

Количество разрядов в адресе сети определяет максимальное количество хостов, которые могут находиться в такой сети. Чем больше бит в адресе сети, тем меньше бит остается на адрес хоста в адресе.

IP-адрес с адресом хоста из всех нулей представляет собой IP-адрес сети (например: 192.168.1.0/24).

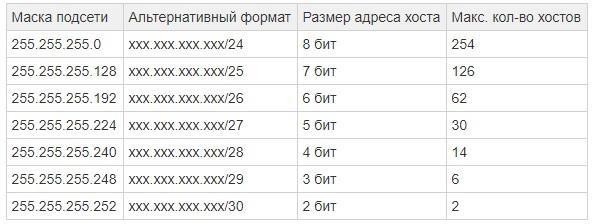
IP-адрес с адресом хоста из всех единиц представляет собой широковещательный адрес данной сети (например: 192.168.1.255/24).Так как такие два IP-адреса не могут использоваться в качестве идентификаторов отдельных хостов, максимально возможное количество хостов в сети вычисляется следующим образом:



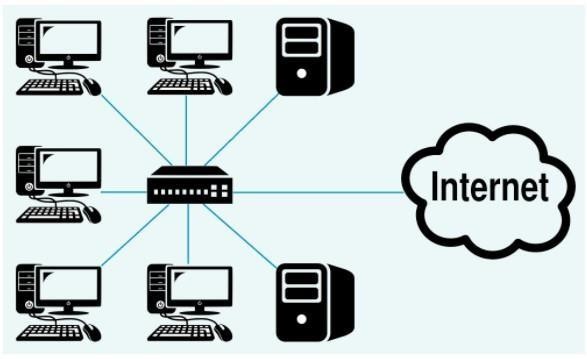
Формат записи

Поскольку маска всегда является последовательностью единиц слева, дополняемой серией нулей до 32 бит, можно просто указывать количество единиц, а не записывать значение каждого октета. Обычно это записывается через слеш после адреса и количество единичных бит в маске.

Например, адрес 192.1.1.0/25 представляет собой адрес 192.1.1.0 с маской 255.255.255.128. Некоторые возможные маски подсети в обоих форматах показаны в следующей таблице:



Формирование подсетей

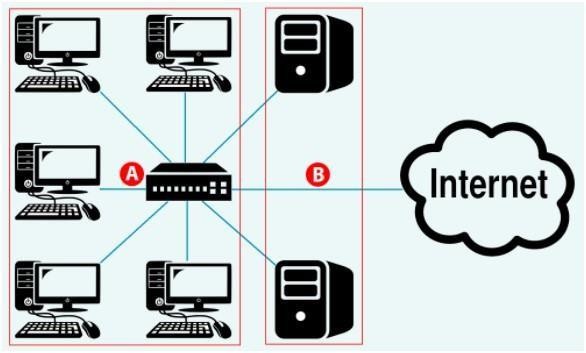
С помощью подсетей одну сеть можно разделить на несколько. В приведенном ниже примере администратор сети создает две подсети, чтобы изолировать группу серверов от остальных устройств в целях безопасности.

В этом примере сеть компании имеет адрес 192.168.1.0. Первые три октета адреса (192.168.1) представляют собой адрес сети, а оставшийся октет

— адрес хоста, что позволяет использовать в сети максимум 28 - 2 = 254 хостов.

Чтобы разделить сеть 192.168.1.0 на две отдельные подсети, нужно

«позаимствовать» один бит из адреса хоста. В этом случае маска подсети станет 25-битной (255.255.255.128 или /25). «Одолженный» бит адреса хоста может быть либо нулем, либо



единицей, что дает нам две подсети: 192.168.1.0/25 и 192.168.1.128/25. Четыре подсети

В предыдущем примере было показано использование 25-битной маски подсети для разделения 24- битного адреса на две подсети. Аналогичным образом для разделения 24- битного адреса на четыре подсети потребуется «одолжить» два бита идентификатора хоста, чтобы получить четыре возможные комбинации (00, 01, 10 и 11). Маска подсети состоит из 26 бит (11111111.11111111.11111111.11000000), то есть

255.255.255.192.

Каждая подсеть содержит 6 битов адреса хоста, что в сумме дает 26 - 2 = 62 хоста для каждой подсети (адрес хоста из всех нулей — это сама подсеть, а из всех единиц — широковещательный адрес для подсети).



Подсеть 169.254.0.0/16 используется для автоматического назначения IP операционной системой в случае, если настроено получение адреса по DHCP, но ни один сервер не отвечает.

1. Практическое задание
2. Определить тип используемых МАС и IP адресов персональных компьютеров, размещенных в лаборатории, а также маску подсети:

* Выполнить вызов меню (комбинацией клавиш windows+R)
* В появившимся окне ввести команду cmd, нажать выполнить (ENTER)
* В появившейся командной строке вводим команду **ipconfig /all**
* Записать и проанализировать полученные данные:
  1. Определить из каких частей состоит **МАС-адрес**
  2. Определить из каких частей состоит **IP-адрес**

1. Сформировать виртуальную сеть и заполнить таблицу IP-

адресов подсетей (согласно вышеуказанными примерам в разделе 1) по вариантам:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Вариант 1** | **Вариант 2** | **Вариант 3** | **Вариант 4** | **Вариант 5** | **Вариант 6** |
| **Кол-во ПК** | 5 | 6 | 8 | 4 | 7 | 9 |
| **Количество подсетей** | 2 | 3 | 4 | 2 | 3 | 3 |

Контрольные вопросы

1. В чем назначение IP-адреса?
2. Из чего состоит IP-адрес?
3. Что такое частные IP-адреса?
4. Для чего используется маска подсети?
5. От чего зависит размер сети?
6. Как построен формат записи?
7. Каким образом адреса используются для деления сетей?

Содержание отчета

1. Наименование и цель лабораторной работы
2. Таблицу с полученными результатами задания 3.
3. Скриншоты выполнения лабораторной работы.
4. Выводы по лабораторной работе.
5. Ответы на контрольные вопросы.

**Практическая работа №14** Настройка удаленного доступа к компьютеру

**Цели работы:** Получение практических навыков создания и настройки удаленного доступа к компьютеру в локальной сети.

Теоретическая часть

В ОС Windows (ещё с её версии NT) присутствует своя, родная утилита для удалённого доступа – **RDP** (сокращённо от *Remote Desktop Protocol*, сетевого протокола, использующего по умолчанию порт TCP 3389). Протокол изначально предназначен для удалённого подключения к терминальным серверам, но любой домашний пользователь может использовать этот протокол для, соответственно, домашних нужд. Но удалённое подключение по RDP - это не только штатный функционал Windows, это ещё и кроссплатформенное решение, способное соединять устройства на разных платформах. И если имеется локальная сеть, то пользователь может управлять всеми доступными ПК, ноутбуками, планшетами, а также смартфонами на расстоянии из разных помещений **без потери в скорости доступа**, как это происходит, когда мы удалённо подключаемся через Интернет посредством серверов Microsoft с помощью инструмента удалённого помощника или с помощью программ типа TeamViewer или Ammyy Admin через серверы их создателей.

Возможность штатного подключения по протоколу RDP присутствует во всех редакциях Windows 7, 8.1 и 10, начиная с Pro. Подключаться к компьютерам на базе других операционных систем можно посредством созданных для них приложений для удалённого доступа по RDP. В числе таких систем – Mac, Linux, iOS, Android и др.

Чтобы иметь возможность подключаться к удалённому сетевому компьютеру, на этом ПК необходимо настроить соответствующее разрешение в системных настройках. Также на нём должна быть запаролена та учётная запись Windows, в которую будет осуществляться удалённый вход. Это правило, кстати, можно обойти, и подключаться к незапароленной учётной записи, если в парольной защите компьютеров локальной сети нет надобности.

*Комментарий:* подключение по RDP осуществляется по IP-адресу удалённого компьютера, и если он динамический, т.е. постоянно меняющийся, его нужно сделать статическим.

Практическая часть

1. Выполнить настройку удаленного ПК
2. Сделать скриншоты основных окон.
3. Написать выводы по лабораторной работе.

