МОСКОВСКИЙ ФИНАНСОВО-ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ МФЮА

Кафедра Информационные системы и технологии

Направление / специальность 09.02.02 Компьютерные сети

К ЗАЩИТЕ

(РЕКОМЕНДОВАНО / НЕ РЕКОМЕНДОВАНО)

(ученая степень, ученое звание)

(подпись) *(И.О. Фамилия)*

« ___ » _____ 2023 г.

ДИПЛОМНАЯ РАБОТА

На тему: Разработка локальной сети с резервированием полосы пропускания и отсутствием конфликтов (на примере ООО «Совинто», г. Москва)

(тема дипломной работы)

Обучающийся « ___ » _____ 2023 г. Волков Виктор Игоревич

_____ _____
(подпись) *(инициалы, фамилия)*

Индивидуальный номер 29184301 группа 13КСи8810
(ИНС) *(шифр группы)*

Руководитель « ___ » _____ 2023 г. К.А. Василенко
(подпись) *(уч. степень, уч. звание, инициалы, фамилия)*

Содержание

Ведение……...…….3

1. АНАЛИТИЧЕСКАЯ ЧАСТЬ

1.1 Способы организации компьютерных сетей……..…….……..……4

1.2 Топология локальных сетей……...……..5

1.3 Протоколы передачи данных в локальных сетях…….....…….11

1.4 Используемое сетевое оборудование……12

1.5 Характеристика качества обслуживания вычислительных сетей…… 24

1.6 Регулирование выделения полосы пропускания в каналах передачи данных локальных сетей……..……...…29

1.7 Причины возникновения конфликтов и методы их предупреждения……..…
37

2. ПРАКТИЧЕСКАЯ ЧАСТЬ

2.1 Описание предприятия ООО "Совинто"……..…….……
42

2.2 Организация локальной сети предприятия "Совинто"……..……..43

2.3 Первичное проектирование схемы подключения оборудования……
44

2.4 Выбор сетевого оборудования……
45

2.5 Проектирование сети……...……...…49

3. ОЦЕНКА ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ПРОЕКТА

3.1. Определение параметров проекта автоматизации ……..51

3.2 Расчет показателей экономической эффективности…..……
58

ЗАКЛЮЧЕНИЕ…….....…64

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ…….66

ПРИЛОЖЕНИЕ…….69

Введение

В крупных, да в принципе в любых, образовательных учреждения без локальной информационной сети не обойтись. В настоящее время все больше учебные заведения используют в своей работе высокотехнологичное оборудование, а следовательно, их деятельность напрямую зависит от непрерывности функционирования и производительности ИТ-систем. В свою очередь, ИТ-системы зависят от защищенности и надежности всего комплекса оборудования, сердцем которого являются серверы, коммутационное оборудование. Так же не маловажную роль играет локальная информационная сеть.

Объектом выпускной квалификационной работы: процесс создания локальной сети с резервированием полосы пропускания и отсутствием конфликтов ООО «Совинто».

Предметом выпускной квалификационной работы разработка проекта информационной сети ООО «Совинто».

Целью выпускной квалификационной работы является реализация проекта локальной информационной сети ООО «Совинто.

Задачи выпускной квалификационной работы:

– провести анализ области;

– выбрать оборудование;

– описать кабельную систему, выбрать топологию;

– произвести прокладку кабельной системы.

Практическая значимость выпускной квалификационной работы состоит в реализации разработки проекта локальной информационной сети ООО «Совинто» для преподавателей и студентов МФЮА, отвечающей современным требованиям качества, производительности и безопасности.

Структура выпускной квалификационной работы состоит из введения, трех разделов, заключения, библиографического списка.

1. АНАЛИТИЧЕСКАЯ ЧАСТЬ.

1.1 Способы организации компьютерных сетей

В зависимости от роли подключенного к сети компьютера, сети делят на одноранговые и иерархические.

В одноранговой сети компьютеры имеют равные права. При формировании такой сети пользователь делит свои ресурсы на доступные и недоступные для общего использования. Компьютеры находят друг друга при помощи уникального адреса или по имени.

В иерархической сети права доступа к сетевым ресурсам настраиваются выделенным сервером. Задача сервера – следить, чтобы адреса в сети не повторялись и информация, которая была послана одному из пользователей, была недоступна другим компьютерам сети. Процесс распределения адресов и управления правами доступа называется администрированием и выполняется сетевыми администраторами.

Одноранговые сети проще в администрировании, чем иерархические, хотя и не обеспечивают высокую степень защиты информации. Иерархические сети наоборот обладают повышенной надежностью и защищенностью информации, хранящейся на сервере.

При подключении персональных компьютеров на предприятии к локальной сети их, в зависимости от выполняемых ими функций, подразделяют на два вида: рабочая станция (Workstation) и сервер (Server). Рабочая станция может использовать только те ресурсы локальной сети, которые ей доступны.

Сервер, с другой стороны, выполняет действия по запросам рабочих станций и предоставляет им доступ к своим ресурсам (оборудованию).

Взаимодействие в сети происходит на программном уровне. Т. е. программа–клиент посылает запрос программе–серверу. Серверная программа обрабатывает его и отправляет ответ.

Существует несколько разновидностей серверов:

– сервер печати;

– Web–сервер;

– файловый сервер;

– сервер баз данных и т.д.

Классификация серверов по характеру использования:

– выделенный сервер;

– невыделенный сервер.

Выделенный сервер может функционировать без клавиатуры и монитора. Такой сервер предназначен для предоставления своих ресурсов для общего пользования. Выделенный сервер обычно обладает такими характеристиками, как надежность аппаратного и программного обеспечения, а также повышенная мощность. Для выделенных серверов в основномиспользуют следующие операционные системы: Microsoft Windows 2008 Server/2012 R2 Server, Linux и другие.

Невыделенный сервер выступает как рабочая станция, ресурсы которой выделены для общего доступа. На невыделенном сервере операционной системой может быть Microsoft Windows 7/8, Linux и другие.

1.2 Топологии локальных сетей

Топология вычислительной сети – это способ соединения отдельных её компонентов (компьютеров, периферийных устройств, серверов) . Топология определяет тип кабелей, требования к оборудованию, надежность работы и многое другое.

Перед созданием локальной вычислительной сети необходимо определится с топологией такой сети. Рассмотрим способы подключения компьютеров к сети.

Существуют три базовые топологии:

– шина (bus);

– звезда (star);

– кольцо (ring).

Топология шина

Компьютеры соединены последовательно. При подобной структуре топологии все клиенты имеют равноправный доступ к сети (рис. 1).

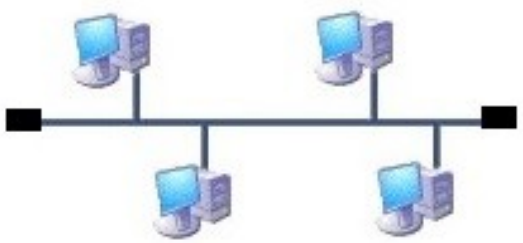


Рис. 1. Топология шина

Все клиенты сети могут легко контактировать с любым компьютером, поскольку они все подключены к общему каналу передачи данных. Передача информации в шинной топологии осуществляется следующим образом: данные передаются на все компьютерные сети в виде электрических сигналов, но информация принимается только тем компьютером, адрес которого совпадает с адресом получателя.

В топологии шина отсутствует центральный узел, следовательно, увеличивается надежность передачи, так как при отказе любого из компьютеров, исправные машины всё равно смогут продолжить обмен информацией. Если происходит обрыв кабеля в сети с топологией шина, то получаются две вполне работоспособные шины (рис. 2).

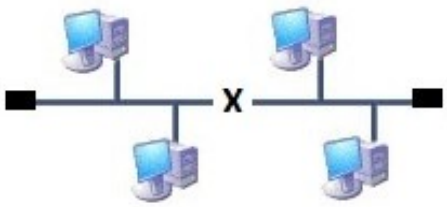


Рис. 2 Обрыв кабеля в сети с топологией шина

Из–за особенностей распространения электрических сигналов необходимо включение специальных устройств – терминаторов (ограничителей,). Если их не включить, то связь по сети станет невозможной, поскольку сигнал, отражаясь от конца линии, сильно искажается.

Преимущества топологии шина:

1. Компьютеры можно подключать независимо друг от друга (нет необходимости останавливать передачу информации в сети при подключении нового клиента).

2. Легкость настройки и конфигурации.

3. Информация доступна каждому компьютеру.

4. Высокая надежность (отказ одного из компьютеров не влияет на работоспособность всей сети).

5. Экономическая выгода (отсутствие затрат на прокладку дополнительной линии при подключении нового компьютера).

Недостатки топологии шина:

1. Трудность в определении дефектов соединения.

2. Низкая скорость передачи информации (все данные циркулируют по одной шине).

3. Низкая безопасность (информация с любого компьютера доступна всем пользователям сети).

4. Быстродействие (чем больше компьютеров в сети, тем медленнее происходит передача данных).

Организация данного типа подключения на предприятии не целесообразно, т. к. является дорогостоящим и ненадежным.

Топология звезда

К каждому компьютеру подходит отдельный кабель из одного узла – сервера или концентратора. Информация между клиентами сети передается через выделенный центр (рис. 3).

Передача информации в рассматриваемой топологии происходит по следующему принципу: от отправителя данные передаются через центральный узел всем компьютерам сети, но принимают их только те станции, которым они предназначены.



Рис. 3. Топология звезда

Преимуществом топологии звезда является то, что из–за отказа одного из компьютеров, работоспособность системы не нарушится, однако если выйдет из строя центральный узел, то сеть полностью перестает функционировать. В топологии звезда на каждой линии связи находится только два клиента. Для их соединения используют две линии связи, каждая из которых передает информацию в одном направлении. Эта передача называется точка–точка. За счет этого происходит упрощение сетевого оборудования по сравнению с шиной. Следовательно, нет необходимости использовать дополнительные внешние терминаторы. Несмотря на упомянутые плюсы, в топологии звезда есть серьезный недостаток – жесткое ограничение количества компьютеров. Центральный узел может обслуживать только до 48 периферийных абонентов, то есть подключение новых клиентов возможно только в этих пределах. Если же в сети используется большее количество компьютеров, то тогда вместо периферийного подключают еще один центральный узел, который также сможет обслуживать еще 48 абонентов.

Преимущества топологии звезда:

1. Отсутствие накладок в передаче данных (информация между компьютером и центральным узлом передается по отдельному каналу).

2. Возможность централизованного управления.

3. Быстродействие сети (общая производительность зависит от производительности центрального узла).

4. Легкость подключения нового персонального компьютера (ПК).

Недостатки топологии звезда:

1. Отказ центрального узла влияет на работу всей сети.

2. Расход кабеля (каждому новому клиенту необходимо вести отдельную линию).

Данный тип подключения удовлетворяет требованиям предприятия, поэтому компьютеры будет объединены в сеть при помощи топологии звезда.

Топология кольцо

Все компьютеры связаны в кольцо. Функции сервера распределены между компьютерами сети (рис.4).



Рис. 4. Топология кольцо

В топологии кольцо сигнал идет в одном направлении, проходя через каждый компьютер. Передача информации происходит следующим образом: последовательно по кольцу передается специальный сигнал (маркер); его получает клиент, который хочет передать данные; получив маркер, компьютер создает «пакет», куда помещает адрес получателя и данные, затем отправляет его по кольцу; данные передаются через каждый компьютер до тех пор, пока не окажутся у того, чей адрес совпадает с адресом получателя; затем принимающий

компьютер посылает отправителю подтверждение факта получения данных; после получения подтверждения передающий компьютер создает новый маркер и возвращает его в сеть. Если выходит из строя хотя бы один компьютер сети, то нарушается функционирование сети в целом, так как сигнал проходит по кольцу последовательно, от одного компьютера к другому. Такие же последствия наблюдаются при обрыве или коротком замыкании в любом из кабелей, поэтому в топологии кольцо предусматривают прокладку двух и более параллельных линий связи (одна из которых находится в запасе).

Преимущества топологии кольцо:

1. Эффективная пересылка сообщений (отправка нескольких сообщений по кольцу друг за другом).

2. Протяженность сети (компьютеры могут подключаться друг к другу на значительных расстояниях без специальных усилителей).

Недостатки топологии кольцо:

1. Отключение работы сети при подключении нового клиента.

2. Низкая надежность сети (отказ одного из компьютеров влечет за собой отказ всей системы).

3. Скорость работы при большом количестве клиентов сильно замедляется, так как данные проходят через каждый компьютер.

Данный тип подключения является не выгодным и неустойчивым к отказам.

Кроме трех базовых топологий существуют и другие. В основном это сочетание нескольких базовых (комбинированные топологии). Одна из распространенных комбинированных топологий называется звезда–шина. В такой топологии сети с топологией звезда объединяют друг с другом при помощи линейной шины. Если один компьютер становится неисправным, то это

никак не влияет на работоспособность всей сети. Если же становится неисправным концентратор, то взаимодействие подключенных к нему компьютеров и концентраторов становится невозможным.

Еще один распространенный способ соединения компьютеров между собой называется звезда–кольцо. Он имеет некоторые сходства с топологией звезда–шина. Компьютеры подключают к концентратору, который формирует шину или кольцо. Но в топологии звезда–кольцо концентраторы на основе главного узла образуют звезду.

При создании локально–информационной сети можно использовать любую из перечисленных топологий. Выбор топологии зависит от количества компьютеров и их расположения в помещении.

1.3 Протоколы передачи данных в локальных сетях

В локальных сетях используются различные протоколы для обеспечения передачи данных между устройствами. Некоторые из наиболее распространенных протоколов включают в себя:

- Ethernet: наиболее распространенный протокол, который используется для передачи данных в локальных сетях. Он обеспечивает быструю передачу данных и широко поддерживается различным сетевым оборудованием.

- Wi-Fi: беспроводной протокол, который используется для обеспечения доступа к Интернету и передачи данных между устройствами в локальной сети.

- TCP/IP: протокол, который используется для передачи данных между устройствами в Интернете и в локальных сетях. Он обеспечивает надежную передачу данных и используется практически во всех компьютерных сетях.

