**Введение**

Программный пакет Packet Tracer представляет собой программный симулятор работы сети, выпускаемый фирмой [Cisco Systems](http://ru.wikipedia.org/wiki/Cisco_Systems). Он позволяет создавать работоспособные модели сети, настраивать [маршрутизаторы](http://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80) и [коммутаторы](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BC%D1%83%D1%82%D0%B0%D1%82%D0%BE%D1%80), взаимодействовать между несколькими пользователями. Кроме того есть [серверы](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80) [DHCP](http://ru.wikipedia.org/wiki/DHCP), [HTTP](http://ru.wikipedia.org/wiki/HTTP), [TFTP](http://ru.wikipedia.org/wiki/TFTP), [FTP](http://ru.wikipedia.org/wiki/FTP), рабочие станции, различные модули к компьютерам и маршрутизаторам, устройства [WiFi](http://ru.wikipedia.org/wiki/WiFi), различные кабели.

Была поставлена задача разработать комплекс лабораторных работ по дисциплине «Передача данных в информационных управляющих системах»

В результате проекта будет выполнен лабораторный практикум и будут подготовлены методические указания к нему, показывающие возможности программного продукта Packet Tracer.

**Актуальность**

Cisco Packet Tracer - это мощная программа моделирования сети, которая позволяет студентам экспериментировать с функционированием сети. Packet Tracer предоставляет моделирование, визуализацию, создание, оценку, а также возможности совместной работы, что облегчает преподавание и изучение сложных понятий технологии.

Эта программа полезна для студентов и преподавателей. Имеет понятный интерфейс, различное физическое оборудование, разбитое по классам, что позволяет студентам создавать сети с практически неограниченным количеством устройств. Позволяет применить на практике знания по настройке сетей, обнаружению и устранению неполадок. Cisco Packet Tracer помогает студентам развивать навыки, таких как принятие решений, творческого и критического мышления и решения проблем.

При помощи Packet Tracer можно легко создавать целые виртуальные сети различной топологии и с различным количеством устройств. Для подключения предложены все основные типы оборудования выпускаемого Cisco (маршрутизаторы, коммутаторы, конечные станции, точки доступа, VPN и т.п.), подключившись к которым, можно менять настройки, моделировать обмен данными. Кроме этого «реализованы» все технологии и протоколы, используемые в оборудовании Cisco, поэтому настройка в Packet Tracer практически ничем не отличается от реального оборудования.

Packet Tracer дополняет программу сетевых академий Cisco, позволяя преподавателям легко учить и демонстрировать сложные технические концепции и дизайн сетевых систем. В данный момент у нас уже есть методические указания к выполнению нескольких лабораторных работ, в которых изучаются базовые сетевые соединения и настройки оборудования. Большинство литературы сейчас на английском языке, поэтому студентам в Российских вузах не предоставляется в полной мере оценить всю функциональной данного программного продукта. Поэтому была поставлена задача изучить возможности программного продукта Cisco Packet Tracer и подготовить задания и методические указания для проведения лабораторных работ для студентов по дисциплине «Передача данных в ИУС».

1. **Анализ существующих подходов к разработке лабораторных работ.**

Ни один проект крупной сети со сложной топологией в настоящее время не обходится без исчерпывающего моделирования будущей сети. Программы, выполняющие эту задачу, достаточно сложны и дороги. Целью моделирования является определение оптимальной топологии, адекватный выбор сетевого оборудования, определение рабочих характеристик сети и возможных этапов будущего развития. Ведь сеть, слишком точно оптимизированная для решений задач текущего момента, может потребовать серьезных переделок в будущем. На модели можно опробовать влияние всплесков широковещательных запросов или реализовать режим коллапса (для Ethernet), что вряд ли кто-то может себе позволить в работающей сети. В процессе моделирования выясняются следующие параметры:

* Предельные пропускные способности различных фрагментов сети и зависимости потерь пакетов от загрузки отдельных станций и внешних каналов.
* Время отклика основных серверов в самых разных режимах, в том числе таких, которые в реальной сети крайне нежелательны.
* Влияние установки новых серверов на перераспределение информационных потоков (Proxy, Firewall и т.д.).
* Решение оптимизации топологии при возникновении узких мест в сети (размещение серверов, DNS, внешних шлюзов, организация опорных каналов и пр.).
* Выбор того или иного типа сетевого оборудования (например, 10BaseTX или 100BaseFX) или режима его работы (например, cut-through, store-and-forward для мостов и переключателей и т.д.).
* Выбор внутреннего протокола маршрутизации и его параметров (например, метрики).
* Определение предельно допустимого числа пользователей того или иного сервера.
* Оценка необходимой полосы пропускания внешнего канала для обеспечения требуемого уровня QOS.
* Оценка влияния мультимедийного трафика на работу локальной сети, например, при подготовке видеоконференций.

Перечисленные задачи предъявляют различные требования к программам. В одних случаях достаточно провести моделирование на физическом (MAC) уровне, в других нужен уже уровень транспортных протоколов (например, UDP и TCP), а для наиболее сложных задач нужно воспроизвести поведение прикладных программ. Все это должно учитываться при выборе или разработке моделирующей программы. Ведь нужно учесть, что ваша машина должна в той или иной мере воспроизвести действия всех машин в моделируемой сети. Таким образом, машина эта должна быть достаточно быстродействующей и, несмотря на это, моделирование одной секунды работы сети может занять при определенных условиях не один час.

В данный момент у нас уже есть методические указания к выполнению нескольких лабораторных работ Cisco Packet Tracer, в которых изучаются базовые сетевые соединения и настройки оборудования. Большинство литературы сейчас есть только на английском языке, поэтому студентам в Российских вузах не предоставляется в полной мере оценить всю функциональной данного программного продукта.

Список лабораторных работ, к которым уже существуют методические указания:

1. Знакомство со средой
2. Введение в межсетевую операционную систему IOS компании Cisco.
3. Статическая маршрутизация
4. Динамическая маршрутизация

**2. Выбор программного комплекса для лабораторных работ.**

* 1. **Программа Cisco Packet Tracer**

Компания Cisco является лидером в производстве оборудования для работы в сети. То различные коммутаторы, точки доступа, межсетевые экраны, протоколы и т.д. Теперь эта компания разработала собственное программное обеспечение для эмуляции сетей.

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 весьма правдоподобное 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 обнаружить неисправности.

С помощью приложения Cisco Packet Tracer можно создавать сети практически любой сложности. Но виртуально. Эта программа позволяет проверить работоспособность сети для передачи данных на программном уровне. Это очень важно, поскольку создание сложной сети предполагает значительные расходы. Утилита Cisco Packet Tracer  позволяет эмулировать работу сети, находить слабые места и устранять все проблемы в работе. Благодаря этому инженеры сетей могут на программном уровне создать сеть, протестировать ее, и только потом приступать к ее монтажу.

Таким образом, можно экономить средства и время. Для крупных организаций, где возникает необходимость создания огромных сетей сложной номенклатуры, программам Cisco Packet Tracer  будет просто незаменима. Но даже для домашнего использования будет полезно сначала создать виртуальную сеть, а потом уже прокладывать кабель и устанавливать оборудование.

Программу Cisco Packet Tracer  скачать бесплатно может каждый желающий.

Если необходимо создать более сложную сеть и проверить ее работоспособность перед установкой оборудования – можно воспользоваться программой Cisco Packet Tracer. Это удобное и функциональное приложение.

Функциональные возможности программы позволяют применять самые разнообразные маршрутизаторы, точки доступа, сетевые экраны, серверы DHCP, FTP, TFTP, рабочие станции и обычные компьютеры. Кроме того, можно создавать сети, как с помощью разнообразных кабелей, так и по каналам беспроводной связи.

Стоит отметить, что приложение cisco packet tracer не работает со всеми устройствами. Эта программа предназначена, в основном, для прокладки сетей с использованием оборудования компании Cisco. Другие устройства доступа в сеть могут работать не совсем корректно. По этой причине использовать Cisco Packet Tracer  нужно в том случае, если вы планируете использовать оборудование этой компании. В противном случае данные, по которым будет прокладываться виртуальная сеть, могут не совсем соответствовать действительности.

Последняя версия программы Cisco Packet Tracer  поддерживает синхронизацию баз данных с облачным сервером компании. Благодаря этому виртуальная прокладка сетей для связи компьютеров и доступа в интернет становится еще проще.

Cisco Packet Tracer  может быть использован не только как симулятор, но и как сетевое приложение для симулирования виртуальной сети через реальную сеть, в том числе Интернет. Пользователи разных компьютеров, независимо от их местоположения, могут работать над одной сетевой топологией, производя ее настройку или устраняя проблемы. Эта функция многопользовательского режима Cisco Packet Tracer  широко применяется для организации командной работы, а также для проведения игр и соревнований между удаленными участниками.

Помимо этого, с помощью 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. Помимо перечисленных характеристик, в Cisco Packet Tracer  есть возможности, предусмотренные непосредственно для преподавателей. В их числе – режим автоматического контроля проведения лабораторных работ. Задача инструктора – подготовить задание или воспользоваться уже разработанными учебными шаблонами, а результат автоматически проконтролирует программа. Особенно симулятор Cisco Packet Tracer  незаменим во время лекций, так как позволяет, не выходя из класса, демонстрировать поведение сетевого оборудования. Если к реальному оборудованию сложно получить доступ в лабораторных целях, а работа подразумевает проведение эксперимента и использование большого числа сетевых устройств, виртуальные возможности Cisco Packet Tracer  легко решают задачи, стоящие перед инструкторами.

Интерфейс программного продукта прост и понятен человеку, который имеет базовые знания в сфере сетевых технологий, поэтому студенты могут работать в Packet Tracer без особых проблем.

В пакете Packet Tracer существует два режима работы: Режим реального времени и режим симуляции. В режиме реального времени мы наблюдаем за работой сетевого оборудования как в жизни, можем смотреть через какое время будет канальная связь между маршрутизаторами после включение порта на последнем.

В режиме симуляции мы можем послать пакет от одного устройства к другому и посмотреть, как идет пакет. Например: в случае, когда отказоустойчивой системе был поврежден или отключен основной путь, по которому идет пакет, он шел через резервный канал. Так же в режиме симуляции.

* 1. **Программа Dynamips**

Dynamips - это программный эмулятор аппаратной части маршрутизаторов сisco. Dynamips хорош в случаях, когда необходимо:

* быстро проверить конфигурацию маршрутизатора для непосредственного её применения последствие на реальной железке;
* получить лабораторный стенд достаточно мощный для обучения или демонстрации;
* опробовать преимущества и возможности операционной системы Cisco IOS без необходимости покупки самого маршрутизатора.

Помимо аппаратного обеспечения маршрутизаторов cisco существует возможность эмулировать сетевые устройства, такие как:

* Мост (используя который можно соединить эмулированный маршрутизатор с реальной сетью или другому виртуальному маршрутизатору);
* Ethernet-коммутатор;
* ATM-коммутатор;
* ATM-мост (Ethernet <-> ATM);
* коммутатор Frame-Relay.

Замечательной способностью Dynamips является то, что он может работать в режиме гипервизора. То есть одновременно есть возможность запускать не один эмулятор, а целую сеть со всеми возможностями dynamips: коммутаторами, маршрутизаторами, мостами. Таким образом появляется возможность выполнять лабораторные работы без реального оборудования. Или же демонстрационные стенды. Причём практически любой сложности. Управление гипервизором осуществляется по сети TCP/IP. Следует заметить, что запущенный по умолчанию, эмулятор сильно загружает компьютер. Даже на 100%. Чтобы снизить нагрузку, создана опция "Idle PC". С её помощью можно снизить нагрузку на процессор и, таким образом, запустить второй, третий и более эмуляторов cisco одновременно без существенной нагрузки процессора. Значение IdlePC специфично для каждого образа IOS.   
Dynamips представляет из себя один исполняемый файл. Причём есть варианты под Linux, Mac OS и Windows. Но при запуске принимает множество аргументов, для задания особых параметров эмуляции.

* 1. **Программа Boson Netsim**

Boson NetSim это приложение, которое имитирует работу сетевого оборудования Cisco Systems и программного обеспечения и предназначен для того, чтобы помочь пользователю изучить команды Cisco. Boson NetSim обеспечивает больше гибкости и поддержки, чем любое другое программное обеспечение моделирования сетей на рынке. Программное обеспечение также включает в себя лабораторию, которая содержит уроки и лабораторные работы по изучению протоколов маршрутизации, Cisco устройств, коммутации, топологии и многое другое.

Boson NetSim является универсальным инструментом, как в классе, так и для корпоративного использования, но и может использоваться и для самостоятельного изучения. Для многих людей возможности приобрести маршрутизаторы и коммутаторы Cisco ограничены. Стоимость и хрупкость оборудования делает покупку или аренду нецелесообразной для самостоятельного изучения. Выходом может стать использование программы Boson NetSim. Она позволяет спроектировать и настроить сеть с 42 различными моделями маршрутизаторов без необходимости платить деньги за оборудование, или беспокоиться о его транспортировке и повреждениях.  Кроме того, Boson NetSim имитирует как переключение моста таблицы и таблицы маршрутизации протокола. Дополнительные функции Boson NetSim:

* Поддерживает 42 маршрутизатора и 6 переключателей
* Имитирует сетевой трафик с помощью технологии виртуальных пакетов
* Обеспечивает два разных стилея просмотра: режим Telnet или консольный режим
* Поддерживает до 200 устройств на одной топологии сети
* Включает в себя лаборатории, которые поддерживают моделирование SDM
* Включает в себя не-Cisco устройств, таких как TFTP сервер, TACACS + и генератор пакетов
  1. **Программа NetCracker Professional**

NetCracker - программа представляет собой CASE-средства автоматизированного проектирования, моделирования и анализа компьютерных сетей. Позволяет провести эксперименты, результаты которых могут быть использованы для обоснования выбора типа сети, сред передачи, сетевых компонент оборудования и программно-математического обеспечения.

Программные средства NetCracker позволяют выполнить сбор соответствующих данных о существующей сети без остановки ее работы, создать проект этой сети и выполнить необходимые эксперименты для определения предельных характеристик, возможности расширения, изменения топологии и модификации сетевого оборудования с целью дальнейшего ее совершенствования и развития.

С помощью NetCracker можно проектировать компьютерные сети различного масштаба и назначения: от локальных сетей, насчитывающих несколько десятков компьютеров, до межгосударственных глобальных сетей, построенных с использованием спутниковой связи. В составе программного обеспечения NetCracker имеется мощная база данных сетевых устройств ведущих производителей: рабочих станций, серверов, сред передачи, сетевых адаптеров, повторителей, мостов, коммутаторов, маршрутизаторов, используемых для различных типов сетей и сетевых технологий.

NetCracker позволяет разрабатывать многоуровневые проекты с заданной проектировщиком степенью детализации; при этом имеется достаточно удобный интерфейс и средства быстрого просмотра всех уровней проекта. Для реализаций функций имитационного моделирования в составе NetCracker предусмотрены средства задания характеристик трафиков различных протоколов; средства визуального контроля заданных параметров; средства накопления статистической информации и формирования отчетной документации о проведенных экспериментах.

**3. Описание возможностей пакета Packet Tracer**

Cisco Packet Tracer - это эмулятор сети, созданный компанией Cisco. Программа используется для обучения в академии Cisco, позволяет имитировать работу различных сетевых устройств: маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров, IP-телефонов и т.д. Работа с интерактивным симулятором дает весьма правдоподобное ощущение настройки реальной сети, состоящей из десятков или даже сотен устройств. Программа бесплатна, имеется русский интерфейс.

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 весьма правдоподобное 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 обнаружить неисправности.

Cisco Packet Tracer может быть использован не только как симулятор, но и как сетевое приложение для симулирования виртуальной сети через реальную сеть, в том числе Интернет. Пользователи разных компьютеров, независимо от их местоположения, могут работать над одной сетевой топологией, производя ее настройку или устраняя проблемы. Эта функция многопользовательского режима Cisco Packet Tracer широко применяется для организации командной работы, а также для проведения игр и соревнований между удаленными участниками.

Помимо этого, с помощью 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 всё кабельное хозяйство, 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.

**3.1. Пример работы с программой**

3.1.1. Добавление оборудования

Оборудование добавляется очень просто, достаточно выбрать на нижней панели нужный тип устройства:

* Маршрутизаторы (Роутеры)
* Коммутаторы
* Хабы (устарели и почти не используются)
* Беспроводные устройства
* Конечные устройства (компьютеры, ноутбуки, сервера)

А затем выбрать само устройство, например как на рисунке 3.1, роутер Cisco 1841 и закрепить на главном поле:

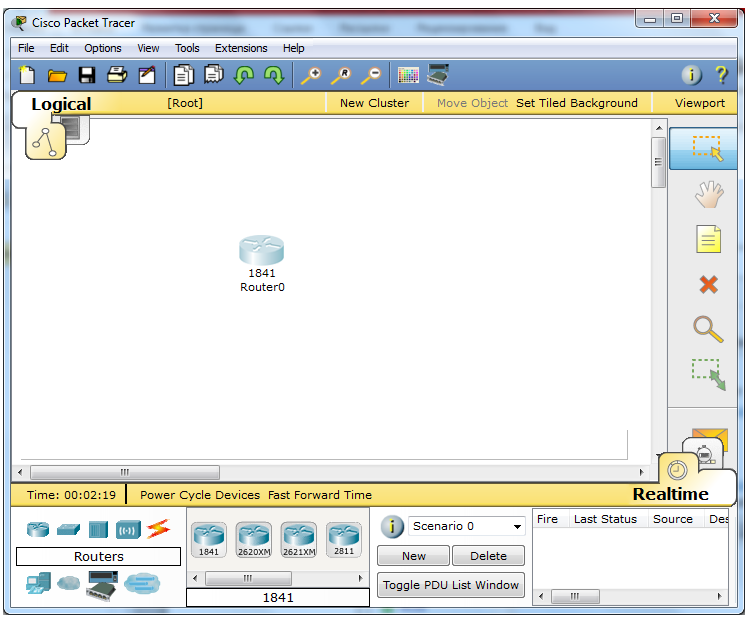


Рис. 3.1.

Для тестирования разных схем, типов маршрутизации обычно надо пару маршрутизаторов, пару коммутаторов, сервер (DHCP, ftp) и пару компьютеров. Все это соединяется с помощью различных видов соединений:

* Консольное (консольный кабель Cisco)
* прямое соединение (2 компьютера или 2 роутера между собой)
* кроссоверное соединение (компьютер — свитч, роутер — свитч)
* Оптическое
* Телефонное
* Коаксильное
* Автоматическое (само выбирает тип соединения)

3.1.2. Конфигурирование

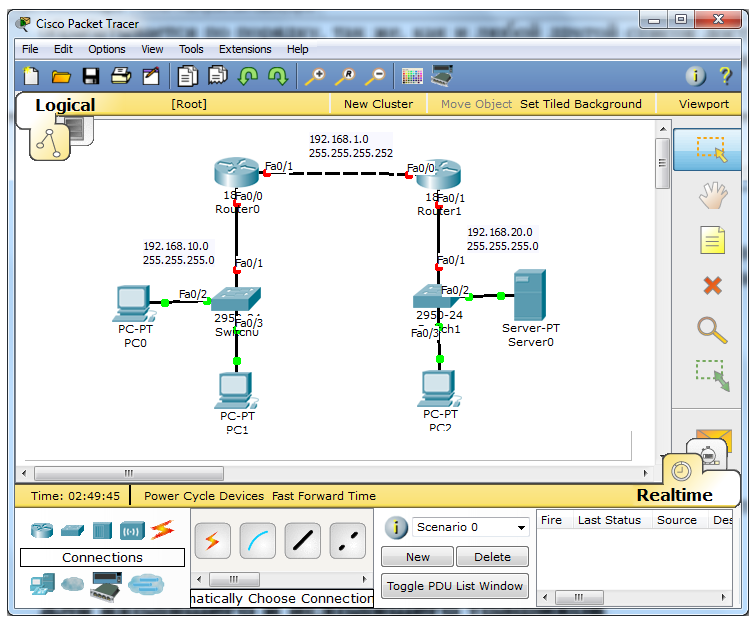


Рис. 3.2.

Приступать к настройке можно сразу после добавления устройства, но лучше сначала все подключить, потому что в режиме онлайн при верных настройках появляется коннект (На рис.3.2. видно, что коннекта между маршрутизаторами нет, а между компьютерами есть.)

Рассмотрим пример первоначальной настройки маршрутизатора. Кликаем по нему и выходит окно с настройками:

* Настройка физической части: установка и замена плат, включение и выключение устройства
* Конфигурирование с помощью графического: настройка сетевых интерфейсов, имени, сохранение/загрузка конфига, стирание startup конфига, настройка vlan(если ставим плату свитча) и простая маршрутизация rip и статика
* Конфигурирование с помощью консоли (аналогично подключение к консоли cisco с помощью кабеля)

Через графический интерфейс настраивать сетевые интерфейсы в разы удобнее и быстрее, можно просто копировать и вставлять нужные параметры. Настройка маршрутизации же наоборот очень неудобная и проще из консоли.

Настройка через, так называемый, Command Line Interface ничем не отличается от настройки физической аппаратуры (Рис. 3.3.).

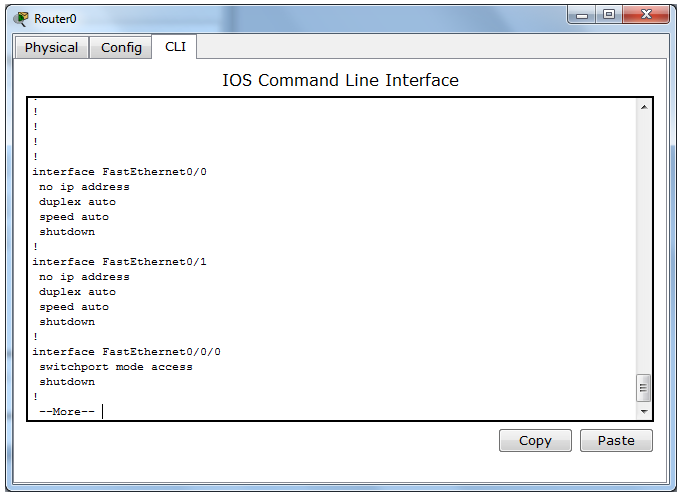


Рис. 3.3.

**4. Разработка структуры лабораторного комплекса**

**4.1 Лабораторный комплекс**

Лабораторный комплекс включает методические указания по каждой лабораторной работе. Описание лабораторных работ должно быть изложено связно, в методической последовательности. Название лабораторной работы должно включать порядковый номер работы в составе комплекса.

Структура лабораторного комплекса включает:

1. Содержание.
2. Введение.
3. Цель работы.
4. Задачи.
5. Теоретическая часть.
6. Практическая часть.
7. Задание для самостоятельной работы.
8. Требования к содержанию и оформлению отчета.
9. Контрольные вопросы.
10. Литература.

4.1.1 Структура лабораторного комплекса

Сформируем структуру будущего комплекса лабораторных работ. Комплекс включает в себя пять лабораторных работ:

Лабораторная работа №1 «Создание и настройка VLAN. Виртуальные интерфейсы»

В первой лабораторной работе рассматриваем вопрос создания виртуальных локальных сетей, студенту предстоит: познакомиться с настройкой VLAN, настройкой портов доступа и транковых портов, созданием виртуальных интерфейсов.

Лабораторная работа №2 «Протокол маршрутизации STP и его разновидности (RSTP, PVSTP, MVSTP)»

Данная лабораторная работа является продолжением первой работы, в ней создается древовидная структура сети, и настраивается работа протокола STP. Так же наглядно демонстрируется задействование резервного канала связи при отказе основного.

Лабораторная работа №3 «Совместная работа протоколов RIP и RIPv2»

Данная лабораторная работа направлена на проверку совместной работы протоколов динамической маршрутизации RIP и RIP версии 2.

Лабораторная работа №4 «Протокол маршрутизации OSPF, разбиение на 2 зоны»

Данная лабораторная работа является продолжением предыдущей, в ней убираются протоколы маршрутизации RIP, и настраиваются OSPF. Так же работа OSPF разделена на несколько зон.

Лабораторная работа №5 «IP - телефония»

В данной лабораторной работе настраивается работы сервиса IP- телефонии, настройка персональных компьютеров на работу данного сервиса, настройка DHCP сервера, а так же настройка обычного телефона на работу с IP-телефонами.

Это предварительный состав комплекса лабораторных работ, который в процессе разработки может быть видоизменен.

4.1.2 Схема лабораторного комплекса

На рис. 4.1 представлена структура комплекса.

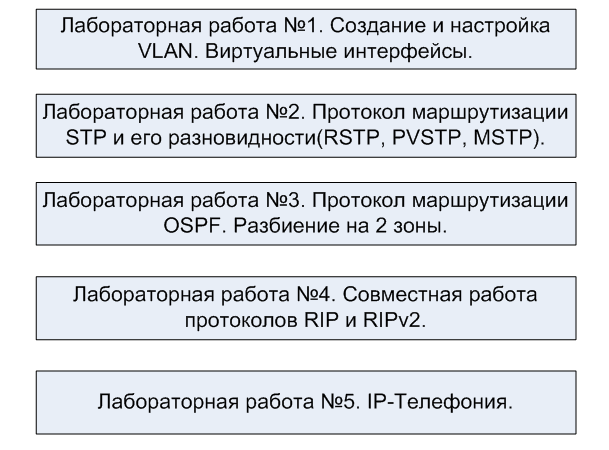
****

Рис. 2.1 – Структура комплекса

**5. Разработка схем для комплекса лабораторных работ**

**5.1 Разработка схем для лабораторных работ №1 и №2**

5.1.1. Лабораторная работа №1.

Для начала создадим топологию, показанную на рисунке 5.1:

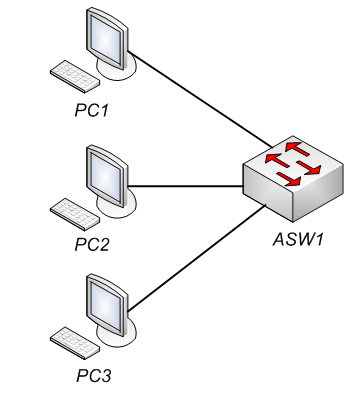


Рис. 5.1.

Назначим компьютерам IP адреса, настроим работу коммутатора. Далее мы добавляем пару коммутаторов и еще один компьютер (рис. 5.2).