# Настройка удалённого компьютера

|  |  |
| --- | --- |
| 1. Чтобы на удалённом компьютере можно было подключение по RDP, в его де Windows необходимо разрешить это о. Жмём клавиши Win+Pause, выбираем  астройка удалённого доступа». | ктивируем галочку разрешения ключения от компьютеров с любой версией лённого рабочего стола. Жмём рименить». |

|  |  |
| --- | --- |
| https://remontcompa.ru/uploads/posts/2019-01/1548615900_1.png | https://remontcompa.ru/uploads/posts/2019-01/1548615908_2.png |
| 3. Возможность удалённого доступа активирована. Но такая вот обычная активация открывает удалённый доступ только к учётным записям администратора. | 4. Далее нам нужно получить IP удалённого компьютера. Запускаем командную строку, вводим: ipconfig |
| https://remontcompa.ru/uploads/posts/2019-01/1548615921_3.png | https://remontcompa.ru/uploads/posts/2019-01/1548615908_4.png  Смотрим IP-адрес компьютера. Кроме IP- адреса, нам для подключения также потребуется имя учётной записи Windows и пароль. |
| Если нужно подключаться к учётным записям обычных стандартных пользователей, войдя в систему с учётной записи администратора, пользователей нужно добавить дополнительно. Жмём  «Выбрать пользователей», далее «Добавить» и указываем имена стандартных учёток.  **Удаленное подключение** | |
| 1. Как теперь удалённо подключиться? Жмём Win+R, вводим: mstsc.exe  Откроется окошко штатной утилиты RDP- подключения. Вводим здесь IP-адрес удалённого компьютера. Жмём «Подключить» | 2. Далее вводим имя учётной записи удалённого компьютера и пароль. Для обычных локальных учётных записей Windows вводится их пароль, а для учётных записей Microsoft – соответственно, их. |
| https://remontcompa.ru/uploads/posts/2019-01/1548615916_5.png | https://remontcompa.ru/uploads/posts/2019-01/1548615907_6.png |

*Комментарий:* не задаваемый на каждом отдельном компьютере местный пин-код, а именно пароль от подключённого веб-аккаунта Microsoft. В качестве имени пользователя при подключённой учётке Microsoft вводится электронная почта аккаунта.



|  |  |
| --- | --- |
| 3. Жмём «ОК» в окне проверки безопасности подключения. | 4. Подключаемся |
| https://remontcompa.ru/uploads/posts/2019-01/1548615892_7.png |  |
| **Возможности удалённого доступа по RDP** | |
| У подключения по протоколу RDP немного функциональных возможностей, если сравнивать с большей частью стороннего софта для удалённого управления по Интернету. | Из таких оптимально востребованных это настройка размера окна подключения (выбор разрешений экрана), возможность подключения звуковых устройств, дисков и различной периферии управляемого компьютера к удалённому. Все эти настройки будут доступны при раскрытии выпадающего окна «Показать параметры». |
| https://remontcompa.ru/uploads/posts/2019-01/1548615879_9.png |
| **Как настроить доступ к удалённому компьютеру без пароля** | |
| 1. Ну а теперь, друзья, давайте поговорим о том, как подключаться по протоколу RDP к удалённому компьютеру, если там учётная запись без пароля. Если мы будем подключаться к незапароленной учётке Windows, увидим такую вот ошибку подключения. | 2. Удалённую учётку только лишь для этих целей можно не запароливать, а просто внести кое-какие настройки в локальные групповые политики Windows. Запускаем на удалённом компьютере редактор **gpedit.msc.** Идём по пути: Конфигурация компьютера – Конфигурация Windows – Параметры безопасности – Локальные политики – Параметры безопасности. Здесь  выбираем параметр «Учётные записи: разрешить использование пустых паролей» |

# Задание

|  |  |
| --- | --- |
| https://remontcompa.ru/uploads/posts/2019-01/thumbs/1548615863_10.png | https://remontcompa.ru/uploads/posts/2019-01/thumbs/1548615907_11.png |
| 3. Здесь активируем пункт «Отключен». Применяем | 4. Теперь можем подключаться. При указании учётных данных в окне подключения поле пароля оставляем пустым. |
| https://remontcompa.ru/uploads/posts/2019-01/1548615913_12.png | https://remontcompa.ru/uploads/posts/2019-01/1548615931_13.png |
| 5. В окне подключения попадём на экран блокировки Windows. И здесь просто жмём вход в систему с пустой формой пароля. |  |
| https://remontcompa.ru/uploads/posts/2019-01/thumbs/1548615855_14.png |  |

1. Ознакомиться с методическими рекомендациями по созданию и настройке удаленного доступа к компьютеру в локальной сети.
2. Выполнить практическую часть в соответствии с методическими рекомендациями.

# Контрольные вопросы

1. Назовите и перечислите особенности утилиты ОС Windows, позволяющую выполнять удаленное подключение к ПК в локальной сети.
2. В чем заключается особенность удаленного подключения к сетевому серверу?
3. Для чего необходим пароль в удаленном подключении?
4. Перечислите возможности удалённого доступа по RDP.

# Содержание отчета

1. Наименование и цель лабораторной работы
2. Скриншоты выполнения лабораторной работы.
3. Выводы по лабораторной работе.
4. Ответы на контрольные вопросы.

**Практическая работа №15** Оборудование беспроводных сетей

DIR-

**Цель работы:** Познакомится с базовой настройкой маршрутизатора D-LINK

**Оборудование:** компьютерный класс, маршрутизатор D-LINK (DIR-100, DIR-300,

615).

## Задание

*Маршрутизатор* – это устройство сетевого уровня эталонной модели OSI,

использующее одну или более метрик для определения оптимального пути передачи сетевого трафика на основании информации сетевого уровня”. Из этого определения вытекает, что маршрутизатор, прежде всего, необходим для определения дальнейшего пути данных, посланных в большую и сложную сеть. Пользователь такой сети отправляет свои данные в сеть и указывает адрес своего абонента. И все. Данные проходят по сети и в точках с разветвлением маршрутов поступают на маршрутизаторы, которые как раз и устанавливаются в таких точках. Маршрутизатор выбирает дальнейший наилучший путь. То, какой путь лучше, определяется количественными показателями, которые называются *метриками* . Лучший путь – это путь с наименьшей метрикой. В метрике может учитываться несколько показателей, например, длина пути, время прохождения и т.д. Маршрутизаторы реализуются по разному. Маршрутизаторы делятся на устройства верхнего, среднего и нижнего классов. Высокопроизводительные маршрутизаторы верхнего класса служат для объединения сетей предприятия. Они поддерживают множество протоколов и интерфейсов, причем не только стандартных, но, подчас, и весьма экзотических. Устройства данного типа могут иметь до 50 портов локальных или глобальных сетей. С помощью маршрутизаторов среднего класса формируются менее крупные сетевые объединения масштаба предприятия. Стандартная конфигурация включает два-три порта локальных сетей и от четырех до восьми портов глобальных сети. Такие маршрутизаторы поддерживают наиболее распространенные протоколы маршрутизации и транспортные протоколы. Маршрутизаторы нижнего класса предназначаются для локальных сетей подразделений; они связывают небольшие офисы с сетью предприятия. Типичная конфигурация: один порт локальной сети (Ethernet или Token Ring) и два порта глобальной сети, рассчитанные на низкоскоростные выделенные линии или коммутируемые соединения. Тем не менее, подобные маршрутизаторы пользуются большим спросом у администраторов, которым необходимо расширить имеющиеся межсетевые объединения.

Маршрутизаторы для базовых сетей и удаленных офисов имеют разную архитектуру, поскольку к ним предъявляются разные функциональные и операционные требования. Маршрутизаторы базовых сетей обязательно должны быть расширяемыми. Маршрутизаторы локальных сетей подразделения, для которых, как правило, заранее устанавливается фиксированная конфигурация портов, содержат только один процессор, управляющий работой трех или четырех интерфейсов. В них используются примерно те же протоколы, что и в маршрутизаторах базовых сетей, однако программное обеспечение больше направлено на облегчение инсталляции и эксплуатации, поскольку в большинстве удаленных офисов отсутствуют достаточно квалифицированные специалисты по сетевому обслуживанию.

Маршрутизатор базовой сети состоит из следующих основных компонентов: сетевых адаптеров, зависящих от протоколов и служащих интерфейсами с локальными и глобальными сетями; управляющего процессора, определяющего маршрут и обновляющего информацию о топологии; основной магистрали. После поступления пакета на интерфейсный модуль он анализирует адрес назначения и принимает команды управляющего процессора для определения выходного порта. Затем пакет по основной магистрали маршрутизатора передается в интерфейсный модуль, служащий для связи с адресуемым сегментом локальной или глобальной сети.

В роли маршрутизатора может выступать рабочая станция или сервер, имеющие несколько сетевых интерфейсов и снабженные специальным программным обеспечением. Маршрутизаторы верхнего класса – это, как правило, специализированные устройства, объединяющие в отдельном корпусе множество маршрутизирующих модулей.