- DNS: протокол, который используется для преобразования доменных имен в IP-адреса. Он позволяет пользователям получать доступ к сайтам в Интернете по их доменным именам.

Что касается сетевого оборудования для локальных сетей, то наиболее распространенными устройствами являются маршрутизаторы, коммутаторы и точки доступа Wi-Fi. Маршрутизаторы используются для связи между различными сетями, коммутаторы - для соединения устройств внутри одной сети, а точки доступа Wi-Fi - для беспроводного подключения устройств к сети.

1.4 Используемое сетевое оборудование

Сетевое оборудование является важным компонентом при построении локальной сети. Его выбор очень важен на этапе проектирования сети, ведь стоимость данных средств составляет существенную часть от стоимости сети в целом. При формировании сети будет использоваться следующее сетевое оборудование:

1. Межсетевые экраны TP-LINK ER8411;

Для защиты локальных сетей от нежелательного трафика и несанкционированного доступа применяются различные виды межсетевых экранов. В зависимости от способа реализации, они могут быть программными или программно-аппаратными.

Программный Firewall — это программное обеспечение, которое устанавливается на компьютер и обеспечивает защиту сети от внешних угроз. Это удобное и недорогое решение для частных ПК, а также для небольших локальных сетей — домашних или малого офиса. Они могут применяться на корпоративных компьютерах, используемых за пределами офиса.

Для защиты более крупных сетей используются программные комплексы, под которые приходится выделять специальный компьютер. При этом

требования по техническим характеристикам к таким ПК являются довольно высокими. Использование мощных компьютеров только под решение задач МСЭ нельзя назвать рациональным. Да и производительность FireWall часто оставляет желать лучшего.

Поэтому в крупных компаниях и организациях обычно применяют аппаратно-программные комплексы (security appliance). Это специальные устройства, которые, как правило, работают на основе операционных систем FreeBSD или Linux.

Функционал таких устройств строго ограничивается задачами межсетевого экрана, что делает их применение экономически оправданным. Также security appliance могут быть реализованы в виде специального модуля в штатном сетевом оборудовании — коммутаторе, маршрутизаторе и т. д.

Применение программно-аппаратных комплексов характеризуется следующими преимуществами:

- Повышенная производительность за счет того, что операционная система работает целенаправленно на выполнение одной функции.
- Простота в управлении. Контролировать работу security appliance можно через любой протокол, в том числе стандартный (SNMP, Telnet) или защищенный (SSH, SSL).
- Повышенная надежность защиты за счет высокой отказоустойчивости программно-аппаратных комплексов.

Помимо этого, межсетевые экраны классифицируют в зависимости от применяемой технологии фильтрации трафика. По этому признаку выделяют следующие основные виды МСЭ:

- прокси-сервер;
- межсетевой экран с контролем состояния сеансов;

- межсетевой экран UTM;
- межсетевой экран нового поколения (NGFW);
- NGFW с активной защитой от угроз.

2. Сетевые машрутизаторы Mikrotik hAP ac lite TC;

Маршрутизатор современному пользователю гораздо больше известен под названием «роутер», являющимся простой калькой с английского router. На самом деле, оба этих слова обозначают одно и то же – устройство, которое отвечает за маршрутизацию. Говоря простыми словами, это именно та неприметная коробочка, которая позволяет подключить к единственному кабелю, проведенному интернет-провайдером в квартиру или офис, более одного компьютера, ноутбука или телефона.

Условно все модели роутеров можно разделить на 3 группы:

- Проводные. Позволяют подключать устройства-клиенты исключительно по проводу, с помощью специальных кабелей – патч-кордов. В основном к этой группе относятся так называемые провайдерские маршрутизаторы с большим количеством (до 12-13) Ethernet-портов, использующиеся в качестве основы для построения сети, например, в многоквартирном доме.

- Беспроводные. Имеют как порты для проводного подключения (их куда меньше, обычно не более 4), так и встроенный Wi-Fi- модуль. Для увеличения радиуса действия беспроводной сети в них могут устанавливаться антенны, вынесенные за пределы корпуса, но встречаются модели и без них.

- 3G/4G маршрутизаторы. Их ключевое отличие – возможность получения интернета не по кабелю, а «по воздуху», с помощью мобильной сети. Конфигурация при этом может быть самой разной: от

установки сим-карты в сам роутер и полного отсутствия Ethernet-портов до наличия USB-порта в «обычном» маршрутизаторе для подключения любого USB-модема.

Раз уж мы упомянули порты и антенны, стоит остановиться на основных компонентах и узлах, присутствующих в любом устройстве.

- WAN-порт (Wide Area Network) – порт для подключения интернет-кабеля. Обычно он обозначен синим цветом.

- LAN-порт (Local Area Network) – один или несколько портов, служащих для подключения клиентских устройств. Они нужны не только для обеспечения их доступа в интернет, но и для организации локальной сети, то есть, возможности передачи данных между всеми клиентами, подключенными к одному роутеру. Обозначаются желтым цветом.

- Модуля беспроводного сигнала (Wi-Fi) – он установлен на основной плате и скрыт внутри корпуса. Для передачи сигнала ему обязательно нужна антенна. Обычно ее роль играет отдельная дорожка на плате, но, как уже было сказано, нередко антенна выносится за пределы корпуса с помощью проводов.

- Блока питания – большинство роутеров питается от проприетарных внешних БП с круглым штекером. Бытовые компактные модели также могут питаться от обычного USB-разъема, а в провайдерских маршрутизаторах используется более сложная схема с двумя встроенными БП для подключения резервного источника бесперебойного питания.

3. Сетевые коммутаторы TP-LINK tl-sg1210p;

Коммутатор (он же Ethernet Switch или просто «свитч») – это отдельный узел, служащий для объединения нескольких устройств в локальную сеть. В

отличие от маршрутизатора, подключение производится исключительно по кабелю, то есть, устройство не обеспечивает развертывание беспроводной сети. Собственно, в связи с этим на его панели и располагается большое количество стандартных сетевых разъемов RJ45.

На первый взгляд эта особенность может показаться минусом, так как подключение по Wi-Fi, во-первых, гораздо удобнее, а, во-вторых, позволяет использовать даже такое оборудование, которое не имеет порта для проводного подключения (смартфоны, ультрабуки). На практике же, коммутаторы существуют параллельно с маршрутизаторами и решают несколько другие проблемы. В частности, они могут использоваться:

Для организации сетевого подключения в тех случаях, когда требуется высокая стабильность и скорость, которую не всегда могут обеспечить беспроводные сети.

При подключении большого числа пользователей, например, в крупном офисе, где Wi-Fi сеть может быть «зашумлена».

При создании системы видеонаблюдения с большим количеством камер, передающих изображение на один основной компьютер.

На промышленных объектах, например, для подключения серии датчиков на разных этапах техпроцесса и сбором данных с них на диспетчерском пульте.

Для использования провайдерами в качестве центрального узла при подключении отдельных абонентов к единому интернет-каналу, подведенному к многоквартирному дому.

Это далеко не полный список возможных вариантов. Например, в нем отсутствует использование в домашней сети, когда портов на роутере не достаточно для подключения всех основных устройств по проводу. Использовать сетевой свитч можно и в этом случае, но чаще всего здесь ему на смену приходит концентратор или, как его еще называют, хаб. На самом деле, в

контексте данного материала разница между ними не очень важна, но именно на ней можно проще всего объяснить, за что отвечает коммутатор.

Визуально, как и хаб, он отвечает за подключение нескольких устройств к одной сети, однако «внутри», на уровне логики передачи сигнала, он работает иначе.

В локальной сети все данные передаются кадрами (фреймами) – условными единицами информации, состоящими из двух частей: «кусочка» передаваемого файла и сервисной информации (в частности адреса «получателя»). В итоге из серии фреймов и формируется непрерывный поток – трафик. Самый простой пример – изображение с камеры наблюдения, транслируемое на пульт охраны.

Сетевой коммутатор или хаб в данном случае играют роль промежуточного звена, усиливающего сигнал и перенаправляющего кадры от передающего устройства к конкретному получателю. Подобный процесс именуется forwarding или, по-русски, ретрансляция.

Хаб принятый с одного из портов кадр ретранслирует на все остальные порты, «не разбираясь», кому он на самом деле предназначен, поскольку конечное устройство по сервисным данным само определит, нужно ему обработать поступивший фрейм или можно его проигнорировать. Основным минусом в данном случае является загрузка каналов «лишними» данными и сопутствующее снижение пропускной способности, возрастающее вместе с числом подключенных устройств, потому как к каждому из них постоянно будет направляться непрерывный поток кадров. Во многом по этой причине максимальное количество портов на хабе ограничивается 12.

Коммутатор можно назвать более «умным» устройством. В его внутренней памяти содержится матрица MAC-адресов всех подключенных устройств. Изначально она пуста, но во время работы автоматически заполняется, позволяя свитчу точно знать, к какому порту, какое устройство в данный момент

подключено. Соответственно, при ретрансляции данных каждый фрейм не передается одновременно на все порты, а направляется исключительно от источника к получателю, не нагружая остальные каналы. Таким образом можно получить существенный прирост скорости передачи данных, а точнее, избежать ее ненужного падения даже при большом количестве клиентов и внушительных объемах передаваемых данных. Число стандартных RJ45-портов в свитчах может достигать 48, но во многих случаях одними ими узел не ограничивается и также оснащается дополнительными типами разъемов для подключения, например, оптического кабеля.

4. Проводные средства для передачи информации (витая пара, оптическое волокно).

Коаксиальный кабель представляет собой провод, состоящий из медной жилы и металлической оплетки. Между жилой и оплеткой имеется слой изоляции, защищающий от короткого замыкания жилы и оплетки. Жила служит для передачи данных, оплетка же обеспечивает защиту передаваемых данных от внешних электромагнитных помех. Снаружи кабель покрыт непроводящим слоем из резины. Примером коаксиального кабеля может служить кабель, который используется для подключения внешней антенны к телевизору.

Существует два типа коаксиальных кабелей:

- тонкий коаксиальный;
- толстый коаксиальный.

Тонкий коаксиальный кабель имеет диаметр около 0,5 см и подключается непосредственно к сетевым адаптерам компьютера. Тонкий коаксиальный кабель из-за затухания сигнала обеспечивает передачу данных только до 200 м.

Для подключения тонкого кабеля используются следующие разъемы:

1) BNC-коннектор;

2) Т-коннектор;

3) BNC-терминатор.

К разъему на плате сетевого адаптера подключается Т-коннектор. К Т-коннектору с обеих сторон подключаются BNC-коннекторы, которые связаны с коаксиальным кабелем. При применении коаксиального кабеля электрические сигналы распространяются от одного конца кабеля к другому. Достигая конца кабеля, сигнал отражается, что мешает другим компьютерам осуществлять передачу. Поэтому, после того как данные достигнут адресата, электрические сигналы необходимо погасить. Для этого на концах кабеля устанавливают специальные BNC-терминаторы.

Если необходимо увеличить размер сети, то для соединения отрезков кабеля можно использовать баррел-конвектор (barrel connector) или репитер. Репитер в отличие от коннектора усиливает передаваемый сигнал.

Толстый коаксиальный кабель имеет диаметр около 1 см. Обладает той особенностью, что благодаря, использованию более толстой жилы, обеспечивает передачу данных на расстояние до 500 м. Для подключения к толстому коаксиальному кабелю применяется специальное устройство - трансивер.

Трансивер для подключения к толстому кабелю снабжен специальным разъемом, называемым «зуб вампира»(vampire tap). Этот зуб проникает сквозь изоляцию провода и соприкасается с жилой.

Витая пара. Неэкранированная витая пара состоит из двух изолированных перевитых вокруг друг друга медных проводов. Завивка проводов позволяет избавиться от электрических помех. Максимальная длина неэкранированной витой пары составляет 100 м.

Неэкранированная витая пара разделена на следующие категории:

категория l-традиционный телефонный кабель, по которому передается только голос, но не данные;

категория 2 - кабель, способный передавать данные со скоростью до 4 Мбит/сек и состоящий из 4-х витых пар;

категория 3 - кабель, способный передавать данные со скоростью до 10 Мбит/сек и состоящий из 4-х витых пар с девятью витками на метр;

категория 4 - кабель, способный передавать данные со скоростью до 16 Мбит /сек и состоящий из 4-хвитых пар;

категория 5 - кабель, способный передавать данные со скоростью до 100 Мбит /сек, и состоящий из 4-х витых пар медного провода. Кабель данной категории используется в современных информационных сетях.

Кабель экранированной витой пары имеет медную оплетку, которая обеспечивает дополнительную защиту от помех. Следовательно, экранированная витая пара обеспечивает передачу данных на большее расстояние и с большей скоростью.

Для подключения экранированной и неэкранированной витой пары к компьютеру используются коннекторы RJ-45, которые похожи на телефонные RJ-11, но отличаются по размерам и числу контактов. Коннектор RJ-45 чуть больше по размеру и имеет восемь контактов, а RJ-l1 - только четыре.

Отличительная особенность использования витой пары состоит в том, что каждый компьютер к информационной сети должен подключаться с помощью отдельного кабеля. Общая схема Подключения представлена в Приложении 7

Для создания быстродействующих компьютерных сетей в настоящее время стал широко использоваться оптоволоконный кабель. В нем цифровые данные передаются в виде модулированных световых импульсов. Оптоволоконная линия состоит из световода - оптической жилы, покрытой слоем стекла

(оболочкой). Каждое стеклянное оптоволокно передает сигналы только в одном направлении, поэтому кабель, соединяющий компьютеры, состоит из двух волокон с отдельными коннекторами. Одно из них служит для передачи данных, другое - для приема Оптоволоконный кабель по сравнению с электрическими обладает следующими преимуществами:

- высокая помехозащищенность;
- высокая скорость передачи данных (до 200 Мбит /сек); - большая протяженность линии (до нескольких километров);
- безопасность передачи информации, так как к оптоволоконному кабелю сложно подключиться для перехвата передаваемой информации.