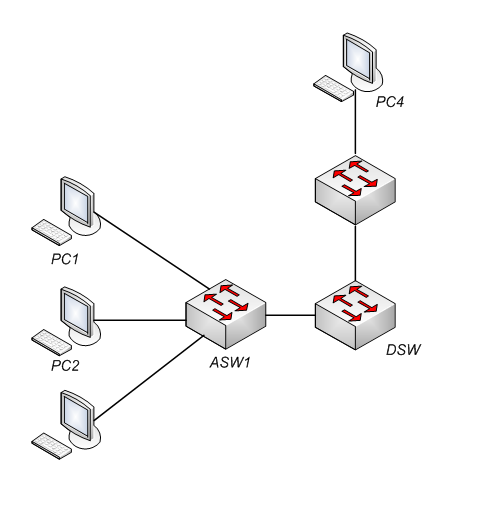


Рис. 5.2.

Следующим этапом будет настройка VLAN в сети, после этого проверка доступности с помощью команды “ping”.

После этого добавим еще 2 коммутатора и 3 сервера (рис. 5.3).

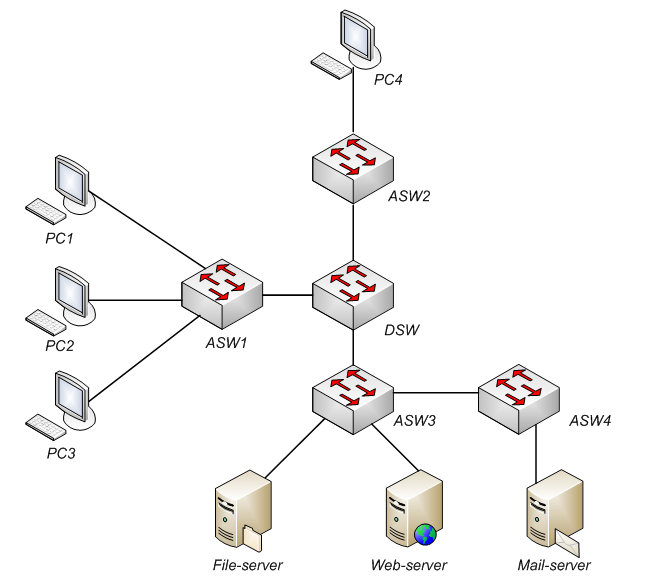


Рис. 5.3.

Аналогичным образом настраиваем VLAN, только уже с другим номером и смотрим доступность. В такой схеме сервера не должны быть доступны с компьютеров, так как у нас разные VLAN. Значит, следующим этапом добавляем маршрутизатор и настраиваем на нем виртуальные интерфейсы. После этого сервера станут доступны для пинга (рис. 5.4).

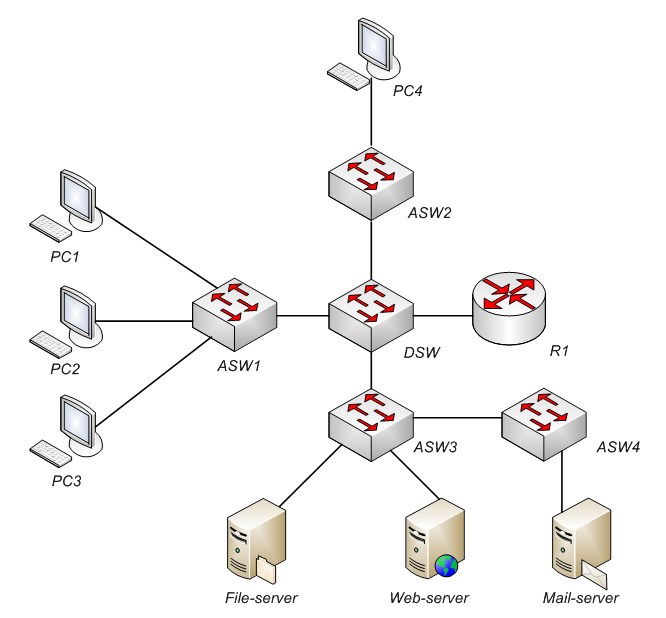


Рис. 5.4.

На этом заканчивается практическая часть лабораторной работы №1. Разработка вариантов будет в разделе 7.

4.1.2. Лабораторная работа №2.

В данной работе я не стал что-либо усложнять, создавая совершенно новую топологию, чтобы рассмотреть работу протокола маршрутизации STP. Таким образом, я взял конечную топологию первой лабораторной работы, и добавил туда еще одну связь между коммутаторами DSW и ASW4 (рис. 5.5).

После этого настраиваем протокол STP на коммутаторах, и за корневой выберем DSW.

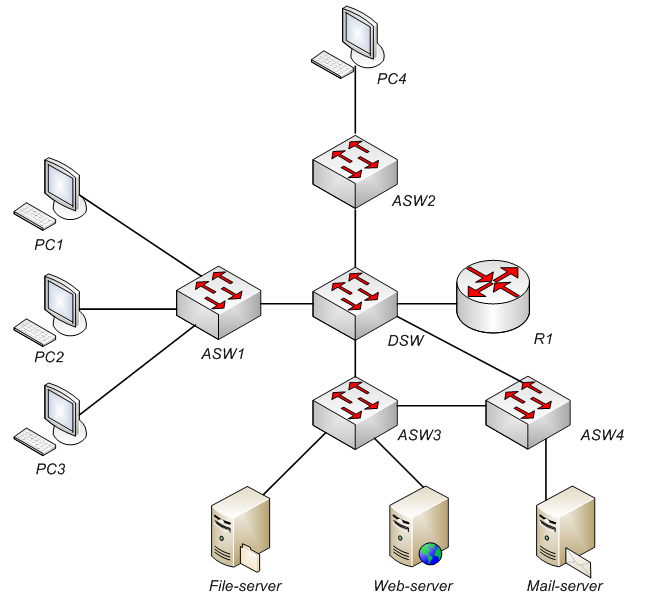


Рис. 4.5.

**5.2. Разработка схем для лабораторных работ №3 и №4.**

5.2.1. Лабораторная работа №3.

Для начала создадим топологию, показанную на рисунке 5.6.

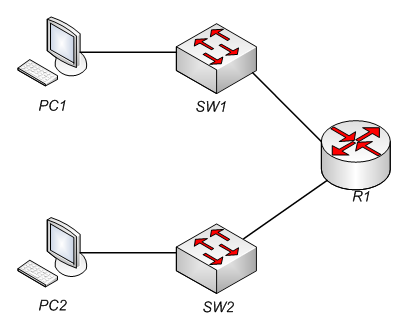


Рис. 4.6.

Настроим компьютеры, коммутаторы и маршрутизатор. Проверим пинги. Это будут первые две подсети. Следующим этапом создадим третью подсеть и аналогичным образом настроим ее (рис. 5.7).

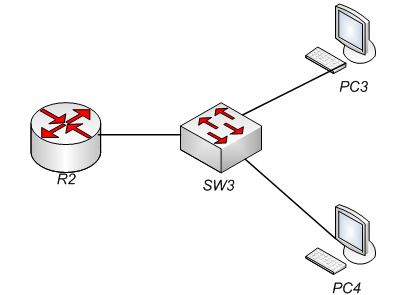


Рис. 5.7.

После этого соединим наши подсети в одну сеть (рис. 5.8).

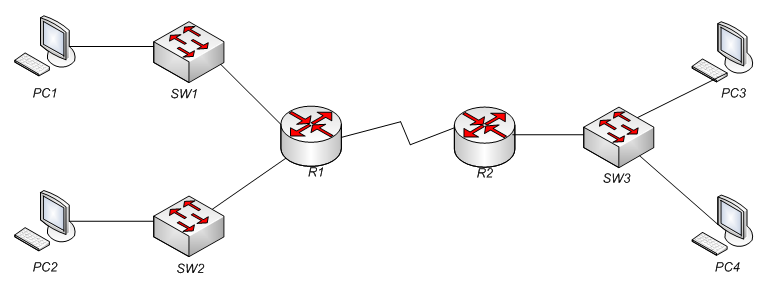


Рис. 5.8.

После этого настраиваем протоколы RIP и RIPv2 и смотрим работу.

5.2.2. Лабораторная работа №4.

Опять-таки, не будем ничего усложнять и возьмем схему из прошлой лабораторной работы, уберем протоколы RIP и RIPv2 и настроим протокол OSPF разбив нашу сеть на 3 зоны (рис. 5.9).

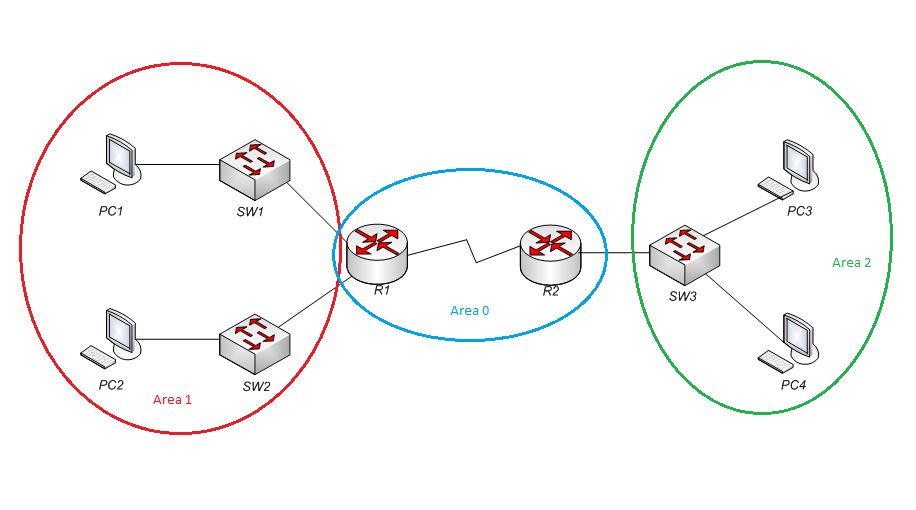


Рис. 5.9.

**4.3. Разработка схем для лабораторной работы №5.**

Для начала создадим топологию, показанную на рисунке 5.10.

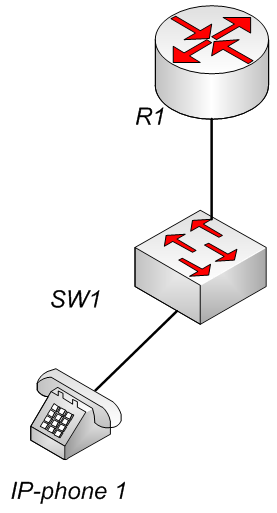


Рис. 5.10.

Далее настроим DHCP сервер на маршрутизаторе, настроим сервис телефонии, и настроим телефон, задав ему номер. Следующим этапом добавим еще 2 телефона и 1 ноутбук (рис. 4.11).

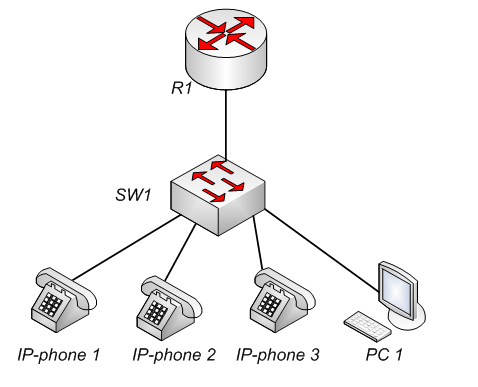


Рис. 5.11.

Зададим номера телефонам и ноутбуку. Далее создаем другую подсеть с обычным домашним телефоном и компьютером (рис. 5.12).

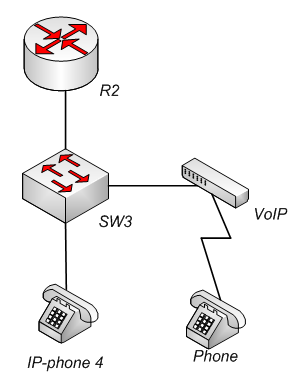


Рис. 5.12.

Чтобы работал обычный телефон, надо подключить его через кодирующее устройство VoIP. Аналогично настраиваем данную подсеть, и следующим этапом соединяем наши подсети (Рис. 5.13).

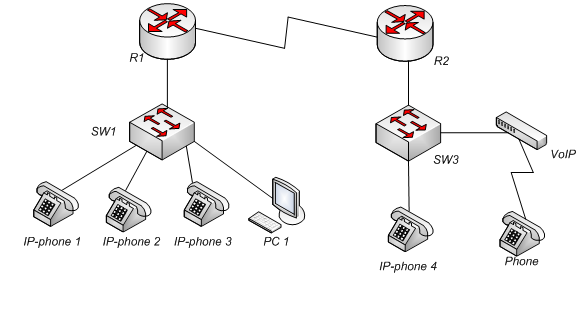


Рис. 5.13.

После этого проверяем дозвоном работу нашей сети.

**6. Тестирование схем и анализ полученных результатов**

**6.1. Тестирование схем лабораторной работы №1.**

Протестируем работу сети первой лабораторной работы. Топология представлена на рисунке 6.1.

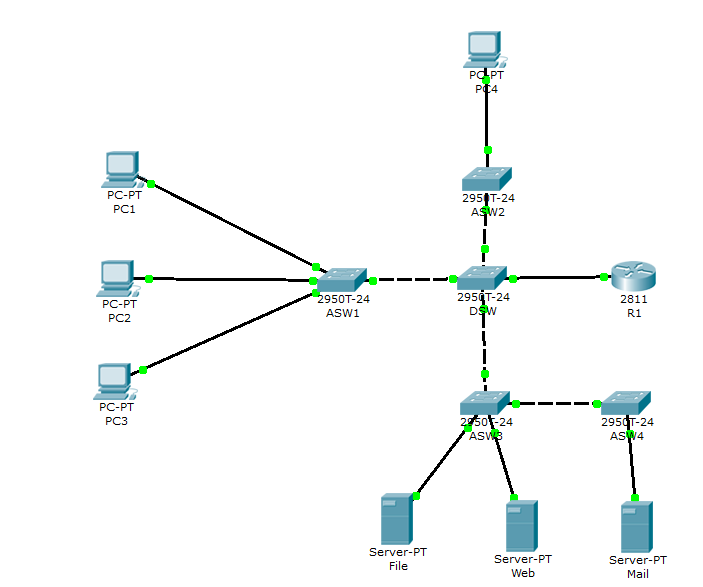


Рис. 6.1.

Сначала попробуем пропинговать с компьютера PC1 компьютер PC4. Далее с компьютера PC4 пропинговать Mail server. С компьютера PC3 пропинговать File server. Ну и последним шагом с File server пропинговать компьютер PC2. Скриншоты пингов представлены на рисунках 6.2, 6.3, 6.4, 6.5.

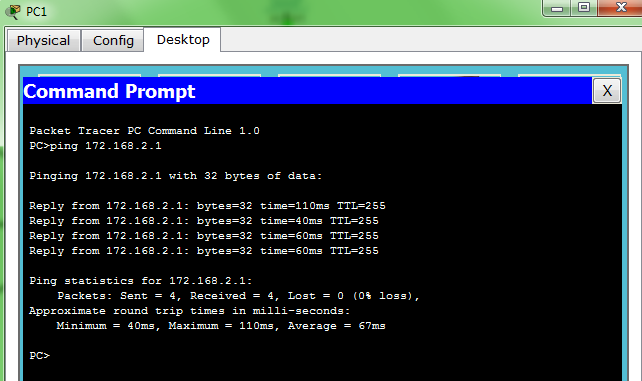


Рис. 6.2.

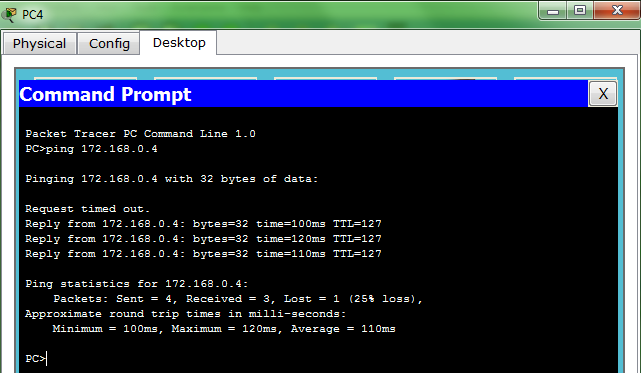


Рис. 6.3.

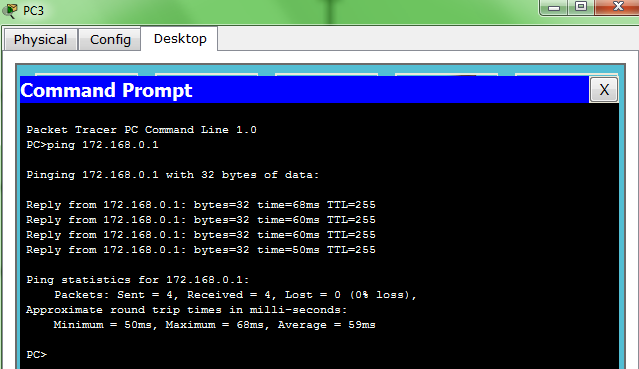


Рис. 6.4.

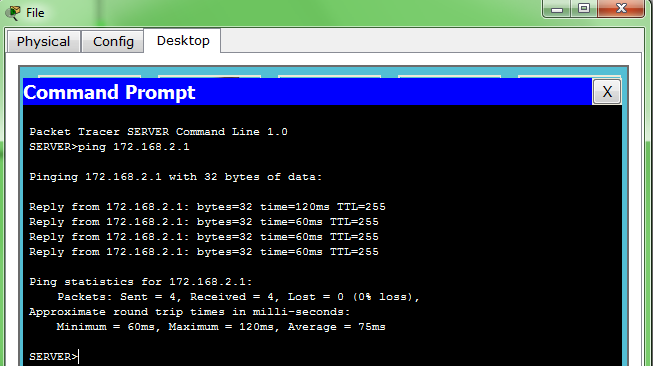


Рис. 6.5.

Как мы видим, все пинги у нас есть, значит сеть настроена правильно.

**6.2. Тестирование схем лабораторной работы №2.**

Протестируем работу сети и протокола STP второй лабораторной работы, топология которой представлена на рисунке 6.6.

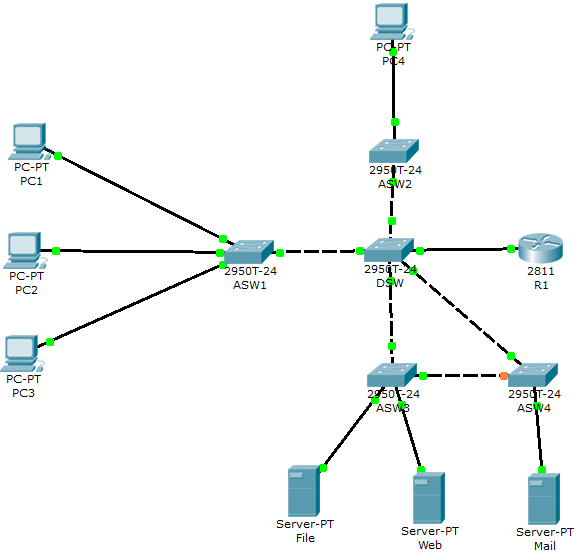


Рис. 6.6.

Проверим работу RSTP, запустим пинг с PC1 на Mail сервер, и отключим интерфейс FA0/3 на коммутаторе ASW4. Данные о пинге представлены на рисунке 6.7. Как мы видим, на перестроение маршрута ушло всего несколько секунд, за это время ни один пакет не потерялся.

Следующим этапом восстановим интерфейс FA0/3 и опять-таки посмотрим на пинг. Данные представлены на рисунке 6.8. Как мы видим, на обратное восстановление маршрута потребовалось чуть больше времени и потерялся всего 1 пакет.

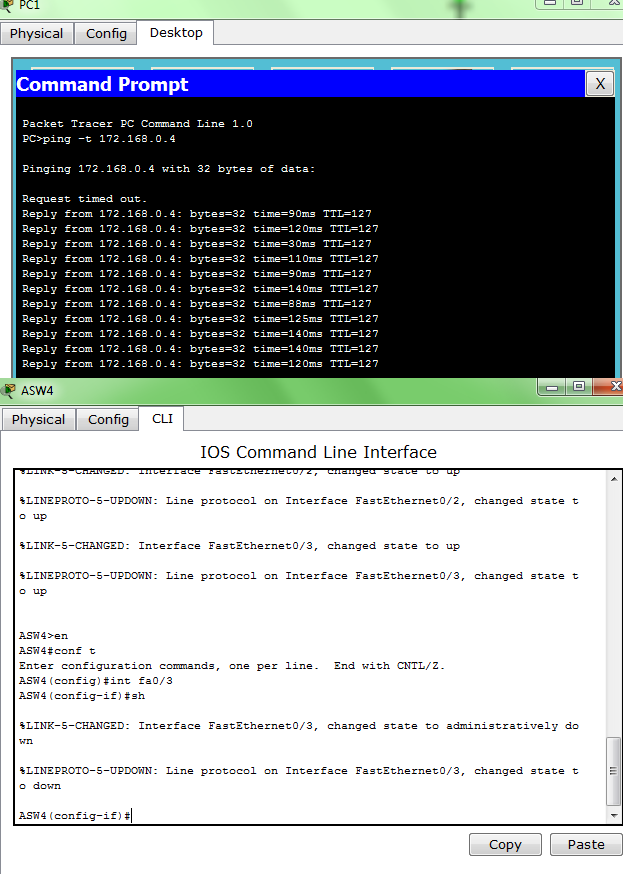


Рис. 6.7.

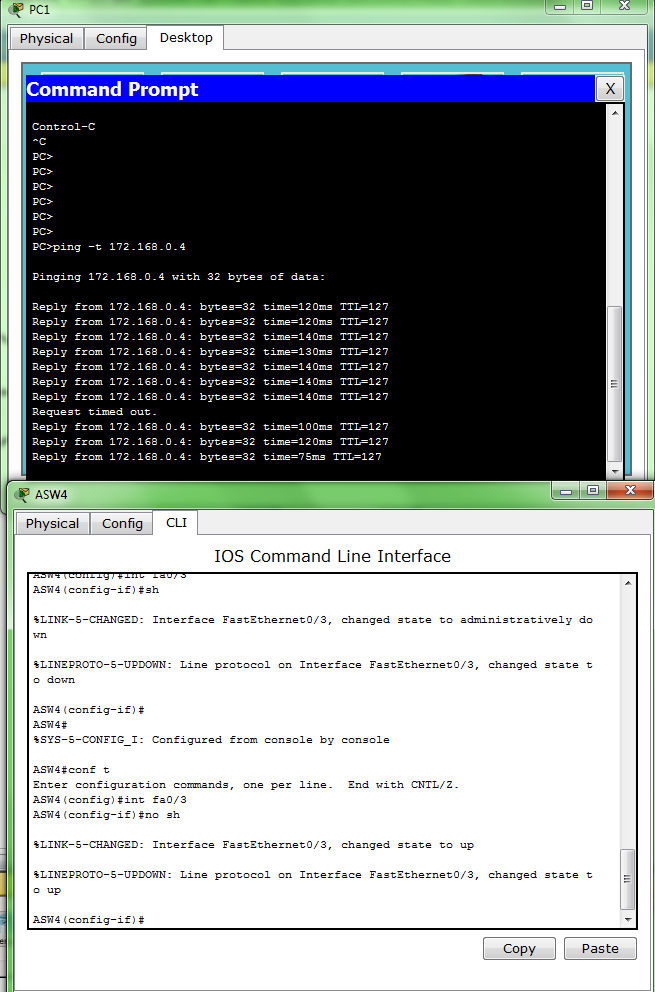


Рис. 6.8.

Таким образом, можно сделать вывод, что в нашей сети протокол RSTP работает нормально.

**6.3. Тестирование схем лабораторной работы №3.**

Протестируем схему лабораторной работы №3, топология которой представлена на рисунке 6.9.

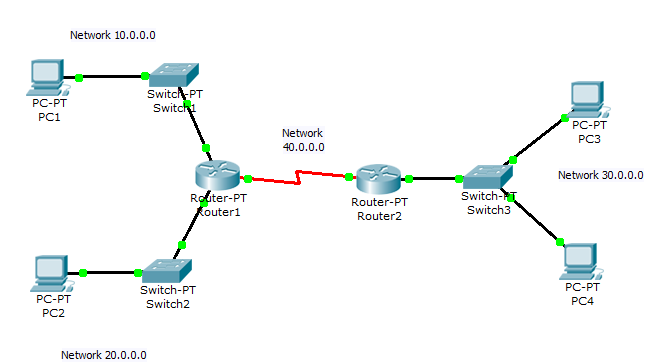


Рис. 6.9.

Проверим версию протоколов на маршрутизаторах Router 1 (рис.6.10) и Router 2 (Рис.6.11).

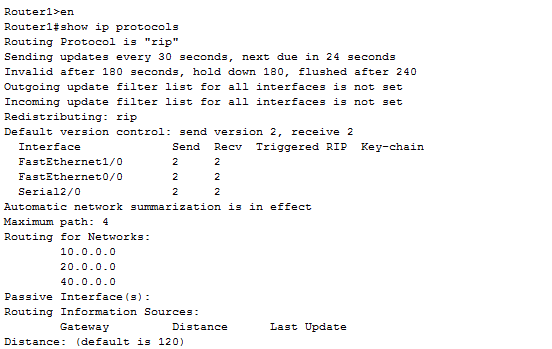


Рис. 6.10.

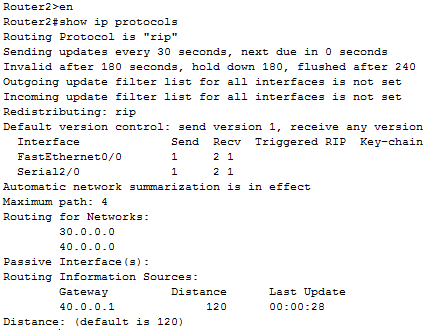


Рис. 6.11.

Посмотрим таблицы маршрутизации на Router 1 (рис. 6.12) и Router 2 (рис.6.13).

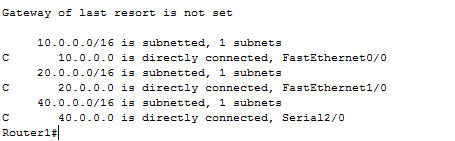


Рис. 6.12.

