МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

кафедра компьютерных технологий

«Допущен к защите»
Заведующий кафедрой _____
_____
(Ф.И.О., ученая степень, звание)
_____ «_____»_____ **20__ г.**
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Разработка автоматизированной системы на основе компьютерных сетей

Специальность Вычислительная техника и программное обеспечение

Выполнил (а) Маденов А.К. (Фамилия и инициалы) ВТ-12-2 группа

Научный руководитель Жантлеуов К.К. к.т.н. ст. пр.
(Фамилия и инициалы, ученая степень, звание)

Консультанты:
по экономической части:
Бекенова А.Ж., к.э.н., доцент
(Фамилия и инициалы, ученая степень, звание)
_____ «06» 06 2016 г.
(подпись)

по безопасности жизнедеятельности:
Мазалов Ч.Ф., к.н., проф.
(Фамилия и инициалы, ученая степень, звание)
_____ «2» 06 2016 г.
(подпись)

по применению вычислительной техники:
Жантлеуов К.К. к.т.н. ст. пр
(Фамилия и инициалы, ученая степень, звание)
_____ «_____» 2016 г.
(подпись)

Нормоконтролер: Жантлеуов К.К. к.т.н. ст. пр.
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____ 20__ г.
(подпись)

Рецензент: Сыдыков Б.Д. д.т.н.
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____ 20__ г.
(подпись)

Алматы 2016 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Факультет Аэрокосмических и Информационных технологий
Специальность Вычислительная техника и программное обеспечение
Кафедра компьютерных технологий

ЗАДАНИЕ
на выполнение дипломного проекта

Студент Мадесов Алмат Курмыбаевич
(фамилия, имя, отчество)

Тема проекта „Автоматизированная система на основе компьютерных сетей"

утверждена приказом ректора № 148 от «19» октября 2015 г.
Срок сдачи законченной работы «___» _____ 20___ г.
Исходные данные к проекту требуемые параметры результатов проектирования (исследования) и исходные данные объекта
Курсы CISCO CCNA, программный продукт - Packet Tracer.

Перечень подлежащих разработке дипломного проекта вопросов или краткое содержание дипломного проекта:
1 Теоретическая часть - структура протокола IP, обзор технологий сетей IPv6
2 Техническая часть - разработка корпоративной сети на IPv6
3. Расчётная часть - расчёт полосы пропускания и скорости передачи пакетов.
4. Экономическое обеспечение
5. Безопасность жизнедеятельности

Перечень графического материала (с точным указанием обязательных чертежей)

Иерархическая структура сети организации, логическая структура сети организации, график пропускной способности IPv6, план помещения.

Рекомендуемая основная литература

1. Документация CISCO
2. Документация „Ways to migrate to IPv6"
3. Э.Д. Еркешева, Боканева Г.М. Методические указания к выполнению семестровых работ для студентов спец-ей

Консультанты по проекту с указанием относящихся к ним разделов

Раздел	Консультант	Сроки	Подпись
БЖД	Мазалов И.Ф	11.05 - 2.06.16	
Экономич. часть	Бекмагамбетова А.Ф.	21.04 - 06.06.16	
Основная часть	Жантлеуов К.К.	11.03 - 06.06.16	
Нормоконтролер	Жантлеуов К.К.	27.05 - 06.06.16	

Г Р А Ф И К
подготовки дипломного проекта

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления руководителю	Примечание
1	Получение задания к ДП	22.02.16	
2	Постановка задачи к ДП	23.02.16	
3	Анализ IPv4	24.02.16	
4	Анализ IPv6	25.02.16	
5	Сравнительный анализ протоколов	29.02.16	
6.	Написание основной части ДП	7.03.16	
7	Написание экономического обоснования ДП	4.04.16	
8	Написание части „Безопасность жизнедеятельности"	2.05.16	

Дата выдачи задания «22» февраля 2016 г.

Заведующий кафедрой _____ _____
(подпись) (Фамилия и инициалы)

Руководитель _____ Жантаев К.К.
(подпись) (Фамилия и инициалы)

Задание принял к исполнению
студент _____ Мадесов А.К.
(подпись) (Фамилия и инициалы)

Аннотация

В данной теме объясняется необходимость внедрения протокола IPv6, одним из достоинств которого является его большое адресное пространство.

В данной дипломной работе осуществлено основное представление преимущества протокола IPv6 над его более старой версией в сети. Эффективность доказана с помощью замеров и расчетов основных показателей компьютерных сетей.

По экономической части методом расчета были доказаны все преимущества данного проекта.

Аңдатпа

Осы тақырып түсіндіріледі енгізу қажеттілігі хаттама IPv6, енгізуінің зары түсіндіреді, бір из нешіншінің абзалдықтарынан оның үлкен мекенжайдың аясы болып табылады.

Бұл дипломдық жобада протоколынан Ipv6-ға көшу ең нәтижиелі әдіспен корпоративтік торапта жүзеге асырылған. Тиімділігі көмегімен өлшеу және есептеу негізгі көрсеткіштерінің компьютерлік желілер дәлелденген.

Экономикалық бөлімде берілген жобаны өндіріске ендірудің тиімділігі және экономикалық нәтижесі дәлелденген.

Abstract

This topic explains the need for the introduction of the IPv6 protocol, one of the advantages is that its large address space.

In this research paper carried out a basic understanding of IPv6 advantages over its older version on a network. The efficacy demonstrated by measurements and calculations of the main indicators of computer networks.

In the economic part of the economic benefit justified the introduction of this project in the enterprise.

Содержание

Введение

В современные дни количество пользователей Интернет сети растает с каждым разом. Необходимость выхода в интернет вызвана большим множеством предоставляемых им возможностей и услуг. Среди одних из важных механизмов в его работе – это межсетевые протоколы и IP-адреса. Принцип работы и основная концепция такова: к каждому пользователю при работе в Интернет сети или при работе в более мелкой сети присваивается IP–адрес. Этот адрес является уникальным идентификатором пользователя. IP–адрес идентифицирует непосредственно сеть, к которой подключѐн пользователь, и сам хост. До недавнего времени в сети Интернет применялся только протокол IPv4. По версии этого протокола на IP–адрес выделяется 32 бита. Но так как число пользователей сети Интернет неумолимо растет, то встает вопрос о нехватке сетевых адресов. В связи с этим был разработан протокол IPv6. По версии этого протокола на IP–адрес пользователя выделяется вместо 32 бит - 128 бит, что позволяет значительно расширить размер адресного пространства. Также у этого протокола есть еще ряд положительных сторон по сравнению с протоколом IPv4: более эффективная маршрутизация, поддержка качества обслуживания (Qos), облегчение заголовка, автоматическая конфигурация адресов и другие.

Самым востребованным и используемым протоколом сетевого уровня в стеке протоколов TCP/IP на сегодняшний день является протокол IP, главная задача которого – обеспечение передачи пакетов данных в сетях, которые состоят из определенного количества более мелких сетей. Именно это объясняет то, что протокол IP прекрасно проявляет себя в сетях подобных топологий и рационально пользуясь наличием подсистем и бережно расходует заданную пропускную способность линий связи с низкими скоростями передачи данных. IP объединяет передачу пакетной информации от одного узла к другому узлу IP-сети, не настраивая при этом соединения между отправителем и получателем информации. Важной составляющей Internet Protocol является то, что он дейтаграммный протокол таким образом во время отправки информации по IP абсолютно каждый пакет отправляется по узлам связи и подвергается обработке в узлах в не зависимости от соседних пакетов.

IP в состоянии обеспечить лишь частичную надежность передачи данных, и основывается на протоколе уровня звена данных, способного проконтролировать передачу данных в физическом пространстве среды. Модуль подпрограмм, который реализует IP, задает маршрут доставки информации через каналы связи сетей до находящегося на пути пакета маршрутизатора, где дейтаграмма отделяется от кадра сети и идет на отправку через другой канал, для которого выбирается соответствующий маршрут. Дейтаграммы имеет смысл разделять на мелкие фрагменты, или определенное

количество дейтаграмм объединить на стыке различных сетей, которые должны поддерживать отправку дейтаграмм различной длины.

Целью дипломного проекта является осуществление эффективного перехода на протокол Ipv6 в смоделированной сети, и доказательство того, что это успешно отразится на ее основных показателях. Предстоит решить следующие задачи:

– проанализировать существующие версии протокола IP;

– оценить преимущества и недостатки каждой из версий;

– выбрать наиболее оптимальный метод перехода на IPv6;

– осуществить моделирование сети на основе технологии IP;

– произвести расчет основных параметров до и после внедрения IPv6;

– рассчитать экономическую эффективность проекта;

– раскрыть вопросы безопасности и жизнедеятельности.

1 Основные понятия IP протокола

1.1 Исторические данные

Работая за персональным компьютером, пользователь имеет доступ ко всей информации, которая хранятся на нём. Современная ЛВМ находит применение во многих бизнес процессах и позволяет управлять информацией локально. С возникновением компьютерных сетей, пользователям предоставляется больший спектр предоставления доступа к своим документам и файлам другим пользователям. Раньше же своей информацией мы могли делится, только записав на съемные носители и передав их на другую ЛВМ.

Появилась идея объединить возможности удаленных друг от друга компьютеров, создав компьютерную сеть, что позволило бы пользователям легко обмениваться данными и совместно использовать ресурсы компьютеров. Это гораздо эффективнее по сравнению, с передачей информации через съемные носители. Компьютерные сети могут быть организованы различными методами и инструментарием, к примеру – с помощью кабелей, по которым осуществляется передача данных. Но в последнее время беспроводные сети стали более популярными. для передачи данных беспроводные сети используют радиоволны или инфракрасное излучение. Различают несколько типов сетей:

- ***ГКС (англ. Wide Area Network, WAN)*** – глобальные компьютерные сети. Территория охвата – страны и континенты.

- ***ЛКС (англ. Local Area Network, LAN)***– локальные компьютерные сети. Самый популярный вид сетей, который встречается в жилых домах, в конторах, в офисах мелких и крупных фирм. Такие сети объединяют абонентские системы, расположенные в пределах небольшой территории.

- ***РКС (англ. Metropolitan Area Network, MAN)*** – региональные компьютерные сети. Их территорией охвата, как правило, является город.

- ***ККС*** – корпоративные компьютерные сети. Сети принадлежащие отдельным корпорациям и компаниям.

Интернет – это технология взаимосвязи отдельно взятых компьютерных сетей. Объединенные сети и компьютеры обмениваются друг с другом информацией по каналам публичных телекоммуникационных инфраструктур (по выделенным телефонным аналоговым и цифровым линиям, спутниковым линиям связи, оптическим каналам связи и радиоканалам). Разработка данной

технологии была организована американскими военными в 60-х годах XX века. Основной задачей, которая ставилась перед технологией «Интернет» – было обеспечение компьютерных сетевых коммуникаций расположенных компьютерных сетей при нападении вражеских сил (в том числе ядерных), при которых возможно уничтожение инфраструктур отдельных сетей.

В 1969 году Министерство Обороны США выоплнило проект по совместному использованию ресурсов Министерства Обороны и других государственных учреждений. После создание система получила название ARPANET (Advanced Research Projects Agency Net). Сначала сеть связывала четыре объекта: Калифорнийский университет в Лос-Анджелесе, Стендфордский Исследовательский центр, Университет штата Юта, Университет штата Калифорния в Лос-Анджелесе.

В 1971 году было создано первое программное обеспечение для отправки электронной почты. В 1973 году Норвегия и Великобритания, как иностранные партнеры США, подключились к данной сети. ARPANET в 70-х годах в частности использовался, как инструмент для отправки электронной почты. В это же время были созданы первые доски объявлений, списки почтовой рассылки и новостные группы. В то время сеть ARPANET еще не могла легко скооперироваться с сетями, которые были построены по иным техническим стандартам.

На закате 70-ых годов активно развивались протоколы передачи данных, стандартизованные и получившие лицензию в 1982-83 годах. В январе 1983 года концепция ARPANET заменила NCP на TCP/IP, который нашел применение в объединении сетей по сегодняшний день. Именно применение сетевых протоколов (сетевого программного обеспечения) TCP/IP обеспечило полноценную связь между компьютерами с кроссплатформенными программными и аппаратными средствами в сети, а так же по мимо всего прочего стек TCP/IP предоставил повышенную надежность компьютерной сети (при непредвиденных сбоях, с помощью заранее продуманных сценариев сеть продолжала функционировать).

В 1983 году ARPANET стал известен как «Интернет». В 1984 году была разработана система доменных имен DNS (Domain Name System).

В 1984 году Научный Фонд США (NFS) организовал обширную межуниверситетскую сеть NFSNet (National Science Foundation Network). Данная сеть была объединение сетей меньшего масштаба и имела большую пропускную способность в сравнении с ARPANET. К NFSNet за было подключено свыше 10 тысяч компьютеров. Данная сеть постепенно подхватывала звание «Интернет».

В 1988 году был разработан протокол IRC (Internet Relay Chat), который обеспечивал общение в реальном времени.

В 1989 году в Европе во время проведения Европейского совета по ядерным исследованиям появилась идея Всемирной паутины, которую предложил Тим Бернерс-Ли – человек, который разработал протокол HTTP,

язык HTML и идентификаторы URL. Данная система получила название World Wide Web (WWW или W3).

1990 год стал закатом для сети ARPANET. Она не сохранила конкурентоспособность к сети NFSNet, чья популярность только росла. Первое подключение к сети Интернет с пощью телефонной линии звязи было зафиксировано в конце 90го года, а именно в декабре 1990 года. В 1991 году Всемирная паутина стала общедоступной в Интернете.

В 1995 году NFSNet вернула свое звание – исследовательская сеть. Маршрутизация всего трафика обеспечивалась теперь сетевыми провайдерами, а не суперкомпьютерами Национального Научного Фонда. В это же время HTTP обошел по трафику FTP, возложив на себя бремя основного поставщика информации в Интернет.

В 90-е года Интернет заключил основную часть существовавших в те времена сетей в одну целую и масштабную сеть. Объединение было привлекательным благодаря отсутствию единого начальства, а также открытости технических стандартов, что сделало сети независимыми от бизнеса.

В 1997 году сеть «Интернет» обзавелась уже около 10 миллионами компьютеров, а так же зарегистрировано более 1 миллиона доменных имен. Интернет обрел весьма удобный и популярный характер обмена информацией, что и было основной целью создания этого детища и его предшественников.

В настоящее время существует большой спектр методов и способов подключения к сети «Интернет». Данную услугу можно реализовать через спутники связи, телефон, сотовую связь, кабельное телевидение, радиоканалы, специальные оптико-волоконные линии связи, электропровода и другие методы. Интернет имеет много плюсов и минусов своего существования. Он является некой базой данных, генерирующей в себе множество различной информации, к которой может получить доусуп любой желающий пользователь. Интернет, так же, как и телефон, может соединить любые два компьютера, подключенные к сети. Информация в сети Интернет распространяется широко и быстро, если к ней есть интерес со стороны пользователей.

1.2 Определение и структура протокола IP

IP-адреса – основной тип адресов, который используется на сетевом уровне модели OSI, и ответственен за передачу пакетов между сетями.

Распределение IP-адресов между хостами выполняется:

– автоматически, с участием специальных протоколов (в частности, с помощью протокола DHCP – Dynamic Host Configuration Protocol, протокол динамической настройки хостов).

– вручную, конфигурируется системным администратором;

Протокол IP функционирует на сетевом (межсетевом) уровне стека протоколов TCP/IP. Задачи протокола IP освещены в стандарте RFC-791 и звучат так: “Протокол IP обеспечивает передачу блоков данных, называемых дейтаграммами, от отправителя к получателям, где отправители и получатели являются компьютерами, идентифицируемыми адресами фиксированной длины (*IP-адресами*). Протокол IP обеспечивает при необходимости также фрагментацию и сборку дейтаграмм для передачи данных через сети с малым размером пакетов”.

IP-протокол посылает и обрабатывает любую дейтаграмму как независимый сборник данных, то есть, он не имеет других связей с другими дейтаграммами в глобальной сети интернет.

После посылки дейтаграммы IP протоколом в сеть, протокол лишается контроля над отправленной дейтаграммой, и она должна быть доставлена в пункт назначения. Но если дейтаграмма, по каким-либо причинам, не может дойти до пункта назначения, она уничтожается. Хотя узел, ответственный за уничтожение дейтаграммы, сообщает о причине сбоя отправителю, по обратному адресу (в основном при помощи протокола ICMP). Гарантия доставки данных возложены на протоколы вышестоящего уровня (транспортный уровень), которые используют для этого специальные механизмы (протокол TCP).

Сетевой уровень модели OSI обеспечивает маршрутизаторы основной деятельностью. Одной из первостепенных задач протокола IP – это обеспечение маршрутизации дейтаграмм или определение оптимального пути следования дейтаграмм от узла-отправителя сети к любому другому узлу сети на основании IP адреса. Алгоритм работы протокола ip на определенном узле сети пропускающего дейтаграмму из сети представлен на рисунке 1.1.

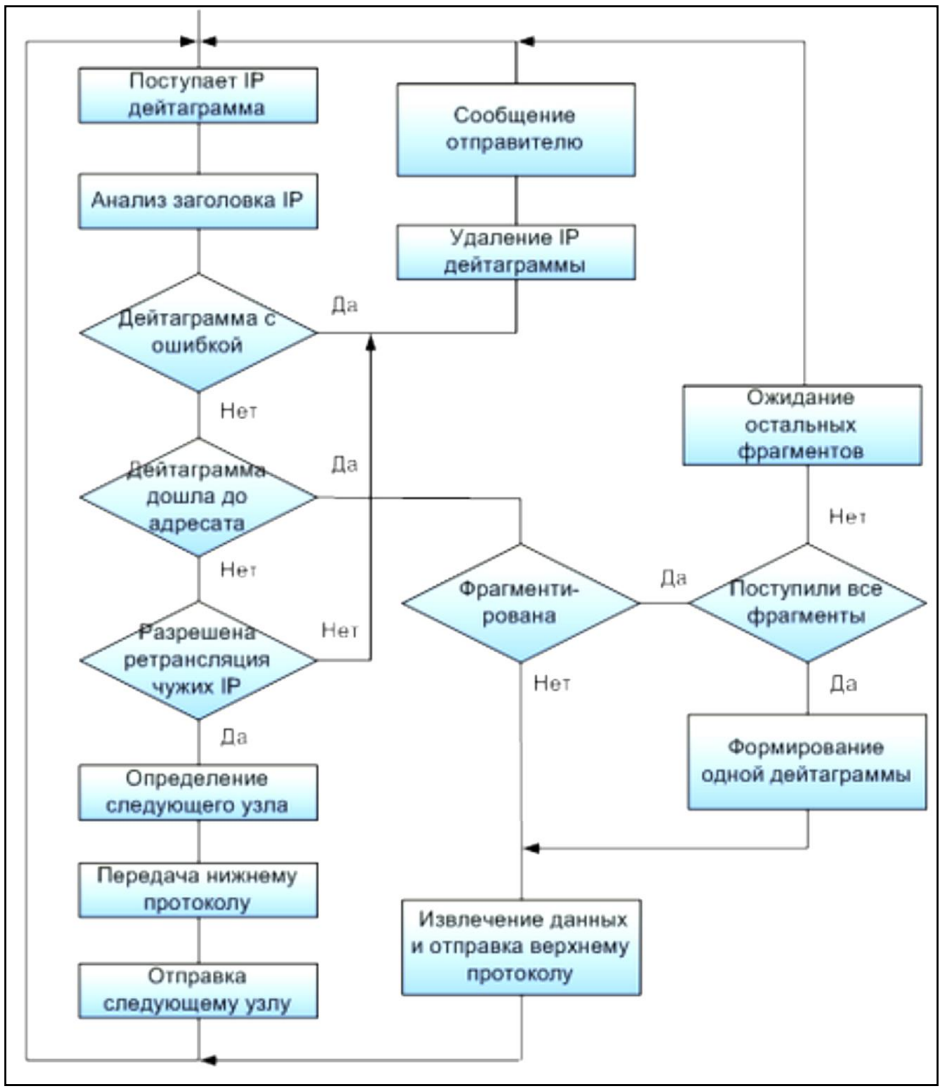

Рисунок 1.1 - Алгоритм работы протокола IP

1.2.1 Формат пакета IP

Существует зависимость с количеством полей пакетного заголовка и функциональной структурой протокола, работающего с этим же заголовком. Простому заголовку соответствует простой протокол. Самая весьма обязывающая деятельность протокола – это обработка служебной информации, которая находится в полях заголовка пакета во время его передачи. Во время изучения назначения каждого поля заголовка IP-пакета, вырисовывается интересная картина о том, что в заголовке пакета есть не только формальные знания о структуре пакета, но и его с основные функции протокола IP.

Поле протокола Ipv4 занимает 4 бита (как показано на рисунке 1.2), что и служит его названием. Сейчас повсеместно используется протокол IPv4. Протокол Ipv6 находит свое применение не так обширно, но скоро настанет такое время, что эта версия будет повсеместно.

Рисунок 1.2 – заголовок IP-пакета

Длина заголовка пакета также составляет 4 бита и измеряется в 32-битных словах. В большинстве случаях заголовок имеет длину в 20 байт (5 32-битных слов), но так же возможно добавление определенной служебной информации, тогда значение будет повышено с помощью лишних битов в поле параметров. Максимально возможная длина заголовка – 60 байт.

Поле типа сервиса (Type of Service, ToS – байт дифференцированного обслуживания (DS-байт). Основная цель этой памяти – хранение свойств, которые задают требования качества обслуживания данных пакетов. В первом случае три бита вмещают в себя приоритетную информацию пакета: от самого низкого – 0 до самого высокого – 7. При получении пакета, маршрутизаторы и компьютеры акцентируют внимание на его приоритет и обрабатывают первостепенно важные пакеты. Следующие 3 бита принадлежащие полю ToS задают критерий выбора маршрута. При значении бита D (Delay – задержка) равному – 1, маршрут задается с минимальной задержкой доставки этого пакета, установленный бит T (Throughput) – для самого большого значения пропускной способности вместе с битом R (Reliability – надежность) – для максимальной надежности доставки. 2 бита, которые остались не задействованными –0.

Благодаря стандартам дифференцированного обслуживания которые были утверждены в 90-ых годах, предоставили новое название данному полю и перераспределили назначения его битов. В DS-байте также применяются в использовании старшие 6 бит. Два младших бита резервируются.