По определению, основное назначение маршрутизаторов – это маршрутизация трафика сети.

Процесс маршрутизации можно разделить на два иерархически связанных уровня:

* Уровень маршрутизации. На этом уровне происходит работа с таблицей маршрутизации. Таблица маршрутизации служит для определения адреса (сетевого уровня) следующего маршрутизатора или непосредственно получателя по имеющемуся адресу (сетевого уровня) и получателя после определения адреса передачи выбирается определенный выходной физический порт маршрутизатора. Этот процесс называется *определением маршрута перемещения пакета*. Настройка таблицы маршрутизации ведется протоколами маршрутизации. На этом же уровне определяется перечень необходимых предоставляемых сервисов;
* Уровень передачи пакетов. Перед тем как передать пакет, необходимо: про верить контрольную сумму заголовка пакета, определить адрес (канального уровня) получателя пакета и произвести непосредственно отправку пакета с учетом очередности, фрагментации, фильтрации и т.д. Эти действия выполняются на основании команд, поступающих с уровня маршрутизации.



Определение маршрута передачи данных происходит программно. Соответствующие программные средства носят названия *протоколов* маршрутизации. Логика их работы основана на алгоритмах маршрутизации. Алгоритмы маршрутизации вычисляют стоимость доставки и выбирают путь с меньшей стоимостью. Простейшие алгоритмы маршрутизации определяют маршрут на основании наименьшего числа промежуточных (транзитных) узлов на пути к адресату. Более сложные алгоритмы в понятие “стоимость” закладывают несколько показателей, например, задержку при передаче пакетов, пропускную способность каналов связи или денежную стоимость связи. Основным результатом работы алгоритма маршрутизации является создание и поддержка таблицы маршрутизации, в которую записывается вся маршрутная информация. Содержание таблицы маршрутизации зависит от используемого протокола маршрутизации. В общем случае таблица маршрутизации содержит следующую информацию:

* Действительные адреса устройств в сети;
* Служебную информацию протокола маршрутизации;
* Адреса ближайших маршрутизаторов.
* Основными требованиями, предъявляемыми к алгоритму маршрутизации являются:
* Оптимальность выбора маршрута;
* Простота реализации;
* Устойчивость;
* Быстрая сходимость;
* Гибкость реализации.

Оптимальность выбора маршрута является основным параметром алгоритма, что не требует пояснений. Алгоритмы маршрутизации должны быть просты в реализации и использовать как можно меньше ресурсов. Алгоритмы должны быть устойчивыми к отказам оборудования на первоначально выбранном маршруте, высоким нагрузкам и ошибкам в построении сети. Сходимость – это процесс согласования между маршрутизаторами информации о топологии сети. Если определенное событие в сети приводит к тому, что некоторые маршруты становятся недоступны или возникают новые маршруты, маршрутизаторы рассылают сообщения об этом друг другу по всей сети. После получения этих сообщений маршрутизаторы производят переназначение оптимальных маршрутов, сто в свою очередь может породить новый поток сообщений. Этот процесс должен завершиться, причем достаточно быстро, иначе в сетевой топологии могут появиться петли, или сеть вообще может перестать функционировать. Алгоритмы маршрутизации должны быстро и правильно учитывать изменения в состоянии сети (например, отказ узла или сегмента сети). Достоинства гибкой реализации не требуют комментариев.

Алгоритмы маршрутизации могут быть:

* Статическими или динамическими;
* Одномаршрутными или многомаршрутными;
* Одноуровневыми или многоуровневыми;
* Внутридоменными или междоменными;
* Одноадресными или групповыми.

Для статических (неадаптивных) алгоритмов маршруты выбираются заранее и заносятся вручную в таблицу маршрутизации, где хранится информация о том, на какой порт отправить пакет с соответствующим адресом. Протоколы, разработанные на базе статических алгоритмов, называют *немаршрутизируемыми*. Примерами немаршрутизируемых протоколов могут служить LAT (Local AreaTransport, транспортный протокол для канальных областей) фирмы DEC, протокол подключения терминала и NetBIOS. Обычно с этими протоколами работают мосты, так как они не различают протоколы сетевого уровня.

При использовании динамических алгоритмов таблица маршрутизации автоматически обновляется при изменении топологии сети или трафика в ней. Динамические алгоритмы различаются по способу получения информации о состоянии сети, времени изменения маршрутов и используемым показателям оценки маршрута.

Одномаршрутные протоколы определяют только один маршрут. Он не всегда оказывается оптимальным. Многомаршрутные алгоритмы предлагают несколько маршрутов к одному и тому же получателю. Такие алгоритмы позволяют передавать информацию по нескольким каналам одновременно, что означает повышение пропускной способности сети. Алгоритмы маршрутизации могут работать в сетях с одноуровневой или иерархической архитектурой. В одноуровневой сети все ее фрагменты имеют одинаковый приоритет, что, как правило, обусловлено схожестью их функционального назначения. Иерархическая сеть содержит подсети (фрагменты сети). Маршрутизаторы нижнего уровня служат для связи фрагментов сети. Маршрутизаторы верхнего уровня образуют особую часть сети, называемую *магистралью* (опорная часть). Маршрутизаторы магистральной сети передают пакеты между сетями нижнего уровня. Иерархическая структура в больших и сложных сетях позволяет значительно упростить процесс управления сетью, облегчает изоляцию сегментов сети и т.д. Например, логическая изоляция сегментов сети допускает установку брандмауэров.

Некоторые алгоритмы маршрутизации действуют только в пределах своих доменов (внутри- доменная маршрутизация), а другие – как в пределах своих доменов, так и в смежных с ними (междоменная маршрутизация). В данном случае домен означает область маршрутизации, в которой работает один или несколько протоколов. В разных доменах работают разные протоколы. Ес- ли необходима связь доменов, используется междоменная

маршрутизация. Одноадресные алгоритмы маршрутизации предназначены для передачи конкретной информации (по одному или нескольким маршрутам) только одному получателю. Многоадресные (или групповые) алгоритмы способны передавать информацию многим получателям одновременно. Когда маршрутизатор получает пакет, он считывает адрес назначения и определяет, по какому маршруту отправить пакет. Обычно маршрутизаторы хранят данные о нескольких возможных маршрутах. Выбор маршрута зависит от нескольких факторов, в том числе:

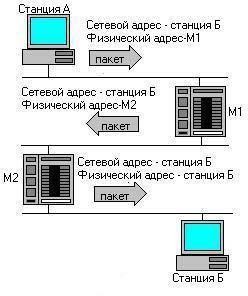
* Применяемой системы измерения длины маршрута (его метрики);
* Маршрутизируемого протокола высокого уровня;
* Топологии сети.

На уровне маршрутизации существуют три основные группы протоколов маршрутизации (деление на группы определяется типом реализуемого алгоритма определения оптимального маршрута):

* Протоколы вектора расстояния;
* Протоколы состояния канала;
* Протоколы политики маршрутизации;

Протоколы вектора расстояния – самые простые и самые распространенные. Протоколы данной группы включают RIP IP, RIP IPX, AppleTalk и Cisco IGRP. Свое название этот тип протокола получил от способа обмена информацией. Маршрутизатор с определенной периодичностью извлекает адреса получателей информации и метрику из своей таблицы маршрутизации и помещает эти данные в рассылаемые соседям сообщения об обновлении. Соседние маршрутизаторы сверяют полученные данные со своими собственными таблицами маршрутизации и вносят необходимые изменения. После этого они сами рассылают сообщения об обновлении. Таким образом каждый маршрутизатор получает информацию о маршрутах всей сети. При очевидной простоте алгоритма говорить о его полной надежности нельзя. Он может работать эффективно только в небольших сетях. Это связано с тем, что в крупных сетях поток сообщений между маршрутизаторами резко возрастает. При этом большинство из них являются избыточными (так как изменения сетевой топологии происходят довольно редко). Как следствие – действительно необходимая информация подчас долго гуляет по сети, и маршрутизаторы обновляют свои таблицы с большой задержкой. Так, более несуществующий маршрут может довольно долго оставаться в таблицах маршрутизации. Трафик, направленный по такому маршруту, не достигнет своего адресата. Протоколы состояния канала были впервые предложены в 1970 году Эдсгером Дейкстрой. Эти протоколы значительно сложнее, чем протоколы вектора расстояния. Вместо рассылки соседям содержимого своих таблиц маршрутизации, каждый маршрутизатор осуществляет широковещательную рассылку списка маршрутизаторов, с которыми он имеет непосредственную связь, и списка напрямую подключенных к нему локальных сетей. Эта информация является частью информации о состоянии канала. Она рассылается в специальных сообщениях. Кроме того маршрутизатор рассылает сообщения о состоянии канала только в случае его изменения или по истечении заданного интервала времени. Протоколы состояния канала трудны в реализации и нуждаются в значительном объеме памяти для хранения информации о состоянии каналов. Примерами этих протоколов служат OSPF, IS–IS, Nowell NLSP и Cisco EIGRP. По Дейкстре, топология сети представляется в виде неориентированного графа. Каждому ребру приписывается некоторое значение. В процессе работы алгоритма вычисляется сумма показателей для ребер, сходящихся в каждом узле графа. Эта оценка называется *меткой* узла. При определении пути подсчитывается сумма меток на возможном пути и выбирается путь с меньшей суммарной меткой. К третьей группе протоколов от- носятся протоколы политики (правил) маршрутизации. Эти протоколы наиболее эффективно решают задачу доставки получателю информации. Эта категория протоколов используется при маршрутизации в Internet и позволяет операторам получать информацию о