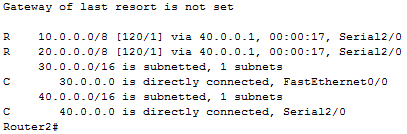


Рис. 6.13.

Проверим пинги с компьютера PC1 на PC2, с PC2 на PC4. Скриншоты представлены на рисунках 6.14 и 6.15.

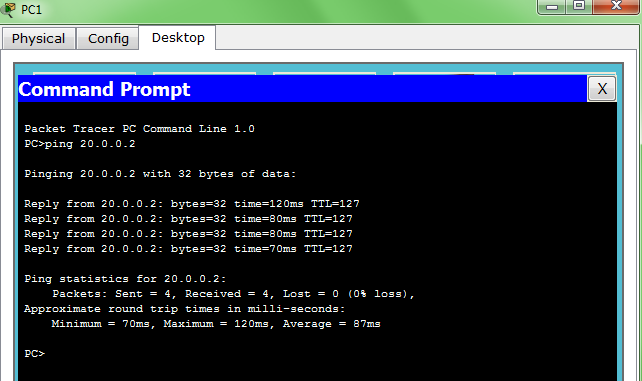


Рис. 6.14.

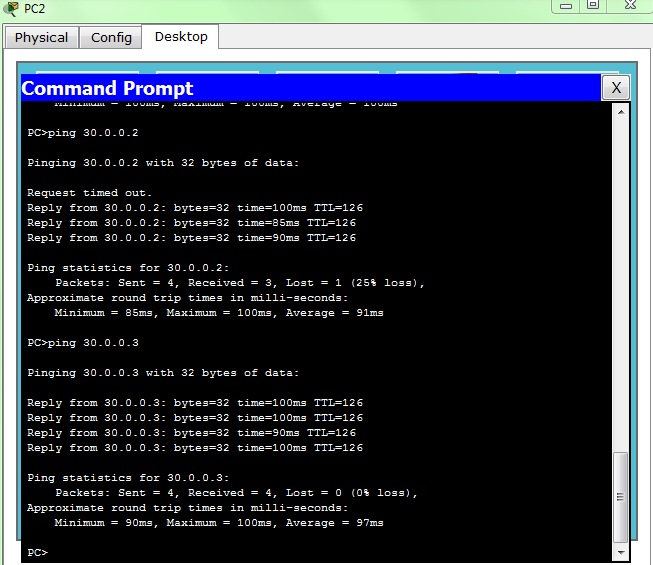


Рис. 6.15.

Как мы видим, пинги есть, отсюда можно сделать вывод, что сеть работает нормально, при совместной работе протоколов RIP и RIP версии 2.

**6.4. Тестирование схем лабораторной работы №5.**

Протестируем работу сервиса IP – телефонии, топология сети которой представлена на рисунке 6.16.

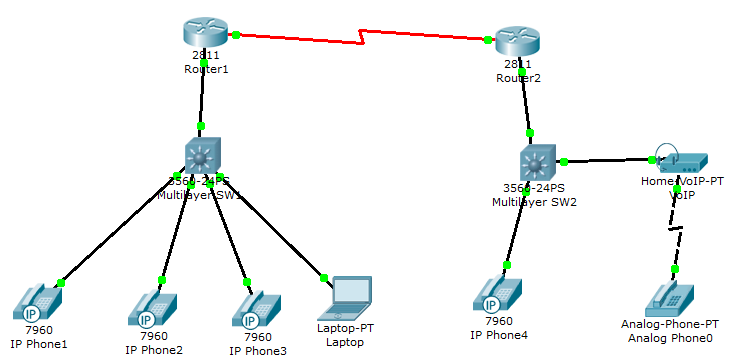


Рис. 6.16.

Попробуем позвонить с IP phone 2 на Analog phone (рис.6.17), с Laptop на IP Phone 4 (рис. 6.18).



Рис. 6.17.



Рис. 6.18.

Как мы видим, соединение устанавливается, таким образом можно сделать вывод, что сервис IP телефонии работает нормально.

**7. Разработка вариантов заданий для лабораторных работ**

**7.1. Варианты заданий для лабораторной работы №1.**

Спроектируем топологию, изображенную на рисунке 7.1.

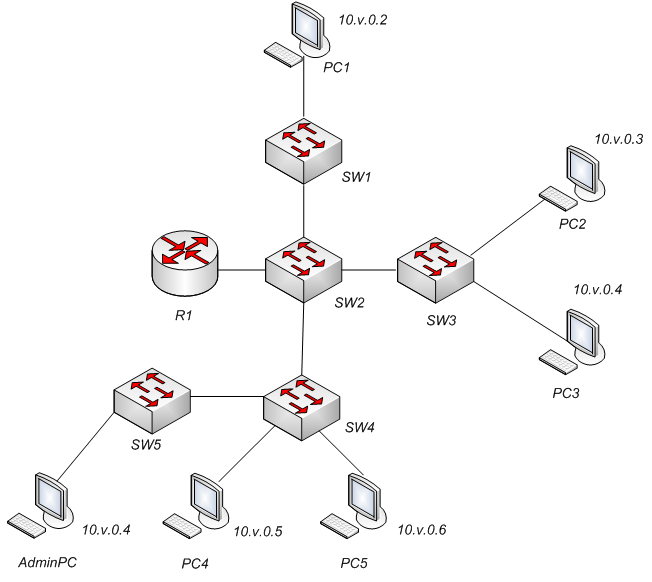


Рис. 7.1.

Вариация заданий для самостоятельной работы будет заключатся в том, что для каждого варианта, назначаются свои IP адреса, ниже приведена таблица с 10 вариантами.

Таблица 7.1.

Варианты заданий для лабораторной работы №1

|  |  |  |  |
| --- | --- | --- | --- |
| Вариант | IP (v) | VLAN данных x / y | VLAN управления |
| 1 | 10 | 4 / 5 | 6 |
| 2 | 0 | 9 / 10 | 11 |
| 3 | 1 | 43 / 44 | 48 |
| 4 | 168 | 6 / 7 | 5 |
| 5 | 50 | 11 / 12 | 10 |
| 6 | 40 | 48 / 48 | 44 |
| 7 | 55 | 7 / 8 | 9 |
| 8 | 100 | 10 / 11 | 15 |
| 9 | 200 | 15 / 14 | 10 |
| 10 | 11 | 6 / 5 | 3 |

После этого идут общие задания для всех вариантов.

**7.2. Варианты заданий для лабораторной работы №2.**

Схему и IP адреса возьмем из прошлой лабораторной работы, но добавим пару связей. Топология представлена на рисунке 7.2.

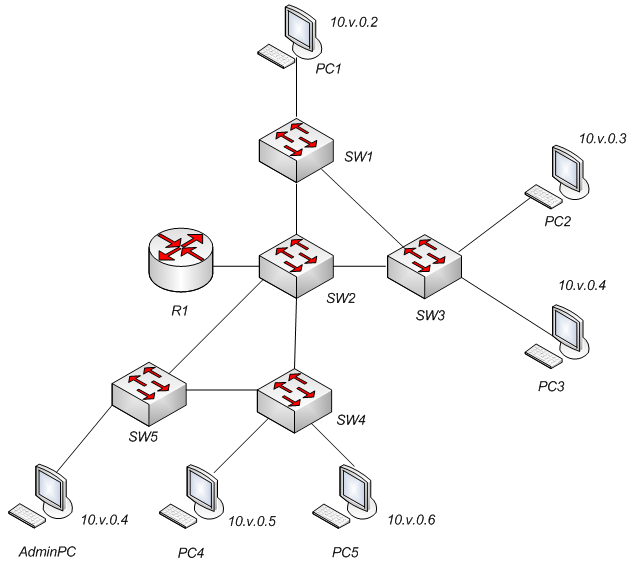


Рис. 7.2.

Вариация заданий будет заключаться в проверке пинга между разными компьютерами. Ниже приведена таблица с вариантами заданий.

Таблица 7.2.

Варианты заданий для лабораторной работы №2

|  |  |
| --- | --- |
| Вариант | Компьютеры |
| 1 | с PC1 на PC3 |
| 2 | с PC2 на AdminPC |
| 3 | c PC5 на PC1 |
| 4 | с PC4 на PC2 |
| 5 | С AdminPC на SW3 |
| 6 | С AdminPC на SW2 |

**7.3.** **Варианты заданий для лабораторной работы №3 и №4**

В данной лабораторной работе, вариация заданий будет заключаться в проектировании различных схем, по вариантам. Всего будет 4 схемы, которые показаны на ниже приведенных рисунках.

Вариант 1:

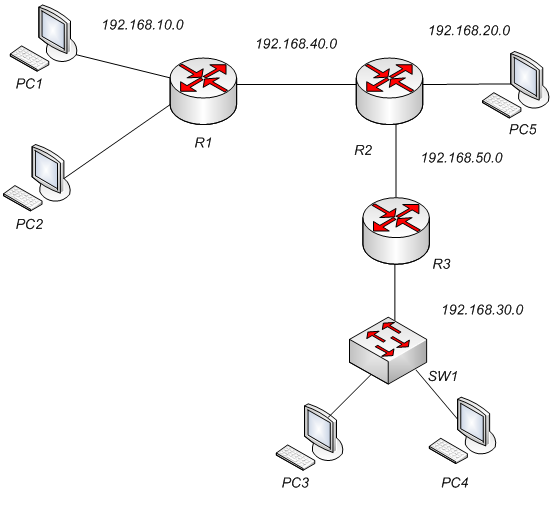


Рис. 7.3.

Вариант 2:

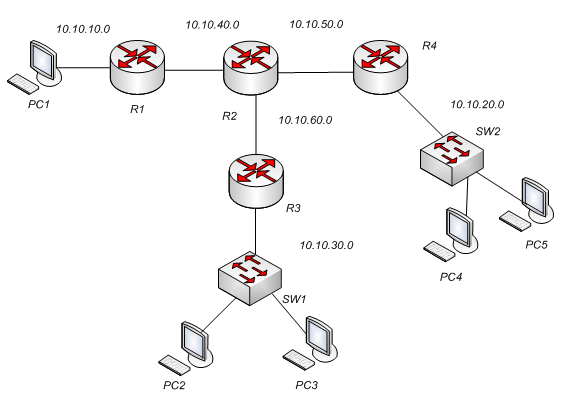


Рис. 7.4.

Вариант 3:

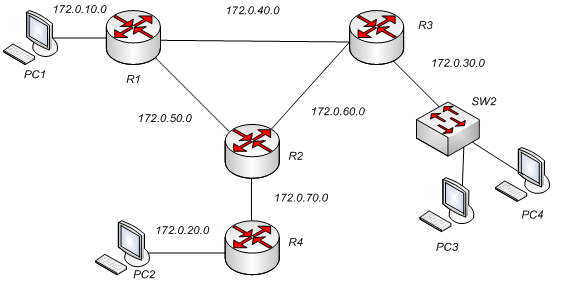


Рис. 7.5.

Вариант 4:

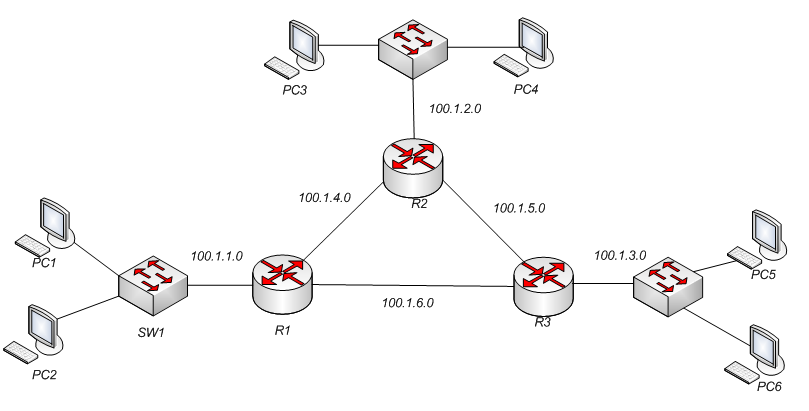


Рис. 7.6.

После создания сети, идет общее задание для всех вариантов.

Для лабораторной работы №4 берутся схемы из лабораторной работы №3.

**7.4. Варианты заданий для лабораторной работы №5.**

Для данной лабораторной работы вариация заданий будет заключаться в различном количестве IP-телефонов и Компьютеров. Топология приведена на рисунке 7.7. Варианты заданий приведены в таблице 7.3. После составления своей схемы сети, студентам будет дано общее задание на проверку работы сервиса IP-телефонии.

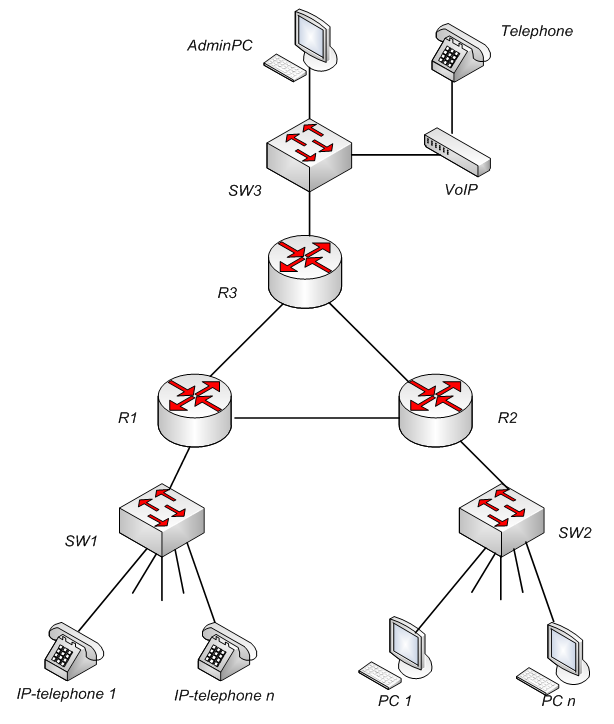


Рис. 7.7.

Таблица 7.3.

Варианты заданий для лабораторной работы №5

|  |  |  |
| --- | --- | --- |
| Вариант | Кол-во PC | Кол-во IP-телефонов |
| 1 | 4 | 5 |
| 2 | 2 | 7 |
| 3 | 6 | 4 |
| 4 | 7 | 2 |
| 5 | 5 | 5 |
| 6 | 3 | 6 |

**8. Разработка методических указаний к лабораторным работам.**

**Лабораторная работа №1. Создание и настройка VLAN. Виртуальные интерфейсы.**

**Теоретическая часть**

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. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств.

***Реализация VLAN в устройствах CISCO***

В устройствах Cisco, протокол VTP (VLAN Trunking Protocol) предусматривает VLAN-домены для упрощения администрирования. VTP также выполняет «чистку» трафика, направляя VLAN трафик только на те коммутаторы, которые имеют целевые VLAN-порты (функция VTP pruning). Коммутаторы Cisco в основном используют протокол 802.1Q Trunk вместо устаревшего проприетарного ISL (Inter-Switch Link) для обеспечения совместимости информации.

По умолчанию на каждом порту коммутатора имеется сеть VLAN1 или VLAN управления. Сеть управления не может быть удалена, однако могут быть созданы дополнительные сети VLAN и этим альтернативным VLAN могут быть дополнительно назначены порты.

Native VLAN — это параметр каждого порта, который определяет номер VLAN, который получают все непомеченные (untagged) пакеты.

***Преимущества***

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

***Настройка в Packet Tracer***

Для того чтобы настроить VLAN порты на коммутаторах в пакете Packet Tracer, необходимо ввести следующие команды:

Для настройки портов доступа:

switch(config-if)#switchport mode access

switch(config-if)#switchport access vlan 2

Для настройки транковых портов:

switch(config-if)#switchport mode trunk

switch(config-if)#switchport trunk allowed vlan 2

***Виртуальные интерфейсы***

Очень часто бывает, что на маршрутизаторах не хватает обычных физических интерфейсов, чтобы решить эту проблему на помощь приходят так называемые sub-интерфейсы. Это такие интерфейсы, которые в принципе имеют те же самые параметры, что и физические, но терминируют только один VLAN.

Для создания виртуального интерфейса сначала указывается физический интерфейс, далее после точки указывается специальный идентификатор, как правило, его выбирают в соответствии с номером VLAN, который данный интерфейс будет терминировать.

Следующей командой указывается, что инкапсуляция будет по стандарту 802.1Q, и указывается метку VLAN. И наконец, задается IP адрес как на обычном интерфейсе.

router(config)#interface fastEthernet 0/0.2

router(config-subif)#encapsulation dot1Q 2

router(config-subif)#ip address 10.0.0.1 255.255.255.0

**Практическая часть**

**Создание топологии сети, назначение IP адресов, выбор интерфейсов.**

Создайте в Packet Tracer топологию, изображённую на рисунке c использованием модели коммутатора с названием – 2950T.

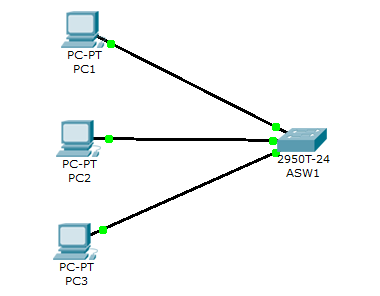


Рис. 1.

Подключите компьютеры PC1, PC2, PC3 в порты коммутатора FA0/1, FA0/2, FA0/3 соответственно.

Назначьте для компьютеров PC1, PC2, PC3 IP-адреса 172.168.2.2, 172.168.2.3, 172.168.2.4 соответственно, маски 255.255.255.0 и основной шлюз 172.168.2.1.

Теперь попробуем с компьютера PC1 послать пакеты на компьютер PC2:

PC>ping 172.168.2.3

Pinging 172.168.2.3 with 32 bytes of data:

Reply from 172.168.2.3: bytes=32 time=15ms TTL=128

Reply from 172.168.2.3: bytes=32 time=8ms TTL=128

Reply from 172.168.2.3: bytes=32 time=7ms TTL=128

Reply from 172.168.2.3: bytes=32 time=9ms TTL=128

Ping statistics for 172.168.2.3:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 7ms, Maximum = 15ms, Average = 9ms

Как мы видим, пинг есть, и это весьма закономерно, поскольку вся наша небольшая сеть является одним большим широковещательным доменом, все устройства в ней могут видеть друг друга прозрачно.

**Настройка VLAN.**

Теперь попробуем настроить на коммутаторе ASW1 VLAN.

Для начала зададим имя устройства (это не обязательно, но крайне желательно).

Switch>en

Switch#conf t

Switch(config)#hostname ASW1

Для начала создадим VLAN для PC1.

Переходим в режим настройки интерфейсов, указываем description (описание интерфейса):

ASW1(config)#interface fa0/1

ASW1(config-if)#description PC1

Следующей командой указываем режим работы порта, поскольку сюда подключается конечный компьютер, указываем access, и указываем какой именно VLAN будет закреплен за этим портом.

ASW1(config-if)#switchport mode access

ASW1(config-if)#switchport access vlan 2

Packet Tracer сказал что такого VLAN не существует и он создал его, но в некоторых версиях он пропадает, так что лучше перестраховаться и создать его вручную:

ASW1(config)#vlan 2

ASW1(config-vlan)#name users

Снова попробуем послать пакеты с PC1 на PC2:

PC>ping 172.168.2.3

Pinging 172.168.2.3 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 172.168.2.3:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Как мы видим, теперь связи между ними нет, т.к. они находятся в разных широковещательных доменах.

Настроим аналогично тот же самый VLAN для компьютеров PC2 и PC3.

ASW1(config)#interface fa0/2

ASW1(config-if)#description PC2

ASW1(config-if)#switchport mode access

ASW1(config-if)#switchport access vlan 2

ASW1(config)#interface fa0/3

ASW1(config-if)#description PC3

ASW1(config-if)#switchport mode access

ASW1(config-if)#switchport access vlan 2

Проверьте доступность компьютеров.

Таким образом, эти 3 компьютера находятся в одном VLAN и ни одно другое устройство подключенное к этому коммутатору не может их видеть, пока мы его не настроим.

**Настройка порта в режиме работы TRUNK.**

Добавим в нашу сеть 2 коммутатора (2950T) и 1 компьютер. Назначим компьютеру PC4 IP адрес 172.168.2.5, подключим его к коммутатору ASW2 через интерфейс FA0/2, а коммутатор ASW2 к DSW через интерфейсы FA0/1 и FA0/2 соответственно.

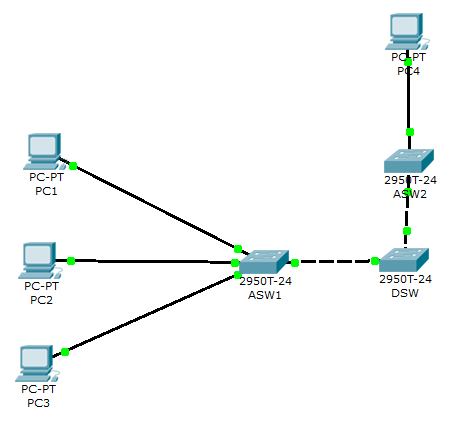


Рис. 2.

Можно проверить, что компьютеры PC1-PC3 не видятся с компьютера PC4:

Pinging 172.168.2.2 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 172.168.2.2:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Для начала настроим коммутатор ASW2, а именно интерфейс FA0/2.

Switch#conf t

Switch(config)#hostname ASW2

ASW2(config)#vlan 2

ASW2(config-vlan)#name users

ASW2(config)#interface fa0/2

ASW2(config-if)#description PC4

ASW2(config-if)#switchport mode access

ASW2(config-if)#switchport access vlan 2

Но и после этого связь у нас не появится. Кадр с компьютера PC4 приходит на коммутатор ASW2, получает метку второго VLAN, и далее должен передать его в порт с таким же VLAN, но он у нас всего один, и передавать кадр некуда.

Чтобы решить эту проблему настроим TRUNK порт на коммутаторе ASW2:

ASW2(config)#int fa0/1

ASW2(config-if)#description DSW

ASW2(config-if)#switchport mode trunk

ASW2(config-if)#switchport trunk allowed vlan 2

Аналогично настроим другие коммутаторы:

**DSW:**

Switch(config)#hostname DSW

DSW(config)#vlan 2

DSW(config-vlan)#name users

DSW(config)#interface fa0/2

DSW(config-if)#description ASW2

DSW(config-if)#switchport mode trunk

DSW(config-if)#switchport trunk allowed vlan 2

DSW(config)#interface fa0/1

DSW(config-if)#description ASW1

DSW(config-if)#switchport mode trunk

DSW(config-if)#switchport trunk allowed vlan 2

**ASW1:**

ASW1(config)#interface fa0/4

ASW1(config-if)#description DSW

ASW1(config-if)#switchport mode trunk

ASW1(config-if)#switchport trunk allowed vlan 2

Теперь можно проверить доступность компьютеров

**PC1 с PC4:**

PC>ping 172.168.2.2

Pinging 172.168.2.2 with 32 bytes of data:

Reply from 172.168.2.2: bytes=32 time=16ms TTL=128

Reply from 172.168.2.2: bytes=32 time=15ms TTL=128

Reply from 172.168.2.2: bytes=32 time=17ms TTL=128

Reply from 172.168.2.2: bytes=32 time=16ms TTL=128

Ping statistics for 172.168.2.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 15ms, Maximum = 17ms, Average = 16ms

**PC4 с PC3:**

PC>ping 172.168.2.5

Pinging 172.168.2.5 with 32 bytes of data:

Reply from 172.168.2.5: bytes=32 time=33ms TTL=128

Reply from 172.168.2.5: bytes=32 time=8ms TTL=128

Reply from 172.168.2.5: bytes=32 time=17ms TTL=128

Reply from 172.168.2.5: bytes=32 time=15ms TTL=128

Ping statistics for 172.168.2.5:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 8ms, Maximum = 33ms, Average = 18ms

**Изменение топологии сети, назначение IP адресов, выбор интерфейсов, добавление VLAN.**

Приведем нашу сеть к более реальной, добавим в нее 3 сервера и 2 коммутатора как показано на рисунке:

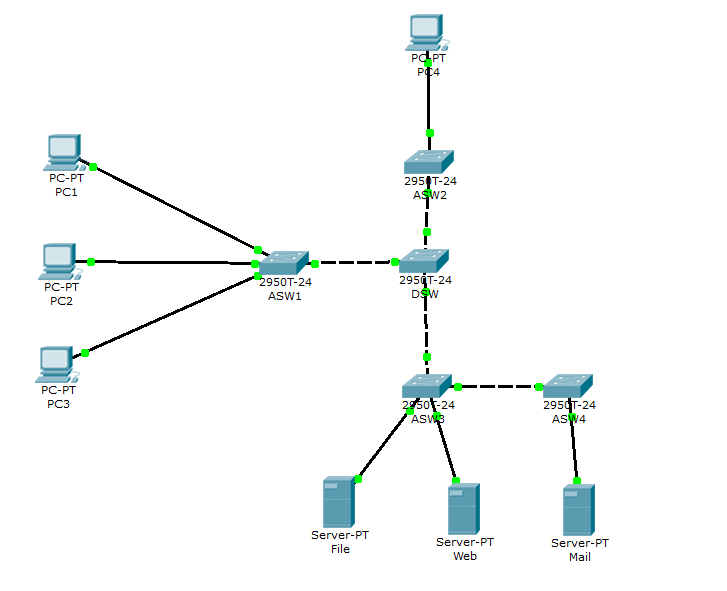


Рис. 3.

Настроим их, серверам дадим имена File, Web, Mail и зададим IP адреса 172.168.0.2, 172.168.0.3 и 172.168.0.4 соответственно, основным шлюзом выберем 172.168.0.1.