5. КШ оборудование ТЕЛКОМ относящихся
TL-9.6.3-П.7035Ш 9U 600x350x490мм
6. КШ ШТН-4U 600x240x450
7. Проставленное коммутатор организацией существует серверное корзина оборудование можно
8. Предоставленный компанией межсетевой экран .

Межсетевой экран (МЭ, брандмауэр, Firewall) — это программа или программно-аппаратный комплекс (аппаратный межсетевой экран), который служит для контроля сетевых пакетов. МЭ отслеживает сетевые пакеты, блокирует или разрешает их прохождение с помощью установленных специальных правил. Основное назначение межсетевых экранов — ограничить транзит трафика, установку нежелательных соединений и т. д. за счет средств фильтрации и аутентификации.

Не так давно на рынке средств ИБ появились межсетевые экраны нового поколения (Next-Generation Firewall, NGFW), которые кроме основных функций брандмауэра имеют еще и дополнительные функции, такие как:

- контроль приложений;
- DPI (Deep Packet Inspection, проверка пакетов на уровне приложений);
- IPS (предотвращение вторжений);
- веб-фильтрация (контроль URL-адресов, к которым обращаются пользователи);
- аутентификация пользователей.

В связи с развитием программы импортозамещения и уходом некоторых зарубежных компаний из нашей страны, на рынке появились отечественные модели МЭ, которые соответствуют всем современным критериям качества.

При выборе МЭ для своей компании следует рассмотреть также такие факторы, как наличие сертификатов ФСТЭК, ФСБ и Минобороны РФ. Ведь для выполнения некоторых задач (к примеру, для работы с государственными системами или на объектах критической информационной инфраструктуры — КИИ) важно установить именно сертифицированный межсетевой экран.

9. И ИБП IPPON Smart Winner New Edition 1000

Источник Бесперебойного Питания (ИБП) – это оборудование, оснащенное преобразователем постоянного тока в переменный и встроенной аккумуляторной батареей. Особенность подобных агрегатов заключается в том, что они имеют как минимум два ввода от первичных источников питания и способны переключаться между ними. Кроме того, по мере прохождения по проводникам ток выравнивается до приемлемых значений, что очень важно для «капризной» домашней или офисной техники. Большинство ИБП обладает несколькими выводами – от двух до шести, для подключения нескольких устройств одновременно.

Для чего нужен ИБП

Нормальной работе домашней или бытовой технике чаще всего мешают именно кратковременные перерывы в подаче электроэнергии, когда счет идет на доли секунды. В таких случаях требуется мгновенное подключение альтернативного

источника питания. Для этого и используют ИПБ. Но у него имеются и другие функции:

- выравнивание входного/выходного напряжения;
- фильтрация подаваемого тока, снижение помех;
- защита от короткого замыкания или перегрузки.

Следует отметить, что мощность батареи ограничена компактными размерами устройства, поэтому срок автономной работы не превышает 4-15 минут (в зависимости от модели, мощности агрегата).

Конструкция и характеристики

Бытовые ИБП выглядят как небольшой пластиковый короб. На нем размещаются кнопки питания (у продвинутых моделей это может быть полноценная панель управления с жидкокристаллическим дисплеем), индикаторы, вентиляционные решетки и несколько штепсельных розеток. На корпусе также могут находится интерфейсы для подключения сторонних устройств. Промышленные агрегаты-бесперебойники имеют большие габариты, могут оснащаться металлическим корпусом, выносным блоком управления. Внутри оборудования обычно находятся:

- Электронакопитель. Это могут быть свинцово-кислотные, никелево-кадмиевые (или менее распространенные никелево-металлогидридные) литий-ионные батареи. Эффективность бесперебойника на 30% зависит от характеристик АКБ – емкости, самопотери заряда, количество циклов, глубины разряда, диапазона рабочих температур.
- Инвертор – для преобразования постоянного напряжения в переменное и наоборот.
- Изолирующие трансформаторы. Обычно их два – входной/выходной, для обеспечения гальванической развязки между входом и выходом ИБП.

- Стабилизатор для выравнивания показателей переменного напряжения.
- Интерфейс для контроля и управления состоянием источника бесперебойного питания. Производители поставляют программное обеспечение, которое позволяет мониторить и анализировать возникающие ситуации. Обычно оно устанавливается на компьютер, а на корпусе устройства размещается порт для подключения.

  В некоторых случаях в ИБП устанавливают THD-фильтры для уменьшения влияния на напряжение в сети питания, особенно если коэффициент нелинейных искажений свыше 3-5%. Также могут монтировать блок байпаса для питания «очищенным» напряжением, без затрагивания главной схемы бесперебойника.

  При выборе стоит обратить внимание на следующие ключевые характеристики ИБП:

  - Выходная мощность. Основной критерий, измеряется в ваттах или вольт-амперах и показывает допустимую максимальную нагрузку. Должна с запасом покрывать потребляемую мощность подключенных устройств.
  - Время переключения на АКБ. Единица измерения – миллисекунды. Показатель варьируется от 0 до 15 с.
  - Время автономной работы. Определяется в минутах и в среднем составляет 4-20 мин. Для промышленного оборудования срок увеличивается до 30-45 мин. Дополнительный плюс некоторых моделей – возможность установки батарей с увеличенной емкостью.
  - Входное напряжение. Чем больше диапазон – тем меньше переходов с сети на батарею + дольше срок службы устройства.
  - Преобразование выходного напряжения при колебаниях входного. Каким бы не было входящее напряжение, на выходе оно должно быть в пределах

нормы. Повышенный или пониженный вольтаж одинаково опасен для подключенных приборов.

- Действия при перегрузках. Когда бесперебойник работает на АКБ и происходит скачок напряжения, прибор должен автоматически выключаться. Желательно наличие световой или звуковой индикации.
- Фазность. Встречаются одно- и трехфазные модели.
- Регулировка частоты. Параметр актуальный для онлайн ИБП. Частота питающего напряжения имеет большое значение для аудиоустройств, лабораторного или медицинского оборудования.
- Возможность холодного старта. Полезная функция, позволяющая запустить ИБП даже при обесточенной сети, для кратковременных действий с подключенными устройствами.
- Срок службы. Зависит от типа АКБ, качества материалов, сборки. Минимальный показатель (для изделий со свинцовыми батареями) – 2-3 года, в среднем – 5-10 лет.

Некоторые параметры зависят от исполнения корпуса ИБП – настольный, напольный, в стойку или универсальный, а также от размещения АКБ – внешнее или внутреннее.

1.5 Характеристики качества обслуживания информационных сетей

Один из ключевых факторов, который должен учитываться в процессе проектирования сетей связи, в частности, даже сетей следующего поколения (ССП, NGN – Next Generation Network) заключается в обеспечении качества обслуживания. Специфика пакетных сетей заключается в их способности к

передаче в одном и том же информационном потоке разнородного трафика. Этим они принципиально отличаются от сетей с коммутацией каналов. При этом для каждого из типов трафика характерна совокупность своя совокупность параметров, как критичной значимости, так и некритичной. Чтобы передавать, например, голосовой трафик, через пакетные сети введено понятие классов обслуживания, которые дают возможность оценки качества предоставления услуг в пакетной сети.

Безусловно, определение качества обслуживания в сети сейчас носит субъективный характер. В основе этого определения лежит применение метода экспертных оценок, что делает фактически невозможной абсолютную гарантию заложения в ходе проектирования сети сетевых характеристик, однозначно обеспечивающих необходимое качество. Вместе с тем, пакетные сети обладают достаточно развитыми механизмами обеспечения качества обслуживания, применение которых оказывает положительное влияние на предоставление услуг связи в процессе эксплуатации .

Суть функций качества обслуживания (QoS) состоит в обеспечении дифференцированного и гарантированного обслуживания трафика сети с помощью делегирования контроля за использованием ресурсов и загруженностью сети ее оператору. QoS включает в себя совокупность требований, которые предъявляются к сетевым ресурсам в процессе передачи потока данных. Благодаря QoS достигается сквозная гарантия передача данных и мониторинг средств увеличения производительности IP-сети, в частности, механизма распределения ресурсов, механизмов отбрасывания пакетов, коммутации, маршрутизации, механизмов обслуживания очередей. Данный мониторинг основывается на определенной системе правил.

Целесообразно привести ключевые достоинства качества обслуживания.

– обеспечение поддержки существующих и только появляющихся служб и приложений мультимедийного типа;

– возможность для провайдеров услуг Internet предоставлять клиентам дополнительные услуги вместе с основной услугой, заключающейся в доставке данных без определенных гарантий (иначе говоря, предоставлять услуги согласно так называемому классу обслуживания – Class of Service, CoS);

– существенная роль в развитии актуальных сетевых технологий, например, виртуальных частных сетей (Virtual Private Network – VPNs);

– делегирование контроля сетевых ресурсов и их использования сетевому оператору. Предоставление гарантий, связанных с обслуживанием и дифференциации трафика сети. Данный аспект относится к обязательным для объединения видео/аудиотрафика с трафиком приложений в рамках одной IP-сети.

Классификация возможности сети реализовывать различные уровни обслуживания, которые запрашиваются различными сетевыми приложениями, вместе с обеспечением мониторинга за параметрами производительности – задержкой/дрожанием, полосой пропускания – может быть выполнена в соответствии с тремя нижеперечисленными категориями:

1. Негарантированная доставка данных (best-effort service). В этом случае обеспечивается связность узлов, при этом определенное время и вообще сам факт доставки пакета получателя не гарантируются. Операция отбрасывания пакета возможна только при переполнении буфера входной или выходной очереди маршрутизаторов.

2. Дифференцированное обслуживание (differentiated service). При данном виде обслуживания осуществляется разделение трафика на классы в соответствии с требованиями к качеству обслуживания. Для каждого класса трафика выполняется обработка и дифференцирование сетью согласно определенным для данного класса механизмам QoS. Такая схема обеспечения качества обслуживания часто именуется схемой CoS.

Необходимо учитывать, что при дифференцированном обслуживании вообще говоря речь не идет об обеспечении гарантий предоставляемых услуг.

Данная схема подразумевает распределение трафика в соответствии с классами, каждый из которых обладает своим собственным приоритетом. Именно поэтому дифференцированное обслуживание имеет второе название – мягкий QoS (soft QoS). Подобный вид обслуживания наиболее эффективен в сетях, трафик приложения в которых характеризуется высокой интенсивностью.

3. Гарантированное обслуживание (guaranteed service). В этом случае речь идет о резервировании ресурсов сети для обеспечения требований специфического характера к обслуживанию со стороны потоков трафика.

Механизм гарантированного обслуживания осуществляет предварительное резервирование ресурсов сети по всему маршруту прохождения трафика. Такой вид обслуживания часто называют жестким QoS (hard QoS) из-за наличия строгих требований, предъявляемым к сетевым ресурсам. Необходимо с сожалением констатировать, что осуществление резервирования ресурсов на всем маршруте прохождения отдельных потоков трафика не представляется возможным в масштабах магистрали Internet, осуществляющей в отдельный временной промежуток обслуживание тысяч потоков данных.

Реализация механизмов QoS подразумевает необходимость обеспечения со стороны сети соединения, на которое накладывается ряд ограничений, связанных с производительностью. В качестве ключевых характеристик производительности сетевого соединения выступают полоса пропускания, дрожание, задержка и уровень потери пакетов.

Термин «полоса пропускания» (bandwidth) применяется для выражения номинальной пропускной способности среды передачи информации, соединения или протокола [3].

Чаще всего любое соединение, которому необходимо гарантированное качество обслуживания, предъявляет к сети требования, связанные с резервированием минимальной полосы пропускания. Например, приложения, в

которых осуществляется передача оцифрованной речи, формируют поток информации, интенсивность которого составляет 64 Кбит/с. Такие приложения практически невозможно использовать с необходимой эффективностью при уменьшение полосы пропускания ниже данной величины на каком-нибудь участке соединения.

Задержка при передаче пакета (packet delay), либо латентность (latency) на каждом из переходов включает в себя задержку сериализации, задержку распространения и задержку коммутации. Ниже подробнее описаны все перечисленные виды задержек.

Под задержкой сериализации (serialization delay) принято понимать время, необходимое устройству для осуществления передачи пакета при определенной ширине полосы пропускания. На данный вид задержки оказывают влияние как ширина полосы пропускания канала передачи информации, так и размер передаваемого пакета. Например, для передачи пакета, размер которого 128 байт, при заданной полосе пропускания 3 Мбит/с составит всего 342 нс. Влияние на задержку сериализации полосы пропускания на самом деле очень значительно. Время передачи того же самого пакета в 64 байта с заданной полосой пропускания 38,4 Кбит/с составит уже 52 мс. Задержка сериализации может еще называться задержкой передачи (transmission delay).

Временной интервал, необходимый переданному биту информации для достижения устройства-приемника на другом конце канала, называется задержкой распространения (propagation delay). Данная величина достаточно важна, так как в самом лучшем случае скорость передачи информации можно сопоставить со скоростью света. На величину задержки распространения оказывают непосредственное влияние расстояние и используемая среда передачи информации, а не полоса пропускания. В линиях связи глобальных сетей порядок задержки распространения составляет миллисекунды. Например, в трансконтинентальных сетях США данная задержка составляет 45 мс.

Наконец, задержка коммутации (switching delay) представляет собой промежуток времени, требующийся устройству, которое получило пакет, для начала его транспортировки следующему устройству. Величина данного значения обычно не превышает 12 нс.

Каждый из пакетов, входящий в тот или иной поток трафика, передается с разным значением задержки. Изменение задержки при передаче пакетов происходит в соответствии с состоянием промежуточных сетей.

В случае отсутствия в сети перегрузок в маршрутизаторах не происходит постановка пакетов в очередь, соответственно общее время задержки при передаче пакета складывается из суммы задержки сериализации и задержки распространения на каждом из промежуточных переходов. В такой ситуации можно утверждать, что задержка при передаче пакетов через заданную сеть является минимально возможной. Следует учитывать, что если пропускная способность канала велика, то величина задержки сериализации рассматривается как незначительная в сравнении с задержкой пакета при передаче .