маршрутизации от соседних операторов на основании специальных критериев. То есть в процессе обмена вырабатывается список разрешенных маршрутов (путей). Алгоритмы политики маршрутизации опираются на алгоритмы вектора расстояния, но информация о маршрутах базируется на списке операторов сети Internet. Примерами протоколов данной категории могут служить BGP и EGP. Все вышесказанное относилось к уровню маршрутизации. Уровень передачи пакетов реализуется на алгоритмах ком- мутации и, как правило, одинаков для большинства протоколов маршрутизации. Промежуточный маршрутизатор, имея адрес следующего маршрутизатора, посылает ему пакет, адресованный специально на физический адрес (МАС-уровня) этого маршрутизатора, но с адресом (сетевого уровня) получателя. По адресу получателя маршрутизатор определяет, знает ли он, как передать пакет следующему маршрутизатору в пути. Если знает, то пакет отсылается следующему маршрутизатору путем замены физического адреса получателя на физический адрес следующего маршрутизатора. Если маршрутизатор не знает, то пакет игнорируется. На следующем маршрутизаторе все повторяется. По мере прохождения пакета через сеть, его физический адрес меняется, но адрес сетевого уровня остается неизменным. Этот процесс проиллюстрирован на рисунке:



Основная задача уровня передачи пакетов – это коммутация пакетов от разных пользователей. Общая схема передачи пакетов такова: выбирается один из возможных транзитных узлов (эта информация поступает с уровня маршрутизации, на котором она вычисляется по адресу получателя), формируется выходной заголовок канального уровня и осуществляется посылка пакета. Кроме того, на этом этапе может производиться фрагментация пакетов, проверка контрольной суммы и т.д. Маршрутизаторы (точнее – уровень маршрутизации) работают на сетевом уровне эталонной модели OSI. Уровень продвижения пакетов функционирует на канальном уровне. Работа на сетевом уровне позволяет производить интеллектуальную обработку пакетов. Поскольку маршрутизаторы в основном работают с протоколом IP, они должны поддерживать связь без создания логического соединения между абонентами. При этом каждый пакет обрабатывается и отправляется получателю независимо. Производители при создании маршрутизаторов используют три основных типа архитектуры:

* Однопроцессорная;
* Усиленная однопроцессорная;
* Симметричная многопроцессорная.

При однопроцессорной архитектуре на центральный процессор маршрутизатора возлагается вся нагрузка по обработке трафика: фильтрация и передача пакетов, обновление таблиц маршрутизации, выделение служебных пакетов, работа с протоколом

SNMP, формирование управляющих пакетов и т.д. Это приводит к тому, что маршрутизатор может стать узким местом в сети при увеличении нагрузки. Даже применение мощных RISC-процессоров не решает проблему. Для преодоления недостатков такой архитектуры применяют усиленную однопроцессорную архитектуру. В функциональной схеме маршрутизатора выделяют модули, ответственные за выполнение тех или иных специальных задач. Каждый такой модуль маршрутизатора оснащается своим (периферийным) процессором. При этом происходит частичная разгрузка центрального процессора, который отвечает только за те задачи, которые нельзя поручить периферийному. В целом, и эта архитектура не способна решить все задачи связанные с производительностью. Симметричная много-процессорная архитектура лишена перечисленных недостатков, так как происходит прямое распределение нагрузки на все модули. Но теперь каждый модуль содержит свой процессор, который выполняет все задачи маршрутизации и имеет свою копию таблицы маршрутизации. Преимущества такой архитектуры признаны всеми производителями маршрутизаторов. Данная архитектура позволяет достичь теоретически неограниченной производительности маршрутизаторов.

В заключение нашего анализа маршрутизаторов можно сказать, что они обладают несомненными достоинствами. Маршрутизаторы не вносят никаких ограничений в топологию сети. Петли, возникающие в цепях с коммутаторами, не представляют проблемы для маршрутизаторов. Тем не менее, маршрутизаторы по сравнению с коммутаторами и мостами требуют гораздо больше усилий по администрированию. Администраторам сетей необходимо знать целое множество конфигурационных параметров для маршрутизаторов. При этом параметры каждого маршрутизатора должны быть согласованы с параметрами других маршрутизаторов в сети. Сегодня многие организации реализуют межсетевой обмен через маршрутизаторы. Большое число компаний модернизируют свои системы, устанавливая коммутаторы между маршрутизаторами и сетями, которые обслуживаются этими маршрутизаторами. При этом коммутаторы повышают производительность сети, а маршрутизаторы обеспечивают защиту информации и выполняют более сложные задачи, такие как трансляция протоколов. Сегодня четко обозначилась тенденция к вытеснению сложных высокопроизводительных маршрутизаторов и увеличению роли маршрутизаторов начального класса, а ведущие фирмы-производители пришли к выводу, что одним из основных требований покупателей к маршрутизатору является простота его использования.

### Порядок выполнения

Для настройки маршрутизатора необходимо на странице управления маршрутизатором [(http://192.168.0.1,](http://192.168.0.1/) по умолчанию имя пользователя admin, пароль пустой(в NRU пароль admin)) в режиме ручной настройки интернет-соединения выбрать тип подключения Russia PPPoE (Dual Access), указать имя пользователя/пароль, выбрать типа подключения

— всегда (always). Ниже будет приведена пошаговая инструкция.

1. Подключение маршрутизатора



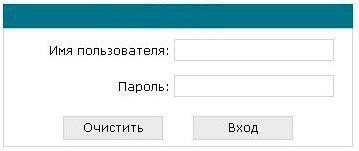
Подключите провод провайдера в порт Internet. Компьютер подключите прилагающимся кабелем в порты LAN 1-4.

1. Базовая настройка соединения

Пункт 1. Проверяем что компьютер получил настройки от маршрутизатора. Для этого открываем состояние подключения по локальной сети. Для Windows XP на вкладке Поддержка, для Windows Vista и Windows 7 — в пункте Сведения, проверяем что Адрес IP (IPv4) был получен и имеет вид 192.168.0.Х, где Х — любое число, как правило 100. Если адрес отличается — проверьте, что сто- ит автоматическое получение IP адреса в свойствах протокола TCP. Если адрес не получен — про- верьте кабель от компьютера до маршрутизатора, настройки файрволов и антивирусов.

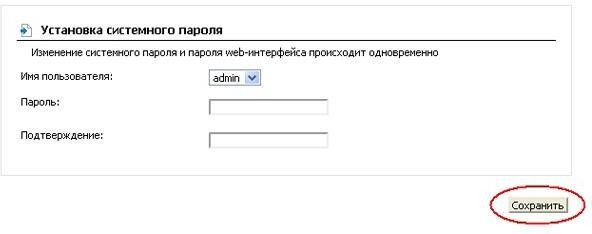
* [**DIR 300NRU**](http://www.rastrnet.ru/internet/setup/router_dlink/#tabs1)
* [DIR 300, 615](http://www.rastrnet.ru/internet/setup/router_dlink/#tabs2)

Пункт 2. Открываем страницу управления маршрутизатором [http://192.168.0.1](http://192.168.0.1/) Для входа исполь- зуем имя пользователя admin, пароль admin.



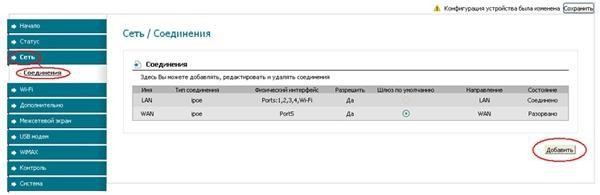
Пункт 3. Установка системного пароля, введите пароль, который будет запрашивать маршрутиза- тор в при следующей попытке входа в настройки.