На коммутаторах ASW3, ASW4 и DSW настроим VLAN 3:

ASW3:

ASW3(config)#vlan 3

ASW3(config-vlan)#name servers

ASW3(config)#int fa0/1

ASW3(config-if)#description DSW

ASW3(config-if)#switchport mode trunk

ASW3(config-if)#switchport trunk allowed vlan 3

ASW3(config-if)#int fa0/2

ASW3(config-if)#description ASW4

ASW3(config-if)#switchport mode trunk

ASW3(config-if)#switchport trunk allowed vlan 3

ASW3(config)#interface fa0/3

ASW3(config-if)#description File-server

ASW3(config-if)#switchport mode access

ASW3(config-if)#switchport access vlan 3

ASW3(config)#interface fa0/4

ASW3(config-if)#description Web-server

ASW3(config-if)#switchport mode access

ASW3(config-if)#switchport access vlan 3

ASW4:

ASW4(config)#vlan 3

ASW4(config-vlan)#name servers

ASW4(config)#int fa0/1

ASW4(config-if)#description ASW3

ASW4(config-if)#switchport mode trunk

ASW4(config-if)#switchport trunk allowed vlan 3

ASW4(config)#interface fa0/2

ASW4(config-if)#description Mail-server

ASW4(config-if)#switchport mode access

ASW4(config-if)#switchport access vlan 3

DSW:

DSW(config)#vlan 3

DSW(config-vlan)#name servers

DSW(config)#int fa0/3

DSW(config-if)#description ASW3

DSW(config-if)#switchport mode trunk

DSW(config-if)#switchport trunk allowed vlan 3

Теперь попробуем пропинговать File-server с компьютера PC1:

PC>ping 172.168.0.2

Pinging 172.168.0.2 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 172.168.0.2:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Как мы наблюдаем, пинг не проходит, это объясняется тем, что они находятся в разных VLAN, и с помощью обычных коммутаторов нам эту проблему не решить, для таких случаев используют маршрутизаторы.

**Добавление маршрутизатора в сеть.**

Добавим маршрутизатор CISCO 2811 (R1) в нашу сеть как показано на рисунке:

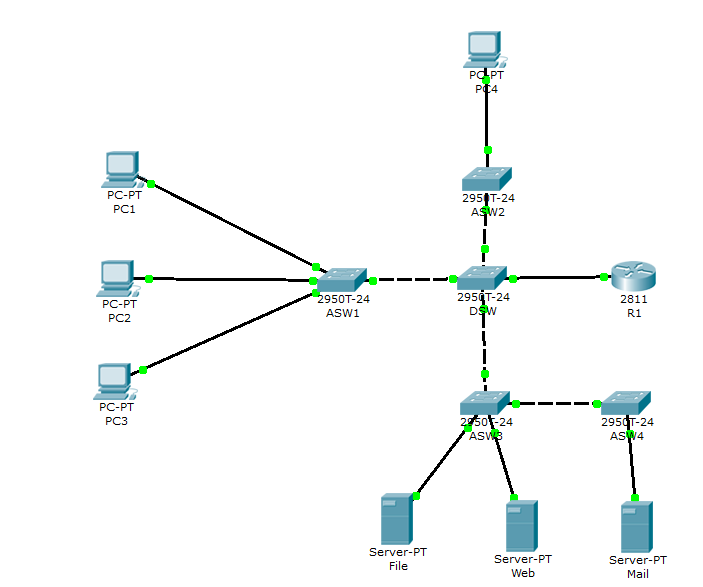


Рис. 4.

Настроим порт FA0/4 коммутатора DSW:

DSW(config)#int fa0/4

DSW(config-if)#description R1

DSW(config-if)#switchport mode trunk

DSW(config-if)#switchport trunk al vl 2,3

**Настройка маршрутизатора R1, создание виртуальных интерфейсов.**

Для начала зайдем в конфигурацию маршрутизатора R1

R1#conf t

Для создания виртуального интерфейса сначала указывается физический интерфейс, далее после точки указывается специальный идентификатор, как правило его выбирают в соответствии с номером VLAN который данный интерфейс будет терминировать.

Следующей командой мы указываем, что инкапсуляция будет по стандарту 802.1Q, и указываем метку VLAN. И наконец задаем IP адрес как на обычном интерфейсе.

Произведем настройку виртуального интерфейса для пользовательских компьютеров с номером VLAN – 2:

R1(config)#interface fastEthernet 0/0.2

R1(config-subif)#description Users

R1(config-subif)#encapsulation dot1Q 2

R1(config-subif)#ip address 172.168.2.1 255.255.255.0

Аналогично настраиваем виртуальный интерфейс для серверов с номером VLAN - 3:

R1(config)#interface fastEthernet 0/0.3

R1(config-subif)#description Servers

R1(config-subif)#encapsulation dot1q 3

R1(config-subif)#ip address 172.168.0.1 255.255.255.0

Теперь можно пропинговать почтовый сервер допустим с PC2:

PC>ping 172.168.0.4

Pinging 172.168.0.4 with 32 bytes of data:

Request timed out.

Reply from 172.168.0.4: bytes=32 time=22ms TTL=127

Reply from 172.168.0.4: bytes=32 time=30ms TTL=127

Reply from 172.168.0.4: bytes=32 time=29ms TTL=127

Ping statistics for 172.168.0.4:

Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),

Approximate round trip times in milli-seconds:

Minimum = 22ms, Maximum = 30ms, Average = 27ms

Так же сделаем трассировку, чтобы увидеть, как идут наши пакеты:

PC>tracert 172.168.0.4

Tracing route to 172.168.0.4 over a maximum of 30 hops:

1 9 ms 8 ms 13 ms 172.168.2.1

2 31 ms 28 ms 30 ms 172.168.0.4

Trace complete.

**Задание для самостоятельной работы**

1. Создайте топологию, изображенную на рисунке, и назначьте IP адреса соответствующие своему варианту:

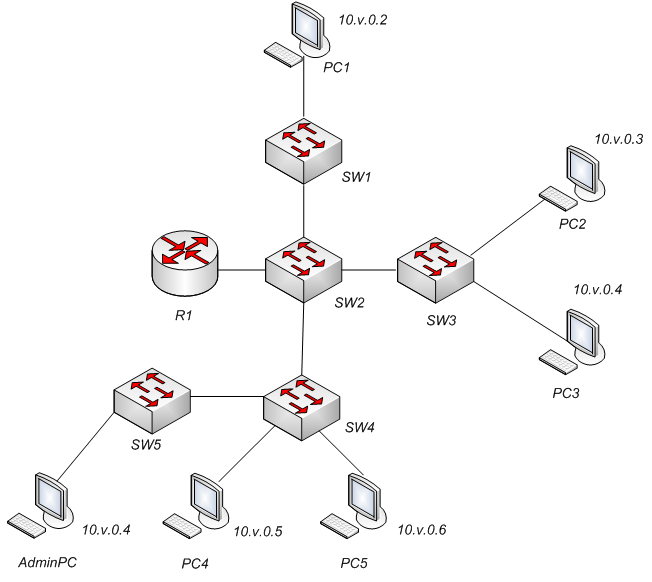


Рис. 5.

|  |  |  |  |
| --- | --- | --- | --- |
| Вариант | IP (v) | VLAN данных x / y | VLAN управления |
| 1 | 10 | 4 / 5 | 6 |
| 2 | 0 | 9 / 10 | 11 |
| 3 | 1 | 43 / 44 | 48 |
| 4 | 168 | 6 / 7 | 5 |
| 5 | 50 | 11 / 12 | 10 |
| 6 | 40 | 48 / 48 | 44 |
| 7 | 55 | 7 / 8 | 9 |
| 8 | 100 | 10 / 11 | 15 |
| 9 | 200 | 15 / 14 | 10 |
| 10 | 11 | 6 / 5 | 3 |

1. Маску сети выберите 255.255.255.0, основной шлюз 10.v.0.1 .
2. Проверьте пинги между компьютерами, сделайте хотя бы 3 скриншота.
3. Компьютеры PC1, PC2, PC3 объедините в один VLAN (выберите из таблицы в соответствии со своим вариантом VLAN данных “x”).
4. Проверьте пинг между ними, а так же попробуйте пропинговать другие компьютеры, сделайте выводы.
5. Компьютеры PC4 и PC5 объедините в один VLAN (VLAN данных “y”).
6. Проверьте пинг между ними, а так же попробуйте пропинговать другие компьютеры, сделайте выводы.
7. Настройте VLAN управления так, чтобы с AdminPC можно было пропинговать любой коммутатор.
8. Сделайте так, чтобы с AdminPC можно было посылать/принимать сообщения на любой другой VLAN.

**Контрольные вопросы:**

1. Что такое VLAN?
2. Зачем нужно разбивать сеть на различные VLAN’ы?
3. Как настроить порт на работу VLAN?
4. В чем отличие между портами доступа и транковыми портами?
5. Для чего нужны Sub-интерфейсы?

**Порядок выполнения и сдачи работы**

1. Изучить теоретическую и практическую часть.
2. Выполнить в Packet Tracer практическую часть.
3. Предъявите преподавателю результат выполнения.
4. Получите вариант и выполните в Packet Tracer задание для самостоятельной работы.
5. Предъявите преподавателю результат выполнения пунктов 7-9 задания для самостоятельной работы.
6. Оформите отчёт.
7. Защитите отчёт.

**Лабораторная работа №2. Протокол маршрутизации STP и его разновидности (RSTP, PVSTP, MSTP).**

**Теоретическая часть**

Spanning Tree Protocol (STP) (протокол связующего дерева) — сетевой протокол. Основной задачей STP является устранение петель в топологии произвольной сети Ethernet, в которой есть один или более сетевых мостов, связанных избыточными соединениями. STP решает эту задачу, автоматически блокируя соединения, которые в данный момент для полной связности коммутаторов являются избыточными.

Необходимость устранения топологических петель в сети Ethernet следует из того, что их наличие в реальной сети Ethernet с коммутатором с высокой вероятностью приводит к бесконечным повторам передачи одних и тех же кадров Ethernet одним и более коммутатором, отчего пропускная способность сети оказывается почти полностью занятой этими бесполезными повторами; в этих условиях, хотя формально сеть может продолжать работать, на практике её производительность становится настолько низкой, что может выглядеть как полный отказ сети.

STP относится ко второму уровню модели OSI. Протокол описан в стандарте IEEE 802.1d.

***Принцип действия***

* В сети выбирается один корневой мост (англ. Root Bridge).
* Далее каждый, отличный от корневого, мост просчитывает кратчайший путь к корневому. Соответствующий порт называется корневым портом (англ. Root Port). У любого некорневого коммутатора может быть только один корневой порт.
* После этого для каждого сегмента сети, к которому присоединён более чем один порт моста, просчитывается кратчайший путь к корневому порту. Мост, через который проходит этот путь, становится назначенным для этой сети (англ. Designated Bridge), а соответствующий порт — назначенным портом (англ. Designated port).
* Далее во всех сегментах, с которыми соединены более одного порта моста, все мосты блокируют все порты, не являющиеся корневыми и назначенными. В итоге получается древовидная структура (математический граф) с вершиной в виде корневого коммутатора.

***Важные правила***

* Корневым (root) портом назначается порт с самой низкой стоимостью пути (path cost).
* Возможны случаи, когда стоимость пути по двум и более портам коммутатора будет одинакова, тогда выбор корневого (root) порта будет происходить на основании порядкового номера порта, например fa0/1, fa0/2, fa0/3 и корневым (root) станет порт с наименьшим номером.
* Коммутаторы, по умолчанию, не измеряют состояние загрузки сети в реальном времени и работают в соответствии со стоимостью (cost) интерфейсов в момент построения дерева STP.
* Каждый порт имеет свою стоимость (cost), обратно пропорциональную пропускной способности (bandwidth) порта и которую можно настраивать вручную.

***Эволюция и расширения***

*Rapid Spanning Tree Protocol (RSTP)*

Rapid STP (RSTP) является значительным усовершенствованием STP. В первую очередь необходимо отметить уменьшение времени сходимости и более высокую устойчивость. В немалой степени это достигнуто за счет идей, использованных Cisco Systems в качестве проприетарных расширений STP. RSTP описан в стандарте IEEE 802.1w (впоследствии включен в 802.1D-2004).

Rapid STP совместим с STP — если некое устройство использует STP, то RSTP тоже будет использовать STP с этим устройством, но в этом режиме может оказаться, что наличие RSTP на остальных устройствах не дает преимуществ по сравнению с STP.

*Per-VLAN Spanning Tree Protocol (PVSTP)*

Per-VLAN STP (PVSTP) в соответствии с названием расширяет функционал STP для использования VLAN. В рамках данного протокола в каждом VLAN работает отдельный экземпляр STP. Является проприетарным расширением Cisco. Изначально протокол PVST работал только через ISL-транки, потом было разработано расширение PVST+, которое позволяло работать через гораздо более распространённые 802.1Q-транки. Существуют реализации, объединяющие свойства PVST+ и RSTP, поскольку эти расширения затрагивают независимые части протокола, в результате получается (в терминологии Cisco) Rapid PVST+. PVST+ совместим с STP, и даже коммуницирует «через» коммутаторы, не поддерживающие ни PVST+, ни Rapid PVST+, за счёт использования мультикастовых фреймов. Но Cisco Systems рекомендует не смешивать в одной сети коммутаторы различных производителей, чтобы избежать проблем совместимости разных имплементаций и вариаций STP.

*Multiple Spanning Tree Protocol (MSTP)*

Вышеописанные вариации протоколов STP можно классифицировать по количеству экземпляров STP в случае, когда число VLAN более единицы. Имеются вариации протоколов, у которых на все VLAN приходится единственный экземпляр STP (собственно STP, RSTP), и вариации, у которых каждому VLAN соответствует свой экземпляр STP (PVST, PVST+, Rapid PVST+).

Некоторая избыточность вариаций с отдельным экземпляром STP для каждой VLAN состоит в том, что если топология нескольких VLAN совпадает, то соответствующие им экземпляры STP полностью повторяют работу друг друга. В таком случае в принципе ненужная работа по сути дублирующих друг друга экземпляров STP оборачивается ненужной дополнительной нагрузкой на процессор коммутатора, и в конечном счете может вынудить конструкторов оборудования для обеспечения его устойчивой работы выбирать более мощный процессор с большим энергопотреблением, что может повлечь за собой дополнительные затраты на электропитание и охлаждение, как при изготовлении оборудования, так и эксплуатации.

В этом отношении особняком стоит Multiple STP (MSTP). В один экземпляр MST могут входить несколько виртуальных сетей, при условии, что их топология одинакова (в смысле входящих в VLAN коммутаторов и соединений между ними). Минимальное количество экземпляров MSTP соответствует количеству уникальных топологически групп VLAN в домене второго уровня (опять же на уровне коммутаторов и соединений между ними). MSTP налагает важное ограничение: все коммутаторы, участвующие в MSTP, должны иметь одинаково сконфигурированные группы VLAN (MST instances), что ограничивает гибкость при изменении конфигурации сети.

MSTP описан в стандарте IEEE 802.1s (впоследствии включен в 802.1Q-2003).

**Практическая часть**

**Добавление дополнительного канала связи между коммутаторами DSW и ASW4.**

Возьмем топологию сети из прошлой лабораторной работы и добавим дополнительный канал между коммутаторами DSW и ASW4.

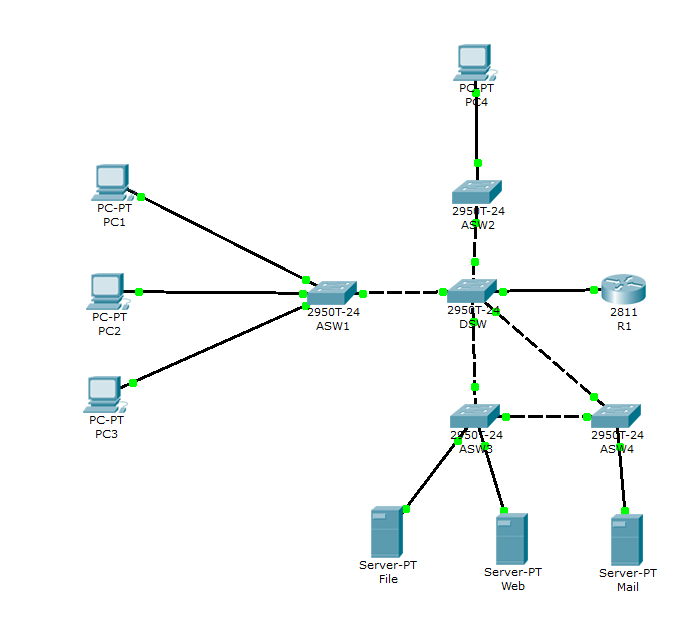
****

Рис. 1.

Настроим транковые порты на этих коммутаторах:

DSW(config)#int fa0/5

DSW(config-if)#switchport mode trunk

DSW(config-if)#switchport trunk allowed vlan 3

DSW(config-if)#description ASW4

ASW4(config)#int fa0/3

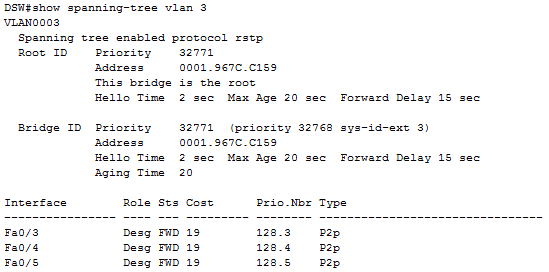
ASW4(config-if)#switchport mode trunk

ASW4(config-if)#switchport trunk allowed vlan 3

ASW4(config-if)#description DSW

По умолчанию STP уже включен на всех коммутаторах и по идее он должен заблокировать избыточные связи. Проверим статус STP на коммутаторе DSW.

DSW#show spanning-tree vlan 3



Мы видим что данный коммутатор является корневым “This bridge is the root”, т.е. весь трафик идущий на сервера сначала посылается на этот коммутатор.

Если DSW не является ROOT, то настройте его вручную:

DSW(config)#spanning-tree vlan 3 root primary

**STP в действии, настройка RSTP.**

Посмотрим на работу STP в реальном времени, по сути STP является холодным резервом, поэтому если мы разорвем один из каналов связи, то трафик, через некоторое время, должен пойти по другому пути.

Запустим пинг с одного из компьютеров на почтовый сервер.

Ping –t 172.168.0.4

Пинг идет по следующему пути PC1 – ASW1 – DSW – ASW4 – MAIL.

Разорвем связь между DSW и ASW4.

ASW4(config)#int fa0/3

ASW4(config-if)#sh

В теории, на перестроение маршрута тратится до 30 секунд, за это время часть пакетов может быть утеряна, разорваны разговоры и другие неприятные ситуации.

Посмотрим, что случилось с пингом.

Reply from 172.168.0.4: bytes=32 time=23ms TTL=127

Reply from 172.168.0.4: bytes=32 time=21ms TTL=127

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Reply from 172.168.0.4: bytes=32 time=26ms TTL=127

Reply from 172.168.0.4: bytes=32 time=25ms TTL=127

Reply from 172.168.0.4: bytes=32 time=17ms TTL=127

Reply from 172.168.0.4: bytes=32 time=18ms TTL=127

Мы видим что потерялось 5 пакетов, после этого работа сети была восстановлена и трафик пошел по маршруту PC1 – ASW1 – DSW – ASW3 – ASW4 – MAIL.

Но еще одной проблемой данного протокола является то, что при восстановлении канала связи потребуется, на обратное перестроение маршрута потребуется столько же времени, и опять будут утеряны пакеты.

ASW4(config)#int fa0/3

ASW4(config-if)#no sh

Ping –t 172.168.0.4

Reply from 172.168.0.4: bytes=32 time=30ms TTL=127

Reply from 172.168.0.4: bytes=32 time=27ms TTL=127

Reply from 172.168.0.4: bytes=32 time=30ms TTL=127

Request timed out.

Request timed out.

Request timed out.

Request timed out.

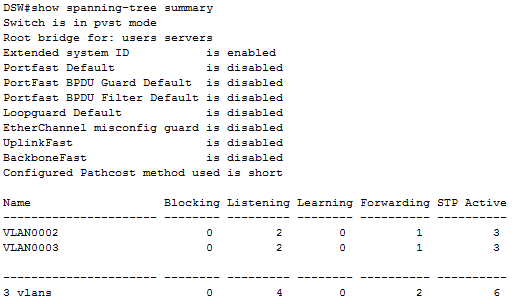
Request timed out.

Reply from 172.168.0.4: bytes=32 time=18ms TTL=127

Reply from 172.168.0.4: bytes=32 time=25ms TTL=127

Убедимся что STP работает в режиме PVSTP.

DSW#show spanning-tree summary

****

Переведем все коммутаторы в режим RSTP.

DSW(config)#spanning-tree mode rapid-pvst

ASW3(config)#spanning-tree mode rapid-pvst

ASW4(config)#spanning-tree mode rapid-pvst

Очень часто при изменении протоколов, Packet Tracer начинает работать не правильно, не блокируются лишние каналы связи, и возникает широковещательный шторм, для устранения данной проблемы сохраните проект и откройте его заново.

Проверим работу RSTP, запустим пинг с PC1 на Mail сервер, и отключим опять же интерфейс FA0/3 на коммутаторе ASW4.

ASW4(config)#int fa0/3

ASW4(config-if)#sh

Ping –t 172.168.0.4

Reply from 172.168.0.4: bytes=32 time=30ms TTL=127

Reply from 172.168.0.4: bytes=32 time=31ms TTL=127

Reply from 172.168.0.4: bytes=32 time=22ms TTL=127

Reply from 172.168.0.4: bytes=32 time=28ms TTL=127

Reply from 172.168.0.4: bytes=32 time=29ms TTL=127

Reply from 172.168.0.4: bytes=32 time=32ms TTL=127

Reply from 172.168.0.4: bytes=32 time=35ms TTL=127

Как мы видим потери пакетов не обнаружено, и трафик пошел по другому маршруту. Теперь включим интерфейс FA0/3 и продолжим смотреть на пинг.

ASW4(config-if)#no sh

Reply from 172.168.0.4: bytes=32 time=17ms TTL=127

Request timed out.

Reply from 172.168.0.4: bytes=32 time=17ms TTL=127

Reply from 172.168.0.4: bytes=32 time=19ms TTL=127

Reply from 172.168.0.4: bytes=32 time=17ms TTL=127

Reply from 172.168.0.4: bytes=32 time=25ms TTL=127

Потерялся всего один пакет.

**Задание для самостоятельной работы**

1. Загрузите топологию из прошлой лабораторной работы, и добавьте связи между SW5 и SW2, SW2 и SW1.

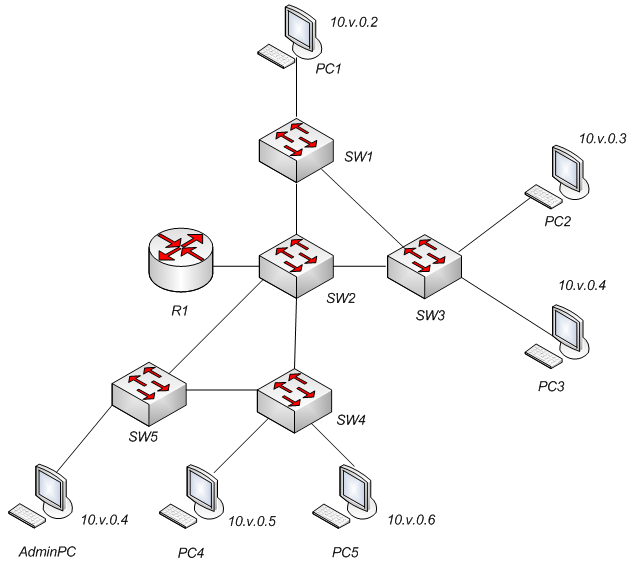


Рис. 2.

1. Настройте протокол STP на всех коммутаторах.
2. В качестве корневого коммутатора выберете SW2.
3. Сделайте постоянный пинг в соответствии со своим вариантом:

|  |  |
| --- | --- |
| Вариант | Компьютеры |
| 1 | с PC1 на PC3 |
| 2 | с PC2 на AdminPC |
| 3 | c PC5 на PC1 |
| 4 | с PC4 на PC2 |
| 5 | С AdminPC на SW3 |
| 6 | С AdminPC на SW2 |

1. Выключите какой-нибудь интерфейс на коммутаторах, чтобы увидеть время, требующееся на перестроение маршрута для пакетов.
2. Сделайте скриншоты с потерей пакетов, сделайте выводы.
3. Включите интерфейс обратно, посмотрите на пинг, сделайте скриншоты.
4. Настройте на каждом коммутаторе RSTP.
5. Повторите пункты 4-7.

**Контрольные вопросы:**

1. Что такое STP?
2. Для чего нужны эти протоколы?
3. В чем разница между PVSTP, RSTP?
4. Как поменять режим работы STP?

**Порядок выполнения и сдачи работы**

1. Изучить теоретическую и практическую часть.
2. Выполнить в Packet Tracer практическую часть.
3. Предъявите преподавателю результат выполнения.
4. Получите вариант и выполните в Packet Tracer задание для самостоятельной работы.
5. Оформите отчёт.
6. Защитите отчёт.

**Лабораторная работа №3. Совместная работа протоколов RIP и RIPv2.**

**Теоретическая часть**

Протокол маршрутной информации (англ. Routing Information Protocol) — один из самых простых протоколов маршрутизации. Применяется в небольших компьютерных сетях, позволяет маршрутизаторам динамически обновлять маршрутную информацию (направление и дальность в хопах), получая ее от соседних маршрутизаторов.

***Техническая информация***

RIP — так называемый протокол дистанционно-векторной маршрутизации, который, оперирует транзитными участками в качестве метрики маршрутизации. Максимальное количество хопов, разрешенное в RIP — 15 (метрика 16 означает «бесконечно большую метрику»). Каждый RIP-маршрутизатор по умолчанию вещает в сеть свою полную таблицу маршрутизации раз в 30 секунд, довольно сильно нагружая низкоскоростные линии связи. RIP работает на прикладном уровне стека TCP/IP, используя UDP порт 520.

В современных сетевых средах RIP — не самое лучшее решение для выбора в качестве протокола маршрутизации, так как его возможности уступают более современным протоколам, таким как EIGRP, OSPF. Ограничение на 15 хопов не дает применять его в больших сетях. Преимущество этого протокола – простота конфигурирования.

***Формат RIP пакета***

|  |  |  |
| --- | --- | --- |
| 0 - 7 | 8 - 15 | 16 - 31 |
| Command (1) | Version (1) | Routing Domain (0x0000 для RIP-1) (2) |
| RIP Entry (20) | | |

* Command — команда, определяет назначение датаграммы (1 — request; 2 — response)
* Version — номер версии, в зависимости от версии, определяется формат пакета
* Routing Domain — идентификатор RIP-системы, к которой принадлежит данное сообщение; часто — номер автономной системы (не используется в версии RIP-1, должно быть нулём). Используется, когда к одному физическому каналу подключены маршрутизаторы из нескольких автономных систем, в каждой автономной системе поддерживается своя таблица маршрутов. Поскольку сообщения RIP рассылаются всем маршрутизаторам, подключенным к сети, требуется различать сообщения, относящиеся к «своей» и «чужой» автономным системам.
* RIP Entry (RTE) — запись маршрутной информации RIP. RIP пакет может содержать от 1 до 25 записей RIP Entry.