В случае перегрузки сети задержки, связанные с организацией очередей в маршрутизаторах, начинают оказывать значительное влияние на суммарную задержку при передаче пакетов. Результатом такой ситуации является появление разницы в задержке в ходе передачи различных пакетов, принадлежащим одному и тому же потоку. Колебание задержки при передаче пакетов стало называться джиттер-пакетов (oacket-jitter).

Значимость данного параметра достаточно велика, так как именно он характеризует наибольшую (максимальную) задержку в ходе приема пакетов на стороне конечного приемника. Принимающая сторона, в соответствии с типом используемого приложения, может сделать попытку компенсации дрожания пакетов путем организации приемного буфера для хранения принятых пакетов на временной интервал, меньший или равный наибольшему значению дрожания.

Такими возможностями обладают приложения, предназначенные для передачи/приема потоков данных в непрерывном режиме, в частности, IP-телефония или приложения, выполняющие обеспечение проведения видеоконференций.

1.6 Регулирование выделения полосы пропускания в каналах передачи данных локальных сетей

Требуемое качество обслуживания обеспечивается с помощью использования так называемой архитектуры интегрированных услуг (IntServ, Integrated Service, RFC 1633). Она способна обеспечить сквозное (End-to-End) качество обслуживания с гарантией требуемой пропускной способности . Для достижения этих задач в IntServ применяется протокол сигнализации RSVP. Также IntServ дает возможность приложениям выражать сквозные требования к ресурсам. Данная архитектура включает в себя механизмы, ориентированные на выполнение этих требования. Наиболее точной краткой характеристикой IntServ является «резервирование ресурсов» (Resource reservation). Далее целесообразно остановиться на описание протокола RSVP.

Этот протокол обеспечивает отправку приложениями сигналов в сеть, касающихся своих QoS-требований, для каждого из потоков. Для определения количественных характеристик данных требований, для управления доступом, применяются служебные параметры.

Применение протокола RSVP наиболее эффективно в приложениях, осуществляющих групповую рассылку. К таким, например, относятся приложения аудио- и видеоконференций. Однако, несмотря на первоначальную ориентацию протокола RSVP на трафик мультимедийного типа, он позволяет выполнять резервирование полосы пропускания для однонаправленного трафика, например для управляющего трафика виртуальных частных сетей

(Virtual Private Network – VPN) и трафика сетевой файловой системы (Network File System – NFS).

Выдача сигналов, касающихся запросов резервирования ресурсов, осуществляется протоколом RSVP по существующему доступному маршрутизируемому сетевому пути. Следует отметить, что в протоколе RSVP не предусмотрена собственная маршрутизация. Наоборот, при разработке данного протокола предполагалось использование других, являющихся более мощными, протоколов маршрутизации. Аналогично любому другому IP-трафику, путь для данных и управляющего трафика определяется в протоколе RSVP с помощью используемого в конкретной сети протокола маршрутизации.

Протокол RSVP применяется конечными системами для запрашивания у сети требуемого уровня QoS от имени потока данных приложения. Далее осуществляется передача RSVP-запросов по сети при прохождении каждого узла, используемого для передачи потока. При этом протоколом RSVP делаются попытки резервирования ресурсов для потока данных на каждом из данных узлов.

С помощью маршрутизаторов, поддерживающих протокол RSVP, требуемые потоки данных доставляются в определенную точку назначения. На Рисунок представлены ключевые модули, информация о потоке данных и информация об управляющих потоках маршрутизатора и клиента, поддерживающих протокол RSVP.

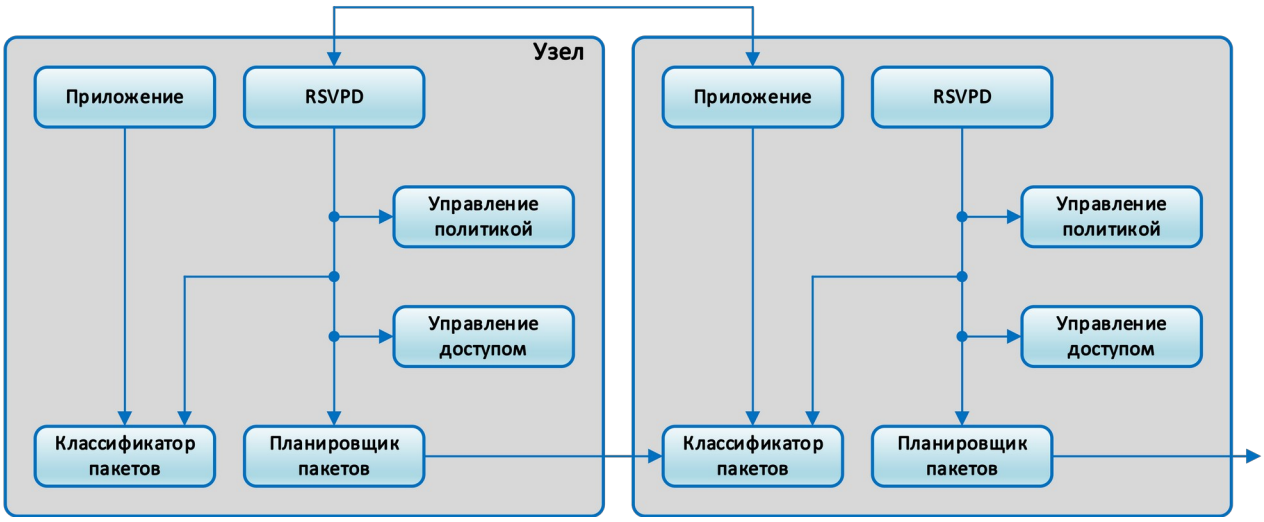


Рисунок 5 – Ключевые модули RSVP

Перед, непосредственно, резервированием ресурсов, осуществляется соединение RSVP-демона маршрутизатора с двумя модулями принятия решений локального типа. Они называются: модуль управления доступом (admission control) и модуль управления политикой (policy control). Модуль управления доступом выполняет проверку, обладает ли узел достаточным объемом свободных ресурсов для обеспечения необходимого (запрошенного) уровня QoS. Соответственно, модуль управления политикой проверяет пользователя на наличие прав, необходимых для выполнения резервирования. В случае отрицательного результата хотя бы одной из проверок RSVP-демоном осуществляется отправка сообщения процессу приложения, являющемуся источником данного запроса об ошибке.

Если проверки пройдены успешно, RSVP-демон выполняет установку параметров классификатора пакетов (packet classifier) и планировщика пакетов (packet scheduler) для формирования необходимого уровня QoS. Далее классификатором пакетов определяется класс QoS для каждого из пакетов. Планировщик пакетов выполняет передачу пакетов в соответствии с определенным классом QoS. На уровне планировщика поддержка QoS обеспечивается взвешенным алгоритмом равномерного обслуживания очередей

(Weighted Fair Queuing – WFQ) и взвешенным алгоритмом произвольного раннего обнаружения (Weighted Random Early Detection – WRED).

Следует отметить, что в ходе процесса принятия решения модулем управления доступом резервирование затребованной полосы пропускания осуществляется исключительно при выполнении условия, касающегося достаточности оставшейся части для запрашиваемого класса трафика. Если ее недостаточно, производится отклонение запроса на доступ, однако при этом все равно происходит передача трафика, а качество обслуживания соответствует определенному по умолчанию для трафика данного класса.

Достаточно часто, даже в случае отклонения запроса на доступ на одном или более маршрутизаторах, у модуля еще существует возможность обеспечения реализации необходимого качества обслуживания. Это достигается путем установки резервирования на перегруженных маршрутизаторах. Такая возможность обусловлена тем, что другими потоками может не в полной мере использоваться заказанная ими полоса пропускания.

Вообще говоря, весь процесс, связанный с установкой резервирования, может быть разделен на несколько (конкретно, пять) отдельных этапов:

– этап 1: выполняется посылка управляющих сообщений RSVP PATH отправителями (передатчиками) данных по тому же маршруту, по которому ими выполняется отправка обычного трафика с данными. Эти сообщения содержат в себе описание данных, уже отправляемых или находящихся в очереди на отправку;

– этап 2: каждым RSVP-маршрутизатором осуществляется перехват PATH сообщения. Выполняется сохранение IP-адреса предыдущей точки назначения, вместо него записывается свой адрес, после чего обновленное сообщение отправляется далее по тому же маршруту, по которому происходит передача данных приложения;

– этап 3: станциями получателя (приемника) производится выбор подмножества сеансов, для которых ими была получена PATH-информация. После этого они делают запрос на резервирование ресурсов у предыдущего маршрутизатора с помощью RSVP RESV-сообщения. Маршрут RSVP RESV-сообщений проходит от получателя к отправителю, то есть является противоположным маршруту, который проходят RSVP PATH-сообщения;

– этап 4: RSVP-маршрутизаторами определяется возможность выполнения (удовлетворения) данных RESV-запросов. В случае отрицательного ответа осуществляется отказ в резервировании. Если же возможность существует, RSVP-маршрутизаторами производится объединение полученных запросов на резервирование с последующей передачей запроса предыдущему маршрутизатору;

– этап 5: после получения запросов на резервирование от соответствующих маршрутизаторов, отправителями факт резервирования ресурсов принимается состоявшимся. Другими словами, для реального резервирования ресурсов используется механизм RESV-сообщений.

Схема механизма RSVP-резервирования представлена на Рисунок .

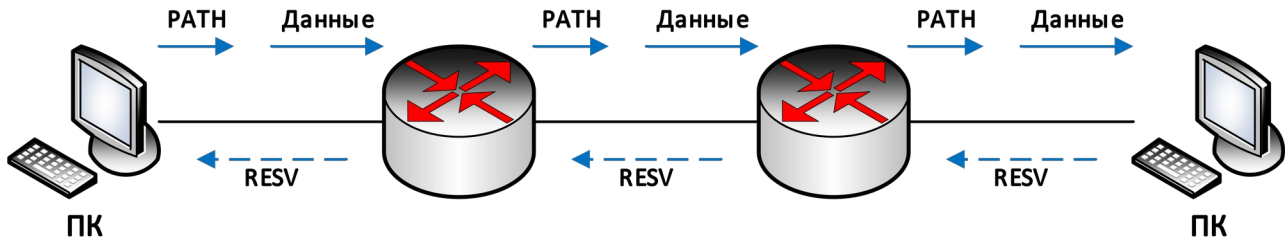


Рисунок 6 – Схема механизмов RSVP-резервирования ресурсов

Необходимо перечислить все RSVP-компоненты и выполняемые ими функции:

– RSVP-отправитель (RSVP-sender) – представляет собой приложение, которое является инициатором отправки трафика в RSVP-сеансе. Спецификации

потока, возможность передачи которых RSVP-отправителями по RSVP-сети существует следующие: средняя скорость передачи данных; наибольший (максимальный) размер всплеска;

Необходимо сказать, что по сети, в состав которой входят RSVP-совместимые маршрутизаторы (RSVP-enabled router network), осуществляется прокладка пути между RSVP-отправителями и RSVP-получателями (источниками и приемниками).

– RSVP-получатель (RSVP-receiver) – является приложением, получающим трафик в ходе RSVP-сеанса. ВО время проведения конференций и в процессе передачи голоса по протоколу IP (Voice over IP – VoIP) приложение выступает и в роли RSVP-отправителя, и в роли RSVP-получателя. Целесообразно представить спецификации потока, являющиеся доступными для передачи RSVP-получателями по сети: средняя скорость передачи данных; наибольший (максимальный) размер всплеска; QoS, в том числе: обслуживание с управляемой нагрузкой, при котором маршрутизаторами гарантируется исключительно минимизация сетевых задержек; гарантированное обслуживание, при котором в PATH-сообщениях осуществляется описание максимально возможных задержек в сети.

RSVP-резервирование ресурсов для потока включает в себя два ключевых типа, а именно: индивидуальное и общее.

Применение индивидуального резервирования (distinct reservations) целесообразно в приложениях, в которых существует возможность одновременной отправки информации несколькими источниками данных. Например, в видеоприложениях каждым отправителем осуществляется генерация индивидуального потока данных. В этом случае появляется необходимость обеспечения отдельного управления доступом и планирования очереди на протяжении всего пути к получателю. Таким образом, для подобного потока необходимым является отдельное резервирование ресурсов для каждого из отправителей и для каждого из каналов в пути.

В качестве наиболее простого случая применения индивидуального резервирования можно привести приложение с одноадресным трафиком, содержащее только одного отправителя и только одного получателя.

Применение общего резервирования (shared reservations) характерно для приложений, в которых у источников данных нет склонности к передачи информации в одновременном режиме. Такими, например, являются цифровые аудиоприложения, приложения VoIP. В них, поскольку в любой отдельно взятый временной интервал разговор осуществляется небольшим количеством людей, передача информации производится только небольшим, ограниченным количеством отправителей. В подобном потоке отсутствует необходимость в отдельном резервировании ресурсов для каждого из отправителей. Он нуждается только в одном резервировании, которое, в случае возникновения необходимости, может быть применено к любому отправителю, входящему в группу.

Используя термины протокола RSVP, такой поток называют общим потоком (shared flow). Для его установки достаточно группового или общего явного резервирования. При этом существуют следующие стили резервирования:

– в случае общего явного (Shared Explicit – SE) резервирования необходимо отдельное указание потоков, резервирующих сетевые ресурсы;

– использование группового фильтра (Wildcard Filter – WF) делает возможным резервирование полосы пропускания и характеристик задержек для любого отправителя. Вместе с тем, использование подобного фильтра исключает возможность задание отправителей в отдельном режиме – он принимает всех отправителей. Об этом, в частности, свидетельствует установка фильтром в ноль адреса источника и порта.

В протоколе RSVP предусмотрено два типа интегрированных услуг, доступных для получателей с помощью отправки сообщений RSVP RESV.

Первая услуга – это служба регулируемой нагрузки, вторая называется службой битовой скорости.

Служба регулируемой нагрузки (controlled load service) необходима для обеспечения гарантии достижения зарезервированным потоком своего пункта назначения, при этом вмешательство со стороны трафика, доставка которого осуществляется без подобных гарантий, является минимальным. Кроме этого, некоторые реализации, например, от компании Cisco, предусматривают изоляцию отдельных зарезервированных потоков. Благодаря изоляции потока, очевидно, исключается влияние на резервирование ресурсов других находящихся в сети зарезервированных потоков.