Пункт 4. Нажимаем на кнопку **Сеть** и выбираем пункт **Соединения**. В появившемся окне



нажимаем кнопку **Добавить**.

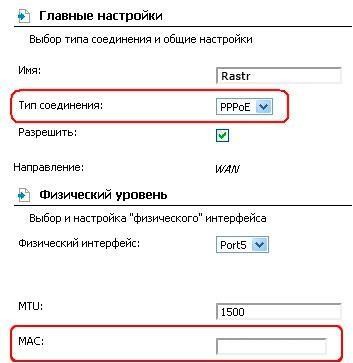
Пункт 4. Указываем необходимые параметры.



**Имя**: Rastr

**Тип соединения**: PPPoE

**MAC**: Вводим физический адрес вашей сетевой карты(Смотрим в состоянии подключение по ло- кальной сети), ставим двоеточие через каждые 2 символа, ***пример****: 00:00:00:00:00:00*

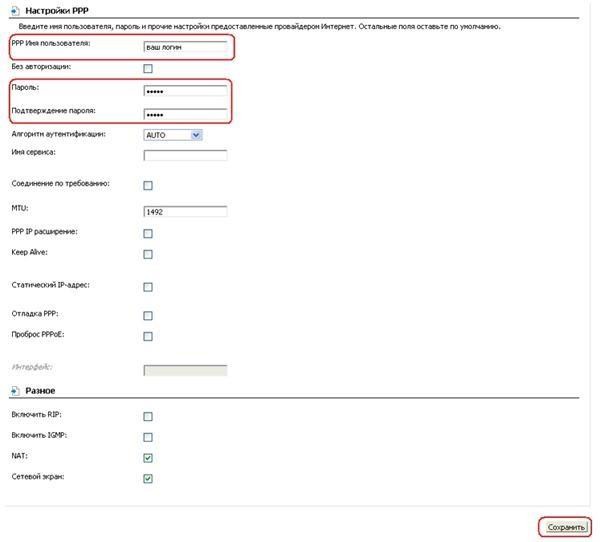


Пункт 5. В окне **Соединения** появилось новое: Rastr, Нажимаем на него. Вводим следущие данные:

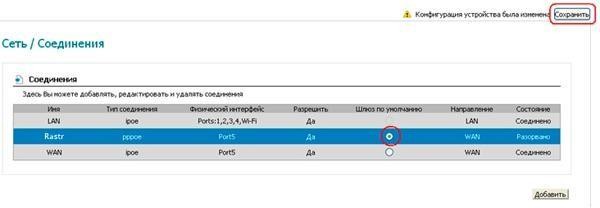
**PPP Имя пользователя**: Ваш логин указанный в договоре

**Без авторизации**: Убедитесь что галочка не стоит.

**Пароль**: Ваш пароль указанный в договоре. **Подтверждение пароля**: см. пункт выше. **MTU**: Если не указано, выставляем 1492.



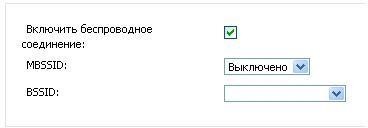
Нажимаем кнопку **Сохранить**.

Пункт 5. В окне **Соединения** ставим галочку **Шлюз по умолчанию** на соединение Rastr

Нажимаем кнопку **Сохранить**.

1. Настройка беспроводной сети

Пункт 1. Перейдите в меню **Wi-Fi** выберите пункт **Общие настройки** и проверьте, чтобы стояла галочка **Включить беспроводное соединение**.



Пункт 2. Перейдите в меню **Wi-Fi** выберите пункт **Основные настройки**.

**Скрыть точку доступа** – не ставьте галочку

**SSID** – пропишите имя беспроводной сети. Можно использовать латинские буквы и цифры

**Страна** – оставьте RUSSIAN FEDERATION

**Канал** – вместо AUTO установите любой канал с 1 по 11

**Беспроводной режим** – можете оставить без изменений или выбрать другой режим



Нажмите **Изменить**

После изменения настроек нажмите **Сохранить** в правом верхнем углу. Пункт 3. Перейдите в меню **Wi-Fi** выберите пункт **Настройки безопасности**.

**Сетевая аутентификация** – рекомендуется устанавливать шифрование WPA-PSK/WPA2- PSKmixed

**Ключ шифрования PSK** – можете использовать ключ по умолчанию или установить свой (от 8 до 63 символов, можно использовать латинские буквы и цифры)

**WPA** -шифрование – выберите TKIP+AES



Нажмите **Изменить**

После изменения настроек нажмите **Сохранить** в правом верхнем углу.

### Содержание отчета

Отчет должен содержать:

* Название работы
* Цель работы
* Базовые настройки маршрутизватора.

### Контрольные вопросы

1. Что такое маршрутизатор?
2. Какие режимы работы поддерживает маршрутизатор?
3. Объясните принцип MAC-фильтрации.

**Практическая работа №16** Настройка свойств Web-браузера.

### Цель работы

Научиться использовать расширенные возможности Web-браузера

**Оборудование:** компьютерный класс.

### Задание

Веб-обозреватель, или браузер (от англ. Web browser) — это программное обеспечение для поиска, просмотра веб-сайтов, то есть для запроса веб-страниц (преимущественно из Сети), для их обработки, вывода и перехода от одной страницы к другой.

Большинство браузеров также наделены способностями к просмотру оглавления FTP- серверов.

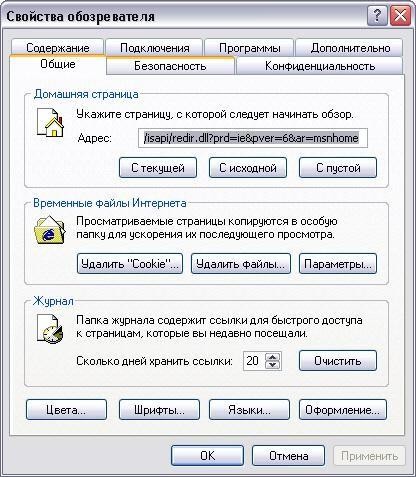
Браузеры постоянно развивались со времён зарождения Всемирной паутины, и с её ростом становились всё более важной программой типичного персонального компьютера. Ныне браузер

— комплексное приложение для обработки и вывода разных составляющих веб- страницы, и для предоставления интерфейса между веб-сайтом и его посетителем. Практически все популярные браузеры распространяются бесплатно или «в комплекте» с другим приложением: Internet Explorer (как неотъемлемая часть Microsoft Windows), Mozilla Firefox (бесплатно, свободное ПО), Opera (бесплатно, начиная с версии 8.50), Safari (совместно с Mac OS или бесплатно для Windows).

### Порядок выполнения

Запустите приложение Internet Explorer. Произведите тонкую настройку браузера и про- верьте результаты при использовании сети Интернет.

Обозреватель Internet Explorer, как и все программы, входящие в Microsoft Office, можно настроить. Для настройки используется диалоговое окно Свойства обозревателя (рис.1), открываемое при выборе одноименной команды в меню Сервис. Среди настраиваемых параметров: вид домашней страницы обозревателя Internet Explorer, цвет текста и фона Web- страниц, используемые шрифты и языки, защита передаваемой и получаемой информации, ограничение доступа к Web-страницам и т. п. Рассмотрим более подробно диалоговое окно Свойства обозревателя и настраиваемые с его помощью параметры работы программы.



## Рис. 1. Диалоговое окно Свойства обозревателя

Для настройки основных параметров обозревателя Internet Explorer предназначена вкладка Общие диалогового окна Свойства обозревателя.

Область Домашняя страница позволяет задать страницу, называемую домашней и загружаемую по умолчанию при каждом запуске обозревателя. Именно к этой странице осуществляется переход при нажатии кнопки Домой на панели инструментов окна обозревателя. В области Домашняя страница расположено поле, содержащее адрес страницы, и три кнопки: С текущей, С исходной, С пустой. При нажатии кнопки С текущей в поле Адрес заносится адрес страницы, открытой в обозревателе в данный момент. Нажатие кнопки С исходной приводит к установке в качестве домаш- ней страницы

— страницы Microsoft, имеющей адрес [http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=5.5&ar=msnhome.](http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=5.5&ar=msnhome) Кнопка С пустой устанавливает в качестве домашней пустую страницу.