***Формат RIP Entry для протокола RIP-1***

Поле Version = 1

|  |  |
| --- | --- |
| 0-15 | 16-31 |
| Address family identifier (2) | must be zero (2) |
| IPv4 address (4) | |
| Must be zero (4) | |
| Must be zero (4) | |
| Metric (4) | |

* Address family identifier (AFI) — тип адреса, обычно поддерживается только запись AF\_INET, которое равно 2 (т. е. используется для протокола IP).
* Must be zero — должно быть нулём.
* IPv4 address — IP адрес места назначения (хост или сеть)
* Metric — метрика маршрута

***Формат RIP Entry для протокола RIP-2***

Поле Version = 2.

|  |  |
| --- | --- |
| 0-15 | 16-31 |
| Address family identifier (2) | Route Tag (2) |
| IPv4 address (4) | |
| Subnet mask (4) | |
| Next hop (4) | |
| Metric (4) | |

* Address Family Identifier (AFI) — тип адреса, обычно поддерживается только запись AF\_INET, которое равно 2 (т.е. используется для протокола IP).
* Route Tag (RT) — тег маршрута. Предназначен для разделения «внутренних» маршрутов от «внешних», взятых, например, из другого IGP или EGP.
* IP Address — IP адрес места назначения.
* Subnet Mask — маска подсети
* Next Hop — следующий хоп. Содержит IP адрес маршрутизатора к месту назначения. Значение 0.0.0.0 — хопом к месту назначения является отправитель пакета. Необходимо, если протокол RIP не может быть запущен на всех маршрутизаторах.
* Metric — метрика маршрута.

**Практическая часть**

1. Создайте топологию изображенную на рисунке:

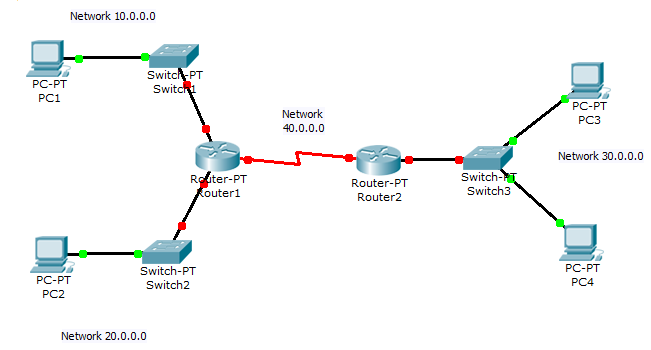
****

Рис. 1.

1. Назначьте IP-адреса компьютерам PC1 – PC4 : X.0.0.2, основной шлюз X.0.0.1, и маску 255.255.0.0, где X = 10, 20, 30.
2. Настройте Router1:

Сначала настроим интерфейс для сети 10.0.0.0:

Router1(config)#int fa0/0

Router1(config-if)#ip address 10.0.0.1 255.255.0.0

Router1(config-if)#no sh

Аналогично для сети 20.0.0.0:

Router1(config-if)#int fa1/0

Router1(config-if)#ip address 20.0.0.1 255.255.0.0

Router1(config-if)#no sh

Последним шагом настроим для сети 40.0.0.0

Router1(config-if)#int s2/0

Router1(config-if)#ip address 40.0.0.1 255.255.0.0

Router1(config-if)#clock rate 64000

Router1(config-if)#no sh

1. Настройте Router2:

Router2(config)#int s2/0

Router2(config-if)#no sh

Router2(config-if)#ip address 40.0.0.2 255.255.0.0

Router2(config)#int fa0/0

Router2(config-if)#ip address 30.0.0.1 255.255.0.0

Router2(config-if)#no sh

1. Теперь попробуем послать пакеты между сетями:

* С PC1 на PC2:

**PC>ping 20.0.0.2**

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 20.0.0.2: bytes=32 time=15ms TTL=127

Reply from 20.0.0.2: bytes=32 time=7ms TTL=127

Reply from 20.0.0.2: bytes=32 time=10ms TTL=127

Reply from 20.0.0.2: bytes=32 time=11ms TTL=127

Ping statistics for 20.0.0.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 7ms, Maximum = 15ms, Average = 10ms

* С PC3 на PC4:

**PC>ping 30.0.0.3**

Pinging 30.0.0.3 with 32 bytes of data:

Reply from 30.0.0.3: bytes=32 time=8ms TTL=128

Reply from 30.0.0.3: bytes=32 time=9ms TTL=128

Reply from 30.0.0.3: bytes=32 time=9ms TTL=128

Reply from 30.0.0.3: bytes=32 time=8ms TTL=128

Ping statistics for 30.0.0.3:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 8ms, Maximum = 9ms, Average = 8ms

* С PC1 на PC4:

**PC>ping 30.0.0.3**

Pinging 30.0.0.3 with 32 bytes of data:

Reply from 10.0.0.1: Destination host unreachable.

Reply from 10.0.0.1: Destination host unreachable.

Reply from 10.0.0.1: Destination host unreachable.

Reply from 10.0.0.1: Destination host unreachable.

Ping statistics for 30.0.0.3:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Как мы видим между сетями соединенными маршрутизаторами у нас не идут, посмотрим таблицы маршрутизации на них:

**Router1#show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/16 is subnetted, 1 subnets

C 10.0.0.0 is directly connected, FastEthernet0/0

20.0.0.0/16 is subnetted, 1 subnets

C 20.0.0.0 is directly connected, FastEthernet1/0

40.0.0.0/16 is subnetted, 1 subnets

C 40.0.0.0 is directly connected, Serial2/0

Как мы видим на маршрутизаторе Router1 есть только 3 статических маршрута, и сеть 30.0.0.0 он не видит.

Аналогично на маршрутизаторе Router2:

**Router2#show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

30.0.0.0/16 is subnetted, 1 subnets

C 30.0.0.0 is directly connected, FastEthernet0/0

40.0.0.0/16 is subnetted, 1 subnets

C 40.0.0.0 is directly connected, Serial2/0

1. Настройка протоколов RIP.

Настроим протокол RIP на маршрутизаторах Router1 и Router2:

Router1(config)#router rip

Router1(config-router)#network 10.0.0.0

Router1(config-router)#network 20.0.0.0

Router1(config-router)#network 40.0.0.0

Router2(config)#router rip

Router2(config-router)#network 40.0.0.0

Router2(config-router)#network 30.0.0.0

Проверим таблицы маршрутизации и попробуем пропинговать:

**Router1#show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/16 is subnetted, 1 subnets

C 10.0.0.0 is directly connected, FastEthernet0/0

20.0.0.0/16 is subnetted, 1 subnets

C 20.0.0.0 is directly connected, FastEthernet1/0

R 30.0.0.0/8 [120/1] via 40.0.0.2, 00:02:24, Serial2/0

40.0.0.0/16 is subnetted, 1 subnets

C 40.0.0.0 is directly connected, Serial2/0

**Router2#show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

R 10.0.0.0/8 [120/1] via 40.0.0.1, 00:00:23, Serial2/0

R 20.0.0.0/8 [120/1] via 40.0.0.1, 00:00:23, Serial2/0

30.0.0.0/16 is subnetted, 1 subnets

C 30.0.0.0 is directly connected, FastEthernet0/0

40.0.0.0/16 is subnetted, 1 subnets

C 40.0.0.0 is directly connected, Serial2/0

**PC>ping 30.0.0.3**

Pinging 30.0.0.3 with 32 bytes of data:

Reply from 30.0.0.3: bytes=32 time=22ms TTL=126

Reply from 30.0.0.3: bytes=32 time=18ms TTL=126

Reply from 30.0.0.3: bytes=32 time=17ms TTL=126

Reply from 30.0.0.3: bytes=32 time=17ms TTL=126

Ping statistics for 30.0.0.3:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 17ms, Maximum = 22ms, Average = 18ms

Как мы видим, у нас появились динамические маршруты в отдаленные сети, и появился пинг.

1. Настройка протокола RIPv2:

Поменяем версию протокола для маршрутизатора Router1:

Router1(config-router)#version 2

Посмотрим параметры протокола командой show ip protocols:

**Router1#show ip protocols**

Routing Protocol is "rip"

Sending updates every 30 seconds, next due in 18 seconds

Invalid after 180 seconds, hold down 180, flushed after 240

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Redistributing: rip

Default version control: send version 2, receive 2

Interface Send Recv Triggered RIP Key-chain

FastEthernet0/0 2 2

FastEthernet1/0 2 2

Serial2/0 2 2

Automatic network summarization is in effect

Maximum path: 4

Routing for Networks:

10.0.0.0

20.0.0.0

40.0.0.0

Passive Interface(s):

Routing Information Sources:

Gateway Distance Last Update

Distance: (default is 120)

Теперь попробуйте пропинговать PC1 с PC4 и тд.

Как мы можем заметить, с изменением версии протокола для одного из маршрутизаторов, работа сети не поменялась. Таким образом, можно сделать вывод, что протоколы RIP и RIPv2 отлично работают в паре.

**Задание для самостоятельной работы.**

1. Создайте топологию сети, изображенную на рисунке, в соответствии со своим вариантом:

Вариант 1:

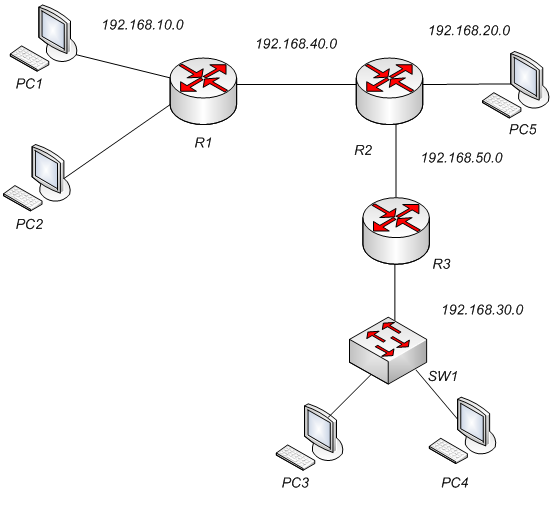


Рис. 2.

Вариант 2:

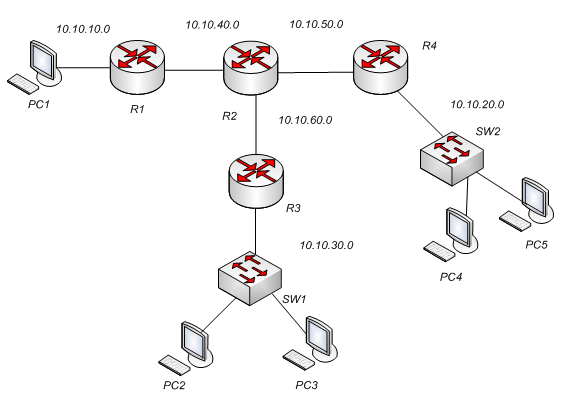


Рис. 3.

Вариант 3:

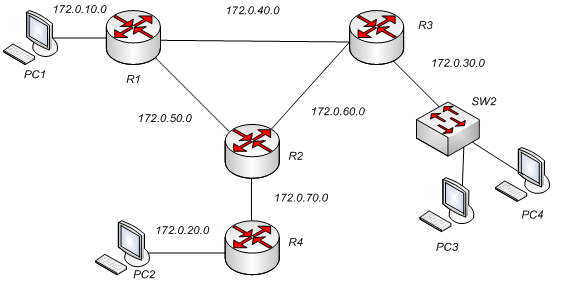


Рис. 4.

Вариант 4:

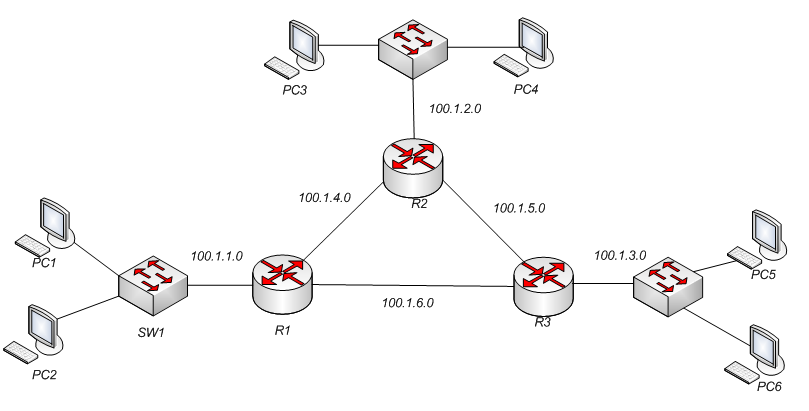


Рис. 5.

1. Настройте IP адреса компьютеров.
2. Посмотрите таблицы маршрутов на маршрутизаторах, сделайте скриншоты.
3. Настройте на маршрутизаторах протокол RIP.
4. Проверьте таблицы маршрутов, сделайте скриншоты, сделайте выводы.
5. Проверьте пинги в отдаленные сети, сделайте пару скриншотов.
6. Настройте на 1-2 маршрутизаторах протокол RIPv2.
7. Проверьте работу сети, сделайте выводы.

**Контрольные вопросы:**

1. Что такое RIP?
2. Зачем нужен протокол RIP?
3. В чем отличие между RIP и RIPv2?
4. Что такое метрика?
5. Как узнать, какой протокол запущен на маршрутизаторе?
6. Как настроить протокол RIP?
7. Что такое таблица маршрутизации?

**Лабораторная работа №4. Протокол маршрутизации OSPF. Разбиение на 2 зоны.**

**Теоретическая часть**

OSPF (англ. Open Shortest Path First) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути Алгоритм Дейкстры (Dijkstra’s algorithm).

Протокол OSPF был разработан IETF в 1988 году. Последняя версия протокола представлена в RFC 2328. Протокол OSPF представляет собой протокол внутреннего шлюза (Interior Gateway Protocol — IGP). Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.

OSPF имеет следующие преимущества:

* Высокая скорость сходимости по сравнению с дистанционно-векторными протоколами маршрутизации;
* Поддержка сетевых масок переменной длины (VLSM);
* Оптимальное использование пропускной способности (т. к. строится минимальный остовный граф по алгоритму Дейкстры);

***Описание работы протокола***

1. Маршрутизаторы обмениваются hello-пакетами через все интерфейсы, на которых активирован OSPF. Маршрутизаторы, разделяющие общий канал передачи данных, становятся соседями, когда они приходят к договоренности об определённых параметрах, указанных в их hello-пакетах.
2. На следующем этапе работы протокола маршрутизаторы будут пытаться перейти в состояние смежности со своими соседями. Переход в состояние смежности определяется типом маршрутизаторов, обменивающихся hello-пакетами, и типом сети, по которой передаются hello-пакеты. OSPF определяет несколько типов сетей и несколько типов маршрутизаторов. Пара маршрутизаторов, находящихся в состоянии смежности, синхронизирует между собой базу данных состояния каналов.
3. Каждый маршрутизатор посылает объявления о состоянии канала маршрутизаторам, с которыми он находится в состоянии смежности.
4. Каждый маршрутизатор, получивший объявление от смежного маршрутизатора, записывает передаваемую в нём информацию в базу данных состояния каналов маршрутизатора и рассылает копию объявления всем другим смежным с ним маршрутизаторам.
5. Рассылая объявления внутри одной OSPF-зоны, все маршрутизаторы строят идентичную базу данных состояния каналов маршрутизатора.
6. Когда база данных построена, каждый маршрутизатор использует алгоритм «кратчайший путь первым» для вычисления графа без петель, который будет описывать кратчайший путь к каждому известному пункту назначения с собой в качестве корня. Этот граф — дерево кратчайших путей.
7. Каждый маршрутизатор строит таблицу маршрутизации из своего дерева кратчайших путей.

При разделении автономной системы на зоны, маршрутизаторам принадлежащим к одной зоне не известна информация о детальной топологии других зон.

Разделение на зоны позволяет:

* Снизить нагрузку на ЦП маршрутизаторов за счёт уменьшения количества перерасчётов по алгоритму OSPF
* Уменьшить размер таблиц маршрутизации
* Уменьшить количество пакетов обновлений состояния канала

Каждой зоне присваивается идентификатор зоны (area ID). Идентификатор может быть указан в десятичном формате или в формате записи IP-адреса. Однако идентификаторы зон не являются IP-адресами и могут совпадать с любым назначенным IP-адресом.

Существует несколько типов зон:

1. Магистральная зона (backbone area)

Магистральная зона (известная также как нулевая зона или зона 0.0.0.0) формирует ядро сети OSPF. Все остальные зоны соединены с ней, и межзональная маршрутизация происходит через маршрутизатор соединенный с магистральной зоной. Магистральная зона ответственна за распространение маршрутизирующей информации между немагистральными зонами. Магистральная зона должна быть смежной с другими зонами, но она не обязательно должна быть физически смежной; соединение с магистральной зоной может быть установлено и с помощью виртуальных каналов.

1. Стандартная зона (standard area)

Обычная зона, которая создается по умолчанию. Эта зона принимает обновления каналов, суммарные маршруты и внешние маршруты.

1. Тупиковая зона (stub area)

Тупиковая зона не принимает информацию о внешних маршрутах для автономной системы, но принимает маршруты из других зон. Если маршрутизаторам из тупиковой зоны необходимо передавать информацию за границу автономной системы, то они используют маршрут по умолчанию. В тупиковой зоне не может находиться ASBR. Исключение из этого правила — ABR может быть и ASBR.

1. Totally stubby area

Totally stubby area не принимает информацию о внешних маршрутах для автономной системы и маршруты из других зон. Если маршрутизаторам необходимо передавать информацию за пределы зоны, то они используют маршрут по умолчанию.

1. Not-so-stubby area (NSSA)

Зона NSSA определяет дополнительный тип LSA — LSA type 7. В NSSA зоне может находиться ASBR.

***OSPF в Packet Tracer:***

Для запуска OSPF маршрутизации служит команда

Router(config)#**router ospf N,**

где N-номер вычислительного процесса OSPF. Он может быть различным для разных маршрутизаторов автономной системы. OSPF область Area организуется командой

Router(config-router)# **network network-number area Area**

и определяет автономную систему.

В OSPF network-number имеет особый формат. Для подключаемой в процесс маршрутизации сети используетя инверсная маска. Так, чтобы сеть 10.0.0.0 255.255.255.0 поместить в область 3 OSPF маршрутизации следует дать команду

Router(config-router)# **network 10.0.0.0 0.255.255.255 area 3**

Команда show ip ospf interface для каждого интерфейса выводит всю OSPF информацию: IP адрес, область, номер процесса, идентификатор маршрутизатора, стоимость, приоритет, тип сети, интервалы таймера.

Команда show ip ospf neighbor показывает важную информацию, касающуюся состояния соседей.

**Практическая часть**

1. Возьмем топологию из прошлой лабораторной работы:

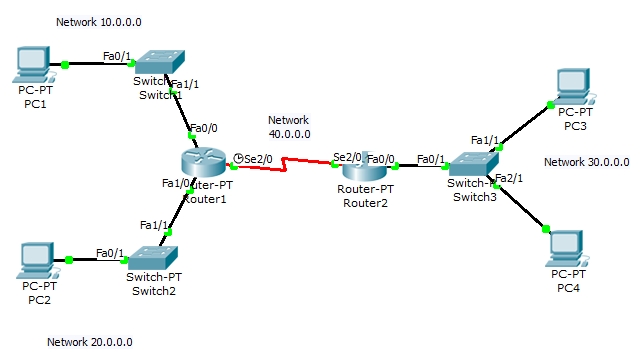
****

Рис. 1.

1. Уберем настроенные RIP протоколы на маршрутизаторах:

Router1(config)#no router rip

Router2(config)#no router rip

1. Проверим маршруты:

**Router1# show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/16 is subnetted, 1 subnets

C 10.0.0.0 is directly connected, FastEthernet0/0

20.0.0.0/16 is subnetted, 1 subnets

C 20.0.0.0 is directly connected, FastEthernet1/0

40.0.0.0/16 is subnetted, 1 subnets

C 40.0.0.0 is directly connected, Serial2/0

**Router2#show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

30.0.0.0/16 is subnetted, 1 subnets

C 30.0.0.0 is directly connected, FastEthernet0/0

40.0.0.0/16 is subnetted, 1 subnets

C 40.0.0.0 is directly connected, Serial2/0

Как мы видим, все динамические маршруты пропали, и сети 10.0.0.0 (20.0.0.0) и 30.0.0.0 не видят друг друга.

1. Настройка OSPF:

Мысленно разобьем нашу сеть на 3 зоны.

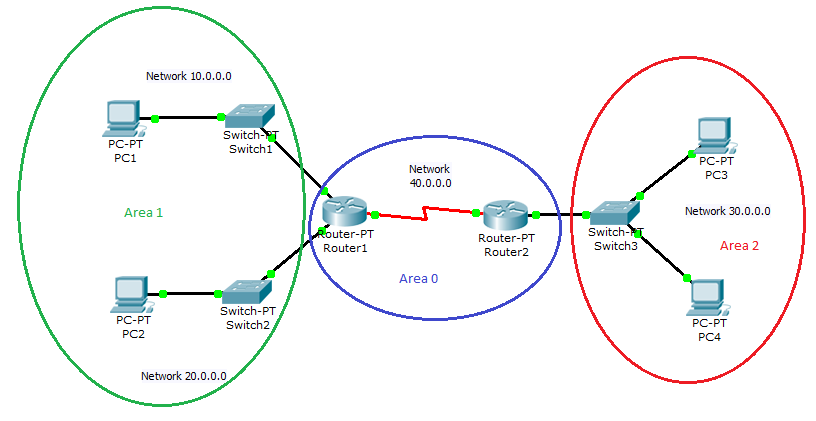


Рис. 2.

Настроим OSPF на маршрутизаторе Router1:

Router1(config)#router ospf 1

Router1(config-router)#network 10.0.0.0 255.255.0.0 area 1

Router1(config-router)#network 20.0.0.0 255.255.0.0 area 1

Router1(config-router)#network 40.0.0.0 255.255.0.0 area 0

Аналогично на Router2:

Router2(config)#router ospf 1

Router2(config-router)#network 30.0.0.0 255.255.0.0 area 2

Router2(config-router)#network 40.0.0.0 255.255.0.0 area 0

Обратите внимание что зона, которая соединяет различные зоны, должна быть с идентификатором 0.

Посмотрим таблицы маршрутизации:

**Router1#show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/16 is subnetted, 1 subnets

C 10.0.0.0 is directly connected, FastEthernet0/0

20.0.0.0/16 is subnetted, 1 subnets

C 20.0.0.0 is directly connected, FastEthernet1/0

30.0.0.0/16 is subnetted, 1 subnets

O IA 30.0.0.0 [110/65] via 40.0.0.2, 00:00:20, Serial2/0

40.0.0.0/16 is subnetted, 1 subnets

C 40.0.0.0 is directly connected, Serial2/0

**Router2#show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/16 is subnetted, 1 subnets

O IA 10.0.0.0 [110/65] via 40.0.0.1, 00:04:04, Serial2/0

20.0.0.0/16 is subnetted, 1 subnets

O IA 20.0.0.0 [110/65] via 40.0.0.1, 00:04:04, Serial2/0

30.0.0.0/16 is subnetted, 1 subnets

C 30.0.0.0 is directly connected, FastEthernet0/0

40.0.0.0/16 is subnetted, 1 subnets

C 40.0.0.0 is directly connected, Serial2/0

Как мы видим, в таблице маршрутов появились динамические маршруты между различными зонами OSFP.

Проверим пинги:

* PC1 to PC3:

**PC>ping 30.0.0.2**

Pinging 30.0.0.2 with 32 bytes of data:

Reply from 30.0.0.2: bytes=32 time=13ms TTL=126

Reply from 30.0.0.2: bytes=32 time=20ms TTL=126

Reply from 30.0.0.2: bytes=32 time=24ms TTL=126

Reply from 30.0.0.2: bytes=32 time=18ms TTL=126

Ping statistics for 30.0.0.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 13ms, Maximum = 24ms, Average = 18ms

* PC4 to PC2:

**PC>ping 20.0.0.2**

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 20.0.0.2: bytes=32 time=14ms TTL=126

Reply from 20.0.0.2: bytes=32 time=20ms TTL=126

Reply from 20.0.0.2: bytes=32 time=21ms TTL=126

Reply from 20.0.0.2: bytes=32 time=12ms TTL=126

Ping statistics for 20.0.0.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 12ms, Maximum = 21ms, Average = 16ms

**Задание для самостоятельной работы:**

1. Загрузите свою топологию из прошлой лабораторной работы.
2. Уберите на всех маршрутизаторах протоколы RIP и RIPv2.
3. Проверьте таблицы маршрутов, сделайте скриншоты.
4. Настройте работу протокола OSPF, каждую подсеть занесите в отдельную зону.
5. Проверьте таблицы маршрутов, сделайте скриншоты.
6. Пропингуйте отдаленные компьютеры, сделайте пару скриншотов.
7. Сделайте выводы.

**Контрольные вопросы:**

1. Что такое OSPF?
2. Зачем нужен протокол OSPF?
3. Зачем разделять на несколько зон?
4. Как работает протокол OSPF?
5. Какие типы зон существуют?
6. Что такое сходимость протоколов?
7. Какие параметры влияют на сходимость?
8. Как настроить протокол OSPF?

**Лабораторная работа №5. IP – телефония.**

**Теоретическая часть.**

IP-телефония — голосовая связь по протоколу IP. Под IP-телефонией подразумевается набор коммуникационных протоколов, технологий и методов, обеспечивающих двустороннее голосовое общение (в том числе при видео общении) по сети Интернет или по любым другим IP-сетям. Сигнал по каналу связи передаётся в цифровом виде и, как правило, перед передачей преобразовывается (сжимается) с тем, чтобы удалить избыток информации.

Строго говоря, IP-телефония является приложением более общей технологии VoIP (англ. Voice over IP (VoIP)) для организации двустороннего общения. Технология VoIP в общем случае подразумевает все варианты передачи голоса через IP, в том числе не имеющие никакого отношения к телефонии и общению людей. Например, технология VoIP применяется для передачи звука в системах IP видеонаблюдения, в системах оповещения, при трансляции веб семинаров, при просмотре фильмов в режиме он-лайн и т.п.

***Функциональность***

IP-телефония реализует задачи и решения, которые с помощью технологии телефонной сети общего пользования реализовать будет труднее, либо дороже.