Поле общей длины заполняет память в 16 бит и описывает общую длину пакета при сравнении заголовка и полей данных. Максимальное значение длины пакета ограничено разрядностью поля, которое определет эту величину, и составляет 524280 бит, но в 90% компьютеров и сетей такие большие размеры пакетов не применяются. Во время передачи данных в сетях различного рода, длина пакета заложена с учетом максимальной длины пакета протокола нижнего уровня, несущего IP-пакеты. Если это кадры

Ethernet, то опредеяются пакеты с максимальной длиной 12000 бит, умещающиеся в поле данных кадра Ethernet. В стандартах TCP/IP предусмотрено то, что все хосты обязаны быть готовы принимать пакеты длиной вплоть до 1152 бит.

Идентификатор пакета занимает 16 бит и применяется в качестве распознавания пакетов, которые образовались путем деления на части (фрагментации) исходного пакета. Эти части должны включать в себя одинаковое значение полей.

3 бита выделено под флаги, которые содержат признаки, тесно связанные с фрагментацией. Выставленный в 1 бит DF (Do not Fragment — не фрагментировать) не дает возможности роутерам фрагментировать данную информацию, а заданный 1 бит MF (More Fragments — больше фрагментов) повествует о том, что этот пакет промежуточный фрагмент. Оставшийся бит зарезервирован.

13 бит выделено под смещение фрагмента, которое занимает и предоставляет смещение в памяти поля фрагмента зависящие от начала поля данных исходного пакет говорит от том как же используется в упаковке/распаковке фрагментов пакетов и диктует что смещение должно быть кратно 64 битам.

Поле времени жизни (Time To Live, TTL) занимает 8 бит и применяется как задание максимального времени, в течение которого пакет имеет свободу передвижения по каналам связи сетей. Измерение времени жизни проводится в секундах и устанавливается отправителем. Поскольку современные роутеры обрабатывают пакеты долгое время, чем за одну секунду, то время жизни можно интерпретировать как максимальное число транзитных узлов, которые разрешено пройти пакету. Пакет ликвидируется если значение поля времени жизни нулевое до того, как он достигает пункта назначения. Исходя из этого, время жизни – это часовой механизм самоликвидации пакета.

Поле протокола высшего разряда занимает 2 байта и включает в себя идентификатор, который указывает на протокол верхнего уровня содержащий информацию, и размещен там же. Значение определителей различных протоколов задается по определенным правилам. Например, 6 указывает на то, что в пакете находится сообщение TCP, 17 –UDP, 1 – ICMP.

Контрольная сумма заголовка занимает 16 бит и определяется только по заголовку. Так как одни поля заголовка изменяют значение битов во время отправки пакетов по сети, контрольная сумма сравнивается и повторно определяется в каждом роутере и узле в роли дополнения к сумме всех 16-битных предложений заголовка. Во время определения контрольной суммы значение этого же поля контрольной суммы становится 0.

Поля IP-адресов источника и приемника имеют постоянную длину — 16 байт.

Поле параметров необязательно и применяется только при реконфигурировании сети. Данное поле включает несколько подполей одного из восьми предопределенных типов. В этом подполе можно задавать точный

маршрут, записывать проходимые пакеты роутером, располагать данные системы безопасности или непостоянные заметки. Из-за того, что количество подполей в поле параметров произвольное, то в конце заголовка обязательно добавляется несколько нулевых байтов для выравнивания заголовка пакета по 16-байтной границе.

1.3 Анализ версий протокола IP

Адрес.

IPv4. Длина - 32 бита. Адрес складывается из адреса сети и адреса хоста. Длина данных компонентов напрямую зависима от класса адреса. Адреса делятся на классы A, B, C, D и E. Класс адреса определяется несколькими начальными битами адреса. Общее число адресов IPv4 составляет 4294 967296.

IPv4 имеет следующий текстовый вид: nnn.nnn.nnn.nnn, где 0<=nnn<=255, а каждое значение переменной n – десятичная цифра. Незначащие нули опускают. Максимальная длина адреса составляет 15 символов, без учета маски или префикса сети.

IPv6. Длина –128 бит. На данный момент первые 64 бита отображают номер сети, а вторые 64 бита – номер хоста. Часто в качестве номера хоста или его компонента в адресе IPv6 получается на основе MAC-адреса или другого идентификатора интерфейса.

Архитектура IPv6 на вид и сложнее архитектуры IPv4.

Количество адресов IPv6 в 7,9 септиллионов (79228162514264337593543950336) раз больше числа адресов IPv4.

В текстовом виде адрес IPv6 записывается как hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh, где каждая буква h – это шестнадцатеричная цифра, представляющая 4 бита. Незначащие нули можно не указывать. В текстовом формате вместо любого числа нулей в адресе можно использовать двойное двоеточие(::). Например, адрес ::ffff:10.120.78.40 представляет собой адрес IPv6, преобразованный в IPv4.

Расположение адреса.

IPv4. Изначально распределение адресов проводилось по классам сетей. Но после стремительного уменьшения числа свободных адресов, они были разбиты на более мелкие группы с помощью протокола Бесклассовой междоменнай маршрутизации (CIDR). Адреса не были равномерно распределены между различными организациями и странами.

IPv6. Распределение адресов пока находится на низшей ступени развития данной технологии. Рабочая группа Интернет (IETF) и группа, которая ответственна за проектировку архитектуры Интернет (IAB), предлагали каждой организации, домашнему компьютеру или устройству префикс подсети размером /48 бит. В этом случае еще 16 бит префикса

останется для идентификатора подсети. Пространство адресов безгранично для того, чтобы предоставить каждому жителю планеты собственный префикс подсети длиной /48 бит.

Срок действия адреса.

IPv4. Этот атрибут устанавливается только для адресов IPv4, распределенных DHCP-сервисом.

IPv6. Для адресов IPv6 задается два срока действия: предпочитаемый и допустимый, причем предпочитаемый срок действия всегда <= допустимого.

Префикс адреса.

IPv4. Иногда применяется для отделения адреса сети от адреса хоста. В некоторых случаях указывается в адресе в виде суффикса /dd.

IPv6. Применяется для определения префикса подсети в адресе. Указывается в виде суффикса /hhh (максимум 3 десятичные цифры, 0 <=hhh <= 128). Примером может служить адрес FD80::983:2f5f/10, в котором первые 10 бит – это префикс подсети.

Тип адресов.

IPv4. Адреса IPv4 подразделяются на 3 основных вида: обычные, групповые и широковещательные адреса.

IPv6. Адреса IPv6 делятся на 3 основных вида: обычные, групповые и нечеткие адреса.

Трассировка соединений

Трассировка соединений в IPv4 – средство для сбора подробной информации о пакетах TCP/IP и других пакетах, которые используются и рассылаются системой. Эту же поддержку имеет и IPv6.

Настройка.

IPv4. Чтобы новая система смогла устанавливать соединения с другими системами, в ней нужно настроить IP-адреса и маршруты.

IPv6. Настройка необходима только для применения некоторых функций. Интерфейсы IPv6 настраивают сами себя путем автоматической настройки IPv6 без сохранения состояния. Кроме того, интерфейс IPv6 можно настроить вручную. В результате система сможет подключаться к другим локальным или удаленным системам IPv6, в зависимости от типа сети и наличия маршрутизатора IPv6.

Система имен доменов (DNS).

IPv4. Приложения, используют DNS для конвертирования имен хостов в IP-адреса с помощью API сокетовgethostbyname( ). А так же с помощью DNS приложения могут конвертировать IP-адреса в имена хостов. Для этого

используется API gethostbyaddr( ). В IPv4 для обратного конвертирования используется домен in-addr.arpa.

IPv6. Аналогично.

Протокол динамической настройки хостов (DHCP).

IPv4. DHCP используется для динамической выдачи IP-адреса и других настроек. IBM i поддерживает сервер DHCP для IPv4.

IPv6. Реализация DHCP IBM i не поддерживает IPv6. Но реализацию Сервера ISC DHCP использовать реально.

Таблица хостов.

IPv4. Конфигурирумая таблица связывающая IP-адрес с именем хоста (например, 127.0.0.1, циклический адрес). Эта таблица применяется программой преобразования имен сокетов. Эта программа вызывается перед обращением к DNS, либо после обращения к DNS, если преобразование выполнить не удалось (порядок обращения зависит от приоритета поиска имени хоста).

IPv6. Аналогично.

Интерфейс.

IPv4. Объект логики, который применяется в TCP/IP с целью доставки пакетов. В IPv4 данный термин часто тесно связан с адресом, а иногда эквивалентен ему. Иногда интерфейс называется логическим интерфейсом.

Интерфейсы IPv4 запускаются и завершают работу независимо друг от друга и от TCP/IP. Для запуска и завершения работы интерфейса можно воспользоваться командами STRTCPIFC и ENDTCPIFC, а также System i Navigator.

IPv6. Аналогично.

Протокол управляющих сообщений Интернет (ICMP).

IPv4. Используется в IPv4 для обмена данными о сети.

IPv6. Аналгично, однако протокол управляющих сообщений Интернет версии 6 (ICMPv6) в запасе имеет множество новых атрибутов.

Протокол Интернет для управления группами (IGMP).

IPv4. IGMP используется маршрутизаторами IPv4 для обнаружения хостов, которым должна поступать информация многоцелевой рассылки. А так же, он используется IPv4хостами для оповещения маршрутизаторов IPv4 о наличии на хосте получателей многоцелевой рассылки.

IPv6. IGMP заменен на протокол MLD для IPv6. MLD протокол выполняет те же функции, что и протокол IGMP в IPv4. Он применяет протокол ICMPv6, в котором предусмотрено несколько новых типов, предназначенных для MLD.

Заголовок IP.

IPv4. Длина составляет 160–480 бит относительно числа дополнительных настроек IP.

IPv6. Длина составляет ровно 320 бит. В заголовке IP никакие дополнительные параметры не указываются. Как правило, структура заголовка IPv6 проще, чем в IPv4.

Дополнительные параметры заголовка IP.

IPv4. Различные дополнительные атрибуты, которые можно задать в заголовке IP (впереди заголовка транспортного уровня).

IPv6. В заголовке IPv6 дополнительные параметры не указываются. Вместо них IPv6 добавляет дополнительные заголовки. Такие заголовки могут содержать информацию AH и ESP (как и в IPv4), а также информацию о прохождении транзитных участков, маршруте, фрагменте и получателе. В настоящее время IPv6 поддерживает несколько заголовков расширения.

Байт протокола в заголовке IP.

IPv4. Код протокола транспортного уровня. Примером значения может служить ICMP.

IPv6. Заголовок, который указывается сразу после заголовка IPv6. В нем задаются те же значения, что и в поле протокола заголовка IPv4. После этого заголовок будет определен еще ряд дополнительных заголовков, формат которых может быть расширен. Следующим может быть указан заголовок транспортного протокола, один из дополнительных заголовков или заголовок ICMPv6.

Байт Тип сервиса в заголовке IP.

IPv4. Используется протоколом QoS и дифференцированными службами для определения класса потока данных.

IPv6. Применяет различные коды для обозначения класса трафика IPv6. В настоящее время протокол IPv6 не поддерживает поле TOS.

Соединение LAN.

IPv4. Соединение LAN применяется интерфейсом IP для подключения к физической сети. Существует несколько типов, например, Token Ring и Ethernet. Иногда называется физическим интерфейсом, каналом связи или линией связи.

IPv6. IPv6 может использоваться любым адаптером Ethernet, кроме того, этот протокол применим в виртуальной сети Ethernet между логическими разделами.

Протокол L2TP.

IPv4. Протокол L2TP можно рассматривать как виртуальный протокол PPP. Он может применяться при работе с любой поддерживаемой линией связи.

IPv6. Аналогично.

Циклический адрес.

IPv4. Циклический адрес - это интерфейс с адресом вида 127.·.·.· (как правило,127.0.0.1), который может применяться узлом только для отправки пакета самому себе. Соответствующий физический интерфейс (описание линии) называется ·LOOPBACK.

IPv6. Такой же принцип, как и в IPv4. Предусмотрен единственный циклический адрес -0000:0000:0000:0000:0000:0000:0000:0001, либо ::1 (сокращенный вариант). Соответствующий виртуальный физический интерфейс называется ·LOOPBACK.

Максимальный блок передачи (MTU).

IPv4. Максимальный блок передачи - это максимальное число байт, которое можно передать по линии связи определенного типа, например, линии связи Ethernet или модемной линии. Обычно в IPv4 максимальный блок передачи равен 576.

IPv6. В IPv6 минимальный размер MTU составляет 1280 байт. Следовательно, пакеты IPv6, размер которых меньше этого ограничения, не разбиваются на фрагменты. Для передачи пакетов IPv6 по линии связи с размером MTU меньше 1280 байт эти пакеты должны разбиваться и собираться на уровне канала связи.

Порты.

IPv4. В TCP и UDP применяются разные наборы портов, номера которых находятся в диапазоне от 1 до 65535.

IPv6. В IPv6 применяются аналогичные порты. Поскольку в этом протоколе предусмотрено новое семейство адресов, число наборов портов увеличилось до четырех. Например, предусмотрено два порта TCP с номером 80, к которым могут подключаться приложения: один из них находится в AF_INET, а второй – в AF_INET6.

Внутренние и внешние адреса.

IPv4. Все адреса IPv4 являются внешними. Исключение составляют три диапазона внутренних адресов, определенных организацией IETF в документе RFC 1918: 10.·.·.· (10/8), 172.16.0.0 -172.31.255.255 (172.16/12) и 192.168.·.· (192.168/16). Внутренние адреса обычно применяются в различных организациях. Такие адреса не распознаются в Интернет.

IPv6. В IPv6 применяется аналогичная структура адресов, но с некоторыми существенными различиями. Адреса делятся на внешние и

временные (временные адреса ранее назывались анонимными). Дополнительная информация приведена в RFC 3041. В отличие от внутренних адресов IPv4, временные адреса распознаются в глобальной сети. Они применяются для другой цели. Временный адрес скрывает идентификатор клиента, устанавливающего соединение (по соображениям защиты). Срок действия временного адреса ограничен. Такой адрес не содержит идентификатор интерфейса, то есть адрес канала связи (MAC). Как правило, временный адрес нельзя отличить от обычного внешнего адреса.

В IPv6 также есть понятие ограниченного адресного пространства, связанное с предусмотренным распределением адресов.[4]

Таблица протоколов.

IPv4. В System i Navigator - таблица, содержащая имена протоколов и связанные с ними номера портов. Например: UDP, 17. По умолчанию в таблице есть записи для следующих протоколов: IP, TCP, UDP, ICMP.

IPv6. Эта таблица может применяться в IPv6 без изменений.

Quality of service (QoS).

IPv4. QoS предоставляет возможность задания приоритета пакетов и пропускной способности для приложений TCP/IP.

IPv6. На данный момент QoS который был реализован специально для IBM i, не считывает IPv6 информацию.

Изменение адреса.

IPv4. Изменение адреса осуществляется статически или динамически с помощью DHCP. Данный процесс весьма трудоемкий и его реализация рекомендована лишь в случае крайней необходимости.

IPv6. Одна из наиболее важных встроенных функций IPv6, которая ощутимо автоматизирована, этот процесс проходит без осложнений с префиксом /48.

Маршрут.

IPv4. Любое допустимое количество IP-адресов, которые связанны с парой значений, а так же которое вмещает в себя имя физического интерфейса и IP-адрес последующего транзитного узла. Пакет пересылается по указанному транзитному узлу по заданной линии связи, если адрес получателя IP-пакета входит в pool адресов данного пакета. Маршруты IPv4 тесно связаны с интерфейсом IPv4, что означает, что он связан и и с адресом IPv4. Defaultgetway обеспечивается *DFTROUTE.

IPv6. Аналогично. Но существует одно весомое отличие: маршруты IPv6 связаны с физическим интерфейсом (каналом связи, например, ETH03), а не с логическим интерфейсом. Одна из причин связи маршрута с физическим интерфейсом заключается в том, что в IPv6 и в IPv4 применяются разные алгоритмы выбора адреса отправителя.

Протокол информации о маршрутизации (RIP).

IPv4. RIP - протокол маршрутизации, поддерживаемый демоном routed.

IPv6. На сегодняшний день протокол RIP не поддерживается протоколом IPv6 и наоборот.

Неопределенный адрес.

IPv4. Данного типа адреса нету. В программировании сокетов 0.0.0.0 применяется в качестве INADDR_ANY.

IPv6. Равен ::/128. Отмечается в роли IP-адреса отправителя в некоторых пакетах при поиске соседей и в иных случаях, к например – при работе с сокетами. В приложениях с API сокетов адрес ::/128 применяется в роли in6addr_any.

Запуск и завершение работы.

IPv4. С целью запуска и завершения работы IPv4 используются команды STRTCP и ENDTCP. IPv4 запускается при исполнении STRTCP специально для запуска TCP/IP.

IPv6. Для запуска или завершения работы IPv6 служит параметр STRIP6 или STRTCP и ENDTCP. IPv6 имеет возможность не быть задействованным во время запуска TCP/IP. Запуск возможно произвести отдельно.

1.4 Преимущества и недостатки

Основные недостатки протокола IPv4:

- дефицит адресного пространства;
- слабая расширяемость протокола;
- проблема безопасности коммуникаций;
- отсутствует поддержка качества обслуживания;
- проблемы, связанные с механизмом фрагментации;
- отсутствует механизм автоматической конфигурации адресов;
- проблема перенумерации машин.

За исключением ярко выраженного преимущества в расширении адресного пространства, существуют следующие преимущества IPv6 над IPv4:

- возможность автоматической настройки IP адресов.
- упрощение маршрутизации.
- упрощение заголовка пакета.
- поддержка качества обслуживания (QoS).

Недостатки IPv6

В частности, IPv6 должны быть полезны для поднятия на ступень эволюции нынешнего интернета, у этого протокола имеются ярко выраженные недостатки.

Тем не менее, план перехода с протокола IPv4 на IPv6 еще нигде не был осуществлен. Более того, без необходимого метода перехода невозможно само быстрое развитие нового, надёжного и эффективного интернет протокола. Таким образом, проблема остаётся на данный момент нерешённой и трудно обходимой.

Будущее интернета очень сильно зависит от данного протокола. Потребность во все большем расширении всемирной паутины будет еще долгие годы и на текущий момент ни одному другому протоколу, не под силу решить этот вопрос. Переход на новую версию прокола IP протекает молниеносными темпами, хоть это и незаметно невооруженным глазом, и уже в скором времени вся сеть интернет будет работать под управлением этого протокола, хочет того наша цивилизация или нет.

1.4 Обзор технологий взаимодействия сетей IPv4 и IPv6

Очевидно, что переход на технологию IPv6 не может быть мгновенным. Еще долгое время сетям IPv4и IPv6 придется сосуществовать. Поначалу сети IPv6 будут казаться островами вокруг океана IPv4. Сначала узлы, поддерживаемые протоколом IPv6, не предоставляют необходимых сервисов. Поэтому есть необходимые требование для узлов IPv6: возможность взаимодействия с узлами IPv4; возможность передачи пакетов IPv6 через существующую инфраструктуру IPv4.

Из выше сказанного следует, что необходимы механизмы, которые будут обеспечивать сосуществование сетей IPv4 и IPv6. Этот симбиоз систем, использующих разные стеки протоколов в большинстве случаях осуществляется при помощи применения следующих методов:

– трансляция;
– мультиплексирование.
– инкапсуляция (туннелирование);

Мультиплексирование. В процессе мультиплексирования в сетевое оборудование или в серверные ОС помещаются несколько стеков протоколов. На узлах сети помещается определенное количество стеков коммуникационных протоколов – в зависимости от числа сетей, использующие различные сетевые протоколы. Необходимо настроить бесперебойную обработку запросов определенных протоколов. Для этого используется специальный программный элемент – мультиплексор

протоколов или протокольный менеджер, в задачи которого входит определение пути назначения запроса отправленным клиентом.

Трансляция. Трансляция отвечает за согласование стеков протоколов путем конвертирования форматов сообщений. Помимо этого данный процесс включает в себя – предоставление адресов узлов и сетей, которые различным образом задаются этими протоколами. Данный сервис могут осуществлять: программный или аппаратный шлюз, мост, коммутатор, маршрутизатор и другое сетевое оборудование. Расположение транслирующего элемента находится между взаимодействующими сетями. Данная дислокация наделяет это устройство правами посредника при передаче сообщений из сети, использующей один протокол в сеть, которая использует другой протокол.

Инкапсуляция (туннелирование). Данный процесс является одним из методов, который предоставляет помощь при взаимодействии сетей, использующие различные сетевые протоколы. Инкапсуляция применима, вовремя необходимости осуществления взаимодействия двух сетей с одной технологией посредством транзитной сети, в которой используется другая технология.

Протоколы которые принимают участие в туннелировании:

– протокол инкапсуляции;

– транспортируемый протокол;

– несущий протокол.

Протокол который транспортируется – это протокол на чью долю выпадает синдикат сетей, протокол же транзитной сети по определению будет несущим. Протокол инкапсуляции помогает пакетам транспортируемого протокола помещаться в поле данных несущего протокола. В смешанных сетях IPv4–IPv6 наиболее используемыми методами являются: мультиплексирование и туннелирование. Данные методы позволяют узлам сети, использующей протокол IPv6, производить обмен с узлами другой IPv6 сети посредством сети, в которой применяется протокол IPv4. Для того, чтобы узлы, которые поддерживают протокол IPv6, имели возможность обращаться к ресурсам сети IPv4, необходимы специальные сервисы: шлюзов транспортного и прикладного уровня, трансляторов протоколов и др. Сейчас разрабатываются механизмы, которые предоставляли бы возможность протоколу IPv6 без препятствий действовать поверх сетей, которые поддерживают только протокол IPv4. Но в будущем обязательно потребуются механизмы, которые позволят передавать IPv4 через сети, которые поддерживают только протокол IPv6, так как к определенному моменту он станет основным сетевым протоколом.

Механизм мультиплексирования оказывает одновременную поддержку узлам двух стеков протоколов. Осуществляется это, чтобы каждый узел имел 2 адреса: IPv4 и IPv6. данные адреса не имеют связей друг для друга. Уникальность адресов IPv4 должна сохранятся. К тому моменту как адресное пространство IPv4 исчерпает себя полностью, процесс перехода на IPv6

должен зайти достаточно далеко, чтобы недавно подключенные узлы имели возможность получения всех необходимых услуг, используя исключительно средства протокола IPv6.

Для обеспечения единовременной поддержки 2-ух стеков протоколов необходимы соответствующие инфраструктурные возможности. Например, DNS сервис должен выдавать записи типа «A» – 32-битный IP-адрес, так и записи типа «AAAA» с 128-битным адресом. От результата DNS-запроса может зависеть то, каким стеком воспользоваться.