Программа Internet Explorer при просмотре Web-страниц помещает их содержимое во временные файлы. Эти файлы можно использовать при повторном просмотре Web-страниц, что значительно ускоряет их загрузку. Настройка временных файлов осуществляется в области Временные файлы Интернета. Нажатие кнопки Удалить файлы этой области приводит к удалению временных файлов с диска. Используйте данную кнопку в том случае, если у вас на диске недостаточно места, и вы уверены, что не будете повторно открывать уже просмотренные Web-страницы. Для настройки параметров управления временными файлами воспользуйтесь кнопкой Настройка и открываемым ею одноименным диалоговым окном.

Область Журнал вкладки Общие позволяет указать число дней, в течение которых Internet Explorer будет сохранять ссылки на просмотренные страницы в папке журнала. Нажатие кнопки Очистить приводит к удалению информации из папки.

В нижней части вкладки Общие расположены кнопки, позволяющие задать используемое цветовое оформление Интернета, шрифты, предпочтительный язык для отображения информации, рас- полагаемой на Web-странице, и другие параметры оформления.

## Используемые цвета

При нажатии кнопки Цвета вкладки Общие открывается диалоговое окно Цвета, показанное на рис. 2. Оно разделено на две области.

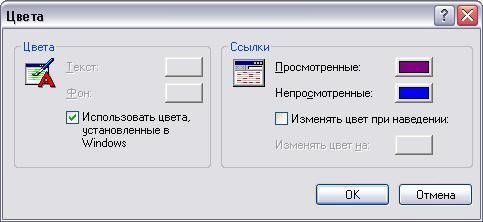


Рис. 2. Диалоговое окно, предназначенное для настройки цветов

Область Цвета позволяет задать цвет текста и фона Web-страниц. Для изменения заданного цвета текста или фона нажмите кнопку, расположенную справа от соответствующей надписи. Откроется диалоговое окно Цвет, содержащее базовую цветовую палитру. Выберите с помощью курсора устраивающий вас цвет и нажмите кнопку ОК.

При установке флажка Использовать цвета, установленные в Windows кнопки, расположенные в области Цвета, не доступны. В этом случае для отображения цвета текста и фона Web-страниц используются стандартные установки Windows.

С помощью кнопок, расположенных в области Ссылки, меняется цвет просмотренных ссылок и ссылок, по которым еще не осуществлялся переход. При установке флажка Изменять цвет при наведении можно задать цвет ссылок при наведении на них указателя мыши.

## Настройка шрифтов

Кнопка Шрифты, находящаяся на вкладке Общие, открывает одноименное диалоговое окно, показанное на рис. 7.3.



Рис.З. Диалоговое окно, используемое для настройки шрифтов

В его верхней части расположен раскрывающийся список, содержащий наборы символов, установленных на компьютере. Ниже него расположены списки, позволяющие установить шрифт следующей информации, содержащейся на Web-странице:

* Шрифт веб-страницы — используется для вывода текста, оформленного с применением форматирования
* Шрифт обычного текста — используется для вывода текста Web-страницы, оформленного без применения форматирования

## Выбор языка

Кнопка Языки, расположенная на вкладке Общие, открывает диалоговое окно Выбор языка (рис. 4), позволяющее задать список языков, используемых Internet Explorer для отображения содержимого Web-страниц. Для добавления в список языка необходимо нажать кнопку Добавить и в от- крывшемся диалоговом окне Добавление языка выбрать используемый язык.

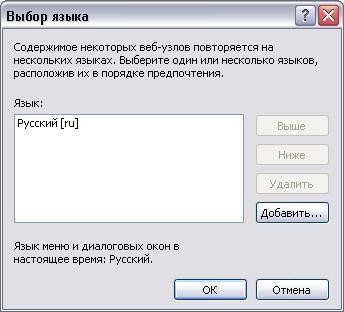


Рис.4. Диалоговое окно Выбор языка

## Оформление Web-страниц

Кнопка Оформление, размещенная на вкладке Общие, открывает диалоговое окно Оформление (рис.5), содержащее флажки, перечисленные в табл. 1.

Таблица 1. Флажки оформления Web-страницы

|  |  |
| --- | --- |
| Флажок | Назначение |
| Не учитывать цвета, указанные на веб-страницах | Флажок устанавливается в случае, если для задания цветовых настроек текста, фона и ссылок используется диалоговое окно Цвета (см. рис.2) |
| Не учитывать шрифты, указанные на веб-страницах | Установка флажка используется в случае задания настроек шрифтов текста в диалоговом окне Шрифты (см. рис.3) |
| Не учитывать размеры шрифтов, указанные на веб- страницах | Установка флажка используется в случае задания настроек размеров шрифтов тек- ста в диалоговом окне Шрифты (см. рис. 3) |
| Оформлять, используя стиль пользователя | Флажок устанавливается в случае, если для оформления всех выводимых страниц используется пользовательская библиотека стилей. Для указания местонахождения библиотеки предназначены расположенное под флажком поле и кнопка Обзор |

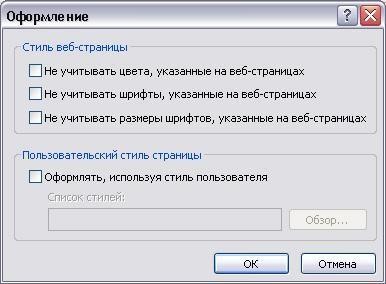


Рис. 5. Диалоговое окно Оформление

## Защита информации

При работе в сети Интернет пользователю необходимо заботиться о том, чтобы пересылаемые им данные, особенно информация конфиденциального характера, не была доступна посторонним пользователям. С другой стороны, проблема безопасности данных встает при пересылке файлов и программ между Web-узлами и вашим компьютером. Без применения системы зашиты вы можете получить программу, которая при запуске повредит хранящиеся в вашем компьютере данные.

Степень надежности Web-узлов в Интернете различна. Программа Internet Explorer позволяет распределять получаемые вами по сети данные по зонам безопасности и устанавливать разные уровни защиты в зависимости от того, кто является их отправителем. Перед загрузкой Web-страницы Internet Explorer проверяет соответствие узла заданной зоне безопасности. Для того чтобы узнать, к какой зоне безопасности относится загруженная страница, посмотрите на строку состояния. В ее правой части размещается название зоны.

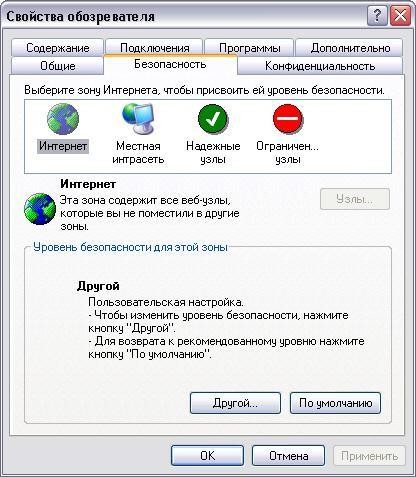


Рис. 6. Вкладка, позволяющая настроить параметры безопасности

Используя вкладку Безопасность (рис. 6) диалогового окна Свойства обозревателя, можно установить для зон Интернета разные параметры безопасности. В верхней части вкладки расположен представленный в виде значков список основных категорий зон, на которые имеется доступ с компьютера пользователя (табл. 2).

Таблица 2. Основные категории зон безопасности

|  |  |
| --- | --- |
| Зона | Назначение |
| Интернет | В эту зону входит все то, что не имеет отношения к вашему компьютеру, внутренней сети или иной зоне. По умолчанию зона обладает средним уровнем защиты |
| Местная интрасеть | Данная зона содержит адреса, для которых использование прокси-сервера не обязательно. Эти адреса назначаются системным администратором с помощью административного комплекта Internet Explorer (IEAK). По умолчанию зона имеет уровень защиты ниже среднего |

|  |  |
| --- | --- |
| Надежные узлы | Зона содержит узлы, которым вы доверяете и с которых можно загружать информацию и программы, не беспокоясь о возможном повреждении ваших собственных данных или компьютера. По умолчанию эта зона имеет низкий уровень защиты |
| Ограниченные уз- лы | Данная зона содержит узлы, которым вы не доверяете. По умолчанию эта зона имеет высокий уровень защиты |

На вкладке содержится ползунок, используемый для задания уровня безопасности зоны, выбран- ной из верхнего списка (табл.3).