Примеры:

* Возможность передавать более одного телефонного звонка в рамках высокоскоростного телефонного подключения. Поэтому IP-телефония используется в качестве простого способа для добавления дополнительной телефонной линии дома или в офисе.
* Свойства, такие как
* конференция,
* переадресация звонка,
* автоматическое повторение номера,
* определение номера звонящего, предоставляются бесплатно или почти бесплатно, тогда как в традиционных телекоммуникационных компаниях обычно выставляются в счёт.
* Безопасные звонки, со стандартизованным протоколом (такие как SRTP). Большинство трудностей для включения безопасных телефонных соединений по традиционным телефонным линиям, такие как оцифровка сигнала, передача цифрового сигнала, уже решены в рамках IP-телефонии. Необходимо лишь произвести шифрование сигнала и его идентификацию для существующего потока данных.
* Независимость от месторасположения. Нужно только интернет-соединение для подключения к провайдеру IP-телефонии. Например, операторы центра звонков с помощью IP-телефонов могут работать из любого офиса, где есть в наличии эффективное быстрое и стабильное интернет-подключение.
* Доступна интеграция с другими сервисами через интернет, включая видео звонок, обмен сообщениями и данными во время разговора, аудио конференции, управление адресной книгой и получение информации о том, доступны ли для звонка другие абоненты.
* Дополнительные телефонные свойства — такие как маршрутизация звонка, всплывающие окна, альтернативный GSM-роуминг и внедрение IVR — легче и дешевле внедрить и интегрировать. Тот факт, что телефонный звонок находится в той же самой сети передачи данных, что и персональный компьютер пользователя, открывает путь ко многим новым возможностям.

Для тестирования работы IP-телефонии в Packet Tracer есть IP-телефоны, специальный сервис IP-телефонии, а так же кодирующее устройство, предназначенное для использования обычного телефона как IP телефон.

Чтобы воспользоваться сервисом IP – телефонии нам нужно настроить его на маршрутизаторе.

Router(config)#telephony-service

Router(config-telephony)#max-ephones n

Router(config-telephony)#max-dn n

Router(config-telephony)#ip source-address 1.1.1.1 port 2000

Router(config-telephony)#auto assign 4 to 6

Router(config-telephony)#auto assign 1 to 5

Команды max-ephones и max-dn определяют максимальное кол-во подключаемых телефонов и прямых номеров. Командой auto assign мы задаем автоматическое назначение внешних номеров к кнопкам.

После этого, мы задаем прямой номер каждому телефону с помощью команд:

Router(config)#ephone-dn 1

Router(config-ephone-dn)#number 1111

**Практическая часть.**

**Создайте топологию, изображенную на рисунке:**

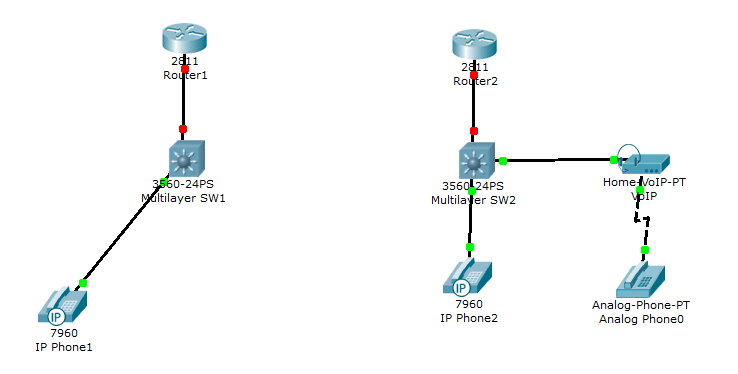
****

Рис.1.

Добавте интерфейс WIC-1T в маршрутизаторы Router1 и Router2 (если вы не сделаете это сейчас, то потом придется настраивать все заново).

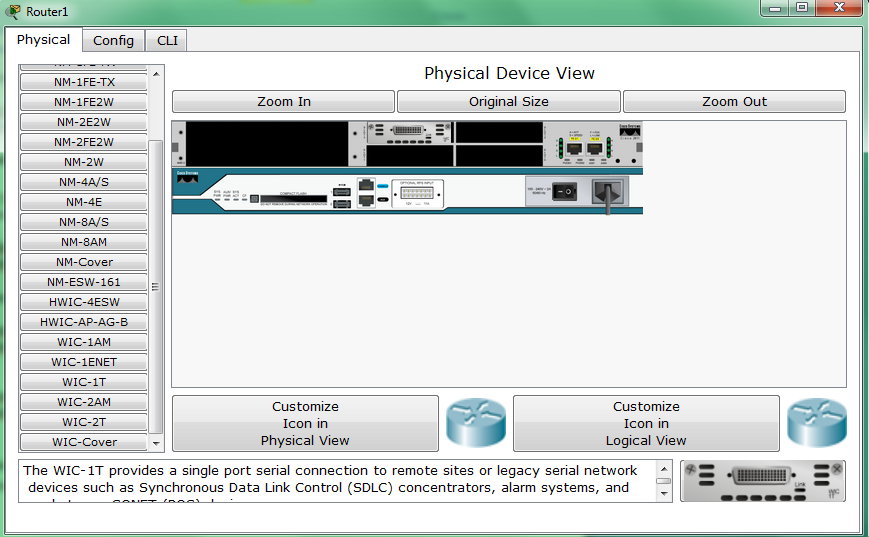


Рис.2.

1. **Настройка DHCP на Router1.**

На Router1 должен быть настроен DHCP, чтобы обеспечить адресами каждый IP-телефон, который подключен. Как только DHCP настроен, мы должны настроить порт FA0/0 и убедиться, что IP-телефон получает IP адрес.

Router1>en

Router1#conf t

Router1(config)#ip dhcp pool CATC

Router1(dhcp-config)#network 1.0.0.0 255.0.0.0

Router1(dhcp-config)#default-router 1.1.1.1

Router1(dhcp-config)#option 150 ip 1.1.1.1 Router1(config)#interface FastEthernet0/0

Router1(config-if)#ip address 1.1.1.1 255.0.0.0

Router1(config-if)#no shutdown

1. **Настройка сервиса IP-телефонии**

Для того чтобы Router1 обрабатывал голосовые пакеты, мы должны настроить сервис IP-телефонии. Так же необходимо указать максимальное количество телефонов и номеров которые будет поддерживать маршрутизатор.

Router1(config)#telephony-service

Router1(config-telephony)#max-ephones 5

Router1(config-telephony)#max-dn 5

Router1(config-telephony)#ip source-address 1.1.1.1 port 2000

Router1(config-telephony)#auto assign 4 to 6

Router1(config-telephony)#auto assign 1 to 5

1. **Настройка портов коммутатора**

Настроим порты коммутатора на пропускание голосовых пакетов и зададим им VLAN.

SW1(config)#interface range fa0/1 – 5

SW1(config-if-range)#switchport voice vlan 1

1. **Настройка IP-телефонов**

IP-Phone1 уже подключен к коммутатору, осталось только задать ему номер. IP адрес присвоится автоматически, так как у нас настроен DHCP.

Router1(config)#ephone-dn 1

Router1(config-ephone-dn)#number 1101

Добавим 2 IP-телефона и произведем их настройку аналогично.

Router1(config)#ephone-dn 2

Router1(config-ephone-dn)#number 1201

Router1(config)#ephone-dn 3

Router1(config-ephone-dn)#number 1301

Если вы все сделали правильно, то вы можете позвонить с одного телефона на другой, с помощью GUI консоли.

Теперь добавим компьютер к нашей сети, настроим его на автоматическое получение IP адресов, и произведем настройку роутера точно так же, как и для телефонов.

Router1(config)#ephone-dn 4

Router1(config-ephone-dn)#number 1401

Попробуем позвонить с его на другие телефоны.

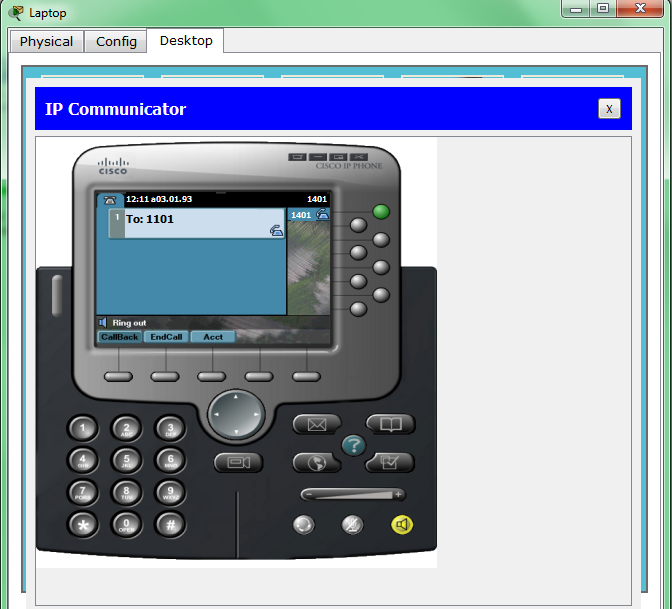
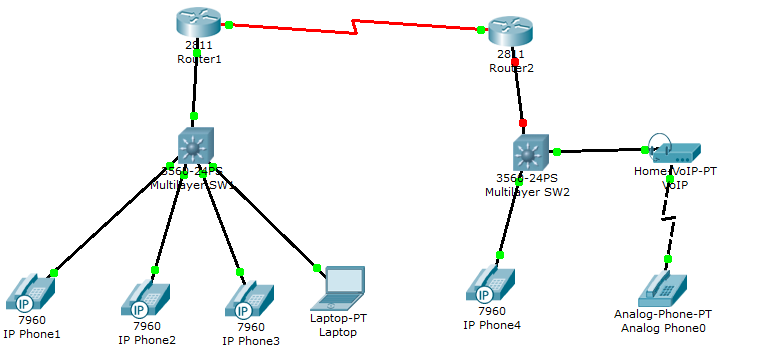


Рис.3.

1. **Соединение двух сетей.**

На данный момент у нас не подключены между собой маршрутизаторы Router1 и Router2. Подключим их с помощью интерфейсов serial 0/3/0 и кабеля Serial DCE.

На данный момент топология сети выглядит так:

Рис.4.

Теперь настроим маршрутизаторы.

Router1(config)#int s0/3/0

Router1(config-if)#ip address 3.0.0.1 255.0.0.0

Router1(config-if)#clock rate 56000

Router1(config-if)#no sh

Router2(config)#int s0/3/0

Router2(config-if)#ip address 3.0.0.2 255.0.0.0

Router2(config-if)#no sh

Пропишем статические маршруты:

Router1(config)#ip route 2.0.0.0 255.0.0.0 serial 0/3/0

Router2(config)#ip route 1.0.0.0 255.0.0.0 serial 0/3/0

Аналогично произведем настройку Router2 и SW2:

Router2(config)#ip dhcp pool CATC1

Router2(dhcp-config)#network 2.0.0.0 255.0.0.0

Router2(dhcp-config)#default-router 2.1.1.1

Router2(dhcp-config)#option 150 ip 2.1.1.1

Router2(config)#int fa0/0

Router2(config-if)#ip address 2.1.1.1 255.0.0.0

Router2(config-if)#no sh

Router2(config)#telephony-service

Router2(config-telephony)#max-ephones 3

Router2(config-telephony)#max-dn 3

Router2(config-telephony)#ip source-address 2.1.1.1 port 2000

Router2(config-telephony)#auto assign 4 to 6

Router2(config-telephony)#auto assign 1 to 5

Router2(config)#ephone-dn 1

Router2(config-ephone-dn)#number 2101

Router2(config)#ephone-dn 2

Router2(config-ephone-dn)#number 2201

SW2(config)#int range fa0/1-4

SW2(config-if-range)#switchport voice vlan 1

Так же укажем в VoIP IP адрес сервера: 2.1.1.1:

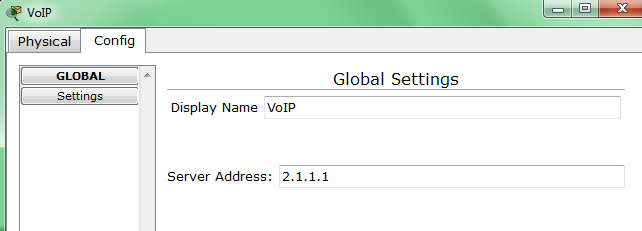


Рис. 5.

Теперь мы можем позвонить с телефона IP phone4 на телефон Phone0 и наоборот, но мы не можем соединиться между сетями. Для этого нужно настроить точку вызова на маршрутизаторах.

Router1(config)#dial-peer voice 1 voip

Router1(config-dial-peer)#destination-pattern 2…

Router1(config-dial-peer)#session target ipv4:3.0.0.2

Router2(config)#dial-peer voice 1 voip

Router2(config-dial-peer)#destination-pattern 1…

Router2(config-dial-peer)#session target ipv4:3.0.0.1

На этом настройка завершена, убедитесь, что все телефоны видят друг друга.



Рис.6.

**Задание для самостоятельной работы.**

1. Создайте топологию, изображенную на рисунке.

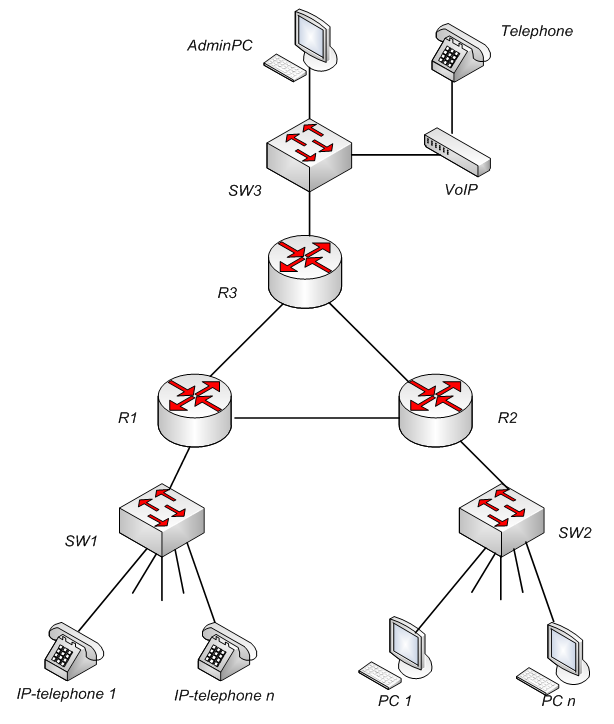


Рис. 7.

1. Количество компьютеров и IP-телефонов выберите в соответствии со своим вариантом.

|  |  |  |
| --- | --- | --- |
| Вариант | Кол-во PC | Кол-во IP-телефонов |
| 1 | 4 | 5 |
| 2 | 2 | 7 |
| 3 | 6 | 4 |
| 4 | 7 | 2 |
| 5 | 5 | 5 |
| 6 | 3 | 6 |

1. Настройте на маршрутизаторах DHCP сервера.
2. Настройте сервис IP-телефонии на маршрутизаторах, в соответствии со своим кол-вом компьютеров и телефонов.
3. Задайте произвольные номера для телефонов и компьютеров.
4. Настройте кодирующие устройство VoIP.
5. Попробуйте позвонить с IP-телефона на компьютер, с телефона на телефон, с компьютера на IP-телефон. Сделайте скриншоты.

**Контрольные вопросы:**

1. Что такое IP-телефония?
2. Как подключить обычный телефон к сети с IP-телефонией?
3. Как настроить IP-телефонию?
4. Зачем нужен сервер DHCP?

**Порядок выполнения и сдачи работы**

1. Изучить теоретическую и практическую часть.
2. Выполнить в Packet Tracer практическую часть.
3. Предъявите преподавателю результат выполнения.
4. Получите вариант и выполните в Packet Tracer задание для самостоятельной работы.
5. Оформите отчёт.
6. Защитите отчёт.

**9. Организационно-экономическая часть**

В организационно-экономической части проекта рассматриваются вопросы оценки стоимости объекта интеллектуальной собственности, а также обоснование постановки на баланс предприятия и коммерциализации идеи.

**9.1. Анализ и оценка стоимости**

Известно несколько десятков методов оценки стоимости объекта интеллектуальной собственности. Выбор того или иного метода оценки зависит от ряда факторов, таких как характер объекта, функции и цели оценки. Рекомендуется выбирать наибольшее количество используемых методов, чтобы при согласовании оценки получить наиболее точную стоимость.

Все методы группируются в три подхода к оценке: затратный, рыночный и доходный. Оценка стоимости объектов интеллектуальной собственности производится с помощью методов, опирающихся на эти подходы. Рассмотрим каждый из подходов подробнее.

9.1.1.Затратный подход

Затратный подход — совокупность методов оценки стоимости объекта оценки, основанных на определении затрат, необходимых для восстановления либо замещения объекта оценки, с учетом его износа.

Основным методом затратного подхода является метод стоимости создания. При этом методе определяется полная стоимость замещения или восстановления нематериального актива.

Затраты на воспроизводство (восстановление) актива. Наиболее последовательное применение затратного подхода – это прямой подсчет затрат на проведение работ, результатом которых стала компьютерная программа. Следует подчеркнуть, что речь идет не о бухгалтерском учете затрат с отражением на счетах, а просто о подсчете. В качестве варианта можно подсчитать, какие затраты понадобились бы на проведение тех же работ с учетом цен и ставок оплаты на дату оценки.

Затраты на замещение. Примерно то же можно сказать о другом варианте реализации затратного подхода, в основе которого лежит идея замещения одного актива другим, равноценным с точки зрения выполняемых функций.

Стоимость объектов интеллектуальной собственности(ОИС) по фактически произведенным затратам за период расчета Т определяется по формуле:

 (9.1)

где  ­­­- сумма всех затрат, связанных с созданием и охраной ОИС,

 - коэффициент приведения разновременных затрат к расчетному году,

 - коэффициент индексации учитывающий изменение цен в определенной отрасли производства в r году.

 - коэффициент, учитывающий степень морального старения

Р – рентабельность, учитывающая размер прибыли владельца ОИС

9.1.2. Рыночный подход

Рыночный подход к оценке активов (в том числе НМА) – это, прежде всего, метод сравнения продаж. Кроме того, в рамках рыночного подхода обычно рассматриваются другие методы, основанные на использовании обобщенной информации о рыночных продажах.

Метод сравнения продаж - в традиционном понимании практически не применим в рассматриваемой сфере за исключением оценки прав на программы для ЭВМ, передаваемых на основе оберточных лицензий. Кроме того, возможно использование метода сравнения продаж в качестве дополнения к доходному методу. Однако все сделки, в которых возникает необходимость оценить ИС, достаточно оригинальны. Найти подходящие аналоги сделок обычно оказывается невозможно.

Использование отраслевых индексов (стандартных ставок роялти) -

одним из вариантов реализации рыночного подхода можно считать использование стандартных отраслевых ставок роялти. В литературе описаны случаи, когда такие отраслевые стандарты устанавливались стихийным путем и действовали в течение ряда лет.

Рыночный подход имеет два несомненных достоинства. Во-первых, он основан на использовании рыночной информации, во-вторых, он прост в применении. Однако второе достоинство очень легко превращается в недостаток. Простота применения рыночного подхода лишь кажущаяся. Стандартные ставки роялти для определенных видов продукции, отраслевые индексы и другие показатели дают очень приблизительные ориентиры для совершения реальных сделок. Вся трудность заключается в учете индивидуальных особенностей конкретной сделки, а именно здесь рыночный подход не дает ни каких ориентиров.

9.1.3. Доходный подход

При доходном подходе стоимость неосязаемого актива или интереса в неосязаемом активе определяется путем расчета приведенной к текущему моменту стоимости прогнозируемых будущих выгод.

Различные методы оценки будут зависеть от характера неосязаемого актива, от устойчивости и природы дохода.

Могут использоваться следующие методы оценки:

* Метод дисконтированного денежного потока (DCF).
* Метод прямой капитализации (превышение поступлений над затратами), которая может извлекаться из неосязаемого актива и которая может возникать, в частности, за счет надбавки к цене, снижения затрат или эффекта масштаба.
* Метод остаточного дохода или распределения остаточного дохода.
* Экспресс – оценка.
* Расчет стоимости роялти или арендной платы, которые пользователь неосязаемого актива должен был бы в ином случае выплачивать законному собственнику неосязаемого актива.
* Метод освобождения от роялти.
* Метод избыточной прибыли.
* Правило 25%.
* Метод реального экономического эффекта.
* Метод экспертной оценки.

1). Метод дисконтирования денежного потока

В методе дисконтирования будущего денежного потока (Discounted Cash Flow - DCF) рассчитываются денежные поступления для всех будущих периодов. Эти поступления конвертируются в стоимость путем применения ставки дисконтирования и использования техники расчета стоимости, приведенной к текущему моменту. Метод дисконтирования используется для ОИС, имеющих конкретные сроки службы. Принятый период времени обычно представляет собой более короткий из двух сроков службы ОИС – экономического или юридического.

Срок полезной службы ***–*** это период, в течение которого неосязаемые активы, как ожидается, принесут собственнику экономическую отдачу от активов и могут оцениваться оценщиком с учетом следующих факторов:

Остающийся юридический срок службы.

Остающийся срок по контракту.

Остающийся физический срок службы.

Остающийся технологический срок службы.

Остающийся функциональный срок службы.

Остающийся экономический срок службы.

Ставки дисконтирования определяются по данным рынка на момент оценки и выражаются как мультипликаторы цен (определенные из данных по открыто продаваемым бизнесам или по сделкам) или как процентная ставка (определяемая по альтернативным инвестициям).

В качестве нормы дисконтирования может быть принят уровень предполагаемой прибыли при альтернативном исполь­зовании средств на создание, производство и реализацию про­дукции, процент за банковский депозит, норма прибыли при вложении средств в ценные бумаги, процентная ставка рефинан­сирования.

Стоимость ОИС за расчетный период времени Т определяется по следующей формуле:

, (9.2)

где  ­­­- прибыль от использования запатентованной продукции в r году,

 – доля прибыли приходящаяся на ОИС. Определяется экспериментальным путем и составляет от 10% до 35%

 - коэффициент дисконтирования,

, (9.3)

где  - ставка дисконтирования в r году.

2). Метод прямой капитализации

Метод прямой капитализации достаточно прост и в этом его главное и единственное достоинство. Однако он статичен, будучи привязанным к данным одного наиболее характерного года, и поэтому требуется особое внимание к правильному выбору показателей чистого дохода и коэффициентов капитализации. Расчет текущей стоимости нематериальных активов данным методом выполняется в три последовательных этапа:

- расчет ежегодного чистого дохода.

- выбор коэффициента капитализации. Коэффициент капитализации должен быть увязан с ранее выбранным показателем капитализируемого дохода.

- расчет текущей стоимости нематериальных активов.

3). Правило 25 %

За время существования патентной охраны сформировалась определенная традиция, согласно которой претендент изъявлял готовность платить патентообладателю 25% ожидаемой валовой прибыли, заработанной конкурентом благодаря лицензии.

При условии применения этого метода оценки объекта лицензиат не заинтересован в раскрытии своих потенциальных показателей, поэтому оценить диапазон прибыли можно на период не более двух лет.

При этом для новой сферы бизнеса и неопределенного размера прибыли пропорции распределения прибыли следует увеличивать в пользу лицензиата, так как он подвергается повышенному риску.

4). Метод преимущества в прибылях

Метод преимущества в прибылях часто применяется при оценке

стоимости изобретений. Стоимость изобретения определяется тем преимуществом в прибыли, которое ожидается получить от их использования. Под преимуществом в прибыли понимается дополнительная прибыль, обусловленная оцениваемым объектом интеллектуальной собственности. Она равна разности между прибылью, полученной при использовании изобретений, и той прибылью, которую производитель получает от реализации продукции без использования изобретения. Это ежегодное преимущество в прибыли дисконтируется с учетом предполагаемого периода его получения.

Таким образом, стоимость ОИС за расчетный период можно рассчитать по формуле:

, (9.4)

где  ­­­- объем продаж в r году. [15]

В данном дипломном проекте для расчета стоимости ОИС будем использовать метод стоимости создания затратного подхода, так как он является наиболее удобным для расчета.

**9.2. Экономическое обоснование затрат на разработку**

9.2.1. Определение трудозатрат

Технология проведения разработок может быть представлена в виде перечней работ, выполняемых в определенной последовательности. Определим перечень этапов и работ по проектированию лабораторного комплекса и сведем в таблицу 9.1.

Таблица 9.1

Перечень этапов и работ по разработке комплекса лабораторных работ по курсу «Передача данных в информационно-управляющих системах»

|  |  |
| --- | --- |
| Этапы работ | Содержание этапа |
| 1. Техническое задание | 1.1. Согласование и утверждение ТЗ |
| 2. Эскизный проект | 2.1. Разработка структуры комплекса |
| 3. Технический проект | 3.1. Разработка схем лабораторных работ |
| 4. Рабочий проект | 4.1. Разработка комплекса лабораторных работ |
| 5. Тестирование и отладка | 5.1. Тестирование разработчиком;  5.2. Обработка результатов, выявление недочётов  разработчиком и руководителем;  5.3. Контрольное тестирование; |
| 6. Заключительный этап | 6.1. Разработка методических указаний  6.2. Разработка вариантов  6.3. Оформление  6.4. Внедрение в эксплуатацию |

9.2.2. Оценка трудоемкости работ

Для определения трудоемкости разработки используются типовые нормы времени по программированию задач для ЭВМ. Нормы времени рассчитаны на комплексы задач и указаны в человеко-днях, человеко-часах или нормо-часах при пятидневной рабочей неделе с продолжительностью рабочего дня 8 час.

Расчет трудоемкости исследования или разработки производится по формуле:

 , (9.5)

где *ti* – трудоемкость работ по стадиям (этапам) разработки, чел-дн.;

*n* – количество работ (стадий, этапов) .

Учитывая такие факторы проекта, как новизна и неопределенность, из всех применяемых методов оценки трудоемкости работ, воспользуемся экспертным методом определения трудоемкости работ на каждый этап процесса. Для оценки трудоемкости работ необходимо задаться количеством исполнителей определенной квалификации. Примем, что разработкой проекта занимаются два специалиста – инженер и руководитель.