Инкапсуляция долгое время применяется в IPv4 для передачи не IP-пакетов. В случае с IPv6 применяется механизм инкапсуляции, который отображен на рис. 1.3. Пакет IPv6 помещается в поле данных пакета IPv4, затем транспортируется по нормальной сети IPv4. На момент прибытия в пункт назначения пакет IPv6 выходит из поля данных пакета IPv4 и идет на обработку обычным образом. У него есть два пути: 1– либо он транспортируется дальше (это происходит уже по IPv6-сети), и 2 – либо он используется получателем. Несущим протоколом является IPv4, а транспортируемым IPv6. Протокол IPv4 играет роль протокола канального уровня с точки зрения IPv6, поэтому поле HopLimit в пакете IPv6 будет уменьшено только на единицу (если потребуется дальнейшее перенаправление пакета). Обычно целый маршрут пакета данных IPv6 подключает множество туннелей по транзитным сетям IPv4.

Рисунок 1.3 – Механизм инкапсуляции

Наличие механизма инкапсуляции увеличивает функциональные возможности узлов, являющимися конечными точками туннеля. Великая сила налагают большую ответственность. Узел который принимает данные должен опознать пакет IPv6 в поле данных пакета IPv4. Проверка в заголовке пакета IPv4 поля «Протокол» провидится именно с этой целью. Значение этого поля в данном случае должно быть равно десятичному числу 41.

Максимально возможный размер пакета – MTU, который должен отправиться через интерфейс IPv6 равно 12240 бит. С целью – предотвратить ненужную фрагментацию, система использует следующие значение MTU пакета IPv6, которое вместе с заголовком поместился в разрешенном значении

MTU пакета IPv4. Пересылаемый IPv6 пакет не предоставляет возможности – разместить его целиком в поле данных пакета IPv4, инкапсулирующий узел имеет возможность послать сообщение ICMPv6 назад к узлу-источнику.

Во время приема пакета IPv4, который несет внутри поля данных пакет IPv6, система должна обычным образом отфильтровать трафик по исходному адресу: пакет игнорируется, если это спец-адрес – для широковещательной или многоадресной рассылки и если этот исходный адрес равен 0.0.0.0 или 127.x.x.x. Затем игнорируется туннелирующий заголовок пакета IPv4, и методы фильтрации применимы уже к пакету IPv6.протокол IPv6 так же имеет особые адреса. Это адреса многоадресной рассылки, неопределенные адреса, особые адреса, полученные отображением IPv4 на IPv6, а также адреса обратной петли. Затем отдается IPv6 стеку и поддается обработке как нормальный пакет данных IPv6. Узел не осуществляет дальнейшую маршрутизацию пакета IPv6, если эти полномочия не возложены на конфигурацию IPv4 адреса, с которого был отправлен пакет. следовательно, маршрутизация этого пакета IPv6 может осуществляться, если узел настроен качестве пункта назначения туннеля, пунктом отправки которого является IPv4-адрес узла-отправителя.

Обработка других сообщений IPv4 зависит от того, что какая либо часть сообщения, вызвавшее ошибку и содержится в ICMP-пакете. В зависимости от передачи ICMP, сообщение этого протокола кроме внешнего заголовка IPv4 может содержать 8 и более байт поля пакета IPv4, которому принадлежит это управляющее сообщение. Если этих данных достаточно для реконструкции заголовка IPv6, то генерируется сообщение ICMPv6 и отправляется узлу-источнику IPv6.

Можно выделить четыре вида туннелей:

1. хост – хост;
2. маршрутизатор – хост;
3. хост – маршрутизатор;
4. маршрутизатор – маршрутизатор.

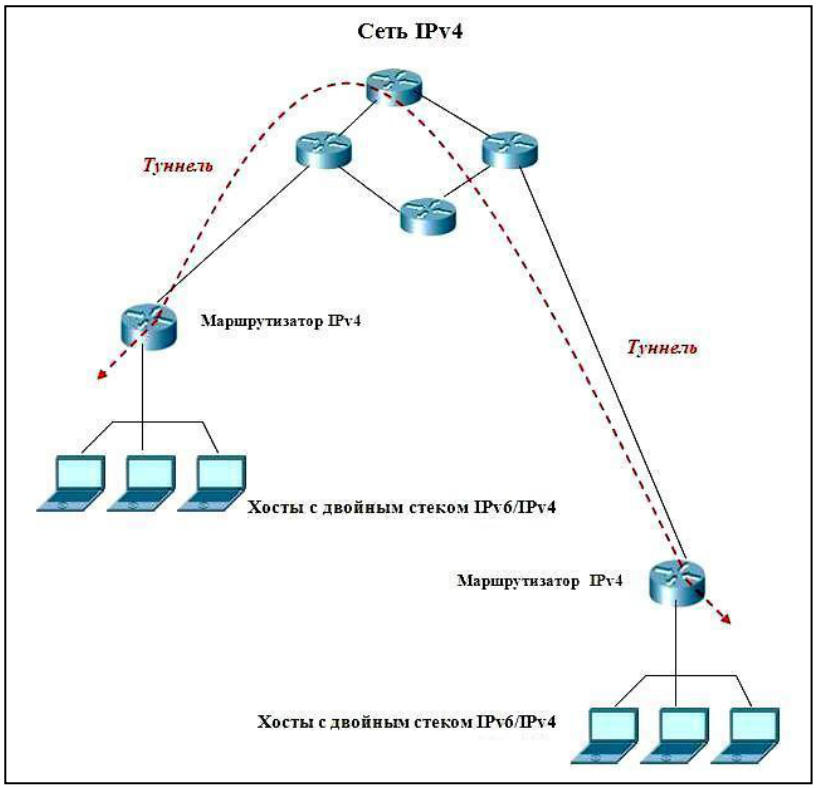

Рисунок 1.4 – Туннель «хост – хост»

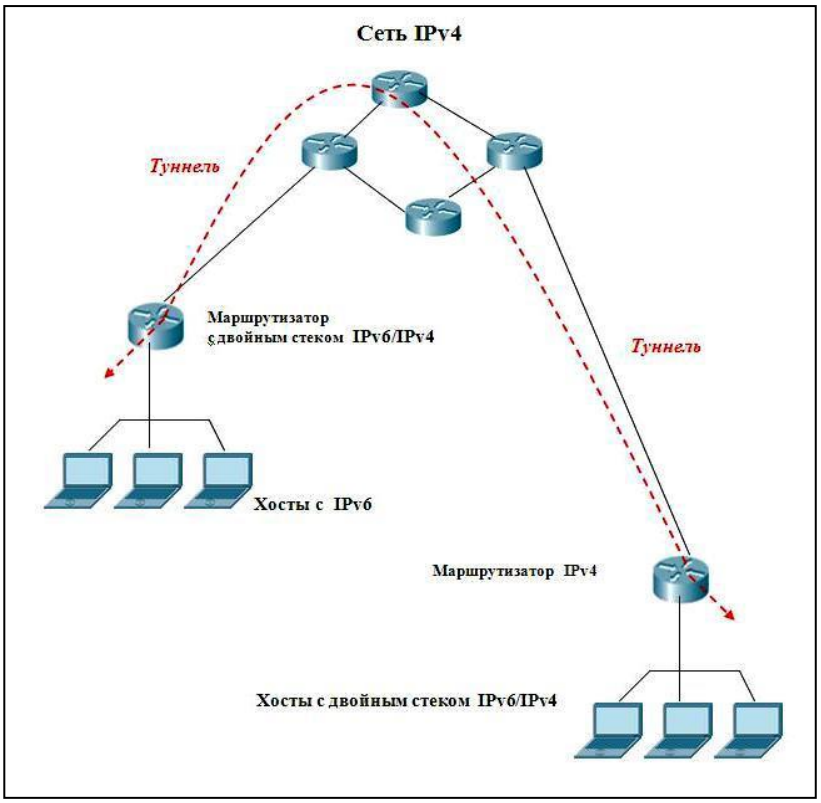

Рисунок 1.5 – Туннель «маршрутизатор – хост»

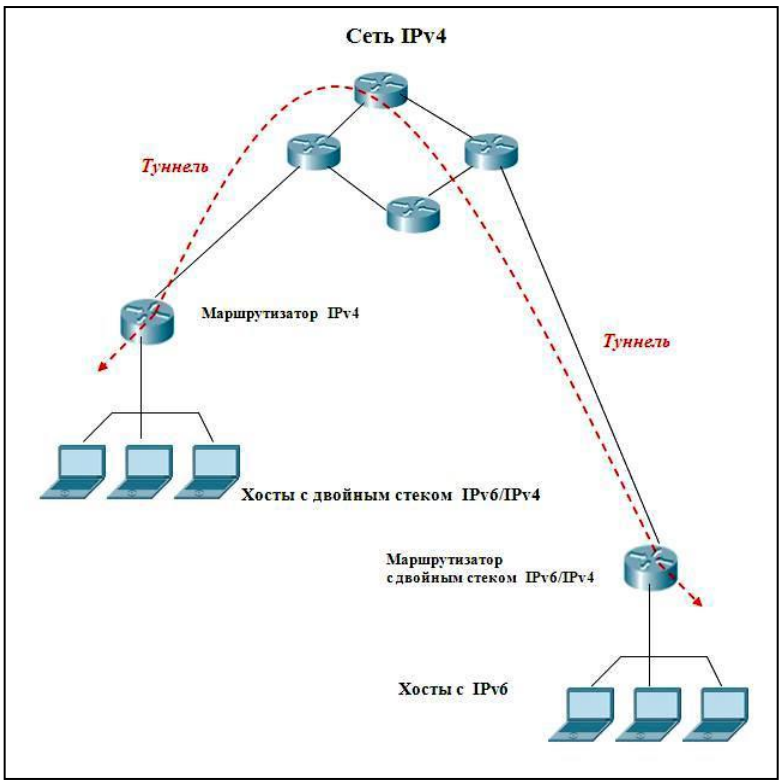

Рисунок 1.6 – Туннель «хост – маршрутизатор»

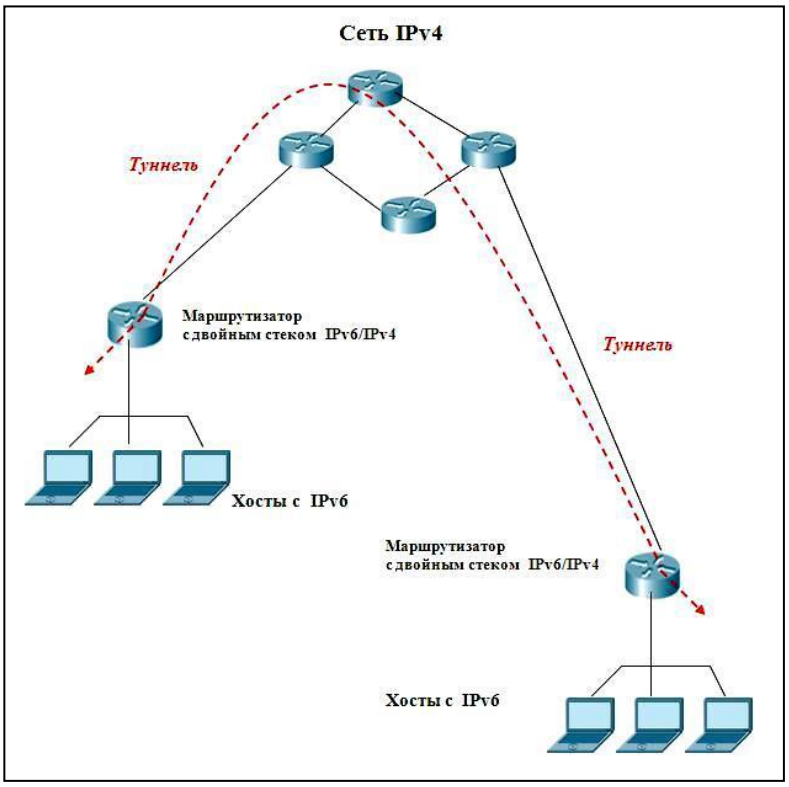

Рисунок 1.7 –Туннель «маршрутизатор – маршрутизатор»

В первых двух разновидностях туннелирования пункт назначения туннеля совпадает с пунктом назначения маршрута IPv6 пакета. Адрес пункта назначения туннеля обязан автоматически генерироваться в качестве функции

адреса целевого хоста. Для возможности автоматического туннелирования необходимо, чтобы IPv6-адреса были IPv4-совместимыми. Т.е приписывание с левой стороны Ipv4 адреса 96 нулевых бит образует IPv6 адрес.

Когда конечная точка туннеля (роутер) не определяется по адресу целевого хоста, то имеется необходимость использовать заранее сконфигурированное туннелирование. При этом параметры туннеля задаются маршрутной таблицей в инкапсулирующем узле. данный подход применим, когда целый адрес не является IPv4-совместимым. В этом случае источник-хост обязан быть знакомым с IPv4-адресом роутера, имеющим двойной стек, который предназначен для организации доставки IPv6-пакета.

Несколько концов туннеля (и автоматического, и вручную сконфигурированного) должны обладать IPv4-совместимыми адресами.

2 Разработка корпоративной сети с Ipv4 адресацией

2.1 Обзор Packet Tracer

Cisco Packet Tracer – программный продукт, основной задачей которого является эмуляция сети а так же изучение построений и настроек сетей, который был создан компанией Cisco. Работа с интерактивным симулятором предоставляет возможность правдоподобного ощущения настройки реальных сетей, состоящих из десятков или даже сотен устройств. Программа в бесплатном доступе, что делает ее по настоящему привлекательной и востребованной в области сетей и коммуникаций. Интерфейс данного ПП изображен на рисунке 2.1.

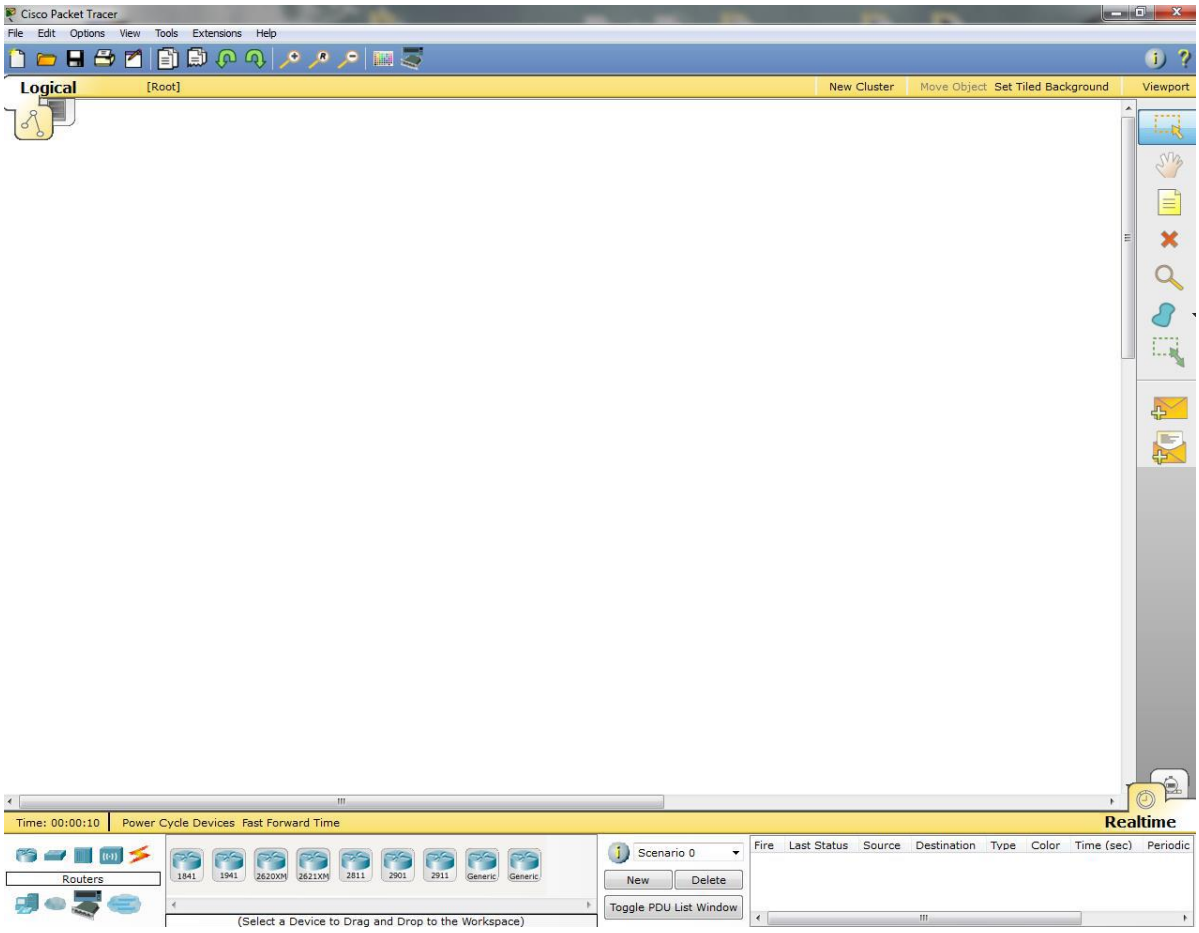

Рисунок 2.1 – Интерфейс программного продукта Packet Tracer

Сверху, над рабочей областью, располагается главная панель программы и ее меню, которые представлены на рисунке 2.2.

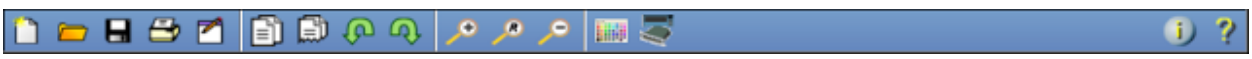

Рисунок 2.2 – Главное меню

Правее рабочей области, располагается боковая панель, которая имеет при себе множество кнопок которые отвечают за смену расположения полотна рабочей области, удаление объектов и т.д. Снизу, под рабочей областью, расположена панель оборудования. Всё это изображено на рисунке 2.3.

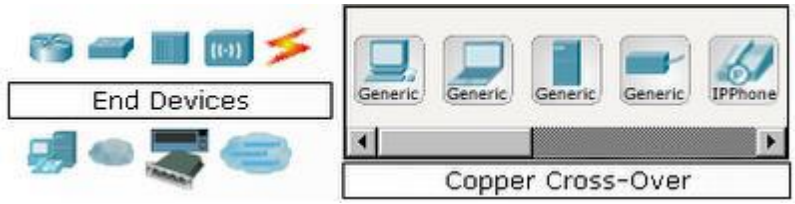

Рисунок 2.3 – Панель оборудования

Во время наведения на любое из устройств, в прямоугольнике, находящемся в центре посреди них будет представлен его тип. Типы устройств, наиболее часто используемые в работах с Packet Tracer, представлены на рисунке 2.4.

Рисунок 2.4 – Основные типы устройств

Рисунок 2.5 – Типы соединений устройств в Packet Tracer

Автоматический тип – при таком виде подключения Packet Tracer автоматически применяет наиболее предпочтительный тип соединения для подключаемых устройств.

Для подключения консоли требуется консольные соединение.

Медное прямое – соединение медным кабелем типа витая пара, оба конца кабеля обжаты в одинаковой раскладке, предпочтительнее для соединений: коммутатор – коммутатор, коммутатор – маршрутизатор, коммутатор – компьютер и другие.

Медный кроссовер – соединение медным кабелем типа витая пара, каждый конец кабеля обжат в качестве кроссовера. Предпочтителен для соединений двух оконечных устройств.

Оптический кабель – соединение с помощью оптического кабеля, необходимо для соединения устройств имеющих оптические интерфейсы.

Телефонный кабель – обычный телефонный кабель, который необходим для подключения телефонных устройств.

Коаксиальный кабель – соединение устройств с помощью коаксиального кабеля.

Бладгодаря возможности режима визуализации, Cisco Packet Tracer предоставляет пользователям отследить транспортировку информации по каналам связи сети, конфигурирование IP-пакетов при прохождении информации по сетевым устройствам, скорость, время и маршрут перемещения пакетов. Анализ событий, которые возможны в сети, предоставляет возможность сменить механизм функционирования данной сети, а так же обнаружить и ликвидировать отказы в системе.

Данный ПП предназначен не только в роли симулятора, но и в роли сетевого приложения эммуляции сетей на основе реально существующих сетей, в том числе Интернет. Пользователям предоставляется возможность работать над одним проектом, управляя им, удаленно друг от друга. Данная привилегия многопользовательской системы очень востребована в организациях совместной проектной деятельности.

Кроме этого Cisco Packet Tracer позволяет пользователям симулировать построение не только логические, но и физические модели сетей, таким образом, получать навыки проектирования. Топология может быть перенесена на проект здания или города а так же спроектировано всё кабельное пространство, размещение устройств в помещениях зданий с учетом физических ограничений, таких как длина и тип прокладываемого кабеля или радиус зоны покрытия беспроводной сети.

Cisco Packet Tracer стал уникальным инструментом для обучения сетевым технологиям с помощью таких сервисов как Многопользовательский режим и Визуализация.

2.2 Анализ требований и задач предприятия

При проектировании компьютерной сети в первую очередь необходимо определить для каких целей она будет использоваться, что в свою очередь предполагает необходимость хотя бы первичного анализа сферы деятельности предприятия, его основных задач и организационной структуры. Согласно варианту коммуникационная сеть будет проектироваться для Банка (ЦАБ – «Центрально Азиатский Банк»). Банк – это организация, оказывающая финансовые услуги. С точки зрения проектирования сети банк – это организация, в которой постоянно проводится большое количество краткосрочных операций (финансовых транзакций, запросов данных) во

внутренней сети организации (интранете). Обеспечение доступа в интернет является второстепенной задачей и необходимо только для определенного ряда подразделений и департаментов. Следовательно, банковская сеть объединяет в структурированную и управляемую замкнутую систему все принадлежащие компании информационные устройства: отдельные компьютеры и локальные вычислительные сети (LAN), серверы, рабочие станции, телефоны, факсы, офисные АТС, сети банкоматов, онлайновые терминалы.

Основываясь на приведенной информации можно выделить основные задачи использования сети:

- доступ к высокопроизводительной системе обмена информацией (Базе данных);
- коллективная работа и совместная обработка информации;
- централизованное резервное копирование всех данных;
- публикация документов во внутренней сети и/или в Интернет (WWW сервер).
- контроль за доступом к важным данным.

При этом основными требованиями, предъявляемыми к сети, являются:

- Безопасность. Большая часть информации, используемой банком, является строго конфиденциальной, за исключением некоторой статистики и отчетностей, поэтому сеть должна быть хорошо защищена;
- Производительность. Банковская сеть предполагает активное использование, не только сотрудниками банка, но и его клиентами через банкоматы, мобильный-банкинг и онлайн терминалы;
- Отказоустойчивость. Отказоустойчивость является одним из наиболее приоритетных аспектов проектирования банковской сети. Стабильность работы сети крайне важна в банковской сфере и критически влияет на работу всей организации в целом.

Предполагается, что «ЦАБ» - это небольшой банк, который только выходит на рынок, планирует активно развиваться и расширяться. В связи с этим возможна переструктуризация организации, появление новых подразделений и отделов.