Чаще всего применение службы регулируемой нагрузки наблюдается в процессе передачи трафика Internet-приложений, обладающих чувствительностью к перегрузкам в сети. Подобные приложения функционируют в штатном режиме в сетях, загрузка которых достаточно низка, однако сразу сигнализируют об определенных проблемах в случае перегрузки сети. В качестве примера можно упомянуть приложение, функционирующее по протоколу FTP (File Transfer Protocol – протокол передачи файлов).

Служба гарантированной битовой скорости (guaranteed bit rate service) необходима для обеспечения ограничения задержки без задействования механизма отбрасыванию дейтаграмм, которые соответствуют характеристикам трафика, в условиях, когда отсутствуют сбои в функционировании сетевых компонентов, а информация, касающаяся маршрутов, является неизменной в течение жизненного цикла потока. Благодаря работе данной службы гарантируется наименьшее влияние, оказываемое трафиком, доставка которого осуществляется без каких-либо гарантий, изоляция (отделение) зарезервированных потоков и числовое выражение наибольшей задержки.

Необходимо учитывать, что служба гарантированной битовой1 скорости обладает возможностью обеспечения исключительно максимальной, а не минимальной или средней задержки дейтаграмм.

В данном случае под наибольшей (максимальной) задержкой очереди следует понимать кумулятивную задержку передачи PATH-сообщения от отправителя до приемника. В PATH-сообщение включается информация, касающаяся задержки на всей протяженности маршрута от отправителя, и в любой момент времени приемник может выполнить ее точную оценку. В частности, информация о задержке может быть использована приемником во время запроса гарантированного обслуживания.

Наиболее целесообразно применение службы гарантированной битовой скорости для приложений, функционирующих в режиме реального времени, то есть дающих возможность воспроизведения видео- и аудиофайлов.

Следует также отметить, что службами регулируемой нагрузки и гарантированной битовой скорости для описания характеристик потока данных используется так называемая корзина маркеров.

Корзина маркеров является механизмом, осуществляющим регулирование интенсивности трафика, определяющим следующие характеристики: средняя скорость (средний объем данных, который может быть передан в единицу времени); квант времени (интервал измерения); размер всплеска (объем данных, который может быть отправлен в течение определенного временного интервала без нанесения ущерба процессу планирования очереди).

В случае необходимости использования обеих служб приемнику необходимо осуществить запрос посредством RESV-сообщения определенной битовой скорости и размера всплеска. Со стороны планировщика WFQ и механизма управления очередью WRED с предпочтительным весом гарантируется достижение трафиком получателя через строго определенный временной интервал.

1.7 Причины возникновения конфликтов и методы их предупреждения

К сожалению, даже использование такого современного протокола, как RSVP, не защищает от возможности возникновения различных конфликтов и коллизий. На данном этапе развития отсутствуют полностью эффективные методы организации доступа к общему разделяемому каналу передачи данных. Ключевой проблемой с точки зрения доступа к каналу можно считать появление конфликтов доступа к общему ресурсу.

Суть механизма возникновения подобного конфликта состоит в непреднамеренной (случайной) передаче сигнала по общему разделяемому каналу в одновременном режиме. Результатом такой ситуации является наложение передаваемых сигналов и искажение передаваемых данных. Следовательно, можно говорить об аналоговом характере подобного конфликта. Действительно, факт его появления поддается фиксации исключительно на физическом уровне. Известно, что на физическом уровне сетевой модели рассматриваются цифровые сигналы, поэтому на способность эффективного выявления повреждения информации непосредственное влияние оказывает выбранный метод (алгоритм) ее цифрового кодирования. Однако, физический уровень не позволяет осуществлять устранение конфликтов доступа с высокой степенью эффективности, следовательно, вся информация, касающаяся конфликта, с помощью jam-последовательности передается на канальный уровень. Именно на нем целесообразна организация разрешения конфликта, причиной которого является одновременное обращение к общему ресурсу [1].

На канальном уровне выполняется оперирование кадрами. При обнаружении переданной jam-последовательности осуществляется фиксация факта возникновения конфликта в так называемом коллизионном домене. На рассматриваемом уровне (канальном) применяются специализированные

протоколы доступа к домену коллизий. Как известно, возникновение коллизии прямо связано с неспособностью протокола решить конфликт доступа к общему ресурсу. Чтобы устранять конфликты с высокой степенью эффективности должен существовать определенный набор правил, регламентирующий доступ к общему ресурсу (часто он называется методом доступа). Следует учитывать, что эффективность любого из методов высока только при наличии определенных условий.

Кроме того, на реализацию метода доступа необходимы достаточно высокие затраты ресурсов. Общепринятыми характеристиками любого сетевого протокола является количество ресурсов, которые необходимо затратить для реализации выбранных методов, а также предельное допустимое число коллизий в коллизионном домене. Поэтому, эффективность передачи находится в прямой зависимости от используемого протокола.

Действительно, возникновение конфликтов доступа к общему разделяемому ресурсу характерно для локальных информационных сетей, мультипроцессорных систем, кластерных систем, для общих шин, осуществляющих связывание контроллеров, а также для общих магистральных шин внутри коммутаторов.

Все факторы появления конфликтов могут быть разделены на следующие три ключевые группы: топологическая (характеристика физического канала передачи информации), временная (правила доступа к каналу), а также вероятностная (загруженность сети передачи данных, число узлов).

Топологическая группа факторов возникновения конфликтов включает в себя совокупность характеристик среды: физические параметры канала связи (протяженность передающей среды, задержка распространения сигнала); параметры структурного характера (логическая организация взаимодействия узлов, иерархичность, вырожденность); алгоритм кодирования цифровых сигналов (частотное/временное кодирование, статическое/динамическое).

Устранение данной группы факторов возникновения конфликтов достигается с помощью внесения изменений архитектурного и схемотехнического характера в структуру сетевого оборудования. Целесообразно привести пример топологической природы причин возникновения конфликтов, связанных с физическими характеристиками канала связи.

С точки зрения физики, в канале, обладающем значительными временными задержками, в процессе передачи сигналов на большие расстояния возникают дополнительные проблемы, относящиеся к распределению доступа к каналу. Причиной проблем является ситуация, при которой информация, относящаяся к использованию общего ресурса, становится доступной участникам в разные моменты времени. Результатом этого является возникновение конфликтных ситуаций, вызванных, в частности, слабой информированностью участников.

Следовательно, корректность функционирования многих методов доступа в таких каналах может оказаться весьма сомнительной, что и является причиной дополнительных конфликтов. Соответственно, для каналов, обладающих высокой скоростью (практически мгновенной) распространения единицы информации, подобные конфликты не являются характерными. Безусловно, каналов, обладающих мгновенной скоростью распространения сигналов на практике не существует. В каждом канале существует определенное время задержки ($t>0$).

Однако, в ситуации, когда значение t во много раз меньше значения времени передачи единицы информации по каналу, подобный канал может быть назван каналом, имеющим мгновенное распространение единицы информации. Следовательно, разрешение конфликтов доступа к общему ресурсу может быть достигнуто с помощью более простых методов. С точки зрения структуры сети, например, сетевая топология «шина» относится к конфликтным топологиям, тогда как «звезда» – нет. Применительно к используемому методу кодирования цифровых сигналов статическое временное распределение канала считается

бесконфликтным, тогда как динамическое временное распределение канала с поочередным доступом к общему ресурсу вполне способно к созданию, при определенных условиях, различных ситуаций конфликтного характера.

В результате практических исследований методов получения доступа к среде передачи данных было установлено, что для локальных сетей характерным является применение каналов связи, разделяемых между группой рабочих станций. Доступ к ним осуществляется в соответствии с определенным алгоритмом (чаще всего встречаются на практике метод случайного доступа, а также метод с передачей маркера доступа по кольцу). Для последних актуальных стандартов и технологий доступа локальных информационных сетей характерна тенденция к применению вместо разделяемой среды передачи данных механизма реализации индивидуальных каналов связи рабочих станций с коммуникационными устройствами сети.

Временная группа факторов, оказывающих непосредственное влияние на возникновение конфликтов, включает в себя параметры, от которых зависит реализация следующих правил доступа к каналу: захват канала, освобождение канала, обнаружение конфликтов, предотвращение конфликтов, устранение последствий конфликтов.

Чтобы устранить временные факторы возникновения конфликтов необходимым является корректирование реализации правил доступа и внесение изменений на микропрограммном уровне в контроллеры сетевого оборудования. В качестве примера временных факторов возникновения конфликтов можно привести следующий: на этапе борьбы за обладание свободным общим разделяемым каналом существует, очевидно, вероятность его одновременного захвата, что неизбежно повлечет за собой возникновение коллизии. В ходе распространения сигнала по каналу, обладающему определенными временными задержками, существует потенциальная возможность, связанная с попыткой доступа к занятому ресурсу, до момента донесения информации о статусе ресурса до всех пользователей. Далее, в процессе использования ресурса при

отсутствии ограничения на доступ к нему во время его использования могут последовать сбои в функционировании канала и, как следствие, потери важной информации.

Реализация принципа закрытия доступа к ресурсу после уведомления всех о его занятости, безусловно, исключает возникновение конфликтов на стадии использования ресурса. Определенный риск существует и на этапе освобождения ресурса при выборе обладающего малой эффективностью способе оповещения об освобождении ресурса.

Действительно, с увеличением задержки прихода такого оповещения понижается вероятность доступа к ресурсу некоторых, относящихся к наиболее удаленных от него в настоящее время пользователей. Помимо этого, должно приниматься во внимание время, которое необходимо затратить на выявление конфликта с последующим его разрешением, восстановление утерянных в ходе конфликта данных, возобновление передачи. И всегда необходимо помнить, что в любой момент времени за доступ к каналу могут спорить множество сетевых узлов.

2. ПРАКТИЧЕСКАЯ ЧАСТЬ

2.1. Общая характеристика компании ООО «Совинто»

Существующие на рынке программного продукта решения не отвечали возросшим требованиям МФЮА к полному и оперативному отражению в Системе данных об учащихся, их успеваемости, о нагрузке преподавателей, не обеспечивали удобный контроль своевременности оплаты договоров и дополнительных услуг, затрудняли контроль руководства за деятельностью деканатов, имевших неограниченный доступ к ведомостям. Основные проблемы возникали из-за большой численности учащихся и наличия большого числа территориально удаленных подразделений (учебных корпусов, филиалов, представительств).

В 2010г. руководство МФЮА приняло решение о заказе разработки и внедрении интегрированной автоматизированной информационной системы управления ВУЗом. К системе были сформулированы следующие требования:

· централизованный, единообразный и полный ввод данных в Систему о структуре организации, номенклатуре специальностей, учебных планах,

номенклатуре цен, личных данных и успеваемости студентов, о преподавателях;

· отказ от бумажного документооборота и создание системы централизованного электронного документооборота с разграничением прав доступа к системе сотрудников приемной комиссии, деканатов и руководящего состава в соответствии с их должностными обязанностями; [9, с.56]

· автоматизация процесса формирования расписания теоретических занятий, сессий и защиты ВКП для учебных корпусов;

· организация учебного процесса на базе единых учебно-методических и контрольно-измерительных материалов (экзаменационных билетов и тестов);

· разработка бизнес-процессов (для согласования работы разных отделов);

· разработка специализированных управленческих отчетов для получения оперативной информации о численности и успеваемости студентов, оплате договоров и дополнительных услуг, нагрузке преподавателей, эффективности использования аудиторного фонда, контроля планового поступления денежных средств.

Для реализации системы была выбрана программа «КРУЗ» Комплексное Решение для Учебных Заведений» на платформе "1С:Предприятие 8.1" Большое внимание уделялось обеспечению функционирования с повышенными характеристиками масштабирования, размерами информационной базы и ее пространственной распределённости и безопасности.

Анализ бизнес-процессов управления

Внедрение программы КРУЗ позволило достичь следующих результатов:

→ Снижение расходов на разработку и сокращение времени внедрения до 3 месяцев.

→ Снижение административных расходов на услуги почты, бумагу, оплату сверхурочных часов работы работникам деканатов на 40%;

→ Снижение количества ошибок ввода данных в систему на 80%;

→ Полный документооборот по контингенту в электронном виде;

→ Реализован учет рабочего времени по системе контроля доступа;

→ Система КРУЗ так же позволяет автоматизировать процесс составления учебных и рабочих планов, расписания по группам;

→ Присутствует механизм хранения учебно-методических комплексов и ВКР, автоматизирована проверка на заимствования (Антиплагиат);

→ Решение интегрировано с call-центром и sms-шлюзом, порталом учебного заведения Битрикс, Microsoft Office 365.

2.2 Организация локальной сети ООО «Совинто»

Обновление локальной информационной сети ООО «Совинто» предназначена для обеспечения надлежавшего уровня сохранности информации и повышения характеристик пропускной способности.

Данная сеть будет иметь смешанную топологию. На межэтажном уровне проведена Шина с двумя разнонаправленными линиями (восходящая и нисходящая), На уровне отдельного этажа проведена Иерархическая (Древесная) топология.

На коммутаторах планируется использовать технологию тегирования портов, это позволит программно установить разграничения доступа к информационным ресурсам сети и упростит управление отдельных сегментов сети. Конечные узлы, то есть компьютеры и сетевые принтеры, планируется подключить к коммутаторам, посредствам кабеля UTP 5e.

2.3 Первичное проектирование схемы подключения оборудования

На каждом из этажей необходим коммутатор, он займёт 1 Units в телекоммуникационном шкафу. Рядом должна располагаться розетка, запитанная от электросети. В целях защиты оборудования от скачков напряжения в коммуникационный шкаф помещается источник бесперебойного питания, занимающий 2 Units. Так же устанавливается патч панель на 1 Units. Итого в шкафу будет занято 4 Units, значит необходим шкаф на 6-9 Units, для удобства обслуживания установленного оборудования.

На рисунке 7 изображена схема подключения оборудования по этажам. На рисунке 8 изображена схема подключения оборудования в шкафу.