Определим максимальное и минимальное время, которое необходимо для разработки каждого пункта. Исходя из этих значений, определим ожидаемое время. Ожидаемое время определяется по формуле:

4338bd279fab97dac8134d87919e12cd82, (9.6)

где *tmin* - минимально возможная продолжительность работы, под которой понимается предполагаемая ее продолжительность при наиболее благоприятных условиях;

*tmax* – максимальная продолжительность работы, под которой понимается ее предполагаемая продолжительность при самых неблагоприятных условиях.

Таблица 9.2

Трудоемкости работ

|  |  |  |  |
| --- | --- | --- | --- |
| Этапы работ | tmin  чел –дн | tmax,  чел-дн | Тож,  чел-дн |
| 1. Техническое задание | 5 | 11 | 8 |
| 2. Эскизный проект | 20 | 31 | 25 |
| 3. Технический проект | 30 | 37 | 34 |
| 4. Рабочий проект | 36 | 44 | 40 |
| 5. Тестирование и отладка | 8 | 15 | 11 |
| 6. Заключительный этап | 14 | 18 | 16 |
| Итого | 113 | 156 | 134 |

Фонд времени работы каждого участника определяется путем распределения работ между исполнителями на каждом этапе.

Таблица 9.3

Списочный состав и фонды времени исполнителей

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Этапы работ | Трудоемкость,  чел-дн | Исполнители | Доля  участия, % | Фонд  времени, дн. |
| 1. Техническое задание | 8 | Руководитель | 60 | 5 |
| Инженер | 40 | 3 |
| 2. Эскизный проект | 25 | Руководитель | 20 | 5 |
| Инженер | 80 | 20 |
| 3. Технический проект | 34 | Руководитель | 21 | 7 |
| Инженер | 79 | 27 |
| 4. Рабочий проект | 40 | Руководитель | 10 | 4 |
| Инженер | 90 | 36 |
| 5. Тестирование и отладка | 11 | Руководитель | 19 | 4 |
| Инженер | 81 | 7 |
| 6. Заключительный этап | 16 | Руководитель | 25 | 4 |
| Инженер | 75 | 12 |
| Итого | 134 |  |  |  |

9.2.3. Расчет численности исполнителей работ

Численность персонала, занятого разработками зависит от масштаба работ, сроков выполнения работ, а также от суммы бюджета. Другими факторами, влияющими на количество исследователей и разработчиков, является эффективность организационной структуры, уровень профессионализма членов группы, степень важности проекта.

В данном дипломном проекте численность исполнителей, учитывая все эти факторы, а также существующее положение вещей, взята равной 2.

Состав и фонды времени исполнителей указаны в таблице 9.3.

1. Примерные обязанности и функции исполнителей в проектировании указаны в таблице 9.4.
2. Таблица 9.4
3. Примерные обязанности и функции исполнителей

|  |  |
| --- | --- |
| Исполнитель | Обязанности и функции |
| Руководитель проекта | Выдает техническое задание, поясняет специалистам суть и цели проекта. На всех этапах контролирует процесс проектирования и выполнение работ. Принимает стратегические решения по развитию проекта. Оказывает помощь специалисту при возникновении затруднений. Общается с заказчиком. |
| Дипломник | Проектирует, разрабатывает, тестирует. Описывает в документации информацию по проекту. |

1. Оплата труда персонала определяется исходя из фонда времени каждого исполнителя и среднедневной оплаты труда. Фонд времени каждого исполнителя определяется экспертным путем по доле участия в каждом этапе работ.

9.2.4. Затраты на выполнение проекта

Для расчета совокупной стоимости проекта рассчитывается сметная стоимость и составляется смета на разрабатываемый проект. Сметная стоимость разработки представляет собой сумму затрат, планируемых на проведение работ, соответствующих составленному перечню.

Расчет сметы затрат рекомендуется осуществлять методом сметных калькуляций по отдельным статьям расходов всех необходимых ресурсов. Сметная калькуляция содержит следующий перечень статей затрат: материалы и комплектующие; оплата труда персонала; отчисления на социальные нужды; специальное оборудование; накладные расходы; командировочные расходы; прочие расходы.

9.2.5. Расчет стоимости материалов и комплектующих.

Таблица 9.5

Расчет стоимости материалов и комплектующих

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Марка,  тип | Ед.  измер | Потреб.  кол-во | Цена за  ед., руб | Стоимость,  руб |
| Материалы | | | | | |
| Интернет | ADSL | Mb | - | - | 539 |
| Комплектующие | | | | | |
| Бумага | Xerox A4 | пач. | 1 | 190 | 190 |
| Бумага | Xerox А1 | шт. | 6 | 60 | 360 |
| Итого *Зм* |  |  |  |  | 1089 |

В статье затрат «материалы и комплектующие» учитывается стоимость всех материальных ресурсов, необходимых для проведения работ: основных и вспомогательных материалов, комплектующих изделий, сборочных единиц и деталей.

9.2.6. Расчет оплаты труда персонала

Оплата плата персонала определяется исходя из фонда времени каждого исполнителя и среднедневной оплаты труда. Фонд времени каждого исполнителя определяется экспертным путем по доле участия в каждом этапе работ. Среднедневная оплата труда каждого участника рассчитывается по формуле:

, (9.7)

где *Змес* – среднемесячная оплата труда, руб;

*Ф* - среднемесячный плановый фонд времени одного работника, дни.

Расчет оплаты труда приведен в таблице 9.6.

Таблица 9.6

Расчёт оплаты труда

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Этапы работ | Трудо-емкость,  чел-дн | Исполнители | Доля  уча-стия, % | Фонд  вре-мени, дн. | Средне-дневная оплата труда, руб. | Фонд платы труда, руб. |
| 1. Техничес-кое задание | 8 | Руководитель | 60 | 5 | 200 | 1000 |
| Инженер | 40 | 3 | 100 | 300 |
| 2. Эскизный проект | 25 | Руководитель | 20 | 5 | 200 | 1000 |
| Инженер | 80 | 20 | 100 | 2000 |
| 3. Техничес-кий проект | 34 | Руководитель | 21 | 7 | 200 | 1400 |
| Инженер | 79 | 27 | 100 | 2700 |
| 4. Рабочий проект | 40 | Руководитель | 10 | 4 | 200 | 800 |
| Инженер | 90 | 36 | 100 | 3600 |
| 5. Тестирова-ние и отладка | 11 | Руководитель | 19 | 4 | 200 | 800 |
| Инженер | 81 | 7 | 100 | 700 |
| 6. Заключи-тельный этап | 16 | Руководитель | 25 | 4 | 200 | 800 |
| Инженер | 75 | 12 | 100 | 1200 |
| Итого *З* |  |  |  |  |  | 16300 |

9.2.7. Расчет отчислений на социальные нужды

Общая максимальная ставка страховых взносов в 2013 году останется такой же, как и ставка ЕСН в 2012 году (30%), и будет состоять из следующих компонентов: Пенсионный фонд — 22%, Фонд социального страхования — 2,9%, Федеральный фонд обязательного медицинского страхования — 5,1%, итого — 30%.

*Зсоц*= 0,3  *З* = 0,3  16300= 4890 (руб.)

9.2.8.Расчет амортизационных отчислений

Под оборудованием для данного проекта понимается комплект ПК. Размер амортизационных отчислений на оборудование определяется по формуле 9.8:

 (9.8)

где *Цоб*– стоимость оборудования (11750 тыс. руб. стоимость ПК);

*Ноб*– нормы отчислений на амортизацию оборудования (30 % в год);

*tр* – время работы оборудования, дней (166 дней для ПК (на нем производятся работы от этапа эскизного проекта до заключительного этапа);

*Тр* – число календарных дней в 2013 году (365 дней).

 (руб.)

1. 9.2.9. Расчёт накладных расходов
2. Накладные расходы берутся в процентах от заработной платы (55%):
3. Зн = 0,55 ⋅ З = 0,55 ⋅ 16300 = 8965 (руб.)
4. 9.2.10. Расчёт затрат на прочие расходы
5. Расчет затрат на прочие расходы определяется в процентном соотношении от суммы предыдущих статей затрат (2%).
6. *Зпроч*= 0,02 ⋅ ∑*Зi* = 0,02 ⋅ (*Зм + З + Зсоц+Зоб + Зн*)= 0,02 ⋅ (1089 + 16300 + 4890 + 1603 + 8965 ) = 0,02 ⋅ 32847 = 656 (руб.)[15].
7. Смета затрат на разработку представлена в таблице 9.7.

Таблица 9.7

Смета затрат на разработку

|  |  |
| --- | --- |
| Статья затрат | Величина затрат, руб. |
| Затраты на материалы | 1089,00 |
| Оплата труда | 16300,00 |
| Затраты на социальные нужды | 4890,00 |
| Амортизация | 1603,00 |
| Накладные расходы | 8965,00 |
| Прочие затраты | 656,00 |
| Итого затрат | 33503 |

1. Таким образом сумма затрат на разработку составила 33503,00 рублей.
2. Диаграммы структурных расходов представлена в Приложении A.

**9.3. Оценка стоимости нематериального актива. Обоснование постановки на баланс предприятия**

Рассчитаем стоимость интеллектуальной собственности (С) по формуле 9.1. Принимаем рентабельность Р=20%, = 1,2 , = 1,1 , = 1. Сумма всех затрат, связанных с созданием лабораторного комплекса З=33503. Подставив в формулу 9.1 данные, получим, что стоимость интеллектуальной собственности по фактически произведенным затратам за период расчета 5 лет равна С= 53068 (руб).

Постановка объекта интеллектуальной собственности на баланс предприятия позволяет организации: увеличивать уставной фонд предприятия, получить дополнительные доходы за передачу прав на использование объектов ИС по средствам оформления лицензионных договоров, производить выплату авторских вознаграждений авторам, а также лицам содействовавшим изобретательству включая эти затраты как затраты на создание объекта ИС. Также при этом амортизационные отчисления на законных основаниях остаются в распоряжении предприятия, включаются в затраты на создание продукции и не облагаются налогом на прибыль.

Для определения амортизационных отчислений установим срок полезного использования разрабатываемого программного продукта равный 5 лет. Воспользуемся линейным способом расчета амортизации. При линейном способе годовая сумма амортизационных отчислений по объекту НМА определяется как произведение его первоначальной стоимости и годовой нормы амортизации, исчисленной исходя из срока полезного использования этого объекта. Годовая норма амортизации рассчитывается в процентах как отношение 100% к сроку полезного использования объекта НМА (в годах). Линейный способ предполагает равномерное начисление амортизации в течение всего срока полезного использования объекта НМА.

Первоначальная стоимость НМА = 53068 (руб). Годовая норма амортизации в этом случае составит 20% (100% : 5 лет). Ежегодная сумма амортизации будет равна 10613 руб.

Для расчета авторского вознаграждения определим ставку роялти = 5%. Рассчитаем авторское вознаграждение: 53068\*5%= 2653 руб. С момента постановки НМА на баланс предприятия ОИС становится имущество предприятия и появляются 2% налог на имущество.

Налог на имущество = 53068\*2%= 1061 руб.

Постановка на баланс оправдана и экономически выгодна[15].

**9.4. Коммерциализация проекта и практическое использование разработки**

Данный проект разработан специально для решения задачи обучения и

освоения студентами материала по курсу «Передача данных в информационно-управляющих системах». Проект будет осуществлять контроль уровня знаний и степени освоения пройденного материала. Комплекс будет использоваться в пределах кафедры автоматизации и вычислительной техники. Распространяться среди студентов в целях обучения на бесплатной основе.

**10. Безопасность и экологичность проекта. Правовые и нормативные основы.**

**10.1. Анализ опасных и вредных факторов при работе на ПЭВМ**

В дипломном проекте лабораторный комплекс реализован с помощью средств ПЭВМ. В настоящее время персональные компьютеры широко используются во всех организациях. Несоблюдение требований безопасности приводит к тому, что через некоторое время работы за компьютером сотрудник начинает ощущать определенный дискомфорт: у него возникают головные боли и резь в глазах, появляются усталость и раздражительность. У некоторых людей нарушается сон, ухудшается зрение, начинают болеть руки, шея, поясница и т.д.

К наиболее распространенным ошибкам, связанным с обеспечением условий труда работающих на компьютерах относятся:

* недостаточные площадь и объем производственного помещения;
* несоблюдение требований, предъявляемых к температуре и влажности рабочих помещений;
* низкий уровень освещенности в помещениях и на рабочих поверхностях аппаратуры;
* повышенный уровень низкочастотных магнитных полей от мониторов;
* произвольная расстановка техники и нарушения требований организации рабочих мест;
* несоблюдение требований к режимам труда и отдыха;
* чрезмерная производственная нагрузка работников;

Вопросы, относящиеся к ответственности за обеспечение охраны труда при работе за компьютером, регулируются Федеральным законом «Об основах охраны труда в Российской Федерации» и Санитарными правилами и нормами СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы».

В соответствии со ст. 14 Закона об охране труда на работодателя возлагается обязанность обеспечить:

* безопасность работников при эксплуатации оборудования;
* применение средств индивидуальной защиты работников;
* соответствующие требования охраны труда, условия труда на каждом рабочем месте;
* соблюдение режима труда и отдыха работников;
* обучение безопасным методам и приемам выполнения работ;
* инструктаж по охране труда;
* организацию контроля над состоянием условий труда на рабочих местах;
* проведение аттестации рабочих мест по условиям труда;
* информирование работников об условиях и охране труда на рабочих местах, существующем риске повреждения здоровья и полагающихся им компенсациях и средствах индивидуальной защиты.

Таким образом, ответственность за соблюдение требований законодательства к условиям труда несет работодатель, возлагающий эти функции на службу охраны труда организации или на привлеченного на договорных началах специалиста по охране труда.

Прежде чем приобрести компьютеры, необходимо соответствующим образом подготовить помещение, где они будут установлены.

В соответствии с СанПиН 2.2.2/2.4.1340-03 помещения для работы на компьютерах должны иметь естественное и искусственное освещение.

Не допускается располагать рабочие места для работы на компьютерах в подвальных помещениях. В случае производственной необходимости использовать помещения без естественного освещения можно только по согласованию с органами и учреждениями Государственного санитарно-эпидемиологического надзора России.

Для внутренней отделки интерьера помещений, где расположены ПЭВМ, должны использоваться диффузно отражающие материалы с коэффициентом отражения для потолка — 0,7 — 0,8; для стен — 0,5 — 0,6; для пола — 0,3 — 0,5.

Помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным заземлением (занулением) в соответствии с техническими требованиями по эксплуатации. Не следует размещать рабочие места с ПЭВМ вблизи силовых кабелей и вводов, высоковольтных трансформаторов, технологического оборудования, создающего помехи в работе ПЭВМ.

В производственных помещениях уровень шума на рабочих местах не должен превышать значений, установленных «Санитарными нормами допустимых уровней шума на рабочих местах», а уровень вибрации — «Санитарными нормами вибрации рабочих мест».

Клавиатуру следует располагать на поверхности стола на расстоянии 100 — 300 мм от края, обращенного к пользователю, или на специальной, регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.

Конструкция рабочего стула (кресла) должна обеспечивать поддержание рациональной рабочей позы при работе на ПЭВМ, позволять изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Тип рабочего стула (кресла) следует выбирать с учетом роста пользователя, характера и продолжительности работы с ПЭВМ.

Экран видеомонитора должен находиться от глаз пользователя на расстоянии 600 — 700 мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов.

Лица, работающие с ПЭВМ более 50% рабочего времени (профессионально связанные с эксплуатацией ПЭВМ, учащиеся), должны проходить обязательные предварительные при поступлении на работу и периодические медицинские осмотры в установленном порядке.

Для предупреждения преждевременной утомляемости пользователей ПЭВМ рекомендуется организовывать деятельность путем чередования работ с использованием ПЭВМ и без него.

При возникновении у работающих с ПЭВМ зрительного дискомфорта и других неблагоприятных субъективных ощущений, несмотря на соблюдение санитарно-гигиенических и эргономических требований, рекомендуется применять индивидуальный подход с ограничением времени работы с ПЭВМ.

В случаях, когда характер работы требует постоянного взаимодействия с ВДТ (набор текстов или ввод данных и т.п.) с напряжением внимания и сосредоточенности, при исключении возможности периодического переключения на другие виды трудовой деятельности, не связанные с ПЭВМ, рекомендуется организация перерывов на 10 — 15 мин. через каждые 45 — 60 мин. работы.

Продолжительность непрерывной работы с ВДТ без регламентированного перерыва не должна превышать 1 ч.

Во время регламентированных перерывов с целью снижения нервно-эмоционального напряжения, утомления зрительного анализатора, устранения влияния гиподинамии и гипокинезии, предотвращения развития позотонического утомления целесообразно выполнять комплексы упражнений, изложенных в Приложениях 9-11 к СанПиН 2.2.2/2.4.1340-03.

**10.2. Решения по охране труда**

Опасные и вредные производственные факторы при работе с ПЭВМ. Комфортные и безопасные условия труда - один из основных факторов влияющих на производительность людей работающих с ПЭВМ. Изучение и решение проблем, связанных с обеспечением здоровых и безопасных условий, в которых протекает труд человека - одна из наиболее важных задач в разработке новых технологий и систем производства. Изучение и выявление возможных причин производственных несчастных случаев, профессиональных заболеваний, аварий, взрывов, пожаров, и разработка мероприятий и требований, направленных на устранение этих причин позволяют создать безопасные и благоприятные условия для труда человека.

Работа сотрудников вычислительных центров непосредственно связана компьютером, а соответственно с вредными дополнительными воздействиями целой группы факторов, что существенно снижает производительность их труда. К таким факторам можно отнести:

а) воздействие вредных излучений от монитора и от компьютера;

б) воздействие электромагнитных излучений;

в) неправильная освещенность;

г) не нормированный уровень шума;

д) не комфортные метеорологические условия;

е) высокое напряжение;

и другие факторы.

Санитарные нормы и стандарты безопасности.

В целях обеспечения безопасности здоровья пользователей в Российской Федерации действуют Санитарные нормы и правила " Гигиенические требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работ" СанПиН 2.2.2/2.4.1340-03. Цель Санитарных норм - определить такие нормированные величины факторов воздействия, чтобы их вред был минимальным, а условия труда - комфортными. Предельно допустимые уровни, генерируемого монитором электромагнитного поля и поверхностного электростатического потенциала установлены СанПиН 2.2.2/2.4.1340-03.

Средства защиты пользователей от ЭМП.

В основном из средств защиты предлагаются защитные фильтры для экранов мониторов. Они используется для ограничения действия на пользователя вредных факторов со стороны экрана монитора, снижает излучение монитора в направлении пользователя.

Мониторы персональных компьютеров и рабочих станций при обязательным сертификационным испытаниям по следующим параметрам:

1. Параметры безопасности – электрическая, механическая, пожарная безопасность.
2. Санитарно - гигиенические требования – уровень звуковых шумов , ультрафиолетовое, рентгеновское излучения и показатели качества изображения.
3. Электромагнитная совместимость – излучаемые радиопомехи.

Также рекомендуется наличие на экранах мониторов антистатического покрытия (antistatic coating) - которое препятствует возникновению на поверхности экрана электростатического заряда, притягивающего пыль и не благоприятно влияющего на здоровье пользователя.

Требования к помещениям с ЭВМ.

Согласно СанПиН 2.2.2/2.4.1340-03, площадь на одно рабочее место с ВДТ или ПЭВМ должна составлять не менее 6 м2, а объем - не менее 20 м3, а в учебных помещениях соответственно не менее 6 м2 и 24 м3. В залах ЭВМ должно предусматриваться автоматическое пожаротушение. Применение для тушения пожара воды, порошковых огнетушителей недопустимо - выводится из строя ЭВМ. Здания и помещения для ЭВМ должны быть оборудованы системами центрального отопления, приточно-вытяжной вентиляции, хозяйственно-питьевого водопровода.

Требование к видеодисплейным терминалам и персональным электронно-вычислительным машинам.

Визуальные эргономические параметры ВДТ являются параметрами безопасности, их неправильный выбор приводит к ухудшению здоровья пользователей. Все ВДТ должны иметь гигиенический сертификат, включающий, в том числе оценку визуальных параметров.

Конструкция ВДТ, его дизайн и совокупность эргономических параметров должны обеспечивать надежное и комфортное считывание отображаемой информации в условиях эксплуатации.

Конструкция ВДТ должна предусматривать наличие ручек регулировки яркости и контраста, обеспечивающие возможность регулировки этих параметров от минимальных до максимальных значений.

Конструкция ВДТ и ПЭВМ должна обеспечивать мощность экспозиционной дозы рентгеновского излучения в любой точке на расстоянии 0,05 м. от экрана и корпуса ВДТ при любых положениях регулировочных устройств не должна превышать 7,74х10 А/кг, что соответствует эквивалентной дозе, равной 0,1 мбэр/час (100 мкР/час).

Требования к микроклимату, содержанию аэрофонов и вредных химических веществ в воздухе помещений эксплуатации мониторов и ПЭВМ.

В производственных помещениях, в которых работа с мониторами и ПЭВМ является основной (диспетчерские, операторские, расчетные, кабины и посты управления, залы вычислительной техники и др.) должны обеспечиваться оптимальные параметры микроклимата.

Для повышения влажности воздуха в помещениях с мониторами ПЭВМ следует применять увлажнители воздуха, заправляемые ежедневно дистиллированной или прокипяченной питьевой водой.

Требования к освещению помещений и рабочих мест с мониторами и ПЭВМ.

Искусственное освещение в помещениях эксплуатации мониторов и ПЭВМ должно осуществляться системой общего равномерного освещения. Допускается использование местного освещения, предназначенного для освещения зоны расположения документов.

Освещенность на поверхности стола в зоне размещения рабочего документа должна быть 300 - 500 лк. Допускается установка светильников местного освещения для подсветки документов. Местное освещение не должно создавать бликов на поверхности экрана и увеличивать освещенность экрана более 300 лк.

Яркость светильников общего освещения в зоне углов излучения от 50 о до 90о с вертикалью в продольной и поперечной плоскостях должна составлять не более 200 кд/ кв. м., защитный угол светильников должен быть не менее 40 о.

Светильники местного освещения должны иметь не просвечивающий отражатель с защитным углом не менее 40 градусов.

Меры безопасности при эксплуатации вычислительной техники.

Для получения хорошего качества изображения должна быть обеспечена достаточная контрастность изображения, которая зависит от соотношения собственной яркости трубки и яркости фона, обусловленного внешней освещенностью экрана.

Для уменьшения влияния на оператора рентгеновского излучения (особенно цветных дисплеев) и электромагнитного поля, необходимо находиться не ближе 1,22 м от задних стенок соседних дисплеев. Экран должен находиться от глаз пользователя на оптимальном расстоянии 0,6-0,7 м, но не ближе 0,5 м. Рабочий стол должен регулироваться по высоте в пределах 680-800 мм(если невозможно, то высота его - 725 мм), под столом должно быть свободное пространство для ног. Рабочий стул должен иметь регуляцию по высоте (400-550 мм) и угла наклона спинки.

Рабочие места операторов располагаются так, чтобы оконные проемы находились сбоку и дальше от экрана ПК, Если экран обращен к окну, необходим экран (ширма) между рабочим местом и окном. Светильники общего освещения должны располагаться сбоку от рабочего места, параллельно линии зрения оператора и стены с окнами. Расстояние между тыльной стороной одного ряда мониторов и экраном монитора из соседнего ряда должно быть не менее 2 м, а расстояние между боковыми поверхностями мониторов - не менее 1,2 м.

При работе на ПК необходимо делать перерывы на 10-15 мин каждые 1,5-2 часа работы в соответствии с СанПиН.

10.2.1. Проектирование электробезопасности

Электрические установки, к которым относится практически все оборудование ПЭВМ, представляют для человека опасность.

Согласно ГОСТ 12.1.019 электробезопасность электроустановок обеспечивается конструкцией электроустановок, техническими способами средствами защиты, организационными и техническими мероприятиями.

В электроустановках переменного и постоянного тока защитное заземление и зануление обеспечивают защиту людей от поражения электрическим током при прикосновении к металлическим нетоковедущим частям, которые могут оказаться под напряжением в результате повреждения изоляции.

Защитному заземлению и занулению подлежат металлические части электроустановок, доступные для прикосновения человека и не имеющие других видов защиты. Так, корпуса электрических машин, трансформаторов, светильников и др. нетоковедущие части могут оказаться под напряжением при замыкании на корпус. Если корпус не заземлен, то прикосновение к нему также опасно, как и прикосновение к фазе. При заземлении корпуса ток через тело человека при его прикосновении к корпусу будет тем меньше, чем меньше ток замыкания на землю и сопротивление цепи заземления и чем ближе человек стоит к заземлителю.

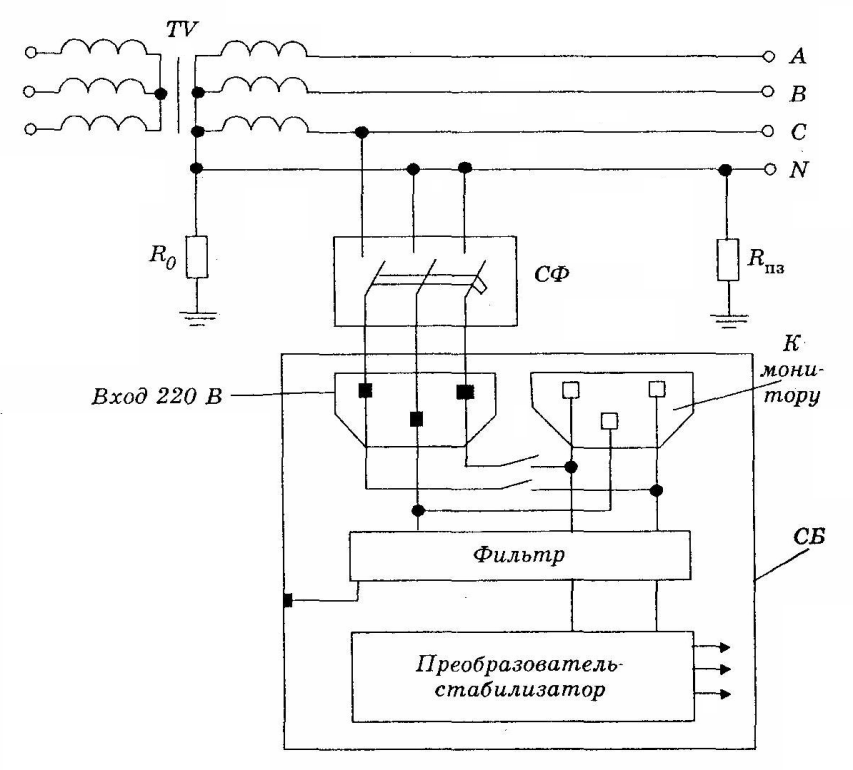
Принцип действия зануления основан на пре­вращении замыкания на корпус ЭУ в однофазное короткое замы­кание между поврежденной фазой и НРП (нулевой рабочий проводник), при котором протека­ет Iкз, достаточный для срабатывания автоматического выключателя, отключающего ЭУ от электрической сети. На рис. 10.1 представлены схемы подключения ПЭВМ к питающей сети.