Таблица. 3. Уровни безопасности

|  |  |
| --- | --- |
| Уровень безопасности | Выполняемое программой действие |
| Высокий | При угрозе безопасности с Web-узла выдается уведомление. Информация, которая может нести угрозу безопасности, не загружается. Небезопасные функции  отключаются |
| Средний | Перед загрузкой небезопасного содержимого с Web-узла выдается уведомление. После предупреждения появляется запрос на подтверждение или отмену загрузки активного  содержимого |
| Ниже среднего | Большая часть содержимого запускается без предупреждения. При угрозе безопасности с Web-узла выдается уведомление |
| Низкий | Обеспечивает минимальный уровень безопасности. При потенциальной угрозе без- опасности с Web-узла выдается уведомление, после чего активное содержимое загружается на компьютер |

Вкладка Безопасность диалогового окна Свойства обозревателя содержит кнопки, перечисленные в табл. 4.

Таблица 4. Кнопки вкладки Безопасность

|  |  |
| --- | --- |
| Кнопка | Назначение |
| Узлы | Позволяет добавить или удалить узел из заданной зоны |
| По умолчанию | Позволяет для выбранной зоны установить уровень защиты, принятый по умолчанию |
| Другой | Открывает диалоговое окно Правила безопасности для определения дополнительных настроек защиты |

### Параметры вкладки Содержание

Вкладка Содержание (рис.7) диалогового окна Свойства обозревателя содержит три области, имеющие следующее назначение:

* Ограничение доступа — позволяет ввести ограничения на просмотр информации в Интер- нете
* Сертификаты — предназначена для просмотра личных сертификатов безопасности, установленных на данном компьютере, сертификатов узлов и издателей
* Личные данные — хранит персональные данные, предоставляемые узлам при запросах

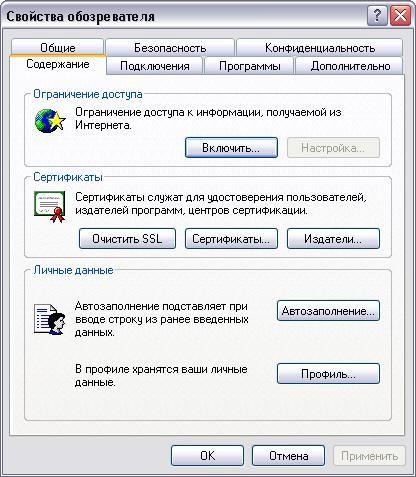


Рис. 7. Вкладка Содержание

Персональные компьютеры появились во многих семьях. При этом постоянно растет число домашних компьютеров, подключенных к Интернету. Используя область Ограничение доступа вкладки Содержание, вы сможете ввести ограничения на просмотр детьми в Интернете информации, использующей ненормативную лексику, текст и рисунки о насилии и сексе.

Область содержит кнопку Включить, при нажатии на которую открывается диалоговое окно Ограничение доступа (рис. 8), содержащее четыре вкладки: Оценки, Разрешенные узлы, Общие и Дополнительно.

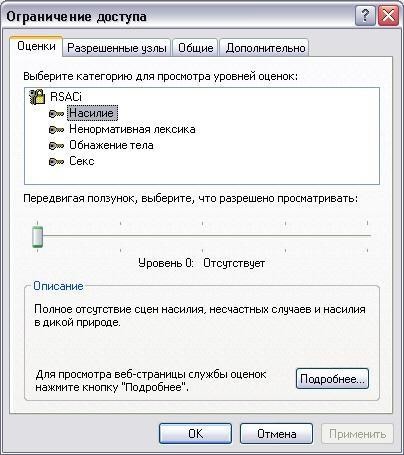


Рис. 8. Диалоговое окно, используемое для ограничения доступа к информации

В верхней части вкладки Оценки расположен список разделов, на которые можно задать ограничения, а ниже него — ползунок, указывающий уровень ограничения. Для изменения уровня запрета на просмотр информации выберите из списка настраиваемую категорию. При этом в области Описание вкладки отображается информация об установленном уровне запрета для данного раздела. Перемещая движок, измените установленный уровень доступности материал данной категории.

Вкладка Разрешенные узлы позволяет сформировать список узлов, которые можно просматривать или, наоборот, не просматривать, несмотря на параметры, установленные на вкладке Оценки.

Флажок Пользователи могут просматривать узлы, не имеющие оценок вкладки Общие определяет разрешение на просмотр не имеющих оценки узлов для пользователей данного компьютера. При установке этого флажка пользователь получает доступ к нежелательному материалу, если рейтинг Web-страницы не определен. Если этот флажок не установлен, пользователь не будет иметь доступа к Web-страницам, не имеющим оценки, даже если они не содержат нежелательного матери- ала.

Установленный флажок Разрешить ввод пароля для просмотра запрещенных узлов вкладки Общие позволяет просматривать запрещенную для просмотра информацию Web- страниц после ввода па- роля.

## Настройка подключения к Интернету

Вкладка Подключение (рис.9) диалогового окна Свойства обозревателя позволяет настроить параметры удаленного доступа.

В верхней части вкладки находится кнопка Установить, при нажатии на нее запускается мастер подключения к Интернету, который поможет установить соединение. Расположенные ниже переключатель и кнопка Настройка позволяют осуществить самостоятельную настройку параметров соединения.

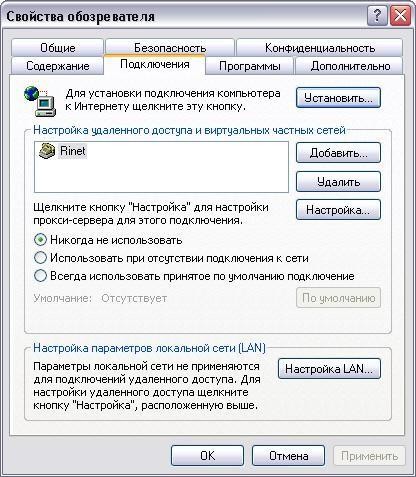


Рис.9. Вкладка, предназначенная для настройки подключения к Интернету

В области Настройка удаленного доступа находится список соединений для удаленного доступа к сети, установленных на компьютере, и три кнопки:

* Добавить — добавляет в список с помощью мастера новое соединение для удаленного до- ступа к сети
* Удалить — удаляет из списка выделенное соединение с Интернетом
* Настройка — открывает диалоговое окно Настройка, позволяющее просмотреть и изменить настройки подключения выбранного соединения

Установленная под списком опция Не использовать указывает на необходимость при подключении к Интернету выбирать используемое соединение вручную.

Опция Использовать при отсутствии подключения к сети указывает, что для выхода в Интернет при отсутствии подключения программа Internet Explorer будет использовать соединение для уда- ленного доступа к сети, принятое по умолчанию.

Установив расположенную под списком опцию Всегда использовать принятые по умолчанию, с помощью кнопки По умолчанию можно указать, какое соединение использовать по умолчанию при подключении к Интернету.

Область Настройка локальной сети позволяет осуществить подключение к Интернету через прок- си-сервер локальной сети, который служит защитным барьером между внутренней сетью и Интернетом, не позволяя другим пользователям Интернета получить доступ к конфиденциальной ин- формации внутренней сети.

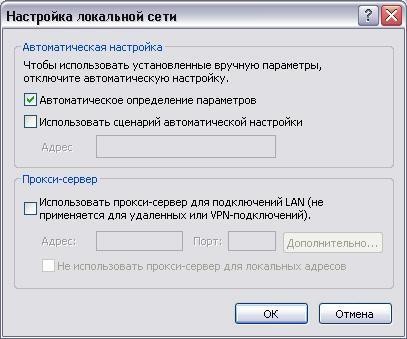
## Настройка соединения

Чтобы настроить соединение для удаленного доступа к сети Интернет, выберите его в списке со- единений на вкладке Подключение и нажмите кнопку Настройка. Откроется одноименное диалоговое окно (рис. 7.10), предназначенное для просмотра и изменения параметров. В его верхней части расположены два флажка:

* Автоматическое определение настроек — при установке флажка осуществляется автоматическое определение настроек прокси-сервера или параметров автоматической настройки, используемых для подключения к Интернету и настройки обозревателя Internet Explorer.
* Использовать сценарий автоматической настройки — при установке флажка для автоматической настройки используется файл, содержащий параметры настройки, предоставленные системным администратором.

При установке флажка Использовать сценарий автоматической настройки становится доступным для ввода информации поле Адрес, предназначенное для задания адреса URL или имени файла, используемого для настройки Internet Explorer.

Рис. 10. Диалоговое окно, предназначенное для настройки соединения



Область Прокси-сервер позволяет осуществить подключение к Интернету через прокси-сервер локальной сети. При установке флажка Использовать прокси-сервер становятся доступными для ввода следующие поля:

* + Адрес — адрес прокси-сервера, предоставляемый системным администратором сети
  + Порт — порт прокси-сервера, используемый для доступа к Интернету

При подключении к Интернету через прокси-сервер локальной сети необходимо осуществить дополнительные настройки прокси-сервера. Для этого нажмите кнопку Дополнительно. Откроется диалоговое окно Параметры прокси-сервера, в котором необходимо ввести адрес и порт прокси- сервера, используемого для доступа к Интернету по протоколам HTTP, Secure, FTP, Gopher и Socks.