Рисунок 7 – схема подключения оборудования по этажам

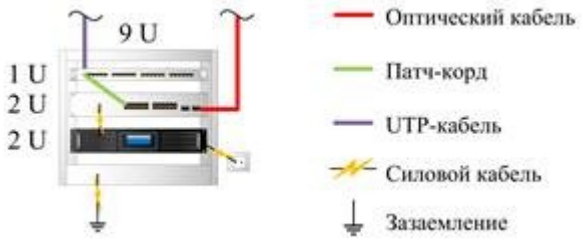


Рисунок 8 – схема подключения оборудования в шкафу

2.4 Выбор сетевого оборудования

Пользовательское оборудование объединено в кабинетные кластеры с помощью коммутаторов TP-LINK tl-sg1210p (рисунок 9)

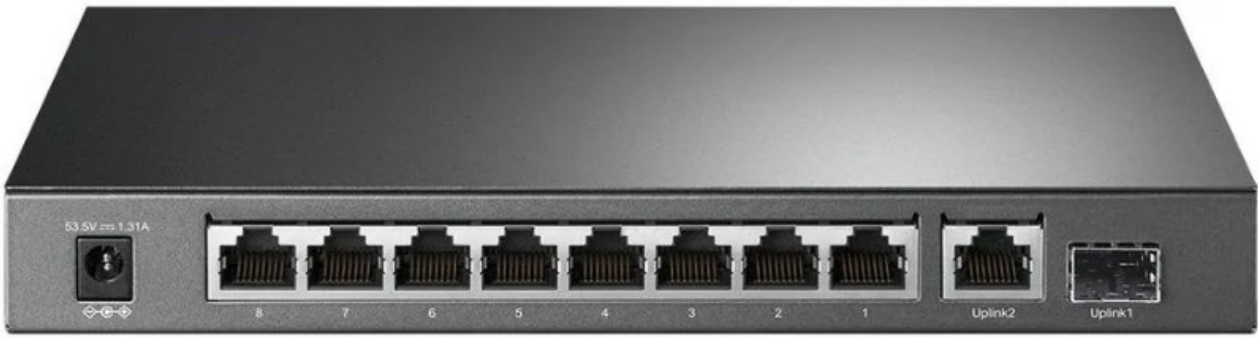


Рисунок 9

И объединяется с основной сетью посредство маршрутизаторов

Mikrotik hAP ac lite TC (рисунок 10). Которые помимо переадресации запросов и подключения автономных устройств сотрудников (Ноутбуки, Нэтбуки, Планшеты), может быть запрограммирован как дополнительный фаерволл, или дополнительная ЛИС этажа.



Рисунок 10

Для защиты сегментов сети от кратковременных сбоев в сети электропитания советуется дополнить ЛИС блоками ИБП Ippon Smart Winner 1000 (рисунок 11).



Рисунок 11

Межэтажный сегмент сети состоит из межсетевых экранов TP-LINK ER8411 (рисунок 12), обеспечивающие сообщения между кабинетами на разных этажах.



Рисунок 12

Также необходим шкаф, в котором будет размещено коммутационное оборудование. Для этих целей подойдет КШ ШТН-4U 600х240х450 (рисунок 12), или при необходимости более габаритный КШ ТЕЛКОМ TL-9.6.3-П.7035Ш 9U 600х350х490мм



Рисунок 13

Патч -корд — это кабель, предназначенный для подключения одного электрического устройства к другому или к пассивному оборудованию передачи сигнала. Для организации соединения коммутатор -патч-панель понадобиться патч -корд Nikomax NMC S/FTP 4 пары (1M) (Рисунок 14).



Рисунок 14

Необходим кабель UTP способный передавать данные со скоростью 1 Гбит /с. Ubiquiti TOUGHCable, промышленного класса экранированный кабель. Внешнего исполнения операторского класса экранированный кабель, который также способен обеспечить повышенную производительность категории 5e. Защита сети от самых жестоких погодных условий с Ubiquiti промышленного класса экранированных Ethernet кабель, TOUGHCable. Ubiquiti TOUGHCable предназначен для работы со всеми продуктами компании. Тестировался на совместимость практически со всеми устройствами производителя (Рисунок 15).



Рисунок 15

Для соединения витой пары UTP с интерфейсами коммутатора необходимы коннекторы интерфейса RJ-45. Ubiquiti коннекторы TOUGHCable Connectors полностью готовы для работы в составе высокоэффективного гигабитного канала. Это небольшой, но очень важный элемент работы защищенной и производительной телекоммуникационной системы на базе устройств Ubiquiti. Коннекторы предназначены для работы со всеми продуктами компании. Тестировался на совместимость практически со всеми устройствами производителя. (Рисунок 16).



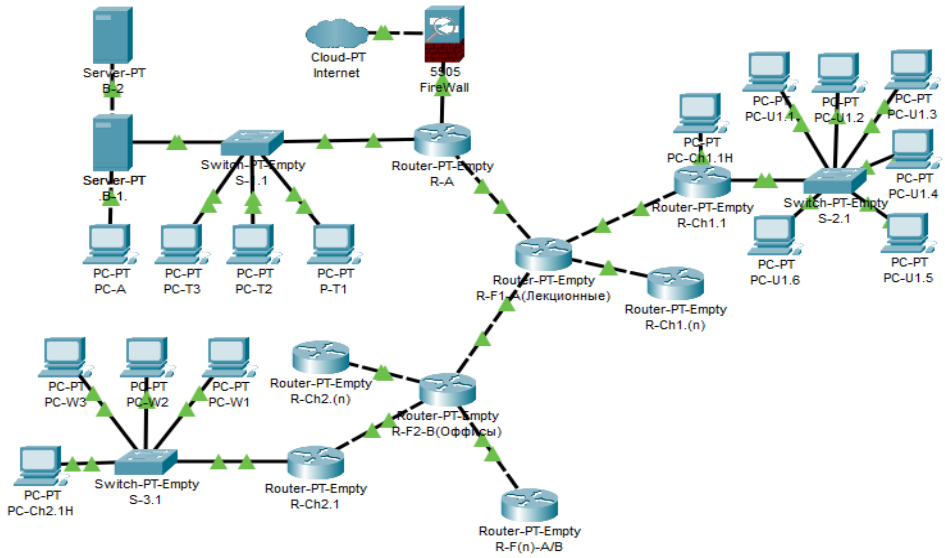
Рисунок 16

2.5 Проектирование сети

При помощи логической топологии или логической схемы сети, у сетевого администратора появляется более ясное понимание принципа работы

компьютерной сети, возможность определить куда пойдет тот или иной запрос и какое устройство будет иметь доступ к ресурсам той или иной сети.

В логическом изображении сеть ООО«Совинто» выглядит следующим образом (схема 1).



На тестовом этаже все устройства соединяться с этажным управляемым маршрутизатором (рисунок 17)



Рисунок 17

Далее этажи могут повторять модули схемы 1, исключая администраторскую.

3. ОЦЕНКА ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ПРОЕКТА

3.1. Определение параметров проекта автоматизации

Для качественного управления вузом и принятия решений разработана автоматизированная система управления (АСУ), которая позволяет комплексно автоматизировать деятельность учебных заведений. Комплексная информатизация любой организации (и вуза, в частности) представляет собой масштабную задачу, для решения которой в настоящее время используют два подхода. Первый подход основан на внедрении так называемых ERPсистем (Enterprise Resource Planning), представляющих собой крупные программные комплексы, требующие серьезных материальных и организационных вложений.

Второй подход состоит в наращивании интегрированной системы управления предприятием (организацией) снизу вверх. В рамках этого второго подхода процесс информатизации управления вуза носит поэтапный характер и опирается на имеющиеся наработки, программные средства и системы.

Ниже перечислены основные положения, которые положены в основу информационной системы управления вузом:

- наличие единой корпоративной сетевой инфраструктуры и единого центра управления разработками, обеспечивающих разработку информационных подсистем, направленных на автоматизацию задач, стоящих перед вузом;
- создание комплексной информационной модели вуза;

- разработка системы, включающей доступ ко всем информационным ресурсам вуза;
- управление персоналом;
- управление учебным процессом;
- управление документооборотом;
- повышение эффективности работы, как структурных подразделений, так и вуза в целом;
- упорядочивание и поддержка всех основных процессов сферы деятельности вуза, поднятие их на качественно новый уровень;
- использование современных средств и технологий для разработки общеуниверситетской системы управления: системы управления базами данных, технологии Internet, OLAP-технологии, специализированных программных средств, систем управления электронным документооборотом.

Текущее состояние автоматизировано-информационной системы любого учебного заведения может быть представлено несколькими взаимосвязанными подсистемами с гибко настраиваемыми функциями (рис. 18) .



Рисунок 18 - Структура схем АСУ

В зависимости от специфики задач все пользователи делятся на Windows-клиентов, программное обеспечение которых устанавливается на их рабочих местах, и Web-клиентов, получающих доступ к системе через Webинтерфейс.

Взаимосвязи подсистем информационной системы университета приведены на рис.19

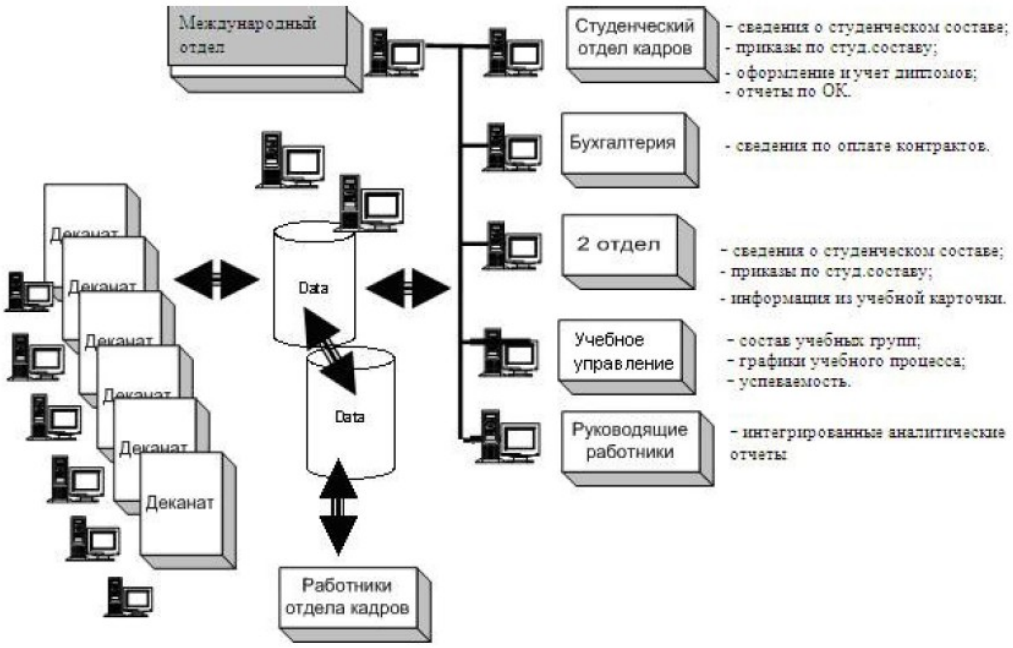


Рисунок 19 – Структура информационной системы

Основой информационной системы является единая база данных. Указанные выше задачи решаются соответствующими подсистемами. В целом информационная система построена по технологии «клиент – сервер» и обеспечивает многопользовательский режим работы в корпоративной информационной сети с большим числом терминалов на кафедрах, факультетах, в отделах учебного управления и др.

АСУ вуза можно рассматривать как человеко-машинную систему с автоматизированной технологией получения результативной информации, необходимой для информационного обслуживания процесса образовательной деятельности и оптимизации ее управления. С помощью АСУ обеспечивается многоуровневость прогнозирования, принимаются рациональные управленческие решения, организуются учет и анализ, обеспечивается достоверность и оперативность получаемой и используемой в управлении информации.

В настоящее время набирает силу и формируется опыт корпоративного управления вузом. Создаются распределенные базы данных для решения определенных задач системы управления. Внедряется электронная система документооборота, что требует изменения содержания, объема и направленности информационных потоков между структурными подразделениями вуза. Важную роль в успешном решении задач по автоматизации управления играет переосмысливание методов организации управления подразделениями вуза, проведение реструктуризации подразделений и создание новых подразделений, выполняющих аналитические функции.

АСУ вузом ставит целью существенное повышение уровня организации и оперативности управления вузом с применением информационной технологии (ИТ) на базе современной компьютерной техники и оргтехники. АСУ вузом позволяет значительно сократить затраты труда структурных подразделений на осуществление функций их работы, используя технические средства сбора, передачи и обработки информации.

Основная направленность работы ориентирована на разработку прикладных систем, способствующих дальнейшему совершенствованию управления образовательными процессами в вузе, а также формированию и упорядочиванию систем документооборота (по планированию, управлению и отчетности) между подразделениями вуза – ректоратом, учебным отделом, деканатами (институтами), кафедрами, отделами кадров и бухгалтериями. Разработанная нами АСУ университета состоит из следующих подсистем (ПС):

1. ПС «Отдел кадров сотрудников» (ОК сотр.)
2. ПС «Учебное Управление» (УУ)
3. ПС «Приемная комиссия» (ПК)

4. ПС «Отдел кадров студентов» (ОК студ.)
5. ПС «Бухгалтерия»
6. ПС «Деканат»
7. ПС «Тест»

Ниже дано краткое описание функций каждой из перечисленных ПС.

1. ПС «Отдел кадров сотрудников» (ОК сотр).

Технология работы данной системы построена на основе взаимосвязи следующих элементов интегрированной системы управления вузом: «работник штатная единица подразделение вуз». Элемент связи «работник штатная единица» позволяет определить списочный состав вуза. Элемент связи «штатная единица подразделение» участвует на этапе работы со штатным расписанием. Элемент связи «подразделение вуз» определяет организационную структуру вуза.