2.3 Определение структуры потоков данных

При проектировании сети необходимо учитывать логическую, физическую и организационную структуру предприятия. Это необходимо для правильной разбивки сети на логические сегменты и созданию её рациональной структуры. Приведем потенциально возможную структуру предприятия для предполагаемого банка, от которой будем отталкиваться в дальнейшем:

- Фондовый отдел;
- Юридический отдел;
- Бухгалтерия;
- Отдел кадров;
- Отдел по работе с клиентами (отделения/кассовые отделы);
- IT – отдел;
- Администрация (управленческий персонал).

Для проектирования была выбрана иерархическая модель сети, что обусловлено возможными изменениями в структуре сети. Разбиение большой сети на небольшие, простые для понимания, модули (уровни) способствует устойчивости сети за счет локализации возникающих проблем. Таким образом при возникновении какого-либо сбоя в сети необходимо определить на каком уровне возникла ошибка, затем приступать к ее решению, не затрагивая при этом другие модули сети. Иерархическая модель делит сеть на 3 основных уровня/модуля:

- Уровень доступа (Access Layer) - предоставляет пользователям или устройствам (принтер, сканер, ip-телефон) доступ к сети.
- Уровень распределения (Distribution Layer) - агрегирует/объединяет уровни доступа и предоставляет доступ к различным сервисам организации.
- Уровень ядра/базовый уровень (Core Layer) - агрегирует/объединяет уровни распределения в больших сетях.

Таким образом, в нашей сети все отделы будут относиться к уровню доступа, к уровню распределения: резервное и маршрутизирующее коммуникационное оборудование внутри локальных сетей, к уровню ядра: маршрутизаторы и магистральные WAN сети для связи филиалов с главным офисом.

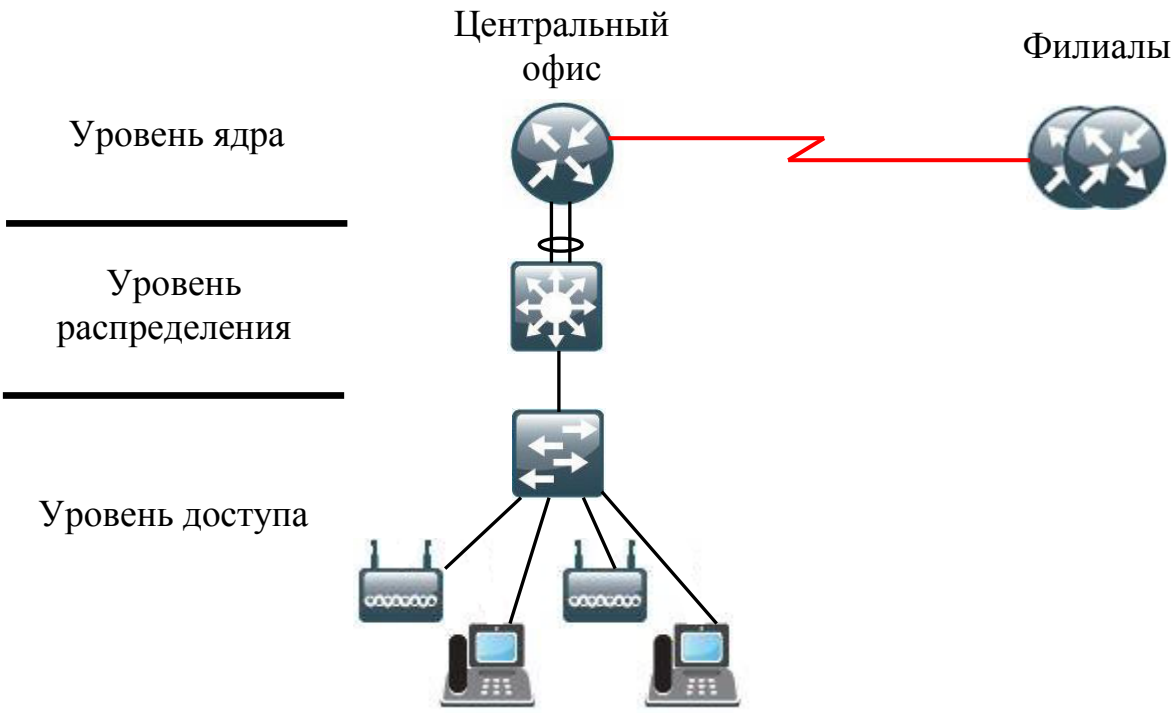

Рисунок 2.6 – Иерархическая структура сети организации

2.4 Построение логической структуры сети

Логическая структура сети определяется организационной структурой предприятия, а также географическим расположением офисов и филиалов. Банк состоит из центрального офиса в Алматы (здание 5 этажей) и филиалов в Ташкенте и Бишкеке (здания 2 этажа).

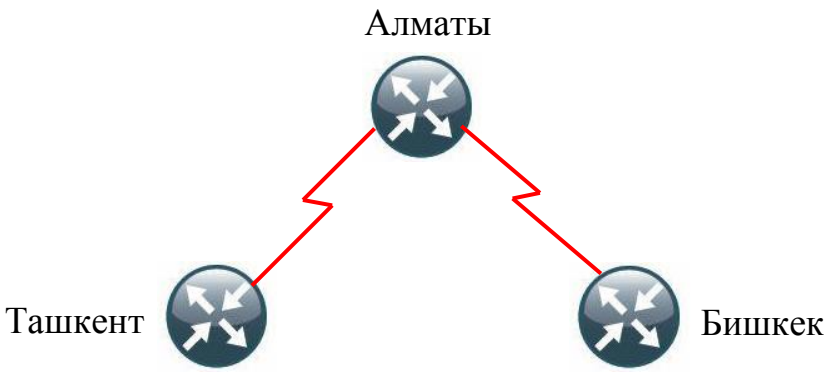

Рисунок 2.7 – Логическая структура сети WAN

В соответствии с принятой структурой предприятия в пункте 1.2 и характеристиками зданий, выбранными согласно варианту, построим

детальную логическую схему сети для каждого из офисов. Ниже приведена схема для центрального офиса в Алматы:

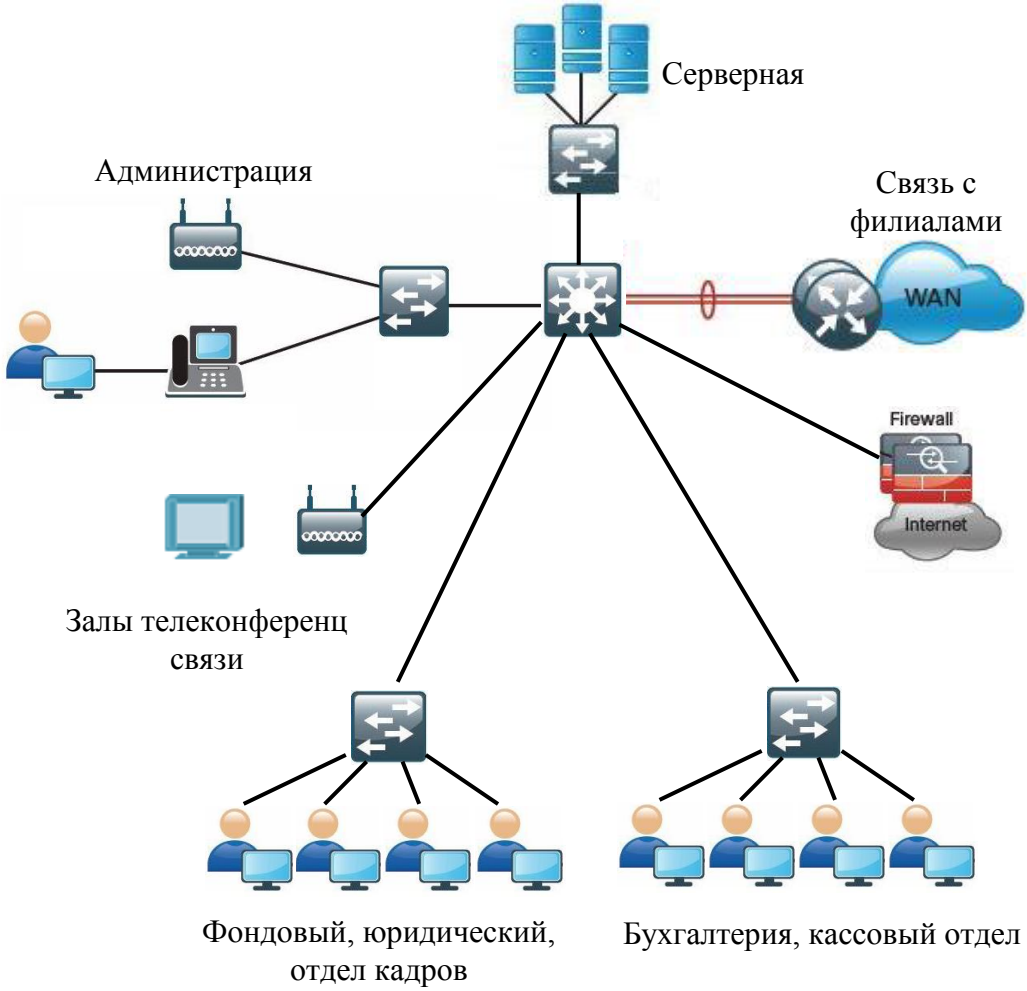

Рисунок 2.8 – Логическая структура сети Алматинского офиса

Офисы филиалов занимают только 2 этажа и включают в себя: кассовый отделы, финансовый отделы, отделы администрации/управления и залы телеконференц-связи.

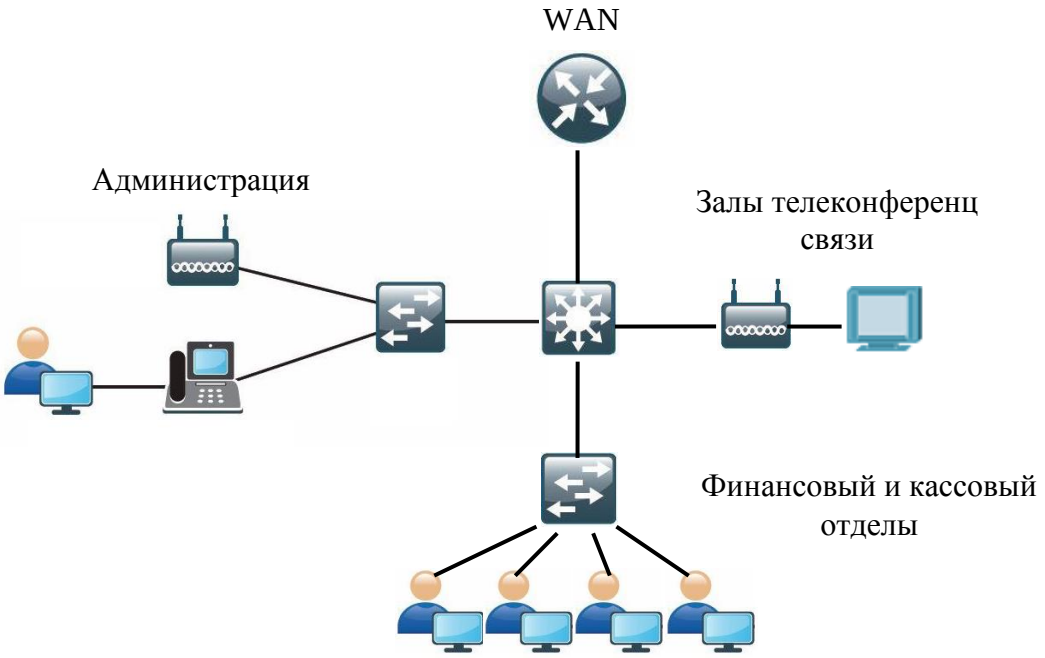

Рисунок 2.9 – Логическая структура сети филиалов

2.5 Выбор технологии локальной сети

Одним из наиболее важных требований, предъявляемых к проектируемой сети является производительность (см. п. 1.1). Для обеспечения достаточной скорости соединения и приемлемого уровня задержек все хосты подключаются по FastEthernet (100BASE-T) к сетевым устройствам уровня доступа UTP-кабелями, все магистральные соединения между устройствами распределения реализуются посредством Gigabit Ethernet (1000BASE-T) с использованием экранированной витой пары (STP).

Для выполнения поставленных задач оптимальным выбором являются: коммутаторы 2-го уровня Cisco 2960 и коммутаторы 3-го уровня Cisco Catalyst 4948. (обоснование см. стр. 20).

2.6 Выбор технологии глобальной сети

Для соединения удаленных локальных сетей и отдельных компьютеров в корпоративной сети применяются разнообразные телекоммуникационные средства, в том числе телефонные каналы, радиоканалы, спутниковая связь. Для выбора необходимой технологии приведем сравнительную таблицу актуальных на сегодняшний день технологий глобальных сетей. (см. метод ук.)

Таблица 2.1 – Сравнение глобальных (WAN) технологий

Технологии				
X.25	**Frame Relay**	**ISDN**	**ATM**	**TCP/IP**
Скорость используемых каналов				
12-64 кб/с ,до 2мб/с	64 кб/с – 2 Мб/с до 44,736мб/с	128кб/с, 1.544 (2,048) Мб/с	25Мб/с –622,08 Мб/с	1.2 Мб/с – 2.048 Мб/с
Тип трафика				
Терминальный, компьютерный	Компьютерный, сжатый голос и видео	Компьютерный, голос, видео	Компьютерный голос, видео	Компьютерный терминальный
Надежность доставки и организация повторной передачи данных				
Гарантирует	Доставку не гарантирует	Не гарантирует	С протоколом SSCOP	Доставку не гарантирует
Наличие в технологии механизмов контроля перегрузок коммутирующих устройств				
Есть	Есть	Нет	Есть	Нет
Возможность групповой доставки (доставки к группе адресов)				
Не обеспечивает	Обеспечивает	Обеспечивает	Обеспечивает	Обеспечивает
Эффективность передачи полезных данных				
	Около 100%	Менее 80%	Зависит от типа услуг 77-90 %	
Обеспечения качества обслуживания				
Не обеспечивает	Не гарантирует задержку передачи данных	Классы доступа	Обеспечивает полностью	С протоколом RSVP

Основными требованиями, предъявляемыми к сети являются: безопасность, отказоустойчивость и производительность. Учитывая специфику организации, можно выдвинуть следующие критерии выбора технологии WAN:

- Надежность и гарантия доставки данных. Один из важнейших критериев, т.к. через банковскую сеть постоянно проходит огромное количество финансовых операций и запросов. «Повисшая» транзакция может стать большой проблемой;
- Трафик транзакций. Обеспечение допустимого времени задержки по вышеуказанным причинам;

- Трафик реального времени. Достаточная скорость соединения для транслирования потокового видео/аудио. Планируется использование услуг телеконференц-связи и ip-телефонии;
- Обеспечение качества обслуживания (QoS) для приоритизации трафика;

Всем перечисленным критериям полностью соответствует технология ATM. Несмотря на свою дороговизну, ATM является необходимым и оптимальным вариантом для выбранной организации.

2.7 Планирование IP – адресации и VLAN

Рассматриваемая сеть строится на IPv4 адресации. Согласно варианту предполагаемое число хостов 50, однако при планировании необходимо учесть, что сеть будет расширяться и не рассчитывать количество доступных адресов «в притык». Для построения сети взят диапазон частных ip – адресов B-класса: 172.16.0.0 — 172.31.255.255. За офисами закреплены следующие адреса:

- Алматы – 172.16.0.0/19;
- Ташкент – 172.17.0.0/18;
- Бишкек – 172.18.0.0/18.

Далее ip – адресация строится на основе логической структуры сети, указанной в пункте 1.3 (см. стр. 7). Для головного офиса в Алматы (5 этажей) было решено каждый из 7-и отделов вынести в отдельную подсеть. Таким образом, сеть 172.16.0.0 нужно разделить минимум на 8 подсетей, с маской длинной /19 бит (255.255.224.0). Таким образом каждая подсеть может содержать до 8160 хостов. В филиалах адрес сети разбивает на 4 подсети, с маской /18. Последние подсети 8-я и 4-я для головного офиса и филиалов соответственно – зарезервированы для возможного расширения сети (в свою очередь также могут быть разбиты на подсети).

В целях уменьшения широковещательного сегмента, повышения производительности сети и защит от различного рода угроз (например ARP-spoofing’a) каждая подсеть помещается в отдельный VLAN. Первая цифра VLAN – указывает этаж, на котором расположен закрепленный за ним отдел, вторая цифра id VLAN’a. (см. таблицу адресации Приложение А).

2.8 Выбор сетевой операционной системы

В качестве сетевой ОС предполагается использование только открытого программного обеспечения, потому что только открытый исходный код даёт полную гарантию отсутствия не доверенного функционала и позволяет наиболее гибко подстраивать ИС под нужды и конкретные задачи организации. Основные требования к сетевой ОС: стабильность, актуальность, поддержка новейшего аппаратного и программного обеспечения.

В итоге выбрана ОС на базе ядра Linux – Red Hat Enterprise Linux 7.0 (дата релиза 10 июня 2014г.). RHEL – является современной, надежной серверной операционной системой, со встроенной поддержкой множества сетевых сервисов и последнего аппаратного обеспечения. Основная особенность дистрибутива — наличие коммерческой поддержки на протяжении 10 лет, с возможностью продления до 13 лет, кроме того обновления безопасности и функционала выходят постоянно. Данная ОС полностью поддерживает СУБД: DB2, dBase, DataFlex, SQLite, MySQL, Oracle (версий 9i, 11g, 12c). Кроме того RHEL является одним из самых успешных и популярных дистрибутивов Linux в корпоративной сфере.

2.9 Надежность и отказоустойчивость системы

Отказоустойчивость сети крайне важна и является одним из наиболее приоритетных критериев при проектировании данной сети, потому как критически влияет на работоспособность всей организации в целом. Должный уровень отказоустойчивости обеспечивается современными методами построения сети и ограничивается финансовыми возможностями организации.

Существует 2 базовых метода повышения отказоустойчивости сети: резервирование каналов и резервирование оборудования. В проектируемой сети применяются оба из них. Предусматривается резервное оборудование уровня распределения в виде коммутаторов 3-го уровня, которое дублируется резервным на случай, если основное выйдет из строя. Поэтому каждый коммутатор уровня доступа связан с несколькими коммутаторами (в данном случае с двумя) 3-го уровня. Также в обязательном порядке закладываются резервные каналы: каждое такое соединение является агрегированным посредством технологии EtherChannel.

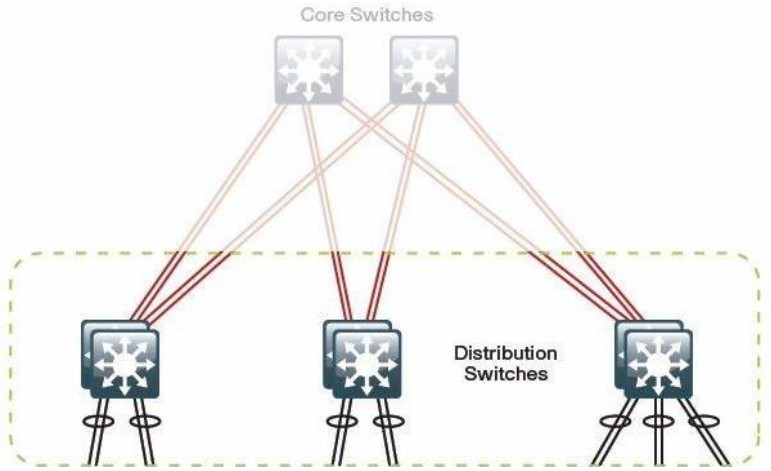

Рисунок 2.10 – Схема резервирования оборудования и каналов

Однако при такой схеме значительно возрастает количество используемых портов, что плохо сказывается на масштабируемости сети, поэтому на линиях связи, не представляющих особой важности, применяется простое резервирование каналов и протокол STP/RSTP, блокирующий резервные каналы в штатном режиме работы, для предотвращения широковещательных штормов.

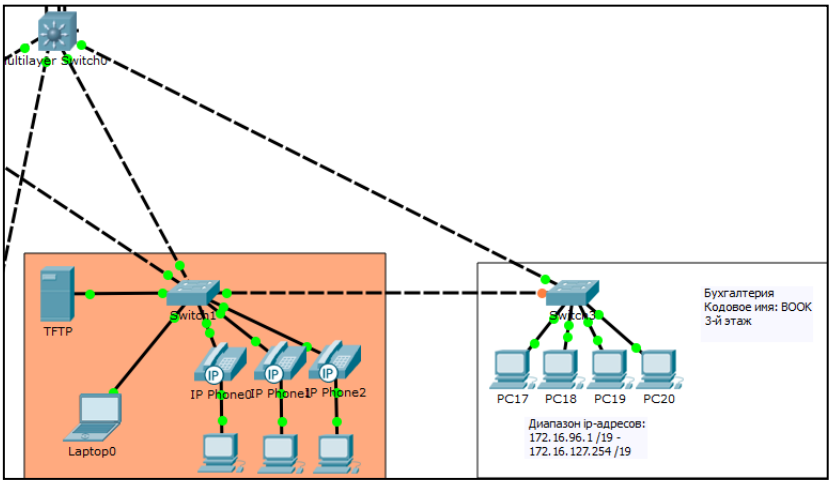

Рисунок 2.11 – Резервирование каналов
(Резервный канал между Switch1 и Switch3 заблокирован STP)

В идеале планируется использование модели Cisco SBA LAN, которая предполагает использование технологию стекирования и агрегированных соединений между сетевыми устройствами. К сожалению последняя версия симулятора сети Cisco Packet Tracer (на момент написания данной работы) не поддерживает стектирование, поэтому это не удастся продемонстрировать на симуляторе, но на реальном оборудовании это реализуемо. Поэтому в реальной сети коммутаторы уровня доступа объединяются в стек (с использованием таких технологий как StackWise Plus). Агрегированный канал образуется при объединении портов разных коммутаторов стека (Рис.7). Другими словами, логический интерфейс образуется объединением двух (или

более) портов, при этом один порт принадлежит первому коммутатору стэка, а второй порт - второму. Оба порта участвуют в передаче трафика. Таким образом оказываются задействованными все устройства, обеспечивая высокую производительность и отказоустойчивость.