Рис.10.1 – Защитное зануление электроустановок

*а - зануление в трёхфазной электрической сети с глухозаземлённой нейтралью; б - зануление в однофазной электрической сети с глухозаземлённым выводом источника тока; A1, A2 - электроустановки; R0 - сопротивление заземления нейтрали; RП - повторное сопротивление заземления нейтрали; НРП - нулевой рабочий проводник; НЗП - нулевой защитный проводник; TV - источник электро­питания; QF1 и QF2 - автоматические выключатели; Iкз - ток короткого замыкания*

Зануление выполняется соединением металлических частей ЭУ с заземленной точкой источника питания при помощи нулевого защитного проводника, при этом в цепи нулевого проводника не допускается установка выключателей, рубильников, т.е. должна быть обеспечена непрерывность цепи от каждого корпуса электрооборудования до заземленной нейтрали источника питания (рис. 10.2).



Условные обозначения:

СФ – *сетевой фильтр;*

R0 – *сопротивление рабочего зануления сети;*

Rпз *- повторное сопротивление заземления нейтрали;*

TV – *источник электропитания;*

СБ – *системный блок.*

Рис.10.2 — Принципиальная схема зануления ПЭВМ

Нулевой провод имеет повторные заземления через каждые 250 м и на концах ответвлений длиной более 200 м, а также на вводах от ВЛ к электроустановкам.

Согласно ГОСТ 12.1.030-81 и ПУЭ защитное заземление и зануление требуется выполнять при напряжении 380 В и выше переменного тока и от 110 до 440 В постоянного тока при работах в условиях повышенной опасности и особо опасных (ГОСТ 12.1.013-78).

В электрических установках до 1000В в сети с заземленной нейтралью, или заземленным выводом однофазного источника питания, а также с заземленной средней точкой в 3-х проводных сетях постоянного тока должно быть выполнено зануление.

При этом проводники должны быть выбраны таким образом, чтобы при замыкании на корпус или нулевой проводник возникал ток короткого замыкания, обеспечивающий отключение автомата или плавление плавкой вставки ближайшего предохранителя. В цепях зануления не должно быть разъединителей и предохранителей.

Кроме того, зануление способствует выносу потенциала по нулевому проводнику на доступные к прикосновению проводящие части неповрежденного оборудования. Оно не защищает, если произойдет замыкание фазы на землю, минуя корпус, и переходное сопротивление в месте замыкания будет малым.

Опасно наличие зануления при обрыве нулевого проводника, когда все корпуса электроприемников за точкой обрыва могут оказаться под напряжением.

Для того чтобы снизить опасные потенциалы при замыкании на корпус, используются повторные заземлители с сопротивлением заземлителя не более 10 Ом.

Произведем расчет защитного зануления ПЭВМ, на котором устанавливается программа.

Принципиальная схема зануления ПЭВМ представлена на рисунке 8.2.

Для питания ПЭВМ используется сеть переменного тока напряжением 220 В, частотой 50 Гц.

В помещении, где производится монтаж сети, питание электроустановок осуществляется от подстанции с трансформатором Р=600 кВт, удаленной от ПЭВМ на 300 м. Питание к распределительному щиту подводится алюминиевым проводом сечением 25 мм2.

В качестве нулевого проводника выбираем стальную полосу сечением 50 мм2.

При использовании зануления должны быть выполнены следующие условия:

** (10.1)

где *k* - коэффициент кратности номинального тока IН0М (А) плавкой вставки предохранителя, k=3.

Номинальным током плавкой вставки IНОМ называется ток, значение которого указано непосредственно на вставке заводом-изготовителем. Номинальный ток IНОМ в помещении 40 А. Значение IКЗ зависит от фазного напряжения сети и сопротивления цепи, в том числе от полного сопротивления трансформатора ZT, фазного проводника ZФ, нулевого защитного проводника ZНЗ, внешнего индуктивного сопротивления петли "фазный провод - нулевой защитный провод" (петли "фаза-нуль") ХП, активного сопротивления заземлений нейтрали обмоток трансформатора Ro и повторного заземления нулевого защитного проводника RП. Поскольку Ro и RП, как правило, велики по-сравнению с другими сопротивлениями, ими можно пренебречь. Выражение для IКЗ будет иметь вид:

*I КЗ* = (10.2)

где ZП= ZФ + ZНЗ + ХП - комплексное полное сопротивление петли "фаза-нуль".

Удельное сопротивление фазного провода и его сечение:

Рал = 0,028 (Ом\*мм2)/м , Sceч = 25 мм2 ,

отсюда сопротивление фазного провода рассчитывается по следующей формуле:

*RФ= * (10.3)

RФ= =0,336 (Ом)

Удельное сопротивление нулевого провода и его сечение:

рст = 0,058 (Ом\*мм2)/м , Sсеч = 50 мм2,

отсюда сопротивление нулевого провода по аналогии рассчитывается по следующей формуле:

*RНЗ= * (10.4)

RНЗ=  =0,348 (Ом)

Значения ХФ и XНЗ малы, ими можно пренебречь.

Значение Хп можно определить по формуле:

*ХП =0,145\*lg* (10.5)

где к = 0,3894,

dcp - расстояние между проводниками,

dФ - геометрический диаметр.

Расчеты дают значение ХП = 0,556 Ом.

Сопротивление электрической дуги берем равной

Rд = 0,02 (Ом), Хд = 0.

В соответствии с мощностью трансформатора

RT = 0,0044 (Ом), Хт = 0,0127 (Ом)

Полное сопротивление петли "фаза-нуль":

*ZП =*  (10.6)

Получаем: ZП = 0,716 (Ом).

При использовании зануления по требованиям ПУЭ (Правила устройства электроустановок)

RНЗ/RФ = 0,348/0,336 < 2, следовательно, ПУЭ выполняются.

Исходя из полученных данных, рассчитаем ток короткого замыкания. Для этого обратимся к формуле 10.2.

IКЗ  = =301,6 (А)

При попадании фазы на зануленный корпус электроустановки должно произойти автоматическое отключение, поскольку должно выполнятся условие формулы 10.1, в нашем случае:

301,6 > 3-40 =120

Защитное зануление выполнено правильно, следовательно, отключающая способность системы обеспечена.

Определим напряжение прикосновения и ток через человека до срабатывания защиты:

** (10.7)

 (10.8)

Расчетная схема представлена на рисунке 10.3.

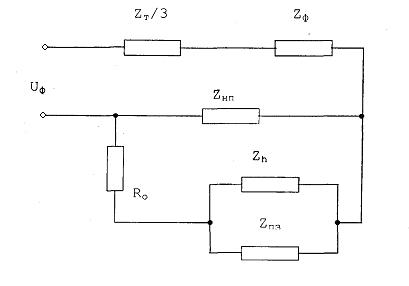


Рис. 10.3 - Расчетная схема зануления

Rпз=0,348(Ом), Rнп=10(Ом), R0=4(Ом), Rh=1(кОм), Uпр=29,9(В)

Такое напряжение безопасно для человека при предельно допустимом времени воздействия. Предельно допустимое время пребывания человека под действием электрического тока находится из следующего соотношения:

 (10.9)

где

 (10.10)

Значит 

Исходя из этого, найдём предельно допустимое время пребывания человека под действием электрического тока, определим по формуле 10.9:



В качестве прибора защитного отключения можно автоматический выключатель, рассчитанный на IНОМ = 40 (А) и tcp = 0,3 (с) при IКЗ = 301 (А). Выберем дифференциальный автомат т.к. он экономичный и выгодный. Тип дифференциального автомата можно выбрать АД-14 ИЭК 4р с установкой срабатывания 40 мA.

 (10.11)



Это должно обеспечить надежную защиту, при этом должно выполняться условие:

 (10.12)

Из расчётов видно, что К = 7,5 на порядок больше чем 1,4 - следовательно условие выполняется.

**10.3. Решения по обеспечению устойчивости функционирования в чрезвычайных ситуациях**

10.3.1. Общие сведения

Чрезвычайная ситуация (ЧС) – это нарушение нормальных условий жизнедеятельности на объекте или на определенной территории, вызванная аварией, опасным природным явлением, катастрофой, стихийным бедствием, экологическим бедствием, эпидемией, эпизоотией, а также применением возможных средств поражения гипотетическим противником, которое может привести к человеческим или материальным потерям, нанести ущерб здоровью людей или окружающей среде, значительные материальные потери и нарушение условий жизнедеятельности людей.

Всякому чрезвычайному событию предшествует те или иные отклонения от нормального хода какого-либо процесса. Характер развития события и его последствия определяются дестабилизирующими фактором различного происхождения. Это может быть и природное, антропогенное социальное или иное воздействие нарушающее функционирование системы.

Имеется пять фаз развития ЧС:

накопление отклонений

инициирование ЧС

процесс ЧС

действие остаточных факторов

ликвидация ЧС

Классификация чрезвычайных ситуаций

1. по сфере возникновения

* техногенные
* природные
* экологические
* социально-политические

2. по масштабу возможных последствий

* локальные
* объектовые
* региональные
* глобальные

3. по ведомственной принадлежности

* на транспорте
* в строительстве
* в промышленности
* в сельском хозяйстве

4. по характеру лежащих в основе событий

* пожар
* авария
* землетрясение
* погодные условия

10.3.2. Действия по сигналам гражданской обороны

Среди защитных мероприятий гражданской обороны, осуществляемых заблаговременно, особо важное место занимает организация оповещения органов гражданской обороны, формирований и населения об угрозе нападения противника и о применении им ядерного, химического, бактериологического (биологического) оружия и других современных средств нападения. Особое значение оповещение приобретает в случае внезапного нападения противника, когда реальное время для предупреждения населения будет крайне ограниченным и исчисляться минутами.

По данным зарубежной печати, считается, что своевременное оповещение населения об возможности укрытия его за 10-15 мин после оповещения позволит снизить потери людей при внезапном применении противником оружия массового поражения с 85 % до 4-7 %. Поэтому защита населения от оружия массового поражения даже при наличии достаточного количества убежищ и укрытий будет зависеть от хорошо организованной системы оповещения, организация которой возлагается на штабы гражданской обороны. Современные системы дальнего обнаружения позволяют быстро определить не только место и направление движения носителя, но и время его подлета. Это обеспечивает передачу сигнала по системе оповещения до штабов гражданской обороны и объектов. Оповещение организуется для своевременного доведения до органов гражданской обороны, формирований и населения сигналов, распоряжений и информаций гражданской обороны о эвакуации, воздушном нападении противника, радиационной опасности, химическом и бактериологическом (биологическом) заражении, угрозе затопления, начале рассредоточения и др. Эти сигналы и распоряжения доводятся до штабов гражданской обороны объектов централизованно. Сроки доведения их имеют первостепенное значение. Сокращение сроков оповещения достигается внеочередным использованием всех видов связи, телевидения и радиовещания, применением специальной аппаратуры и средств для подачи звуковых и световых сигналов. Все сигналы передаются по каналам связи и радиотрансляционным сетям, а также через местные радиовещательные станции. Одновременно передаются указания о порядке действий населения и формирований, указываются ориентировочное время начала выпадения радиоактивных осадков, время подхода зараженного воздуха и время подхода зараженного воздуха и вид отравляющих веществ.

Сигналы, поданные вышестоящим штабом, дублируются всеми подчиненными штабами. С целью своевременного предупреждения населения городов и сельских населенных пунктов о возникновении непосредственной опасности применения противником ядерного, химического, бактериологического (биологического) или другого оружия и необходимости применения мер защиты установлены следующие сигналы оповещения гражданской обороны: "Воздушная тревога" "Отбой воздушной тревоги"; "Радиационная опасность"; "Химическая тревога". В штабах гражданской обороны городов могут устанавливаться разнообразная сигнальная аппаратура и средства связи, которые позволяют с помощью пульта включать громкоговорящую связь и квартирную радиотрансляционную сеть, осуществлять одновременный вызов руководящего состава города и объектов народного хозяйства по циркулярной телефонной сети, принимать, распоряжения вышестоящих штабов и передавать свои распоряжения и сигналы оповещения штабам гражданской обороны объектов и населению. Сигнал "Воздушная тревога" подается для всего населения. Он предупреждает о непосредственной опасности поражения противником данного города (района). По радиотрансляционной сети передается текст: "Внимание! Внимание! Граждане! Воздушная тревогам Воздушная тревога!" Одновременно с этим сигнал дублируется звуком сирен, гудками заводов и транспортных средств. На объектах сигнал будет дублироваться всеми, имеющимися в их распоряжении средствами. Продолжительность сигнала2-3 минуты.

По этому сигналу объекты прекращают работу, транспорт останавливается и все население укрывается в защитных сооружениях. Рабочие и служащие прекращают работу в соответствии с установленной инструкцией и указаниями администрации, исключающими возникновение аварий. Там, где по технологическому процессу или требованиям безопасности нельзя остановить производство, остаются дежурные, для которых строятся индивидуальные убежища. Сигнал "Воздушная тревога" может застать людей в любом месте и в самое неожиданное время. Во всех случаях следует действовать быстро, но спокойно, уверенно и без паники. Строгое соблюдение правил поведения по этому сигналу значительно сокращают потери людей.

Сигнал "Отбой воздушной тревоги" передается органами гражданской обороны. По радиотрансляционной сети передается текст: "Внимание! Внимание граждане! Отбой воздушной тревоги? Отбой воздушной тревоги". По этому сигналу население с разрешения комендантов (старших) убежищ и укрытий покидает их. Рабочие и служащие возвращаются на свои рабочие места и приступают к работе.

В городах (районах, по которым противник нанес удары оружием массового поражения, для укрываемых передается информация об обстановке, сложившейся вне укрытий, о принимаемых мерах по ликвидации последствий нападения, " режимах поведения населения и другая необходимая информация для последующих действий укрываемых.

Сигнал "Радиационная опасность" подается в населенных пунктах и районах, по направлению к которым движется радиоактивное облако, образовавшееся при взрыве ядерного боеприпаса.

По сигналу "Радиационная опасность" необходимо надеть респиратор, противопылевую тканевую маску или ватно-марлевую повязку, а при их отсутствии - противогаз, взять подготовленный запас продуктов, индивидуальные средства медицинской защиты, предметы первой необходимости и уйти в убежище, противорадиационное или простейшее укрытие.

Сигнал "Химическая тревога" подается при угрозе или непосредственном обнаружении химического или бактериологического нападения (заражения). По этому сигналу необходимо быстро надеть противогаз, а в случае необходимости - и средства защиты кожи и при первой же возможности укрыться в защитном сооружении.

Если защитного сооружения поблизости не окажется, то от поражения аэрозолями отравляющих веществ и бактериальных средств можно укрыться в жилых, производственных или подсобных помещениях.

Если будет установлено, что противник применил бактериологическое (биологическое) оружие, то по системам оповещения население получит рекомендации о последующих действиях.

Необходимо быть предельно внимательными и строго выполнять распоряжения органов гражданской обороны. О том, что опасность нападения противника миновала, и о порядке дальнейших действий распоряжение поступит по тем же каналам связи, что и сигнал оповещения.

Основной способ оповещения населения. Содержание речевой информации. Основным способом оповещения населения о возникновении опасности и порядке действий является передача сообщения средствами радио и телевидения.

При аварии на химическом объекте содержание информации может быть следующим: "Внимание! Говорит штаб гражданской обороны города. Граждане! Произошла авария на комбинате с выбросом сильнодействующего ядовитого вещества - аммиака. Облако зараженного воздуха распространяется в направлении улицы Ленина. Населению улиц Предтеченская, Зосимовская находиться в зданиях. Провести герметизацию своих жилищ.

Населению улицы Пречистенская набережная немедленно покинуть жилые дома, учреждения, учебные заведения и выйти в район Драматического театра. В дальнейшем действовать в соответствии с нашими указаниями".

При возникновении угрозы нападения противника местными  
органами власти и штабами ГО с помощью средств массовой информации передаются населению постановления или распоряжения о порядке действий. С этого времени радиоточки, телевизоры должны быть постоянно включены для приема новых сообщений. В кратчайшие сроки население должно принять необходимые меры защиты и включиться в выполнение мероприятий, проводимых ГО.

Очень важно сразу уточнить место ближайшего убежища (укрытий) и пути подхода к нему. Если поблизости нет защитных сооружений, нужно немедленно приступить к строительству простейшего укрытия либо приспособлению заглубленных помещений (даже 1-го этажа каменного здания) под ЯРУ. В этой работе активное участие должны также принять учащиеся старшеклассники. Необходимо привести в. готовность средства индивидуальной защиты, приспособить подручные средства, достать домашнюю аптечку. В жилых помещениях следует провести герметизацию окон, дверей, противопожарные мероприятия; принять меры к предохранению продуктов питания, воды от возможного заражения (загрязнения).

Необходимо подготовить все самое необходимое на случай эвакуации.

В последующем при непосредственной опасности ударов противника с воздуха подается сигнал "Воздушная тревога!"- Ему предшествует сигнал "Внимание всем!", а затем средствами радио и телевидения будет передано: "Внимание! Внимание! Говорит 101 штаб гражданской обороны. Граждане! Воздушная тревога! Воздушная тревога! Отключите свет, газ, воду, погасите огонь в печах. Возьмите средства индивидуальной зашиты, документы, запас продуктов и воды. Предупредите соседей и при необходимости помогите больным и престарелым выйти на улицу. Как можно быстрее дойдите до защитного сооружения или укройтесь на местности.

Соблюдайте спокойствие и порядок. Будьте внимательны к сообщениям гражданской обороны"!

После сигнала "Внимание всем!" может последовать и другая информация, например, о надвигающейся угрозе радиоактивного или бактериологического заражения. И в этих случаях будет передано краткое сообщение о порядке действий и правилах поведения.

Действия населения в зоне радиоактивного заражения (загрязнения).

При нахождении в зоне радиоактивного заражения (загрязнения) необходимо строго выполнять режим радиационной защиты, устанавливаемый штабом ГО в зависимости от степени заражения (загрязнения) района. Если по какой-либо причине не поступит сообщения ГО, некоторое время можно руководствоваться следующим.

В зоне умеренного заражения население находится в укрытии, как правило, несколько часов, после чего оно может перейти в обычное помещение. Из дома можно выходить в первые сутки не более чем на 4 час.

В зоне сильного заражения люди должны быть в убежищах (укрытиях) до трех суток, при крайней необходимости можно выходить на 3-4 ч в сутки. При этом необходимо надевать средства защиты органов дыхания и кожи. В зоне опасного заражения люди должны быть в укрытиях и убежищах трое суток и более, после чего можно перейти в жилое помещение и находиться в нем не менее четырех суток. Выходить из помещения на улицу можно только на короткий срок (не более чем на 4 ч в сутки).

В зоне чрезвычайно опасного заражения пребывание населения возможно только в защитных сооружениях с коэффициентом ослабления дозы облучения около 1000.

Во всех случаях при нахождении вне укрытии и зданий применяются средства индивидуальной защиты. В качестве профилактического средства, уменьшающего вредное воздействие радиоактивного облучения, используются радиозащитные таблетки из комплекта АИ. Типовые режимы радиационной защиты. Режим радиационной защиты - это порядок действий населения, применения средств и способов защиты в зонах радиоактивного заражения (в результате ядерного взрыва), предусматривающий максимальное уменьшение возможных доз облучения.

Режим радиационной защиты № 1 применяется в населенных пунктах в основном с деревянными постройками, обеспечивающими ослабление радиации в 2 раза, и ПРУ, ослабляющими радиацию в 50 Раз (перекрытые щели, подвалы). Режим радиационной защиты № 2 предусматривается для населенных пунктов с каменными одноэтажными постройками, обеспечивающими ослабление радиации в 10 раз, и ПРУ, ослабляющими радиацию в 50 раз. Режим радиационной защиты № 3 разработан для населенных пунктов с многоэтажными каменными постройками, обеспечивающими ослабление радиации в 20-30 раз, и ПРУ, ослабляющими радиацию в 200-400 раз (подвалы многоэтажных зданий). Каждый режим радиационной защиты определяет время, в течение которого необходимо постоянно находиться в ПРУ (1 этап), затем поочередно в ПРУ и дома (2 этап) и, наконец, преимущественно дома с кратковременным выходом на улицу по неотложным делам в целом не более чем на 1 ч (3 этап). В районах сильного радиоактивного загрязнения в результате аварии на АЭС население должно быть эвакуировано в максимально короткие сроки. Жители прилегающих районов, где мощность дозы излучения не превышает 5 мР/ч (так называемых районов строгого контроля), должны выполнять гигиенические требования, в частности, ежедневно проводить влажную уборку жилых помещений, как можно чаще мыть руки с мылом, соблюдать правил хранения продуктов питания и воды (эти правила жизнедеятельности разработаны штабами ГО и органами здравоохранения. Этими же органами проводится полная профилактика населения).

Действие населения в зоне химического заражения. В зоне химического заражения следует находиться в убежище (укрытии) до получения распоряжения о выходе из него. Выходить из убежища (укрытия) необходимо в надетых средствах защиты органов дыхания. Направление выхода из зоны заражения обозначается указательными знаками, при их отсутствии надо выходить в сторону, перпендикулярную направлению ветра. В зоне заражения нельзя брать что-либо с зараженной местности, садиться и ложиться на землю. Даже при сильной усталости нельзя снимать средства индивидуальной защиты. Если капли ОВ, ДЯВ попали на открытые участки тела или одежду надо немедленно провести их обработку с помощью ИПП.

После выхода за пределы зоны заражения снимать средства индивидуальной защиты, и особенно противогаз, без разрешения нельзя, потому что поверхность одежды, обуви и средств зашиты может быт заражена ОВ. Получившим поражения необходимо немедленно оказать первую медицинскую помощь: ввести противоядие (антидот) обработать открытые участки тела с помощью содержимого ИПП. после чего доставить их на медицинский пункт. Все вышедшие из зоны заражения обязательно проходят полную санитарную обработку и дегазацию одежды на специальных обмывочных пунктах.

Действия населения в очаге бактериологического поражения.

В очаге бактериологического поражения для предотвращения распространения инфекционных заболеваний может быть введен специальный режим - карантин или обсервация.

Население, находящееся в очаге бактериологического поражения, должно строго соблюдать требования медицинской службы гражданской обороны, особенно режим питания. В пищу разрешается употреблять только те продукты, которые хранились в холодильниках или в закрытой таре. Кроме того, как пищу, так и воду для шитья следует обязательно подвергать термической обработке.

**Заключение**

В результате дипломного проектирования разработан комплекс методических указаний по курсу «Передача данных в информационно-управляющих системах».

В лабораторный комплекс предложено включить изучение современного пакета визуального проектирования сетей Cisco Packet Tracer.

В ходе разработки дипломного проекта выполнено следующее.

Проведен сравнительный анализ современных пакетов визуального проектирования сетей, на основании которого в качестве исследуемого выбран Cisco Packet Tracer.

Составлены структурная схема комплекса лабораторных работ, а так же схемы для самих работ. Были проведены тесты на правильную работу разработанных схем сети, а так же составлены варианты заданий для самостоятельной работы. Были созданы методические указания к выполнению лабораторных работ.

Комплекс включил в себя 5 лабораторных работ, содержащих теоретические сведения, практическую часть и задания для самостоятельной работы.

Таким образом, разработанный комплекс лабораторных работ является достаточно эффективным в процессе обучения и закрепления пройденного материала на практике.

В разделе «Организационно-экономическая часть» рассчитаны трудовые и финансовые затраты на разработку комплекса.

В дипломном проекте также рассмотрены вопросы по безопасности и экологичности проекта, был проведен анализ основных потенциально опасных факторов. Было выполнено проектирование защитного зануления, рассмотрены действия по сигналам гражданской обороны.

**Список использованных источников**

1. Википедия [Электронный ресурс] – Режим доступа: http://ru.wikipedia.org/
2. LinkMeUp [Электронный ресурс] – Режим доступа: http://linkmeup.ru/
3. Cisco Systems, Inc [Электронный ресурс] – Режим доступа: http://www.cisco.ru/
4. Сообщество начинающих сисадминов [Электронный ресурс] – Режим доступа: http://litl-admin.ru/
5. Хабрахабр [Электронный ресурс] – Режим доступа: http://habrahabr.ru/
6. xgu.ru [Электронный ресурс] – Режим доступа: http://xgu.ru/
7. Компьютерные сети, от простого к сложному [Электронный ресурс] – Режим доступа: http://network.xsp.ru/
8. Форум Cisco Packet Tracer [Электронный ресурс] – Режим доступа: http://fiks-ru.net/forum/6-122-1/
9. Пятибратов А.П. и др. Вычислительные системы, сети и телекоммуникации. 2004г. 512 стр.
10. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Издание 4-ое. 2010г. Уч. для ВУЗов.
11. А.Д. Береснев, А. И. Говоров, А. В. Чунаев. Практические работы по курсу информационные сети. Уч. пособие. 2012г. Сантк-Петербург
12. Учебник для ВУЗов/ С. В. Белов, И. В. Ильницкая и др. ; 7-е издание; М.: Высшая школа, 2007. - 616 с.
13. Седельников, Ф. И. Безопасность жизнедеятельности (охрана труда): учебное пособие (электронная версия) – Вологда, 2001. – 1 дискета.
14. СанПиН 2.2.2/2.4.1340-03 Временные допустимые уровни ЭМП, создаваемых ПЭВМ на рабочих места
15. Учебник «Обеспечение безопасности при работе с ПЭВМ», В. Д. Маньков
16. Гражданская оборона и защита от чрезвычайных ситуаций: Метод. указ. / Сост. В. Ф. Егоров.Тамбов: Изд-во Тамб. гос. техн. ун-та, 2005. 32 с.
17. Атаманюк, В.Г. Гражданская оборона: Учеб. для вузов - 2-е изд./ В.Г. Атаманюк. – М.: Высш. шк., 1997. — 288с.: ил.