Основными процессами по управлению персоналом являются следующие:

- описание организационной структуры вуза и ведение его штатного расписания;
- анализ кадрового ресурса организации/ структурной еди-ницы, оперативное принятие обоснованных решений по кадровому спектру задач;
- традиционные задачи кадрового учета по приказам;
- функции учета персонала со стороны отдела кадров (назначение на должность, увольнение с работы, продление срока работы, возложе-ние исполнения обязанностей, изменение фамилии, освобождение от совместительства, предоставление отпуска, отзыв сотрудника из отпуска, повышение квалификации);

- анализ кадровой структуры организации (численности, профес-сионального и должностного состава сотрудников, динамики при-ема на работу, должностного роста и увольнения работника);
- подготовка информации по аттестации кадров;
- подготовка других отчетных документов.

2. ПС «Учебное Управление» (УУ).

Данная ПС предусматривает:

- создание рабочих учебных планов по специальностям и специ-ализациям;
- закрепление дисциплин за кафедрами;

учет и контроль учебных занятий. Таким образом, подсистема

«Учебное Управление» предназначена для создания и утверждения базовых, рабочих учебных планов по специальностям и специализациям.

3. ПС «Приемная комиссия» (ПК).

Подсистема «Приемная комиссия» предусматривает:

- планирование набора абитуриентов (фиксирование правил при-ема, план набора бюджетный, сверх плана набора по договорам за полную оплату);
- прием заявлений и обработку анкет (допуск к экзаменам, фор-мирование групп для сдачи экзаменов, движение абитуриентов возврат документов, переход на другую специальность и др., регла-ментированная и востребованная статистическая отчетность);
- вступительные экзамены (составление расписания экзаменов, формирование экзаменационных ведомостей, выставление оценок, подсчет суммы баллов, определение статуса абитуриента «подтвердил медаль», «не сдал экзамен», «не явился на экзамен», оперативный анализ итогов);

- зачисление в вуз (формирование списков абитуриентов, реко-мендованных к зачислению, формирование проходного балла, зачисление абитуриентов в число студентов категория зачисления, формирование списков зачисленных, формирование протокола, проекта приказа и приказа о зачислении в вуз);
- подведение итогов приема в вуз (формирование регламенти-рованных и востребованных отчетов о ходе зачисления, формиро-вание групп, зачисленных в студенты, присвоение номеров студен-ческих билетов);
- ведение справочников.

4. ПС «Отдел кадров студентов» (ОК студ.).

Автоматизация функций «Отдел кадров студентов» отслеживает движение контингента студентов и создание средств автоматизации работы с приказами и распоряжениями по контингенту, а также на проведение учета и анализа состава и движения контингента студентов.

- *ПС «Бухгалтерия».* Функционал ПС «Бухгалтерия» содержит следующие блоки:\составление прейскуранта цен на обучение студентов контрактного обучения;
- разделение прейскуранта цен по гражданству (КР; ближнее зарубежье, входящее в межправительственное соглашение; ближнее зарубежье, не входящее в межправительственное соглашение; дальнее зарубежье);
- определение ожидаемого поступления от оплаты за обучение;
- учет оплаты студентов;
- отчеты по оплате за обучение.

6. ПС «Деканат» обеспечивает:

- распечатки экзаменационных ведомостей;
- распечатки экзаменационных листов;

- учет успеваемости студентов;
- анализ успеваемости.

7. *ПС «Тест».* Цели создания системы:

- оценка знаний;
- повышение качества знаний;\оптимизация управления кадровыми ресурсами предприятий путем аттестации реальных знаний сотрудников;
- сбор данных.

Основные функции и возможности АСУ вуза

- Настройка системы на особенности конкретного образовательного учреждения.
- Поддержка всех форм обучения (очная, заочная, дистанционная) и всех видов обучения.
- Охват всех этапов процесса обучения от поступления до выпуска с подготовкой соответствующих документов.
- Разработка и поддержание в рабочем состоянии всех учебных планов в соответствии с Госстандартом.
- Организация синхронной работы всех участников учебного процесса.

Банк данных формируется в соответствии с утвержденными требованиями.

Базовые средства (сегментированные таблицы и индексы) позволяют хранить в базе данных и обрабатывать большие объемы данных без потери, поддерживать как текущие, так и справочные данные. Таким образом, БД должна стать основным источником достоверной информации для ректората, руководителей и специалистов общеуниверситетских служб, отвечающих за определение стратегии развития различных сфер деятельности университета.

Решение указанных задач обеспечивается на основе развитого пользовательского интерфейса, реализации интерактивного режима работы пользователя с выполнением необходимых проверок непосредственно в процессе ввода учебного плана.

3.2. Расчет показателей экономической эффективности

Сметная стоимость проектирования и внедрения ЛС включает в себя следующие затраты, определяемые по формуле (1):

$$C_{пр} = C_{осн} + C_{доп} + C_{соц} + C_{м} + C_{маш.вр} + C_{н}, \quad (1)$$

где

$C_{пр}$ – стоимость проектирования ЛИС;

$C_{осн}$ – основная заработная плата исполнителей;

$C_{доп}$ – дополнительная заработная плата исполнителей, учитывающая потери времени на отпуска и болезни (принимается в среднем 10% от основной заработной платы);

$C_{соц}$ – ЕСН, отчисления во внебюджетные фонды государственного социального страхования (пенсионный фонд, фонд обязательного медицинского страхования, фонд социального страхования), рассчитываются как 0,26% от основной и дополнительной заработной платы;

$C_{м}$ – затраты на используемые материалы;

$C_{маш.вр}$ – стоимость машинного времени;

$C_{н}$ – накладные расходы включают затраты на управление, уборку, ремонт, электроэнергию, отопление и др. (принимаются в размере 60% от основной и дополнительной заработной платы).

На статью «Заработная плата» относят заработную плату научных, инженерно-технических и других работников, непосредственно участвующих в проектировании ЛИС и защите информации. Расчет ведется по формуле (2):

$$З_{исп} = З_{ср} * Т, \quad (2)$$

где

$З_{исп}$ – заработная плата исполнителей, руб.;

$З_{ср}$ – средняя тарифная ставка работника организации разработчика ПО, руб / чел-дней;

Т – трудоемкость разработки ПО, чел-дней.

$З_{ср}$ определяется по формуле (5.5):

$$З_{ср} = С / Ф_{мес}, \quad (3)$$

где

С – зарплата труда на текущий момент времени (руб./мес.);

$Ф_{мес}$ – месячный фонд рабочего времени исполнителя (дни).

Затраты на статью «Заработной платы» приведены в таблице 3.1.

Таблица 3.1 Затраты на заработную плату

Исполнитель	Оклад, руб./мес.	Оклад, руб./день	Трудоемкость, чел-дней	Сумма, руб.
Руководитель	36000	1636	16	26176
Инженер	29000	1318	82	108076
Общая основная заработная плата исполнителей, $С_{осн}$			98	134252

Дополнительная заработная плата на период проектирования ЛИС и защиты информации рассчитывается относительно основной и составляет 10% от ее величины:

$C_{доп} = C_{осн} * 0,1 = 13425.2$ (руб.)

Отчисления на социальное страхование составляют 26%:

$C_{соц} = (C_{доп} + C_{осн}) * 0,26$ (4)

$C_{соц} = (13425.2 + 134252) * 0,26 = 38393.1$ (руб.)

На эту статью относят все затраты на магнитные носители данных, бумагу, для печатных устройств, канцтовары и др. Затраты по ним определяются по экспертным оценкам. Расчет расходов на материалы приведен в таблице 3.2.

Таблица 3.2 Расходы на основные материалы и покупные изделия

№П/п	Наименование материала	Цена за ед., руб.	Кол-во	Всего, руб.
1.	Бумага офисная, пачка	225	2	450
2.	Картридж для принтера, шт.	2590	1	2590
3.	Коммутатор D-link DES-1016A	1043	28	29204
4.	Маршрутизатор ETGEAR FVS318	4371	4	17484
5.	HP Proliant DL380 Gen9	224820	4	899280
6.	D-link DIR-815	2280	20	45600
7.	EVIDENCE NanoStation M2 DV	6353	20	127060
8.	TP-LINK Archer T4UH	500	80	40000
9.	Сетевой кабель, бухта	11250	5	56250
10.	Итого, рублей			1217918

Величина накладных расходов принимается равной 60% от основной зарплаты исполнителей. Формула расчета (5):

$$С_н = С_{осн} * К, \quad (5)$$

где

$С_н$ – накладные расходы, руб.;

$С_{осн}$ – основная заработная плата исполнителей, руб.;

К – коэффициент учета накладных расходов (К = 0,6).

$$С_н = 134252 * 0,6 = 80551,2 \text{ (руб.)}$$

Расчет затрат на машинное время осуществляется по формуле (6):

$$С_{маш.вр} = К_{маш.вр} * З_{маш.вр} \quad (6)$$

где

$К_{маш.вр}$ – тарифная стоимость одного часа машинного времени ($К_{маш.вр}$=50 руб./ч.);

$З_{маш.вр}$ – машинное время, используемое на проведение работ.

Необходимое количество машинного времени для реализации проекта по проектированию ЛИС и защите информации рассчитывается по формуле:

$$З_{маш.вр} = t_i * Т_{см} * Т_{ср.маш}, \quad (7)$$

где

t_i – трудоемкость работ, чел-дней;

$Т_{см}$ – продолжительность рабочей смены (При пятидневной рабочей неделе $Т_{см}$ = 8 ч.);

$Т_{ср.маш}$ – средний коэффициент использования машинного времени ($Т_{ср.маш}$ = 0,7).

Тогда:

$$З_{маш.вр} = 98 * 8 * 0,7 = 548.8 \text{ (ч.)}$$

Стоимость машинного времени составит:

$$С_{маш.вр} = 50 * 548.8 = 27440 \text{ (руб.)}$$

Результаты расчета затрат на проектирование ЛИС сведены в таблице 3.3.

Таблица 3.3 Смета затрат на проектирование ЛИС

Наименование статей	Обозначение	Сумма, руб.	В % к итогу
Основная заработная плата	$C_{осн}$	134252	8,88
Дополнительная заработная плата	$C_{доп}$	13425	0,89
Отчисления на социальные нужды	$C_{соц}$	38396	2,54
Материалы	$C_{мат}$	1217918	80,55
Накладные расходы	$C_{н}$	80551	5,33
Стоимость машинного времени	$C_{маш.вр}$	27440	1,81
Итого:	$C_{пр}$	1511982	100

Таким образом, себестоимость проектирования составляет 1511982 руб.

Диаграмма распределения стоимости проекта по статьям приведена на рисунке 3.1.

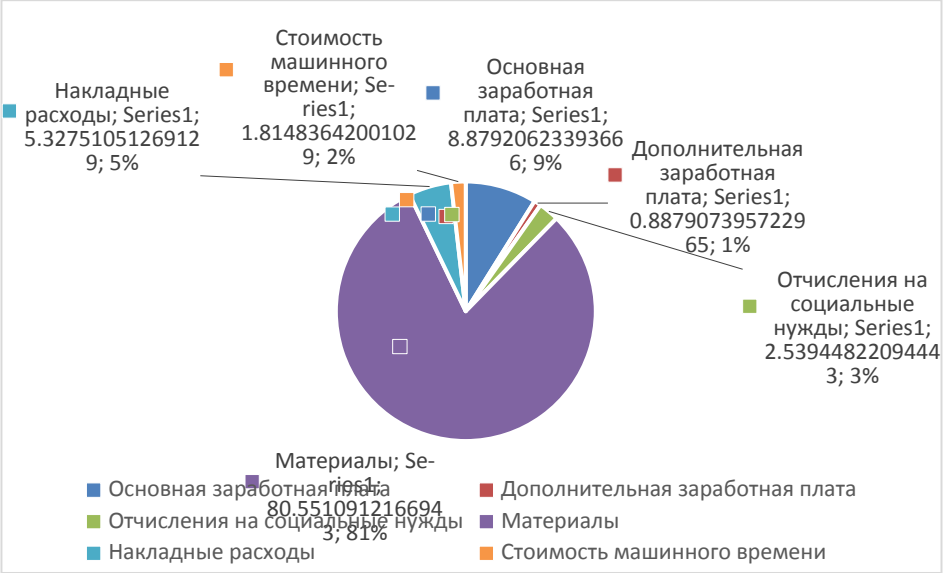


Рисунок 3.1 Диаграмма распределения стоимости проекта по статьям

Экономическая эффективность от использования ЛИС соответствует экономической эффективности от внедрения автоматизированных систем управления, ЛИС в данном случае является необходимым инструментом автоматизированной системы управления.

Таким образом, целесообразность построения локальной информационной сети заключается в невозможности эффективной автоматизации управления производством без ее наличия.

Основные технико-экономические показатели проекта приведены в таблице 3.4.

Таблица 3.4 Основные технико-экономические показатели проекта

Наименование показателя	Ед. измерения	Проектный вариант
Способ обработки информации	-	С применением ЭВМ и программных средств
Используемое оборудование	-	Компьютер, принтер/сканер/копир
Количество работников	чел.	1
Продолжительность проведения	календарных	106

проектирования	дней	
Трудоемкость проведения проектирования	чел-дней	98
Затраты на проведение проектирования	руб.	654536
Получаемый эффект от внедрения:		
- качественное обеспечение бизнес - процесса в		
- ускорится процесс поиска и использования необходимой информации		
- уменьшится документооборот внутри организации		
- повысится надежность хранения данных		
- повысится производительность труда сотрудников		
- доступ всех сотрудников к глобальной сети Internet		

Таким образом, в третьей главе работы проведено тестирование ИВС, расчет ее надежности, экономической эффективности. Полученные результаты позволяют сделать вывод о том, что параметры сети соответствуют стандартным и позволяют внедрить ее в эксплуатацию.

ЗАКЛЮЧЕНИЕ

В результате выполненной работы была спроектирована локальная информационная сеть для использования на территории МФЮА.

Данная тема имеет немаловажное значение для дальнейшего развития учебного заведения. Работа состоит из введения, трех глав, заключения и списка использованных источников.

В первом разделе были определены требования к ЛИС, произведён анализ объекта и обоснована необходимость разработки беспроводной локальной информационная сети, проанализированы существующие технологии построения беспроводных ЛИС.

Во втором разделе произведена сегментация сети и разработана логическая схема сети, произведён выбор конкретного телекоммуникационного оборудования, рассчитано количество необходимых точек доступа и произведено их размещение в помещении корпуса, проведен расчет кабеля.