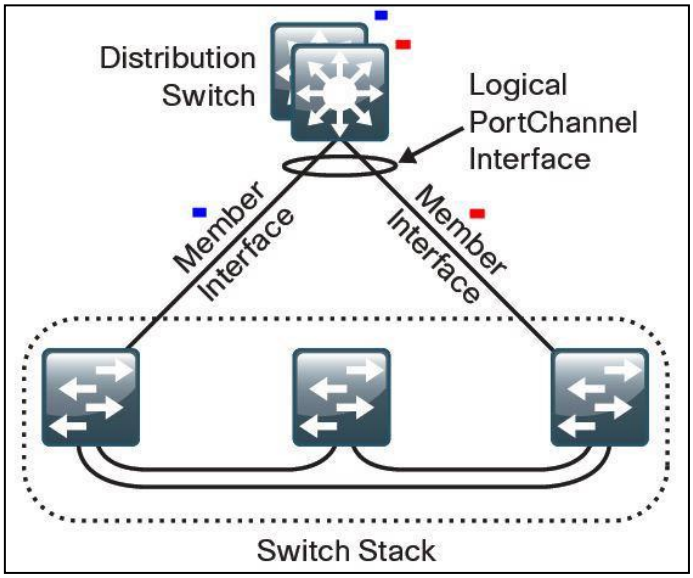

Рисунок 2.12 – Объединение портов стека коммутаторов в один PortChannel

2.10 Политика безопасности

Комплекс мероприятий, которые направлены на безопасность информации включается в Политику безопасности.

Данный комплекс мероприятий включает в себя:

- поддержка целостности информации;
- своевременная доступность и конфиденциальность информации;

Так как на проектируемой сети будет работать распределенная ИС банка, то необходимо выбрать комплексное ПО для обеспечения её безопасности. В соответствии с выбранной ОС (см. п.1.7, стр.12), выбраны следующие технологии: сетевой протокол аутентификации Kerberos, корпоративная лицензия Norton 360 для клиентских машин, PGP для передачи данных внутри корпоративной сети.

2.11 Распределение уровней доступа

Распределение уровней доступа – это основа информационной безопасности, без которой все остальные программные и аппаратные средства защиты являются практически бесполезными. Другими слова должно быть четко определено: кому, к какой информации и какого уровня предоставлен доступ.

Таблица 2.3 – Распределение уровней доступа

группы	**Внутренние ресурсы**	**Уровни доступа**	**Email и Internet access**
Администраторы	Все сетевые ресурсы	Права администратора в каталогах, в том числе изменение уровня и прав доступа	Все сетевые ресурсы
Сотрудники в офисе	Вся информация предприятия (учреждения)	Ограничение доступа к папкам (по необходимости)	Ограничение по IP- адресу (адресата и источника), ограничение по содержанию (входящей и исходящей корреспонденции)
Сотрудники вне офиса	Ограниченная информация. (Ограниченный доступ к базам данных)	Ограничение доступа к папкам (по необходимости)	Ограничение по IP- адресу (адресата и источника), ограничение по содержанию (входящей и исходящей корреспонденции), аутентификация удаленного пользователя перед осуществлением доступа
Поставщики, деловые партнеры, клиенты	Специальные каталоги и папки для производителей, партнеров и клиентов	Доступ только к специально отведенным областям	Ограничение по IP- адресу (адресата и источника). Идентификация и аутентификация удаленного пользователя
Потенциальные клиенты	Специальные каталоги и папки для клиентов	Просмотр объектов (чтение и поиск файлов)	При открытом доступе Интрасеть должна быть изолирована; идентификация пользователя не требуется

2.12 Выбор сетевого оборудования

Учитывая примерное количество узлов на текущий момент - 50 машин и быстрые темпы роста сети, необходимо брать оборудование с запасом на будущее. К примеру головной офис в Алматы содержит 30 узлов подключенных через FastEthernet к коммутаторам уровня доступа, что в среднем, учитывая специфику информации и ограничения, предполагает поток трафика в размере 2,7-2,8Гбит/с. С ростом сети эта цифра пропорционально увеличится следовательно необходимо подбирать оборудование, как минимум с в 2 раза большей пропускной способностью.

На основании данных требований было выбрано следующее оборудование:

Таблица 2.4 – Технические характеристики Cisco 2960-24TT

Общие характеристики	
Тип устройства	коммутатор (switch)
Возможность установки в стойку	Есть
Объем оперативной памяти	64 Мб
Объем флеш-памяти	32 Мб
LAN	
Количество портов коммутатора	24 x Ethernet 10/100 Мбит/сек
Количество uplink/стек/SFP-портов и модулей	2
Максимальная скорость uplink/SFP-портов	10/100/1000 Мбит/сек
Внутренняя пропускная способность	16 Гбит/сек
Размер таблицы MAC адресов	8192
Управление	
Web-интерфейс	есть
Поддержка Telnet	есть
Поддержка SNMP	есть
Маршрутизатор	
Протоколы управления группами интернета	IGMP v1, IGMP v2, IGMP v3
Дополнительно	
Поддержка стандартов	Auto MDI/MDIX, IEEE 802.1p (Priority tags), IEEE 802.1q (VLAN), IEEE 802.1d (Spanning Tree), IEEE 802.1s (Multiple Spanning Tree)
Размеры (ШхВхГ)	445 x 44 x 236 мм
Вес	3.6 кг

Таблица 6 – Технические характеристики Cisco Catalyst 4948

Общие характеристики	
Тип устройства	коммутатор (switch)
Возможность установки в стойку	есть
Объем оперативной памяти	256 Мб
LAN	
Количество портов коммутатора	48 x Ethernet 10/100/1000 Мбит/сек
Количество uplink/стек/SFP-портов и модулей	4
Максимальная скорость uplink/SFP-портов	10 Гбит/сек
Поддержка работы в стеке	есть
Внутренняя пропускная способность	136 Гбит/сек
Размер таблицы MAC адресов	55000
Управление	
Консольный порт	есть
Поддержка Telnet	есть
Поддержка SNMP	есть
Маршрутизатор	
Статическая маршрутизация	есть
Протоколы динамической маршрутизации	RIP v1, RIP v2, OSPF
Протоколы управления группами интернета	IGMP v1, IGMP v2, IGMP v3
Дополнительно	
Поддержка IPv6	есть
Поддержка стандартов	Auto MDI/MDIX, Jumbo Frame, IEEE 802.1p (Priority tags), IEEE 802.1q (VLAN), IEEE 802.1d (Spanning Tree), IEEE 802.1s (Multiple Spanning Tree)
Размеры (ШхВхГ)	440 x 45 x 410 мм
Вес	7.48 кг

Таблица 7 – Технические характеристики Cisco 2911

Общие характеристики Cisco 2911	
Тип устройства	Маршрутизатор (роутер)
Вход (WAN порт)	3x10/100/1000BASE-T Ethernet
Интерфейс подключения (LAN-порт)	3x10/100/1000BASE-T Ethernet
Маршрутизатор	
Межсетевой экран (Firewall)	+
NAT	+
Поддержка VPN (виртуальных сетей)	+
DHCP-сервер	нет данных
Демилитаризованная зона (DMZ)	нет данных
Мониторинг и конфигурирование	
Веб-интерфейс	нет данных
Telnet	нет данных
Поддержка SNMP	+
Дополнительно	
Питание(PoE/адаптер)	+/+
Возможность установки вне помещения	-
Режим моста	нет данных
Прочее	2 порта USB 2.0; форм-фактор 2U; поддержка SSL; содержит два слота под модули GBIC; не стэкируется
Размеры (мм)	438,2x304,8x88,9
Вес (г)	8200

Таблица 8 – технические характеристики сервера БД

Название продукта	Barebone server Asus RS720-X7-RS8, Dual S2011 Xeon, iC602-A, 12 DDR3 ECC, 5xLAN, VGA, 4SATA, 2U
Описание	Мощная серверная система на базе процессорной платформы Intel Xeon
Производитель	ASUS
Модель	RS720-X7-RS8
Чипсет мат. Платы	Intel C602-A PCH
Гнездо процессора	2x Socket LGA2011
Поддержка типов процессоров	Intel Xeon processor E5-2600
QPI (QuickPath Interconnect)	6.4 / 7.2 / 8.0 GT/s
Память	12x DDR3 (4-channel per CPU, 8 DIMM for CPU1, 4 DIMM for CPU2) – 128GB RAM
Максимальный оббъем памяти	Maximum 384GB RDIMM Maximum 384GB LRDIMM/Maximum
Количество разъемов PCI Express	PCI-E x16 (Gen3 x16 Link) + 5 PCI-E x8 (Gen3 x8 Link) PCI-E x16 (Gen3 x8 Link) + 6 PCI-E x8 (Gen3 x8 Link) (PIKE Slot for Stroage Enhancement)
SATA	Intel C602-A 2x SATA3 6Gb/s 4x SATA2 3Gb/s
RAID-контроллер	Опционально возможна установка ASUS PIKE RAID card
Отсеки для накопителей	8 корзин для SAS/SATA HDD с возможностью горячей замены (объединительная панель в комплекте).
Видео	Aspeed AST2300 видеопамять 16MB
Оптический привод	DVD-RW
Сеть	4x Intel 82574L + 1x Mgmt LAN
Набор портов задней панели	2x Serial Port Header 5x RJ-45 (One for ASMB6-iKVM) 4x USB 2.0 Front x 2, Rear x 2) 1x PS/2 mouse 1x Internal A Type USB 1x VGA 1x PS/2 keyboard
Управление	KVM-over-Internet (ASMB6-iKVM for KVM-over-IP)
Питание	1+1 Redundant 770W
Поддерживаемые ОС	CentOS 5.6 32/64-bit Windows Server 2008 R2 Windows Server 2008 R2 Enterprise Windows Server 2008 Enterprise 32/64-bit RedHat Enterprise Linux AS5.6/6.0 32/64-bit SuSE Linux Enterprise Server 11.2 32/64-bit VMWare ESX4.1/ESXi4.1
Высота	2U
Размеры	61.5 x 44.4 x 8.7 см
Вес	22 кг

2.13 Настройка локальной сети в Packet Tracer

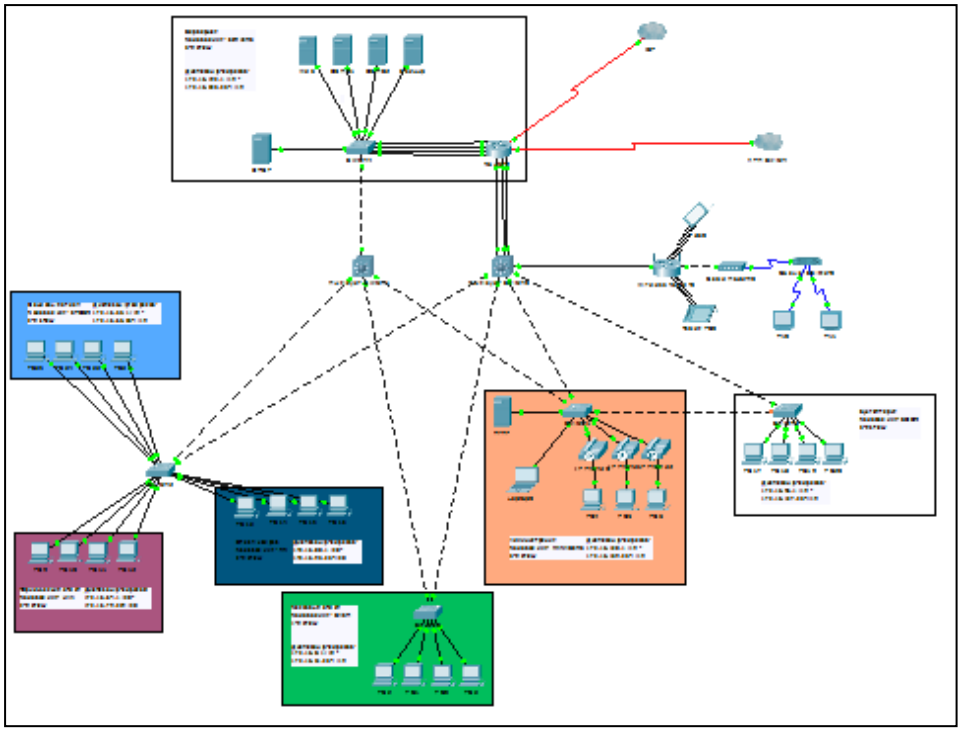

Рисунок 2.12 – Топология локальной сети

Согласно логической структуры сети, каждый отдел помещен в отдельный VLAN и в отдельную подсеть. Коммутаторы уровня доступа подключены к 2-м продублированным коммутатором 3-го уровня для повышения отказоустойчивости сети.

В свою очередь основной коммутатор соединен с роутером агрегированным каналом для обеспечения достаточной пропускной способности и отказоустойчивости.

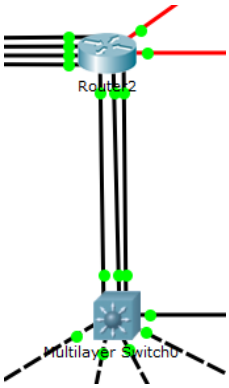

Рисунок 2.13 – Агрегированный канал между роутером и коммутатором

По аналогичным причинам роутер подключен агрегированным каналом к коммутатору в серверной:

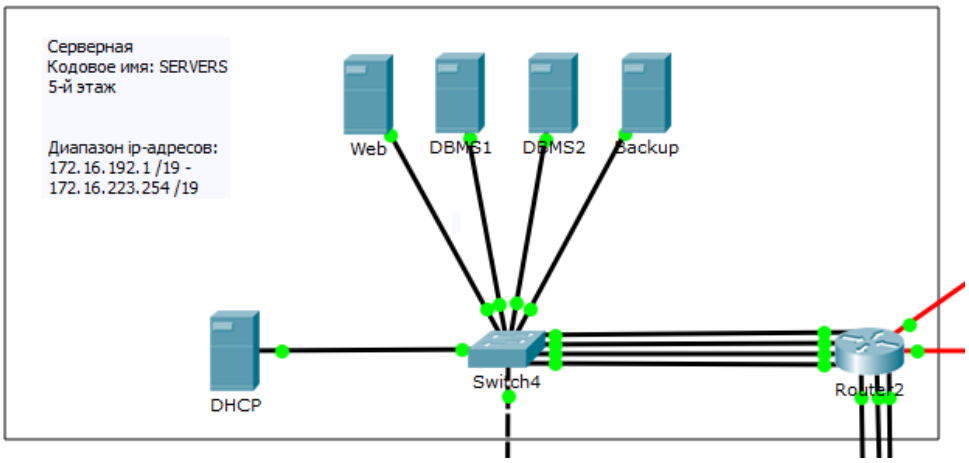

Рисунок 2.14 – Агрегированное соединение EtherChannel

Там же находится DHCP сервер выполняющий раздачу IP – адресов для всех VLAN’ов.

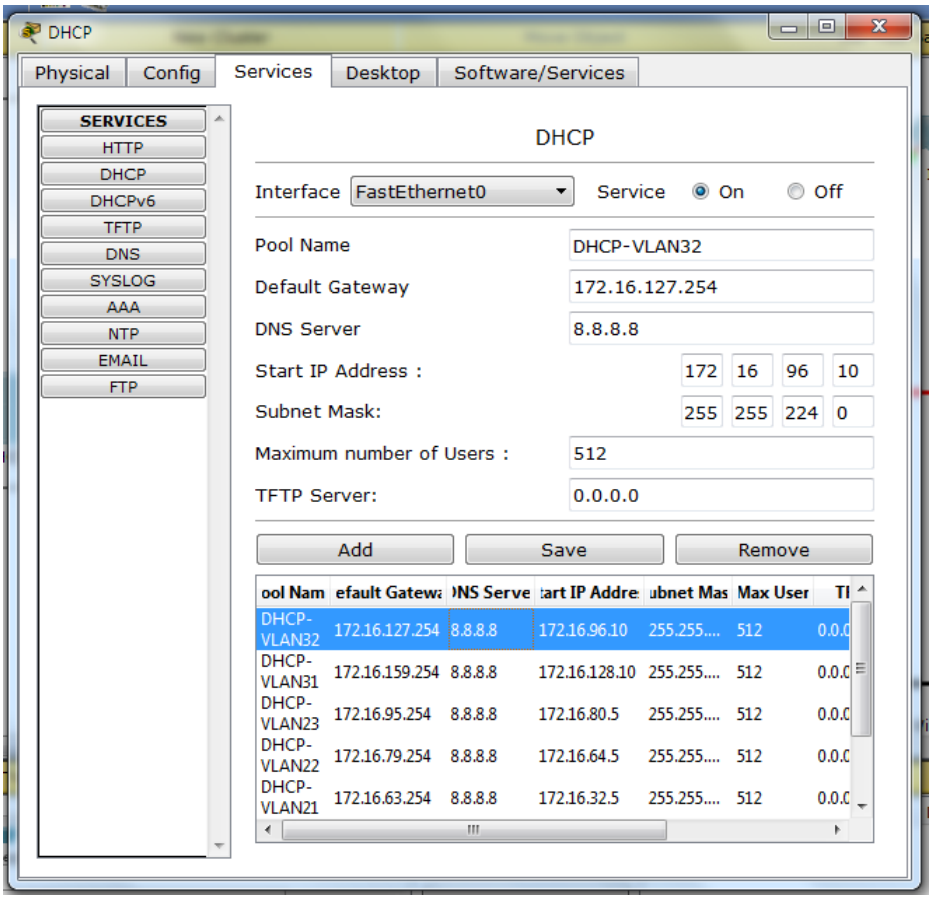

Рисунок 2.15 – Настройки DHCP сервера

Кроме основного DHCP сервера, раздачей IP-адресов по DHCP занимается беспроводная точка доступа Wi-Fi в зале телеконференц-связи для

предоставления выхода в во внутреннюю сеть организации и интернет. Таким образом поддерживает концепция BYOD (Bring your own device).

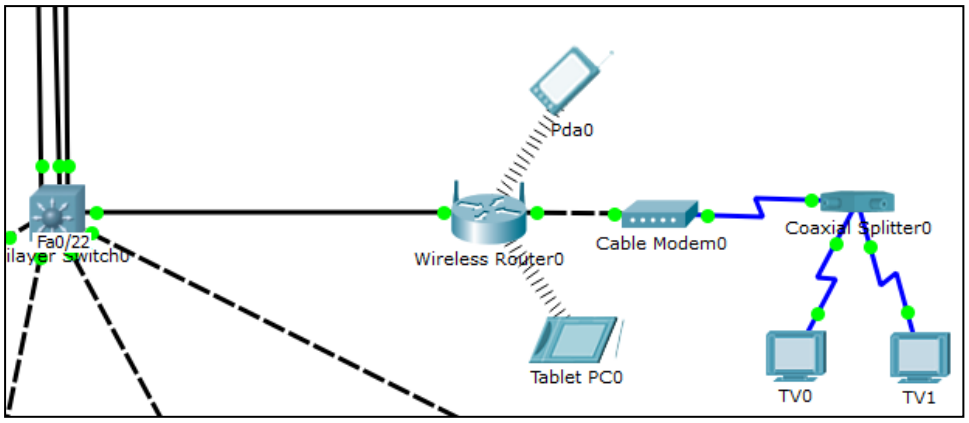

Рисунок 2.16 Топология зала совещаний(телеконференций)

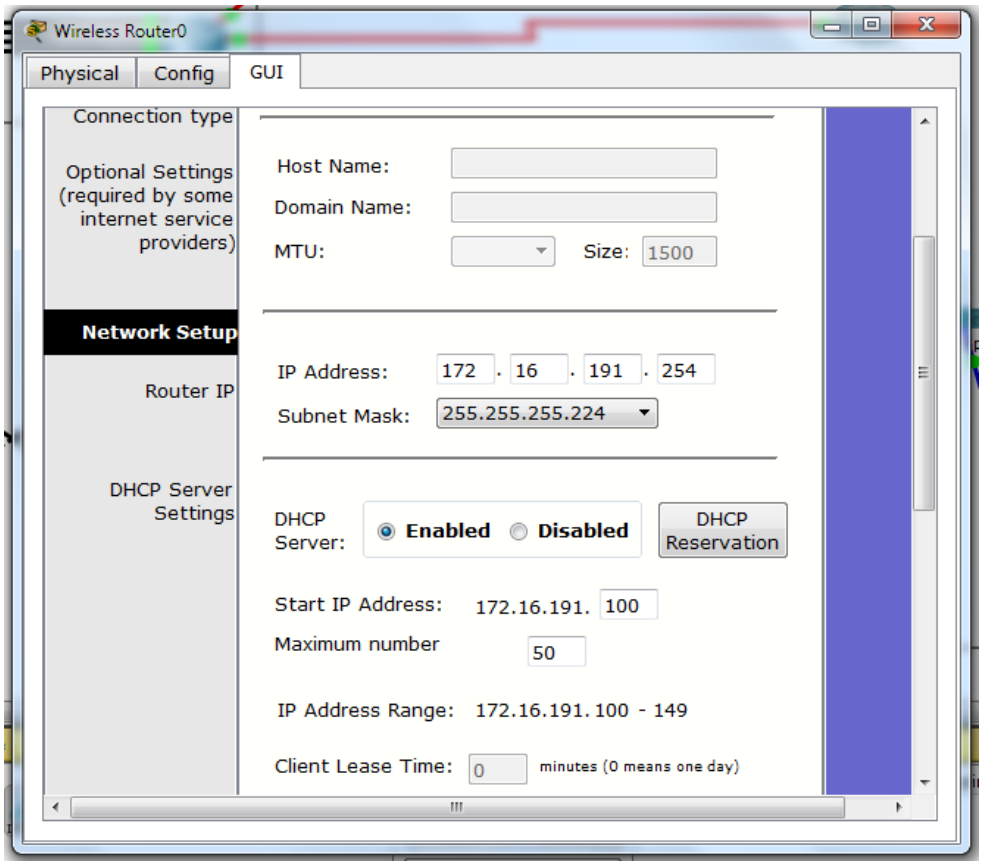

Рисунок 2.17 Настройка DHCP на точке доступа wi-fi

Предусмотрена возможность ip-телефонии. У администрации и в управленческих отделах установлены IP-телефоны.

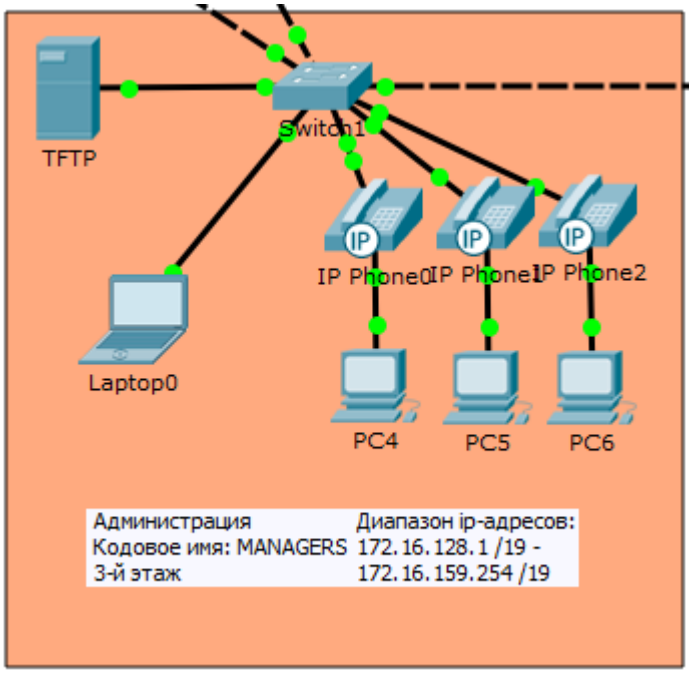

Рисунок 2.18 Топология сети управленческого отдела

Подробные логи настройки и конфиги смотрите в Приложении Б.