Для настройки удаленного доступа предназначена область Настройка удаленного доступа диалогового окна Настройка. Она содержит поля, в которые нужно ввести данные, предоставленные провайдером:

* + Имя пользователя — имя пользователя;
  + Пароль — пароль;
  + Домен — имя домена.

Нажатие кнопки Свойства этой области открывает окно, предназначенное для изменения номера телефона, модема и других дополнительных параметров текущего соединения удаленного доступа к сети.

## Формирование списка используемых программ

Используя вкладку Программы (рис.11) диалогового окна Свойства обозревателя, можно задать применяемые вместе с Internet Explorer программы:

* + редактора HTML — для редактирования HTML-файлов;
  + электронной почты — для работы с электронной почтой;
  + групп новостей — для чтения групп новостей Интернета;
  + вызовов по Интернету — для набора номера;
  + календаря — для просмотра календаря;
  + адресной книги — для работы с адресной книгой.

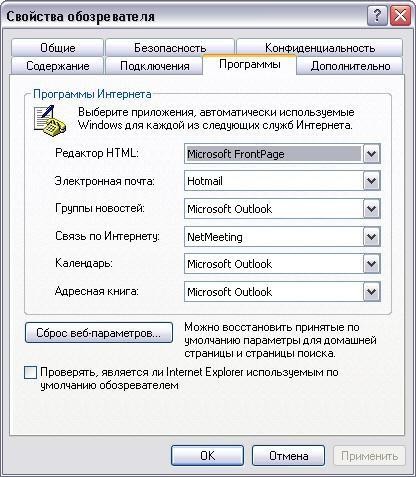


Рис. 11. Вкладка, позволяющая задать список используемых программ

При установке флажка Проверять, является ли Internet Explorer обозревателем, используемым по умолчанию при каждом запуске Internet Explorer выполняет проверку, зарегистрирован ли Internet Explorer в качестве средства просмотра Интернета, используемого по умолчанию. Если зарегистрирована другая программа, будет предложено восстановить применение Internet Explorer в качестве стандартного средства просмотра информации в Интернете.

## Дополнительные настройки обозревателя

Для дополнительных настроек обозревателя используется вкладка Дополнительно (рис.12) диалогового окна Свойства обозревателя, содержащая большой список параметров, сгруппированных по разделам. Для их установки достаточно установить флажок или одну из предлагаемых опций. Чтобы восстановить значения, установленные в системе по умолчанию, нажмите кнопку Восстановить значения по умолчанию.

## Содержание отчета

Отчет должен содержать:

* Название работы
* Цель работы
* Презентацию с выполненным заданием

## Контрольные вопросы

1. Что такое Веб-браузер?
2. Каковы достоинства применения этой технологии?
3. Каковы ограничения применения этой технологии?

## Основные источники:

**Рекомендуемые источники информации Основная литература:**

* 1. Кузин, А. В. Компьютерные сети : учебное пособие / А. В. Кузин, Д. А. Кузин.

- 4-е изд., перераб. и доп. - Москва : ФОРУМ : ИНФРА-М, 2024. - 190 с. - (Среднее профессиональное образование). - ISBN 978-5-00091-453-3. \_ Текст : непосредственный.

* 1. Максимов, Н. В. Компьютерные сети : учебное пособие / Н. В. Максимов, И. И. Попов. - 6-е изд., перераб. и доп. - Москва : ФОРУМ : ИНФРА-М, 2023. - 464 с. - (Среднее профессиональное образование). - ISBN 978-5-00091-454-0. - Текст : непосредственный.
  2. Сети и телекоммуникации : учебник и практикум для вузов / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. - 2-е изд., перераб. и доп. – Москва : Юрайт, 2024. – 464 с. - (Высшее образование). - URL: <https://urait.ru/bcode/536089> (дата обращения: 11.07.2024). - Режим доступа: ЭБС Юрайт, для зарегистрир. пользователей. – ISBN 978-5-534-17315-4. - Текст : электронный.
  3. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях : учебник и практикум для среднего профессионального образования / М. В. Дибров. - 2-е изд., перераб. и доп. - Москва : Юрайт, 2024. - 423 с. - (Профессиональное образование). - URL: <https://urait.ru/bcode/544930> (дата обращения: 11.07.2024). - Режим доступа: ЭБС Юрайт, для зарегистрир. пользователей. – ISBN 978-5-534-16551-7. - Текст : электронный
  4. Замятина, О. М. Инфокоммуникационные системы и сети. Основы моделирования : учебное пособие для среднего профессионального образования / О. М. Замятина. – Москва : Юрайт, 2024. - 167 с. - (Профессиональное образование). - URL: <https://urait.ru/bcode/542346> (дата обращения: 11.07.2024). - Режим доступа: ЭБС Юрайт, для зарегистрир. пользователей. – ISBN 978-5-534-17558-5. - Текст : электронный.
  5. Максимов, Н. В. Компьютерные сети : учебное пособие / Н. В. Максимов, И. И. Попов. - 6-е изд., перераб. и доп. - Москва : ФОРУМ : ИНФРА-М, 2024. - 464 с. - (Среднее профессиональное образование). - URL: https://znanium.com/catalog/product/2122501 (дата обращения: 16.02.2024). - Режим доступа: ЭБС Znanium.com, для зарегистрир. пользователей. - ISBN 978-5-00091-454-0. - Текст : электронный.
  6. Кузин, А. В. Компьютерные сети : учебное пособие / А. В. Кузин, Д. А. Кузин.

- 4-е изд., перераб. и доп. - Москва : ФОРУМ : ИНФРА-М, 2024. - 190 с. - (Среднее профессиональное образование). - URL: https://znanium.ru/catalog/product/2096763 (дата обращения: 16.02.2024).- Режим доступа: ЭБС Znanium.com, для зарегистрир. пользователей. - ISBN 978-5-00091-453-3. - Текст : электронный.

## Дополнительные источники:

1. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. - Москва : Юрайт, 2024. - 464 с. - (Профессиональное образование). - URL: https://urait.ru/bcode/542157 (дата обращения: 16.02.2024). - Режим доступа: ЭБС Юрайт, для зарегистрир. пользователей. - ISBN 978-5-534-17310-9. - Текст : электронный.
2. Дятлов, П. А. Принципы построения и организация компьютерных сетей : учебное пособие / П. А. Дятлов ; Южный федеральный университет, Инженерно- технологическая академия. - Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2022. - 129 с. : ил., табл. - URL: https://biblioclub.ru/index.php?page=book&id=698674 (дата обращения: 16.02.2024). - Режим доступа: ЭБС Университетская библиотека онлайн, для зарегистрир. пользователей. - ISBN 978-5-9275-4109-6. - Текст : электронный.
3. Исаченко, О. В. Программное обеспечение компьютерных сетей : учебное пособие / О. В. Исаченко. - 2-е изд., испр. и доп. - Москва : ИНФРА-М, 2022. - 158 с. - (Среднее профессиональное образование). - ISBN 978-5-16-015447-3. - Текст : электронный.

- URL: https://znanium.ru/catalog/product/2111926 (дата обращения: 16.02.2024). - Режим доступа: ЭБС Znanium.com, для зарегистрир. пользователей. - ISBN 978-5-16-015447-3. - Текст : электронный.

## Электронные издания (электронные ресурсы):

* + - 1. [https://campus.fa.ru](https://campus.fa.ru/) – Образовательный сайт Финансового университета при Правительстве РФ
      2. [http://www.ed.gov.ru](http://www.ed.gov.ru/) – Министерство образования Российской федерации.
      3. [http://www.edu.ru](http://www.edu.ru/) – Федеральный портал «Российское образование».
      4. [http://www.yandex.ru](http://www.yandex.ru/) – Русская поисковая система.
      5. <http://www.firo.ru/> - Министерство образования и науки РФ ФГАУ «ФИРО»
      6. [http://www.consultant.ru](http://www.consultant.ru/). - Справочно-правовая система «Консультант Плюс»
      7. [http://www.garant.ru](http://www.garant.ru/) - Справочно-правовая система «Гарант».
      8. [http://znanium.com](http://znanium.com/) – Электронно-библиотечная система znanium.com
      9. [http://www.urait.ru](http://www.urait.ru/) – электронная библиотека издательства ЮРАЙТ