В организационно-экономическом разделе произведен расчет стоимости сети для МФЮА

Получаемый эффект от внедрения:

- ускорится процесс поиска и использования необходимой информации;
- увеличится доступность учебных ресурсов;
- повысится надежность хранения данных;
- повысится производительность обучения студентов.

Во время прохождения практики была исследована инфраструктура предприятия, изучены должностные инструкции специалиста IT-специалиста.

Были проанализованы организация вычислительной системы и сети предприятия, а также программно-аппаратное обеспечение ВС.

Практика проходила под руководством начальника IT-отдела в качестве специалиста технической поддержки.

В обязанности специалиста технической поддержки входило:

1. Осуществлять оперативную помощь сотрудникам по устранению неисправностей, определять, локализировать и устранять ошибки (сбои).

2. Принимать и фиксировать в HelpDesk системе заявки от пользователей, контролировать процесс их устранения.

3. Выполнять работы по установке и настройке программ и программных средств, утвержденных политикой компании.

4. Устанавливать новые рабочие места и осуществлять перенос существующих.

5. Настраивать ПК и мобильные телефоны на базе IOS, Android, тестировать, выявлять и устранять неисправности компьютеров и копировальной техники.

6. Осуществлять закупку и учет расходных материалов для обеспечения бесперебойного функционирования принтеров и копировальной техники.

7. Осуществлять оформление документов (приход/расход) и учет оборудования на складе IT.

8. Вести учет лицензионного ПО.

9. Выполнять служебные задания, поручения и указания непосредственного руководителя и разовые служебные задания руководителя департамента информационных технологий.

За время прохождения практики были изучены способы настройки маршрутизаторов и коммутаторов, особенности монтажа кабельных каналов и укладки кабеля, основы организации структурированной кабельной сети.

На практике применялись полученные за время обучения знания и навыки работы в области сетевых технологий и администрирования баз данных.

Задачи практики были выполнены в полном объеме

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Алишов Н. И., Петришина О. В. Конфликты доступа в локальных вычислительных сетях // ММС. 2018. №4. С.

2. Бегишев В.О., Сопин Э.С., Молчанов Д.А., Самуйлов А.К., Гайдамака Ю.В., Самуйлов К.Е. Оценка эффективности механизма резервирования полосы пропускания для технологии mmwave в сетях связи пятого поколения // Информационно-управляющие системы. 2019. № 5 (102). С. 51-63.

3. Глушак, Е. В. Протоколы и технологии сетей следующего поколения : учебное пособие / Е. В. Глушак, А. В. Росляков. — Самара : ПГУТИ, 2017. — 56 с. — Текст : электронный // Лань : электронно-библиотечная система.

4. Гулевич, Д. С. Сети связи следующего поколения : учебное пособие / Д. С. Гулевич. — 2-е изд. — М. : ИНТУИТ, 2016. — 213 с. — ISBN 5-94774-647-1. — Текст : электронный // Лань : электронно-библиотечная система.

5. Черникова Е.Б., Белоусов А.О. Многовариантный анализ многопроводных линий передачи для трёхкратного модального резервирования // В сборнике: IEEE XXII Международная конференция молодых специалистов в области электронных приборов и материалов (EDM 2021). Дайджесты. Новосибирск, 2021. С. 160-165.

6. Гришина Н. В., Комплексная система защиты информации на предприятии, Издательство: Форум, 2010 г., 240 стр.

7. Джесси Рассел, Безопасность в беспроводных самоорганизующихся сетях, Издательство: Книга по Требованию, 2012 г., 66 стр.

8. Джон Росс, Беспроводная компьютерная сеть Wi-Fi своими руками, Издательство: Наука и техника, 2012 г., 384 стр.

9. Джуди Новак, Стивен Норткатт, Дональд Маклахен, Как обнаружить вторжение в сеть. Настольная книга специалиста по системному анализу, Издательство: Лори, 2012 г., 384 стр.

10. Кенин А. В.: Самоучитель системного администратора, М., Издательство: BHV, 2012 г., 512 стр.

11. ГОСТ 29099-91 Сети вычислительные локальные. Термины и определения

12. ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на информационные системы. Техническое задание на создание автоматизированной системы.

13. Сергей Клименко, Олег Клименко, Александр Никитин, Компьютерная сеть за один день. Как на базе оборудования D-Link развернуть проводную и Wi-Fi сеть, Издательство: Диалектика, Вильямс, 2010 г., 224 стр.

14. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – Спб.: Питер, 2010. – 944 с.

15. Новиков Ю.В., Кондратенко С.В. Локальные сети. Архитектура, алгоритмы, проектирование. – М.: Эком, 2000. – 308 с.

16. Горальски В. Технологии ADSL иDSL. – М.: Лори, 2000. – 296 с.

17. Новиков Ю.В., Карпенко Д.Г. Аппаратура локальных сетей: функции, выбор, разработка. – М.: Эком, 1999. – 288 с.

18. Стерлинг Д.Д. Техническое руководство по волоконной оптике. – М.: Лори, 1998. – 195 с.

19. Wi–Fi сети. [Электронный ресурс]. URL: http://wificenter.ru/ (Дата обращения 15.04.2023).

20.Определение Active Directory. [Электронный ресурс]. URL: http://luboznaiki.ru/opredelenie/active_directory (Дата обращения 07.05.2023).

21. Сайт ООО «Совинто» . [Электронный ресурс]. URL: http://sovinto.ru/ (дата обращения12.05.2023).

22. Информатизация образования: направления, средства, технологии / Под общ.ред. С.И. Маслова.М.: Изд-во МЭИ, 2004. – 868 с.

23. Управление в высшей школе: опыт, тенденции, перспективы /Под ред. В.М. Филиппова. М.: Логос, 2006. 488 с.

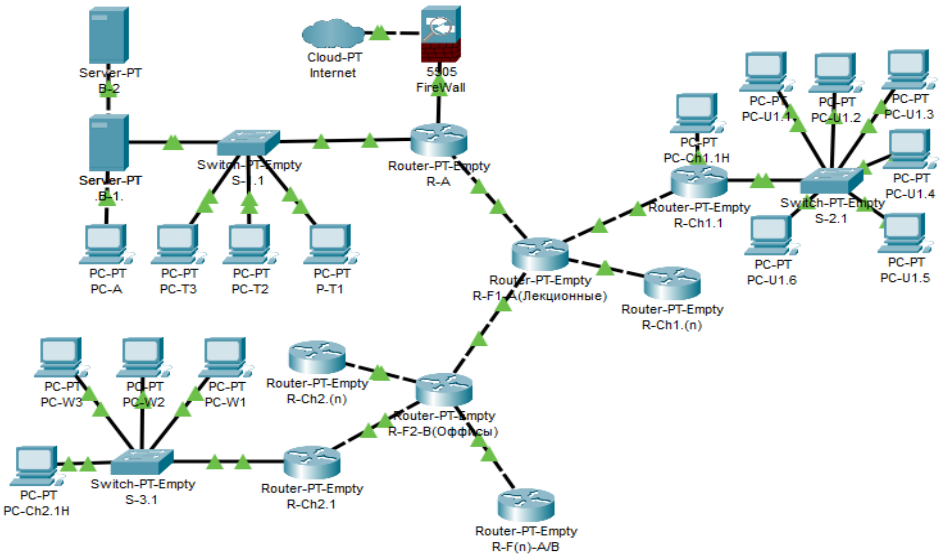
24. Баймухамедов М.Ф. Принципы построения информационной системы управления вузом. / Материалы республиканской на-«Инновационные методы и средства обучения в сфере университетского образования».Костанай, 2004.

25 .Саитов Н.Ж. Программа для ввода и корректировки личных данных студентов и абитуриентов «AVN 2.1» [Текст] / Н.Ж.Саитов //Официальный бюл. Интеллектуальная собственность. Госслужба патентирования Кырг. Респ. Бишкек, 2008. № 12. — С.133-134.

26. Саитов Н.Ж. Программа для расчета и распределения нагрузки кафедр и преподавателей «AVN 6.1» [Текст] /Н.Ж.Саитов // Официальный бюл. Интеллектуальная собственность. Госслужба патентирования Кырг. Респ. Бишкек, 2008. № 12. — С.134.

ПРИЛОЖЕНИЕ

П.1. Схема основной сети с примерами подключения базовых модулей:



П.2. Настройка

Марщрутизатор технического отдела: R-A:

R-A>en

R-A#conf t

R-A(config)#interface fa 0/0

R-A(config-if)#ip address 10.10.0.1 255.255.255.0

R-A(config-if)#no shutdown

R-A(config-if)#exit

R-A(config)#interface fa 1/0

R-A(config-if)#ip address 10.10.0.2 255.255.255.0

R-A(config-if)#no shutdown

R-A(config-if)#exit

R-A(config)#ip route 12.12.12.0 255.255.255.0 fa 0/0

R-A(config)#ip route 3.3.3.0 255.255.255.0 fa 0/0

R-A(config)#ip route 11.11.11.0 255.255.255.0 fa 0/0

R-A(config)#ip route 16.16.16.0 255.255.255.0 fa 0/0

R-A(config)#ip route 7.7.7.0 255.255.255.0 fa 0/0

R-A(config)#ip route 8.8.8.0 255.255.255.0 fa 0/0

R-A(config)#ip route 21.1.1.0 255.255.255.0 fa 0/0

R-A(config)#ip route 20.20.20.0 255.255.255.0 fa 0/0

Маршрутизатор Кабинетов типа А / Лекционных:

R-Ch(n).(m)>en

R-Ch(n).(m)#conf t

R-Ch(n).(m)(config)#interface fa 0/0

R-Ch(n).(m)(config-if)#ip address 10.10.(n).2 255.255.255.0

R-Ch(n).(m)(config-if)#no shutdown

R-Ch(n).(m)(config-if)#exit

R-Ch(n).(m)(config)#interface fa 1/0

R-Ch(n).(m)(config-if)#ip address 1.(n).(m).3 255.255.255.0

R-Ch(n).(m)(config-if)#no shutdown

R-Ch(n).(m)(config-if)#exit

R-Ch(n).(m)(config)#ip route 3.3.3.0 255.255.255.0 fa 0/0

R-Ch(n).(m)(config)#ip route 10.10.10.0 255.255.255.0 fa 0/0

R-Ch(n).(m)(config)#access-list 1 permit 13.13.13.0 0.0.0.255

R-Ch(n).(m)(config)#ip nat pool ax 20.20.20.3 20.20.20.255 netmask 255.255.255.0

R-Ch(n).(m)(config)#ip nat inside source list 1 pool ax

R-Ch(n).(m)(config)#interace fa 1/0

R-Ch(n).(m)(config-if)#ip nat inside

R-Ch(n).(m)(config-if)#exit

R-Ch(n).(m)(config)#interace fa 0/0

R-Ch(n).(m)(config-if)#ip nat outside

R-Ch(n).(m)(config-if)#exit

Маршрутизатор Кабинетов типа B / Оффисов:

R-Ch(n).(m)>en

R-Ch(n).(m)#conf t

R-Ch(n).(m)(config)#interface fa 0/0

R-Ch(n).(m)(config-if)#ip address 10.10.(n).2 255.255.255.0

R-Ch(n).(m)(config-if)#no shutdown

R-Ch(n).(m)(config-if)#exit

R-Ch(n).(m)(config)#interface fa 1/0

R-Ch(n).(m)(config-if)#ip address 1.(n).(m).3 255.255.255.0

R-Ch(n).(m)(config-if)#no shutdown

R-Ch(n).(m)(config-if)#exit

R-Ch(n).(m)(config)#ip route 13.13.13.0 255.255.255.0 fa 0/0

R-Ch(n).(m)(config)#ip route 10.10.10.0 255.255.255.0 fa 0/0

R-Ch(n).(m)(config)#ip route 12.12.12.0 255.255.255.0 fa 0/0

R-Ch(n).(m)(config)#ip route 7.7.7.0 255.255.255.0 fa 0/0

R-Ch(n).(m)(config)#access-list 1 permit 13.13.13.0 0.0.0.255

R-Ch(n).(m)(config)#ip nat pool ax 21.1.1.3 21.1.1.255 netmask 255.255.255.0

R-Ch(n).(m)(config)#ip nat inside source list 1 pool ax

R-Ch(n).(m)(config)#interace fa 1/0

R-Ch(n).(m)(config-if)#ip nat inside

R-Ch(n).(m)(config-if)#exit

R-Ch(n).(m)(config)#interace fa 0/0

R-Ch(n).(m)(config-if)#ip nat outside

R-Ch(n).(m)(config-if)#exit

Межэтажный маршрутизатор:

R-F(n)>en

R-F(n)#conf t

R-F(n)(config)#interface fa 0/0

R-F(n)(config-if)#ip address 10.10.(n).1 255.255.255.0

R-F(n)(config-if)#no shutdown

R-F(n)(config-if)#exit

R-F(n)(config)#interface fa 1/0

R-F(n)(config-if)#ip address 12.12.12.1 255.255.255.0

R-F(n)(config-if)#no shutdown

R-F(n)(config-if)#exit

R-F(n)(config)#interface fa 2/0

R-F(n)(config-if)#ip address 3.3.3.1 255.255.255.0

R-F(n)(config-if)#no shutdown

R-F(n)(config-if)#exit

R-F(n)(config)#interface fa 3/0

R-F(n)(config-if)#ip address 4.4.4.3 255.255.255.0

R-F(n)(config-if)#no shutdown

П.3. Обозначения оборудования:

 PC-U(x)	Рабочий PC студента
 PC-Ch(n).(m)H	PC Преподавателя / Начальника отдела
 PC-W(x)	Рабочий PC работника организации
 S-(n).(m)	Коммутатор кабинета. TP-Link TL-SG3428X
 R-Ch(n).(m) / R-A	Маршрутизатор кабинета, для подключения к главному узлу. Mikrotik hAP ac lite TC
 R-F.(n)-A/B	Межэтажный маршрутизатор TP-LINKER8411
 FireWall.	Межстетевой экран.
 B-(x)	Модульный серверный шкаф.