2.14 Параметры структурированной кабельной системы (СКС)

Предполагаемый размер здания 100х80м, 5 этажей (средняя высота этажа 3м). Чтобы длина используемых кабелей 100BASE-T и 1000BASE-T не превышала рекомендуемых 100м необходимо организовать рациональное расположение сетевого оборудования. Сетевые устройства уровня доступа должны размещать ближе к выходам из помещений. Все кабели и провода должны быть проложены по стенам в коробах из огнеупорного материала (согласно противопожарной безопасности). Оборудование уровня распределения и уровня ядра располагаются в отдельных помещениях.

3 Внедрение протокола Ipv6

3.1 Технология внедрения 6to4

6to4 – это технология перехода, который позволяет отправлять IPv6-пакеты через IPv4-каналы и не требует создания обоюдных туннелей. Данная технология используется, когда пользователь конечного устройства или сайт желают получают соединение с IPv6-Интернетом, но не имеют возможности получить его от провайдера.

6to4 выполняет три функции:

1. Выделяет блок /48 адресного пространства IPv6 каждому хосту, у которого есть глобальный IPv4-адрес.
2. Инкапсулирует пакеты IPv6 в пакеты IPv4 для передачи по сети IPv4.
3. Позволяет передавать пакеты между 6to4-хостами и хостами с «родной» IPv6-сетью.

6to4 имеет следующие преимущества перед другими способами тунеллирования IPv6:

1. Отсутствие регистрации перед его настройкой а так же быстрота и простота конфигурирования.
2. Прямая Связь по IPv6 между любыми двумя машинами – без посредников в виде каких-либо шлюзов или туннельных серверов;
3. Ближайший шлюз, через который пакеты будут направляться другим пользователям IPv6, выбирается полностью автоматически.

Недостатки

Ближайший шлюз, через который пакеты будут направляться другим пользователям IPv6, выбирается полностью автоматически.

Одно из достоинств одновременно является и недостатком. Иногда может статься, что автоматически выбранный шлюз плохо функционирует, перегружен, либо просто не работает. При этом не всегда очевидно, от кого и на каком основании можно требовать исправления этих проблем. Хотя подобные случаи и весьма редки, этот момент заставляет многих предпочитать конфигурируемые вручную туннели от туннельного брокера, где всегда чётко известны контакты техподдержки, которую можно побеспокоить в случае проблем с используемым вами туннельным сервером.

Команды настройки 6to4 приведены в приложении С(см приложение).

3.2 Анализ сети на основе IP

Одним скорость передачи пакета – это один из самых главных параметров в любой сети. ПО Packet Tracer предоставляет возможность замеров с помощью панели симуляции (рисунок 3.1)С помощью данной возможности были произведены замеры в сети на IPv4 и на IPv6. Выбраны наиболее длинные маршруты для передачи. Рассылка пакетов произведена 10 раз для каждого протокола.

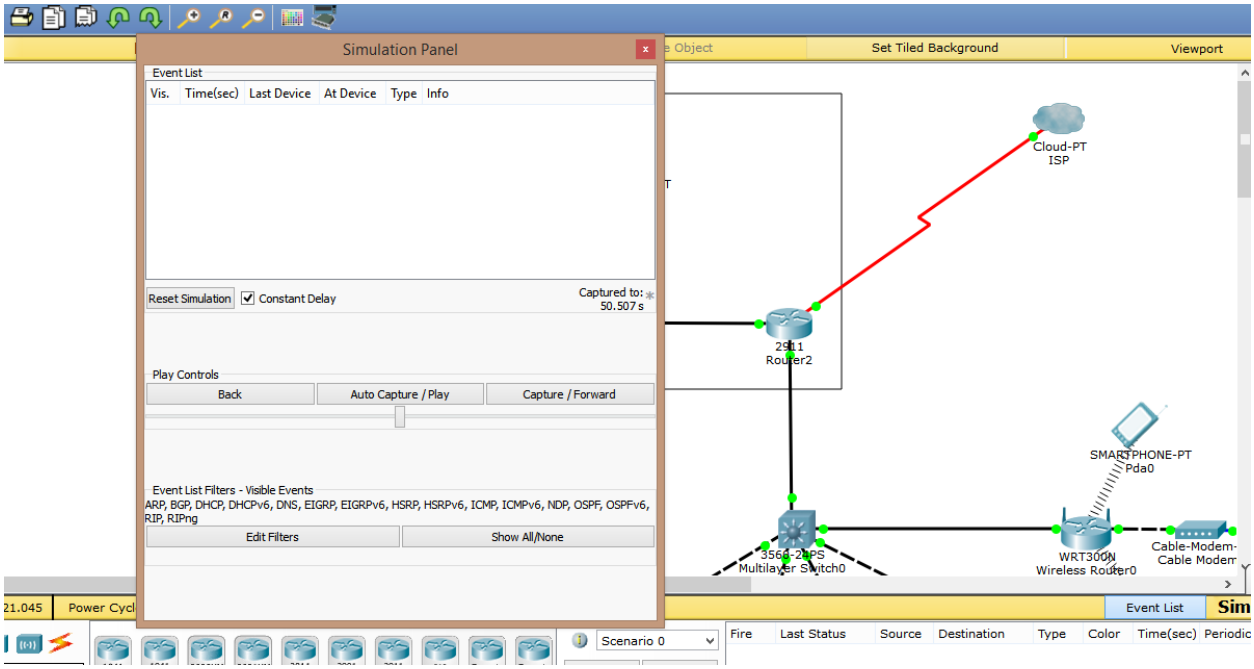

Рисунок 3.1 – Панель симуляции Packet Tracer

На рисунке 3.2 представлены данные о скорости передачи пакетов для версии IPv4.

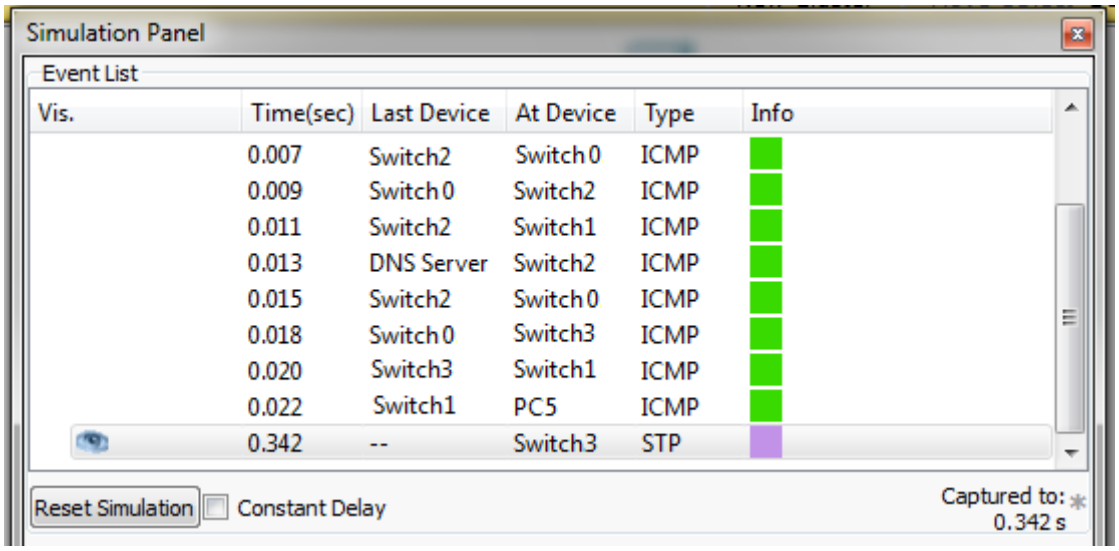

Рисунок 3.2 – Скорость передачи пакетов для IPv4

Данный сервис предоставляет возможность измерения времени передачи пакета на каждом устройстве, через которое прошел пакет, а также тип пакета. На рисунке 3.3 представлена скорость передачи пакета для IPv6.

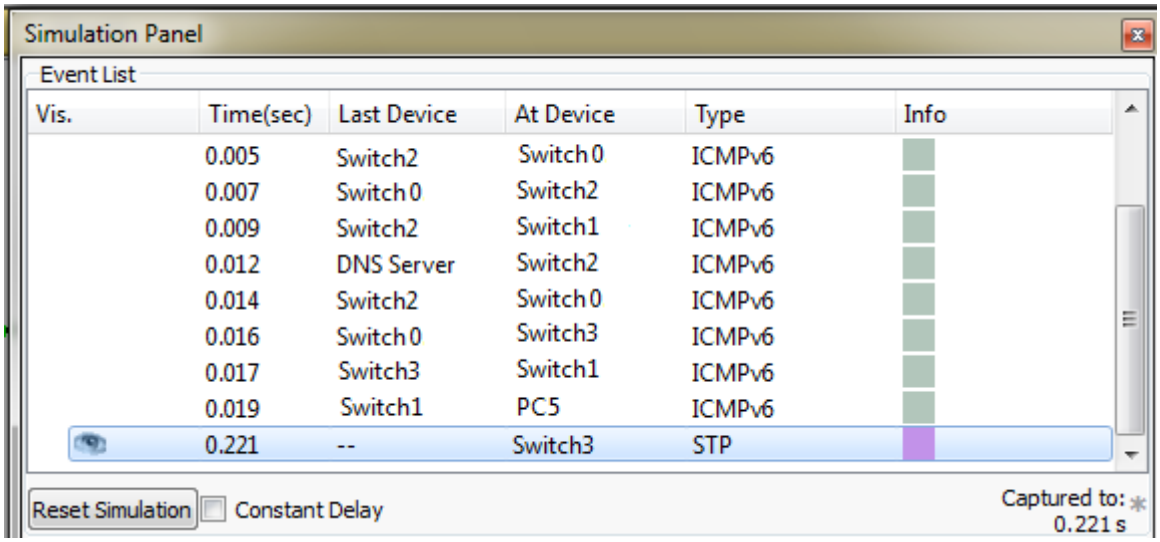

Рисунок 3.3 –Скорость передачи пакетов для IPv6

Из приведенных выше данных произведен расчет средней скорости передачи пакета по формуле:

$$C = \frac{\sum_1^n c}{n} \quad (3.1)$$

Где С является скоростью передачи пакета.

Расчет скорости передачи пакетов для IPv4

$$C = \frac{0,4 + 0,44 + 0,4 + 0,4 + 0,455 + 0,34 + 0,32 + 0,4 + 0,3 + 0,31}{10} = 0,382$$

Расчет скорости передачи пакетов для IPv6

$$C = \frac{0,24 + 0,16 + 0,35 + 0,2 + 0,3 + 0,23 + 0,3 + 0,2 + 0,26 + 0,2}{10} = 0,244$$

3.3 Расчет полосы пропускания

Гарантия качества обслуживания, которая предоставляется оператором конечным пользователям напрямую зависит от полосы пропускания. В общем случае, задержка распространения от пункта отправки к пункту назначения передачи речи не превышает 0.1 с, а вероятность превышения задержки порога в 0.05 с не должна превосходить 0,1, другими словами: $t_p \leq 0.1$с,

$$P[t_p > 50 \text{ мс}] \leq 0.001 \quad (3.2)$$

Задержка от начала до конца складывается из следующих составляющих:

$$t_p = t_{pack} + t_{\text{ад}} + t_{core} + t_{\text{буф}} \quad (3.3)$$

Где t_p – время передачи пакета из конца в конец;

t_{pack} –время преобразования пакетов (тип кодека и трафик влияет на ее значение);

$t_{ад}$ – время задержки транспортировки в сети;

t_{core} – время задержки при распространении в транзитивной сети;

$t_{буф}$ – время задержки в приёмном буфере.

Использование низкоскоростных кодеков снижает задержку в целом. В буфере приёма задержка будет также велика, поэтому на уровень доступа и на транспортный уровень должна оказываться минимальная задержка.

Допускается, что задержка на уровне доступа не превышает 0,005 секунд. Время обработки заголовка IP-пакета принимается константой так как оно практически неизменно и на его значение не влияют другие факторы. Интервалы перераспределены между поступлениями пакетов, что подчиняется экспоненциальному закону. Для данного случая применима формула которая находит среднее время вызова в системе (формула Полячека- Хинчина):

$$\tau_{\text{ад}j} = \frac{\tau_j(1+c_b^2)}{2(1-\lambda_j \cdot \tau_j)} \quad (3.4)$$

где τ_j – среднее время обслуживания одного пакета;

C_b^2 квадрат коэффициента вариации, $C_b^2 \approx 0{,}2$;

$\boldsymbol{\lambda}_j$ – параметр потока, $N_{\sum\_cekj}$,

$t_{адj}$ среднее время задержки пакета в сети доступа, $t_{адj} \approx 0{,}005$ с

коэффициент вариации, который отличен от нуля, поддается влиянию возможным отклонениям для применения их в заголовках IP полей ToS. Время обработки IP-пакета так же сильно поддается влиянию правилам обработки на маршрутизаторе.

На основании формулы (3.3) имеется зависимость средней длительности обслуживания одного пакета (максимальное значение) от среднего времени задержки в сети на уровне доступа.

$$\tau_j = \frac{1}{\lambda_j + \frac{1+c_b^2}{2 \cdot t_{адj}}} \quad (3.5)$$

$$\tau_{j1} = \frac{1}{\lambda_{j1} + \frac{1+c_b^2}{2 \cdot t_{адj}}} = \frac{1}{(82610 + \frac{1+0{,}2}{2 \cdot 0{,}005})} = 12{,}14 \cdot 10^{-6}\ c$$

$$\tau_{j2} = \frac{1}{\lambda_{j2} + \frac{1+c_b^2}{2 \cdot t_{адj}}} = \frac{1}{(129200 + \frac{1+0{,}2}{2 \cdot 0{,}005})} = 7{,}695 \cdot 10^{-6}\ c$$

Данные зависимости построены в MatchCad и отображены на рисунках 3.4 и 3.5.

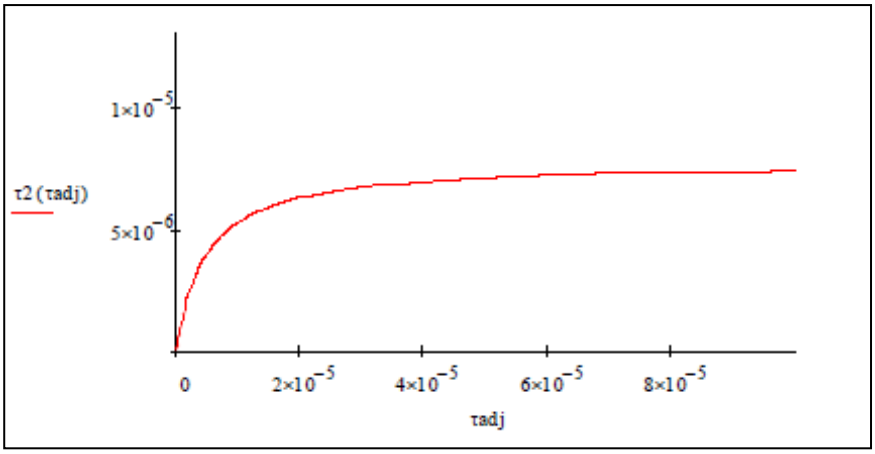

Рисунок 3.4 – Зависимость средней длительности обслуживания одного пакета от среднего времени задержки в сети доступа для IPv4

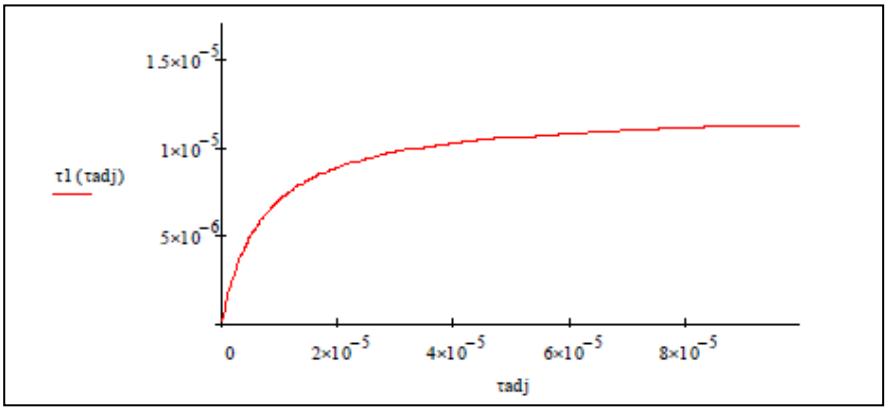

Рисунок 3.5 - Зависимость средней длительности обслуживания одного пакета от среднего времени задержки в сети доступа для IPv6

Расчет полосы пропускания для IPv4. Интенсивность обслуживания зависит от среднего времени задержки пакета в сети доступа и обратно пропорционально ему:

$$\beta_j = \frac{1}{\tau_j} \qquad (3.6)$$

$$\beta_{j1} = \frac{1}{\tau_{j1}} = \frac{1}{12 \cdot 10^{-6}} = 82640 \text{ с}^{-1}$$

$$\beta_{j2} = \frac{1}{\tau_{j2}} = \frac{1}{7{,}7 \cdot 10^{-6}} = 129900 \text{ с}^{-1}$$

Расчет по формулам 3.2 и 3.3 показывает среднее время задержки в сети на уровне доступа а так же интенсивность обслуживания при t_{ad}=0,005с для нескольких типов кодеков. Время *tj* должно выбираться в качестве

минимального из двух возможных значений. Первое значение – величина, которая была получена из последней формулы. Второе значение — то значение величины, которое определяется из условия ограничения загрузки системы — ρ. Обычно значение этой величины не должно превышать 0,5.

При среднем значении задержки в сети на уровне доступа 0,005 коэффициент использования равен:

$$\rho_j = \lambda_j \cdot \tau_j \quad (3.7)$$

$\rho_{j1} = \lambda_{j1} \cdot \tau_{j1} = 82611 \cdot 12{,}14 \cdot 10^{-6} = 1$

$\rho_{j2} = \lambda_{j2} \cdot \tau_{j2} = 129200 \cdot 7{,}695 \cdot 10^{-6} = 0{,}995$

Рассчитан коэффициент использования для случаев с различными кодеками.

При такой высокой степени использования малейшие флуктуации параметров приводят сбою в работе системы. Определены показатели сети при снижении её использования на 50%. Средняя продолжительность обслуживания находится по следующей формуле:

$$\tau_j = \frac{\rho_j}{\lambda_j} \quad (3.8)$$

$\tau_{j1} = \frac{\rho_{j1}}{\lambda_{j1}} = \frac{0{,}5}{82611} = 6 \cdot 10^{-6}\ c.$

$\tau_{j2} = \frac{\rho_{j2}}{\lambda_{j2}} = \frac{0{,}5}{129211} = 3{,}869 \cdot 10^{-6}\ c.$

Интенсивность обслуживания определяется по формуле 3.6:

$\beta_{j1} = \frac{1}{\tau_{j1}} = \frac{1}{6 \cdot 10^{-6}} = 166710\ c^{-1}$

$\beta_{j2} = \frac{1}{\tau_{j2}} = \frac{1}{3{,}869 \cdot 10^{-6}} = 258400\ c^{-1}$

Задержка в сети доступа рассчитывается по формуле 3.4:

$\tau_{\text{ад}j1} = \frac{\tau_{j1}(1+c_b^2)}{2(1-\lambda_{j1} \cdot \tau_{j1})} = \frac{6 \cdot 10^{-6}(1+0{,}2)}{2(1-82611 \cdot 6 \cdot 10^{-6})} = 7{,}14 \cdot 10^{-6}$ с.

$\tau_{\text{ад}j2} = \frac{\tau_{j2}(1+c_b^2)}{2(1-\lambda_{j2} \cdot \tau_{j2})} = \frac{3{,}869 \cdot 10^{-6}(1+0{,}2)}{2(1-129200 \cdot 3{,}869 \cdot 10^{-6})} = 4{,}644 \cdot 10^{-6}$ с.

Расчет вероятности $s(t) = 1 - e^{-\left(\frac{1}{\tau}-\lambda\right)t}$ при известных λ и τ проводить нецелесообразно так как в Y.1541 вероятность P[t>0,005]<0,001 определена для передачи из конца в конец.

На основании известного среднего замера пакета h_j определена полоса пропускания по следующей формуле:

$$\varphi_j = \beta_j \cdot h_j, \text{ бит/сек} \quad (3.9)$$

$$\varphi_{j1} = \beta_{j1} \cdot h_{j1} = 166700 \cdot 220 \cdot 8 = 293{,}3 \cdot 10^6$$
$$\varphi_{j2} = \beta_{j2} \cdot h_{j2} = 258400 \cdot 140 \cdot 8 = 289{,}4 \cdot 10^6$$

На основании полученных данных была построена гистограмма которая приведена на рисунке 3.6:

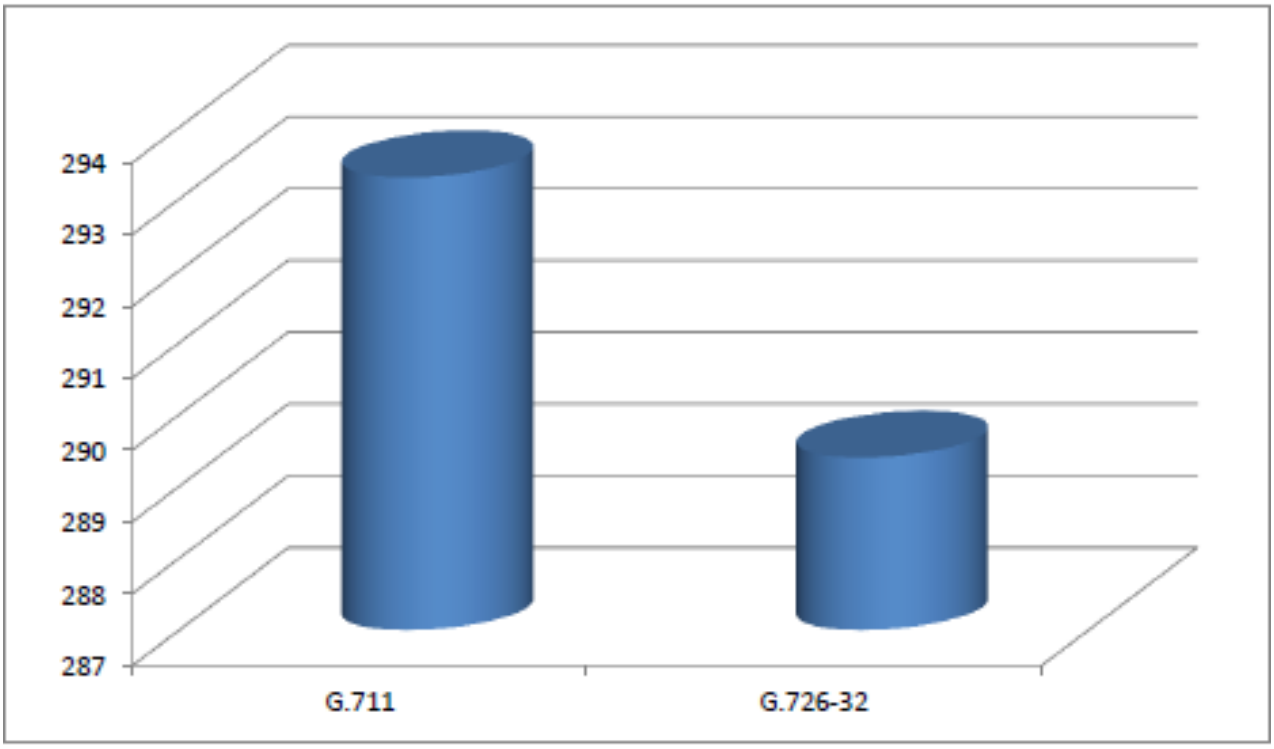

Рисунок 3.6 – Пример отображения результатов расчета: требуемая полоса пропускания

С помощью графика объясняется: Для отправки данных одного размера, необходима различная полоса пропускания, во время отправки кодека G.726-32 (140 байт) необходима меньшая полоса пропускания, чем при использовании кодека G.711(220 байт).

Расчет параметров сети, таких как: время и интенсивность обслуживания одного IP пакета определенной длины зависящий от времени задержки в сети доступа.

4 Технико-экономическое обоснование

4.1 Краткая информация о работе

В данной дипломной работе рассматриваются методы перехода с протокола Ipv4 на Ipv6. Данный переход продемонстрирован на примере отдельно взятой сети.

Процесс выдачи адресов в IPv6 выглядит так: корпорация ICANN, которая выполняет IANA-функции, включающие в себя – распределение адресного пространства, передает определенное количество IP-адресов своему локальному представителю (региональной интернет-регистратуре – RIR). Затем эти адреса распределяют по организациям, которые представляют RIR в каждой стране региона. Далее эстафету подхватывают Интернет-провайдеры, которые, в конечном итоге, делегируют их пользователям Интернета.

Местный представитель от лица Организации, который претендует на получение блока IP-адресов, обязан предоставить региональной интернет-регистратуре двухлетний план по их делегированию конечным пользователям, на основании которого ей будет выдана специальная лицензия. Она действительна в течение определенного срока и может быть аннулирована, а выделенные адреса - отобраны в случае невыполнения организацией указанного выше плана. При этом региональный представитель может пополнять запас IP-адресов случае нехватки ранее выданных.

4.2 Выбора и состав оборудования

Анализ и демонстрация перехода на протокол Ipv6 будет смоделирован на программном продукте Packet Tracer, в арсенал которого входит оборудование Cisco, стоимость которого использована в экономической части проекта. Cisco Systems - мировой лидер в области сетевых технологий. Оборудование Cisco дорогое, но надежное и простое в эксплуатации, и поэтому занимает лидирующую позицию на рынке сетевых технологий. Cisco Systems предоставляет широкий спектр устройств, таких как:

Маршрутизаторы (Routers);

Ethernet-коммутаторы (Switches);

Продукты для IP-телефонии, такие, как IP-PBX, VoIP-шлюзы (часть линеек изначально не являлись собственной разработкой, OEM Polycom);

Устройства сетевой безопасности (межсетевые экраны, VPN, IDS и др.)

Платформы оптической коммутации

ATM-Switches;

Cable Modem;

DSL-оборудование;

Системы видеонаблюдения;

Универсальные шлюзы и шлюзы удалённого доступа;

Сетевое программное обеспечение;

Точки доступа Wi-Fi;

Крупные системы видеоконференций TelePresence (на основе оборудования поглощённой компании Tandberg);

Серверы (UCS, поставляются, в частности, в составе комплексов FlexPod, выпускаемых Cisco совместно с NetApp).

4.3 Финансовый план

Данный раздел технико-экономического обоснования проекта является расчётным. В финансовый план включены: расчет величины, определение источника инвестиций, прогноз объема реализации, доходы от продажи товаров или услуг, издержки, прибыль.

4.3.1 Расчет капитальных затрат

Для перехода на Ipv6 отдельно взятой сети в соответствии с таблицей 4.1 потребуется оборудование на сумму 1770429 тенге, которое будет добавлено либо заменено:

Таблица 4.1 – Спецификация оборудования

Наименование оборудования (Тип + Марка + модель)	Стоимость оборудования, тг.	Количество оборудования, шт.	Общая стоимость оборудования, тг.
Switch Cisco 2950-24	90000	2	180000
Router Cisco 2811	252000	2	504000
Server Cisco UCSC-C240-M3L	364689	1	364689
Моноблок Dell Inspiron 23	120290	6	721740
Всего:			1770429

Расчет стоимости монтажа

Для полноценного использования оборудования в проекте необходимо провести монтажные работы. Суммарная стоимость монтажных работ составляет 1984 900 тенге. Виды проведенных работ и их стоимость показаны в таблице 4.2.

Т а б л и ц а 4 . 2 – Данные по стоимости монтажа

Наименование оборудования и работ, ед. изм.	Кол –во	Цена, тенге	Сумма, тенге
1 Монтаж волоконно– оптического кабеля, метр	500	500,00	250000,00
2 Измерение параметров сети, р.место	131	900,00	117900,00
3 Программирование телефонной системы, шт.	1	300000,00	300000,00
4 Установка программы анализа трафика, шт.	1	240000,00	240000,00
5 Монтаж кабельной системы передачи данных, р.место	131	7000,00	917000,00
6 Измерение параметров волоконного кабеля, фибер	8	20000,00	160000,00
Итого			1 984 900,00

4.3.2 Расчет затрат на проектирование сети

Затраты на внедрение технологии Ipv6 рассчитываются по формуле

$$К_{пр} = ФОТ + О_с + Н + М \quad (4.2)$$

где: ФОТ – фонд оплаты труда;
Ос – отчисления на социальные нужды;
Н – накладные расходы;
М – расходы на материалы.

Расчет затрат на материалы для проектирования сети

К затратам на материалы относятся все затраты на магнитные носители данных, бумагу на печатающих устройствах и другие материалы, необходимые для разработки проекта. В ходе разработки проекта были использованы следующие материалы:

– бумага;

– картридж принтера;

– CD диски.

Общая стоимость материалов составляет 37 600 тенге. Информация о материалах находится в таблице 4.3.

Т а б л и ц а 4 . 3 – Затраты на материалы

Наименование материала	Марка	Единица измерения	Количество	Цена за единицу, тенге	Сумма, тенге
Бумага (Ватман)	А1	шт.	50	300	15000
Бумага писчая	«HP» А4 80% 80 г/м	пачка	10	600	6000
CD диски	CD–RW Catalyst	шт.	15	40	600
Картридж принтера	Cartridge for HP 228	шт.	4	4000	16000
Итого					37 600

4.3.4 Расходы по оплате труда

Расходы на оплату труда включают в себя затраты на основную и дополнительную заработную плату и рассчитывается по формуле:

$$ФОТ = З_{осн} + З_{доп} \quad (4.3)$$

Основная заработная плата рассчитывается сложением оплаты труда всех исполнителей

$$З_{ОСН} = \sum_{i=1}^{n} З_i T_i \quad (4.4)$$

Где $З_i$– зарплата i-го работника в день, тенге;

Ti – затраты времени i–го работника, дней.

Доля Дополнительной з/п от основной составляет 10%

$$З_{доп} = 0{,}1 \cdot З_{осн} \quad (4.5)$$

Затраты на оплату труда зависят от количества задействованного персонала и установленного оклада. Число исполнителей и размер месячной заработной платы отражены в таблице 4.4.

Т а б л и ц а 4 . 4 – Количество исполнителей и их заработная плата

Исполнитель	Количество, человек	Заработная плата за месяц, тенге
Системный инжинер	3	150000
Начальник департамента	1	175000
Итого		625000

Стоимость человека–дня вычисляется по формуле

$$Д = \frac{ЗПм}{Др} \quad (4.6)$$

где ЗПм – з/п за месяц, тенге;

Др – среднемесячное количество рабочих дней.

среднемесячное количество рабочих дней – 24.

Для системного инженера:

$$Т = \frac{150000}{24} = 6250 тг,$$

Для начальника департамента:

$$Т = \frac{175000}{24} = 7291 тг,$$

На основе данных стоимости одного человека дня и продолжительности выполнения каждого этапа рассчитываются затраты на оплату труда для каждой категории работников (таблица 4.5).

Т а б л и ц а 4 . 5 – Трудозатраты

Исполнитель	Дневная зарплата, тенге	Количество дней	Сумма, тенге
Инженер– программист	6250	65	406250
Начальник отдела	7291	65	473915

Основная заработная плата определяется как сумма оплаты труда всех разработчиков:

$$З_{ОСН} = \sum_{i=1}^{n}(З_i T_i) \quad (4.7)$$

$З_{осн}$=406250+406250+406250+473915=1692665 (тенге)

Дополнительная заработная плата составляет 10 % от основной заработной платы:

$$З_{доп} = 0{,}1 \cdot З_{осн} \quad (4.8)$$

$З_{доп}$=0,1·1692665=169266 тг.

Суммарный фонд оплаты труда (ФОТ) составит:

ФОТ = 1692665 + 169266 = 1 861 931 тенге

4.3.5 Расчет социальных отчислений

В соответствии со статьей 385 Налогового кодекса РК социальный налог составляет 11% от начисленных доходов и рассчитывается по формуле:

$$O_C = 0{,}11 \cdot (ФОТ - ПО) \qquad (4.9)$$

где ПО – отчисления в пенсионный фонд;
ФОТ – фонд оплаты труда;
0,11 – ставка на социальные нужды.

Отчисления в пенсионный фонд составляют 10% от ФОТ, социальным налогом не облагаются и рассчитываются по формуле

$$ПО = 0{,}1 \cdot ФОТ \qquad (4.10)$$

ПО = 0,1 · 1861931=186193 тг
Тогда социальный налог будет равен
Ос = 0,11·(1861931-186193)=184331 тг

4.3.6 Расчет накладных расходов

Накладные расходы составляют 25% от общей суммы понесенных расходов и рассчитываются по формуле:

$$Н = 0{,}25 \cdot (ФОТ + O_c + М) \qquad (4.11)$$

И составляют:

$Н = 0{,}25 \cdot (1861931 + 184331 + 37600) = 520965$ тенге

Расходы на проектирование составляют:

$К_{пр} = 1861931 + 184331 + 520965 + 37600 = 2604827$ тенге

Результаты расчетов затрат по проектированию сети представлены в таблице 4.6

Таблица 4 . 6 – Расходы по проектированию сети

Показатель	Сумма, тенге
ФОТ, тенге	1 861 931
Отчисления на социальные нужды, тенге	184 331
Затраты на материалы, тенге	37 600
Накладные расходы, тенге	520 965
Итого	2 604 827

Общая сумма капитальных затрат в соответствии с произведенными расчетами и согласно формуле (4.1) составит:

$\Sigma Кв$ = = 1770429+1984900+2604827 =6360156 тенге

4.4 Эксплуатационные издержки

4.4.1 Протокол Ipv4

Текущие затраты на эксплуатацию определяются по формуле

$$Э_р = ФОТ + О_с + А_о + Э + Н \quad (4.12)$$

Где $ФОТ$ – фонд оплаты труда;
$О_с$ – отчисления на соц. нужды;
$Ао$ – амортизационные отчисления;
$Э$ – электроэнергия для производственных нужд;
$Н$ – накладные затраты

В обслуживании установленной техники задействован начальник департамента и 3 системных администратора:
$З_{осн}$=(12·175000)+ 3·(12·150000)=7500000 тенге
$З_{осн}$=7500000 ·0,1 =750000 тенге
$ФОТ$=7500000+750000=8250000 тенге.

Согласно формуле (4.10) пенсионные отчисления будут равны:

$ПО$=8250000·0,1=825000 тенге
Согласно формуле (4.9) социальный налог составит:
$О_с$=(8250000-82500)·0,11=816750 тенге

Затраты на электроэнергию

$$З_{эл.эн.} = W \cdot T \cdot S \quad (4.13)$$

где W – потребляемая мощность, составляет 5,5 кВт;
S – стоимость киловатт–часа электроэнергии составляет 18,23 тенге.

С учетом 24–часовой непрерывной работы оборудования и количество часов работы за год составит:

T=24·365=8760 часов
В соответствии с формулой (4.14) расходы на электроэнергию составят:

$Э$=5,5 ·8760·18,23 =878321,4 тенге

Годовая амортизация рассчитывается по формуле

$$А=Кв\cdot Н_а \quad (4.14)$$

Где $К_в$ –общая сумма капитальных затрат

$Н_а$ – норма амортизации

Годовая амортизация на устройствах роутеров Ethernet серии Cisco 2950, будет равна:

$$А = \frac{10\cdot 6360156}{100} = 636016 \text{ тенге}$$

Накладные расходы составляют 25 % от ФОТ и рассчитываются по формуле:

$$Н=0,25\cdot ФОТ \quad (4.15)$$

Тогда накладные затраты составят:

$Н$=0,25·8250000=2062500 тенге

Таким образам эксплуатационные издержки по формуле (4.12) составят:

Э= 8 250 000 + 816 750+ 574 626 + 878 321+2 062 500=12 582 197 тенге

Таблица 4.7 – Текущие годовые эксплуатационные расходы при использовании протокола Ipv4

Показатель	Сумма, тенге
ФОТ	8 250 000
Отчисления на социальные нужды (Ос)	816 750
Амортизационные отчисления (А0)	574 626
Затраты на электроэнергию (Э)	878 321
Накладные расходы (Н)	2 062 500
Итого	12 582 197

4.4.2 Протокол Ipv6

После перехода на технологию Ipv6, сокращается количество работников отдела и таким образом сокращаются затраты на оклад труда.

Стоимость поддержки системы после модернизации состоит из следующих составляющих.

Заработная плата IT–отдела

Вычислим годовую зарплату начальника департаментам и 2 системных инженеров:

$З_{осн}$=(12·175000)+2·(12·150000)=5700000 тенге
$З_{доп}$=5700000·0,1=570000 тенге,
ФОТ=5700000+570000=6270000 тенге

Согласно формуле(4.10) пенсионные отчисления буду равны

ПО=6270000·0,1=627000 тенге

Согласно формуле (4.9) социальный налог составит

$О_с$=(6270000-627000)·0,11=620730 тенге

Годовая амортизация оборудования

Годовая амортизация на устройствах роутеров Ethernet серии Cisco 2950, будет равна

$$А = \frac{10 \cdot 5746261}{100} = 574626 \text{ тенге}$$

Накладные затраты составят:

Н=0,25·6270000=1567500 тенге

Таким образам эксплуатационные издержки после перехода на технологию протокола Ipv6 сети составят

Э= 6270000 + 620730+ 574626 + 798474+1567500=9 831 330 тенге

Таблица 4.8 – Годовые эксплуатационные расходы после внедрения протокола Ipv6

Показатель	Сумма, тенге	Сумма, тенге
ФОТ	8 250 000	6 270 000
Отчисления на социальные нужды (Ос)	816 750	620 730
Амортизационные отчисления (А0)	574 626	574 626
Затраты на электроэнергию (Э)	878 321	798 474
Накладные расходы (Н)	2 062 500	1 567 500
Итого	12 582 197	9 831 330

4.5 Экономический эффект от внедрения технологий

Оценка экономической эффективности проекта производиться на основе коэффициента сравнительной экономической эффективности и срока окупаемости.

Величина ожидаемого годового экономического эффекта от внедрения технологии рассчитывается по формуле

Эг=Эуг–К·Ен (4.16)

где Эг – ожидаемый годовой экономический эффект;
Эуг – ожидаемая условно–годовая экономия;
К – капитальные вложения;

Ен – нормативный коэффициент экономической эффективности капитальных вложений.

Ожидаемая условно–годовая экономия определяется по формуле

$$Эуг=С_1–С_2 \quad (4.17)$$

где Эуг – величина экономии.
$С_1$ и $С_2$ – показатели текущих затрат по базовому и внедряемому вариантам.
Величина экономии составляет
$С_1$=12582197 тенге
$С_2$=9831330 тенге

Эуг=12582197–9831330=2750867 тенге

Нормативный коэффициент экономической эффективности капитальных вложений вычисляется по формуле

$$E_н = \frac{1}{T_н} \quad (4.18)$$

где Тн – нормативный срок окупаемости капитальных вложений.

Нормативный срок окупаемости капитальных вложений, принимается исходя из срока морального старения технических средств и проекторных решений, для программных продуктов срок окупаемости принимается равным 4 года.

Расчетный коэффициент экономической эффективности капитальных вложений составляет

$$E_р = \frac{Э_{уг}}{К} \quad (4.19)$$

где Ер – расчетный коэффициент экономической эффективности кап вложений;
Эуг – ожидаемая условно–годовая экономия;
К – капитальные вложения.

Тогда коэффициент экономической эффективности равен

$$E_p = \frac{2750867}{5746261} = 0{,}48$$

Расчетный срок окупаемости капитальных вложений вычисляется по формуле

$$T_p = \frac{1}{E_p} \qquad (4.20)$$

где Ер – расчетный коэффициент экономической эффективности кап вложений.

Тогда срок окупаемости равен

$$T_p = \frac{1}{0{,}48} = 2{,}08 \text{ лет}$$

Таблица 4.9 – Исследование методов обеспечения качества обслуживания в IP сетях.

Показатель	Сумма, тенге
Капитальные вложения (Кв), тенге	5 746 261
Коэффициент экономической эффективности капитальных вложений (Ер)	0,48
Срок окупаемости капитальных вложений (Тр), лет	2,08
Условная годовая экономия	2 750 867

Таблица 4.10 – Сравнение показателей Ipv4 и Ipv6

Показатель	Сумма, тенге для Ipv4	Сумма, тенге Для Ipv6
ФОТ	8 250 000	6 270 000
Отчисления на социальные нужды (Ос)	816 750	620 730
Амортизационные отчисления (А0)	574 626	574 626
Затраты на электроэнергию (Э)	878 321	798 474
Накладные расходы (Н)	2 062 500	1 567 500
Итого	12 582 197	9 831 330

Вывод

Условием эффективности проекта является

$Т_Р \leq Т_Н$ и $Е_р \geq Е_Н$

Соответственно

$2,08 \leq 4$ и $0,48 \geq 0,25$

Показатели экономической эффективности от внедрения проекта «Исследования методов обеспечения качества обслуживания в IP–сетях» представлены в таблице 4.9.

Данное условие соблюдается. Из этого следует, что проект рекомендуется для внедрения.

5 Безопасность жизнедеятельности

5.1 Анализ условий труда в помещении

В данной дипломной работе будет смоделирован переход на протокол Ipv6 в существующей компьютерной сети. Персональный компьютер является камнем преткновения деятельности в офисе. Офис рассчитан на 4 человека каждый из которых имеет свое место. Продолжительность рабочего дня –8 часов, с 9:00 до 18:00.

Помещение оборудовано разнообразной аппаратурой, которая обеспечивает техническую реализацию сети. Рабочий персонал поддерживает контроль и управление сетью.

Условия труда пользователя, работающего с персональным компьютером, определяются:

1) Различными подходами к организации рабочего места;

2) условиями рабочей среды (освещением, микроклиматом, шумом, электромагнитными и электростатическими полями, визуальными эргономическими параметрами дисплея и т. д.);

3) параметрами взаимодействия человека и персональных электронно–вычислительных машин.

В процессе труда на системного инженера, оказывают действие следующие опасные и вредные производственные факторы:

–повышенные уровни электромагнитного, рентгеновского, ультрафиолетового, инфракрасного излучения, недостаточной освещённости.

–отсутствие или недостаток естественного света;

– недостаточная искусственная освещенность рабочей зоны;

– повышенная яркость и контрастность света;

– отраженная и прямая блеклость;

– зрительное напряжение;

– монотонность трудового процесса;

– нервно-эмоциональные перегрузки.

Работа за современными ПК гарантирует постоянное и значительное напряжение функций зрительного анализатора. Одним из основных отличием является особый принцип восприятия информации, чем при обычном чтении. При обычном чтении текста на бумаге, находящимся в горизонтальном положении на столе, считывается работником с наклоненной головой при падении светового потока на текст. При работе на ПК оператор считывает текст, почти не наклоняя голову, глаза смотрят прямо или почти прямо вперед. Так как текст формируется по другую сторону экрана, пользователь не считывает отраженный текст, а смотрит непосредственно на источник света, что вынуждает глаза и орган зрения в целом работать в несвойственном ему стрессовом режиме длительное время.

Нервно–эмоциональное напряжение при работе за ПК возникает вследствие дефицита времени, большого объема и плотности информации, особенностей диалогового режима общения человека и ПК, ответственности за безошибочность информации. Продолжительное считывание информации с дисплея, особенно в диалоговом режиме, может привести к нервно–эмоциональному перенапряжению, нарушению сна, ухудшению состояния, снижению концентрации внимания и работоспособности, хронической головной боли, повышенной возбудимости нервной системы, депрессии.

Повышенные статические и динамические нагрузки у пользователей ПК приводят к жалобам на боли в спине, шейном отделе позвоночника и руках**.** Из всех недомоганий, обусловленных работой на компьютерах, чаще встречаются те, которые связаны с использованием клавиатуры. В период выполнения операций ввода данных количество мелких стереотипных движений кистей и пальцев рук за смену может превысить 60 тыс., что в соответствии с гигиенической классификацией труда относится к категории вредных и опасных. Поскольку каждое нажатие на клавишу сопряжено с сокращением мышц, сухожилия непрерывно скользят вдоль костей и соприкасаются с тканями, вследствие чего могут развиться болезненные воспалительные процессы. Воспалительные процессы тканей сухожилий получили общее название травма повторяющихся нагрузок.

Основной причиной перенапряжения мышц спины и ног являются нерациональная высота рабочей поверхности стола и сидения, отсутствие опорной спинки и подлокотников, неудобное размещение монитора, клавиатуры и документов, отсутствие подставки для ног.

Для снижения боли и избавления от некомфортабильных ощущений, которые возникают у пользователей ПК, нужны частые перерывы в работе и комфортабильные усовершенствования, в том числе оборудование рабочего места таким образом, чтобы исключать неудобные позы и продолжительное напряжение.

К числу факторов, которые оказывает негативное влияние состояние здоровья персонала за времяпрепровождении за компьютерной техникой, присоединяются: акустический шум, электромагнитное поле, электростатическое поле, изменение ионного состава воздуха и параметров микроклимата в помещении. Не последнюю роль имеют эргономические конфигурации расположения экрана монитора, состояние освещенности на рабочем месте, мебель и характеристики помещения.

План помещения изображен на рисунке 3.1.

Параметры помещения таковы:

– ширина – 4 м;

– длина – 7 м;

– высота – 3 м;

– площадь помещения – 28 м^2;

– длина окна 3 м;

– высота окна 1,5 м;
– площадь окна 4,5 м.

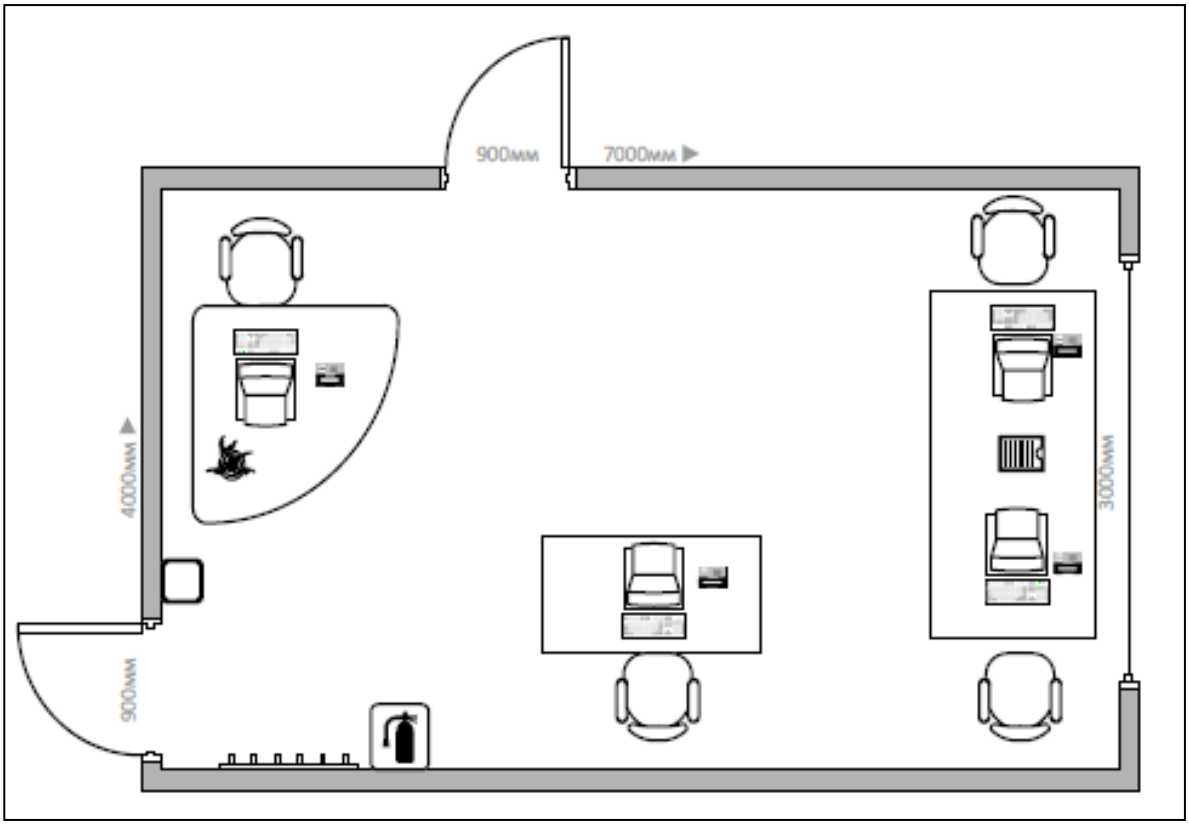

Рисунок 3.1 – План помещения

Установленное оборудование в помещении:

– Intel core i5 969xeon (2.9 ghz, 4 GB ОЗУ):габариты 575×310×575 мм напряжение 400 В, вес 5,6 кг;

– LCD 16.9" Dell:разрешение экрана 1366:768 , потребление энергии 15 Вт , рабочая температура 0 ~ 35°c , размеры 465 :359 : 204 мм, вес 2.39 кг, 0 ~ 40°C;

– лампы ЛД64–4 (5 штук):переменное напряжение 220–250 В, частотой 50 Гц, мощность каждого светильника 64 Вт;

– кондиционер тфпфтщ MH19ZC3: мощность (охлаждение) 5750 Вт, мощность (нагрев) 5560 ВТ, питание 220–240/60(В,ГЦц), уровень шума38/55 Дб, рассчитан на воздухообмен в помещении площадью до 50 м2;

– огнетушитель 1 баллон.

На основании ГОСТ 12.1.005–88 «ССБТ. Оптимальные и допустимые нормы микроклимата, в зависимости от категории работ», работа персонала в помещениях относится к работе лёгкой тяжести (1б).

Во время работы за ПК в помещениях соблюдаются следующие климатические условия:

– оптимальная температура 23–25 С˚, допустимая температура 20–30 С;

– относительная влажность 40–60 %, допустимая влажность 55%;

– скорость движение воздуха относительная 0,1 м/с и допустимая 0,1–0,2 м/с.

И-за того что уровень шума оборудования на выходит за рамки нормы 55±5 Дб, о мероприятиях по снижению шума нет смысла писать.

Абсолютно все электро – и коммуникационные провода изолированы и не являются опасностью, потому что температура летом в помещении достигает более 25^0С, которая является выше оптимальной.

5.2 Расчет системы вентиляции

Для поддерживания оптимального микроклимата в помещении был установлен кондиционер.

Количество приточного воздуха $L_{пр}$, $\frac{м^3}{ч}$, находится по формуле:

$$l_{\text{пр}} = \frac{Q_{\text{изб}}}{\text{с}\cdot \text{р}_{\text{пр}}\cdot(t_{\text{выт}}-t_{\text{пр}})} \qquad (3.1)$$

Где $Q_{изб}$ – избыточное выделение явной теплоты $\frac{\text{кДж}}{\text{ч}}$;

c – удельная теплоемкость воздуха при p=const, и равная $\text{с} = 1\,\frac{\text{кДж}}{\text{кг}\cdot{}^0\text{С}}$;

$p_{пр}$ – плотность поступающего в помещение воздуха, равная $1{,}2\,\frac{\text{кг}}{\cdot м^3}$;

$t_{выт}$ – температура удаляемого из помещения воздуха за пределы рабочей или обслуживаемой зоны, ^0C;

$t_{пр}$ – температура приточного воздуха, ^0C.

Температура удаляемого из помещения воздуха $t_{выт,}$ ^0C, определяется по формуле

$$t_{\text{выт}} = t_{РЗ} + \Delta t\cdot(h_{\text{вп}} - z) \qquad (3.2)$$

где $t_{рз}$ – температура в рабочей зоне, которая не должна превышать допустимую по нормам ($t_{рз}\leq t_{ДОП}$), ^{0}С;

Δt– температурный градиент по высоте помещения ($\Delta t = 0{,}5 - 1{,}5$), ^{0}С;

$H_{вп}$– расстояние от пола до центра вытяжных проемов (кондиц.), м;

H –высота рабочей зоны, м

Поскольку расчет производится для теплого периода года, то примем $t_{рз}$=22^0C.

Внутренняя часть кондиционера расположена на высоте $h_{ап}$=2,5 м

$t_{выт}$= 22 + 1,2· (2,5 – 3)= $21{,}4^0$С

Температура приточного воздуха $t_{пр}$ при наличии избытка явной теплоты должна быть на 5-7^0 С ниже температуры воздуха в рабочей зоне

$t_{пр}$ =22-7=15^0C

Величину избыточного выделения явной теплоты $Q_{изб}$ находят на основании баланса теплоты в помещении по формуле

$$Q_{изб}= \sum Q - \sum Q_{ух} \quad (3.3)$$

где $\sum Q$ – суммарное количество поступающей в помещение явной теплоты;

$\sum Q_{ух}$ – суммарное количество уходящей из помещения теплоты (за счет теплопотерь ограждениями, нагрева поступающего в помещение воздуха и т. п.).

Основными источниками избыточного тепла являются электроустановки, светильники, промышленные печи, люди и др. В данном помещении тепловыделением электронного оборудования можно пренебречь. Поэтому учитываем тепловыделения от искусственного освещения, от людей, количество тепла, поступающего в помещение через окно от солнечной радиации.

Тепловыделения от искусственного освещения Q_2, рассчитывают предполагая, что практически вся затрачиваемая энергия, в конечном счете, преобразуется в тепло, по формуле:

$$Q_2=1000 \cdot N \quad (3.4)$$

Где N – расходуемая мощность светильников, $кВт$

Q_2=1000·0?28 =280$кВт$

Тепловыделения от людей Q_3, определяют по формуле:

$$Q_3=n \cdot q_ч \quad (3.5)$$

где n – число работающих;

$q_ч$ – количество тепла, выделяемое одним человеком, $Вт$.

Q_3 =4·145 = 580 $Вт$

Количество тепла, поступающего в помещение от солнечной радиации $Q_{ост.рад}$, определяется по формуле:

$$Q_{ост.рад} = F_{ост} \cdot q_{ост} \cdot A_{ост} \quad (3.6)$$

для покрытий:

$$Q_{п.рад} = F_п \cdot q_п \cdot k_п \quad (3.7)$$

где $F_{ост}$ и $F_п$ – площадь поверхностей и покрытия, м^2;

$q_{ост}$ и $q_п$ - теплопоступления через 1 м^2 поверхности остекления и поверхности покрытия, при коэффициенте теплопередачи, равном $1\frac{Вт}{м^{2\cdot}\,^0С}$

Значение, выделяемое го тепла от одного человека представлена в таблице 3.1.

Таблица 3.1 – Количество тепла, выделяемое одним человеком в зависимости от категории работ и температуры окружающей среды

Категория работ	Тепло, Вт			
	Полное		Явное	
	При 100^{0}С	При 350^{0}С	При 100^{0}С	При 350^{0}С
Легкая	180^{0}С	145^{0}С	150^{0}С	5^{0}С

Значение $q_{ост}$ в зависимости от географической ориентации поверхности и характеристики окон или фонарей принимается в пределах 70–210, а коэффициента $A_{ост}$ в зависимиости от вида остекления и его солнцезащитных свойств – в пределах 0,25 -1,25, среднее значение теплопоступления от солнечной радиации через покрытие в зависимости от географической широты и вида покрытия принимают в пределах 6 – 24.

$F_{ост}$ =1,5·3 = 4,5 $м^2$

Окно рабочего помещения направлено строго на восток, поэтому примем значение $q_{ост}$ равным 140 $\frac{Вт}{м^{2\cdot}\,^0С}$. Примем $A_{ост}$ = 0,35.

$Q_{ост.рад}$ =4,5 ·140·0,35 = 220,5 $Вт$

Среднее значение теплопоступления для покрытия с учетом географической широты примем равным $Q_{п.рад}$ =18 Вт.

Потери тепла из помещения $Q_{ух}$, кВт через стены двери, окна оценивают ориентировочно по формуле:

$$Q_{ух} = \frac{\lambda \cdot S \cdot (t_{выт} - t_{пр})}{\sigma} \qquad (3.8)$$

Где λ- теплопроводность стен $\frac{Вт}{м\cdot\,^0С}$

S – площадь, м^2;

σ – толщина стен, м.

Стены рабочего помещения изготовлены из тяжелого бетона М600, теплопроводность которого равна 1,2 $\frac{Вт}{м\cdot\,^0С}$. Толщина стен $\sigma = 0{,}5$ м.

$$Q_{ух} = \frac{1{,}2 \cdot 28 \cdot (21{,}4 - 15)}{0{,}5} = 430{,}08\ Вт$$

Суммарное количество поступающей в помещение явной теплоты будет равно:

$$\sum Q = Q_2 + Q_3 + Q_{ост.рад} + Q_{п.рад} \quad (3.9)$$

$\sum Q = 280000 + 580 + 220{,}5 + 18 = 280818{,}5\ Вт$

Вычислим величину избыточного выделения явной теплоты:

$Q_{изб} = 280818{,}5 - 430{,}08 = 280387{,}7\ Вт$

количество приточного воздуха будет равно:

$$L_{\text{пр}} = \frac{280818{,}5}{1 \cdot 1{,}2 \cdot (21{,}4 - 15)} = 36002{,}37 \frac{\text{м}^3}{\text{ч}}$$

Данный объем приточного воздуха обеспечивает кондиционер Samsung MH18ZC2: мощность (охлаждение) 5375 Вт, мощность (нагрев) 5560 ВТ, питание220–240/50(В,ГЦц), уровень шума37/54 Дб, рассчитан на воздухообмен в помещении площадью до 40 м2.

Нормы температуры воздуха в помещениях представлены в таблице 3.2.

Таблица 3.2 – Оптимальные нормы температуры, относительной влажности и скорости движения воздуха в обслуживаемой зоне жилых, общественных и административно–бытовых помещений (СНиП РК 4.02–42– 2006) [11]

Период года	Температура воздуха, 0С	Относительная влажность воздуха, %, не более	Скорость движения воздуха,м/с , не более см
Теплый	20– 22	60–40	0,1
Холодный	22–22	45–30	0,1

5.3 Расчет пожарной безопасности

В помещении функционирует много различного оборудования, за счет чего протекает дополнительная нагрузка на линию электрической проводки, что в свою очередь увеличивает возможность возникновения пожара.

Причины пожара:

– кз(короткое замыкание) в проводке;

– замыкание в электрических схемах оборудования;

– возгорание отделочных материалов от неисправных источников света;

– ошибочные действия работников.

На основании правил пожарной безопасности помещение должно быть оборудовано огнетушителем с расчетом 1 огнетушитель на 100 квадратных метров. Площадь помещения – 28м^2, следовательно 1 огнетушитель на комнату.

Масса огнетушащего вещества для объемного пожаротушения рассчитывается по следующей формуле:

$$m_{dv} = k \cdot g_k \cdot V \quad (3.10)$$

где k – коэффициент компенсации не учитываемых потерь углекислотно–хладонового состава k = 1,2;

g_k – нормативная массовая концентрация углекислотно–хладонового состава gn = 0,04;

V – объем помещения.

$$V = L \cdot W \cdot H \quad (3.11)$$

где L –длина помещения;

W – ширина помещения;

H – высота помещения.

$V = 7 \cdot 4 \cdot 3 = 84 м^3$,

$M_d = 1{,}2 \cdot 0{,}04 \cdot 84 = 4{,}03$ *кг*

Расчетное количество баллонов ε устанавливается на основаннии расчета вместимости в двадцатилитровый баллон 4,0295 кг углекислотно–хладонового состава.

Внутренний диаметр магистрального трубопровода d_{im}, мм, находится по следующей формуле

$$d_{im} = 12 \cdot \sqrt{2} = 16{,}97 \text{мм} \quad (3.12)$$

Равносильная длина магистрального трубопровода l_2, м, находится по следующей формуле

$$l_2 = k_1 \cdot l_2 \quad (3.13)$$

где k_1 – коэффициент увеличения длины трубопровода для компенсации не учитывающих местных потерь k_1 =1,2;

l– длина трубопровода по проекту тогда l=3м;

$l_2 = 1{,}2 \cdot 3 = 3{,}6$

Расход углекислотно–хладонового состава Q, кг/с, напрямую зависимый от эквивалентной длины и диаметра трубопровода, и равен 1,395 кг/с

Расчетное время подачи углекислотно–хладонового состава t, мин, находится по следующей формуле:

$$t = \frac{m_d}{60Q} \quad (3.14)$$

$$t = \frac{4{,}2}{60 \cdot 1{,}4} = 0{,}05 \text{ мин}$$

Масса основного запаса углекислотно–хладонового состава m, кг, определяется по формуле:

$$m = 1{,}1 \cdot m_d \cdot \left(1 + \frac{k_2}{k}\right) \quad (3.15)$$

где $К_2$ – коэффициент учитывающий остаток состава в баллонах трубопроводах $К_2$=0,2.

$$m = 1{,}1 \cdot 4{,}2 \cdot \left(1 + \frac{0{,}2}{1{,}2}\right) = 5{,}39 \text{ кг}$$

Автоматизированные конструкции газового пожаротушения имеют в наличии оборудование для автоматического пуска. Для работы автоматизированной системы пожаротушения необходим 1 баллон вместимостью 20 литров и массой огнетушащей смеси 4,0295 кг [12].

5.4 Вывод по разделу безопасность жизнедеятельности

В этом модуле дипломной работы был осуществлен анализ условий труда и охраны жизнедеятельности. А так же анализ микроклимата помещения и его улучшение для более комфортной работы персонала. Также были определены меры по предотвращению пожара в рабочем помещении. Соблюдение данных мер по оптимизации рабочего места персонала позволяет сохранить работоспособность персонала в течение всего дня, что в свою очередь несет повышение производительности труда.

Заключение

В данной дипломной работе были решены поставленные задачи, такие как – оценка преимуществ и недостатков версий протокола IP.

Были рассмотрены основные технологии перехода на IPv6. Так как невозможно сразу полностью перейти на сети, использующие только протокол IPv6, то был выполнен анализ технологий, позволяющих сетям IPv4 и IPv6 взаимодействовать между собой.

Был выбран метод перехода и осуществлен на программном продукте – PacketTracer. После чего был проведен анализ и изменения в сети, который показал, что протокол версии IPv6 быстрее и надежнее предыдущей версии, несмотря на более широкое использование IPv4. Важность перехода на технологию IPv6 заключается в том, что глобальная паутина «Интернет» будет совершенствоваться и развеваться продолжительное число лет. Благодаря концепции IPv6 в последующие пару столетий, нtт необходимости поиска альтернативных решений проблем расширения сетей которые не в состоянии решить нынешний IPv4.

Список использованной литературы

1 Платонов В.В. Программно-аппаратные средства защиты информации. – М.: Информационная безопасность, 2013 г. – 69 с.

2 Одом У. Компьютерные сети. Первый шаг. – СПб.: «Вильямс», 2006 г. – 240 с.

3 Документация с сайта http://orbit-computer-solutions.com/Ways-to-Migrate-to-IPv6-.php «Ways to Migrate to IPv6»

4 Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. – СПб.: «Питер», 2003 г. – 368 с.

5 З.Д. Еркешева, Г.Ш. Боканова. Методические указания к выполнению семестровых работ для студентов специальности 5В070400 – «Вычислительная техника и программное обеспечение». – Алматы: АУЭС, 2014.

6 Тойгожинова А.Ж. Компьютерные сети. Методические указания к выполнению курсовой работы для студентов специальности 5В070400 – Вычислительная техника и программное обеспечение, 5В070300 – Информационные системы. – Алматы: АУЭС, 2011

7 Купер Д. «Архитектура корпоративных сетей», МПРЕСС 2014

8 Кулаков Ю. А., Луцкий Г.М. Локальные сети. Учебное пособие. – Киев: Юниор, 1998.

9 Новиков Ю. В., Карпенко Д.Г. Аппаратура локальных сетей. Функции, выбор, разработка. – М.: ЭКОМ, 1998

10 Смирнов И. Г. Структурированные кабельные системы — проектирование, монтаж и сертификация. Из-во: Экон-Информ, 2005 г.

11 Документация с сайта http://www.cisco.com - Cisco WAN Modeling Tools User Guide

12 Документация с сайта http://www.cisco.com - cisco wan | Accessing the WAN, CCNA Exploration Companion Guide

Приложение А

Таблица – А.1– IPv4-адресация

Город	Отдел	Адрес сети	Маска подсети	Первый ip-адрес	Последний ip-адрес	Широковещательный адрес	№ VLAN	Имя VLAN
Алматы	Кассовый отдел	172.16.0.0	255.255.224.0	172.16.0.1	172.16.31.254	172.16.31.255	11	CASH
Алматы	Фондовый отдел	172.16.32.0	255.255.224.0	172.16.32.1	172.16.63.254	172.16.63.255	21	STOCK
Алматы	Юрдический отдел	172.16.64.0	255.255.240.0	172.16.64.1	172.16.79.254	172.16.79.255	22	LAW
Алматы	Отдел кадров	172.16.80.0	255.255.240.0	172.16.80.1	172.16.95.254	172.16.95.255	23	HR
Алматы	Бухгалтерия	172.16.96.0	255.255.224.0	172.16.96.1	172.16.127.254	172.16.127.255	32	BOOK
Алматы	Администрация	172.16.128.0	255.255.224.0	172.16.128.1	172.16.159.254	172.16.159.255	31	MANAGERS
Алматы	Залы совещаний	172.16.160.0	255.255.224.0	172.16.160.1	172.16.191.254	172.16.191.255	41	TELEPRESS
Алматы	·зарезервирован·	172.16.224.0	255.255.224.0	172.16.224.1	172.16.255.254	172.16.255.255	-	-
Ташкент	Кассовый отдел	172.17.0.0	255.255.192.0	172.17.0.1	172.17.63.254	172.17.63.255	111	CASH
Ташкент	Финансовый отдел	172.17.64.0	255.255.224.0	172.17.64.1	172.17.95.254	172.17.95.255	211	STOCK
Ташкент	Администрация	172.17.96.0	255.255.224.0	172.17.96.1	172.17.127.254	172.17.127.255	212	MANAGERS
Ташкент	Залы совещаний	172.17.128.0	255.255.192.0	172.17.128.1	172.17.191.254	172.17.191.255	213	TELEPRESS
Ташкент	·зарезервирован·	172.17.192.0	255.255.192.0	172.17.192.1	172.17.255.254	172.17.255.255	-	-
Бишкек	Кассовый отдел	172.18.0.0	255.255.192.0	172.18.0.1	172.18.63.254	172.18.63.255	311	CASH
Бишкек	Финансовый отдел	172.18.64.0	255.255.224.0	172.18.64.1	172.18.95.254	172.18.95.255	311	STOCK
Бишкек	Администрация	172.18.96.0	255.255.224.0	172.18.96.1	172.18.127.254	172.18.127.255	412	MANAGERS
Бишкек	Залы совещаний	172.18.128.0	255.255.192.0	172.18.128.1	172.18.191.254	172.18.191.255	413	TELEPRESS
Бишкек	·зарезервирован·	172.18.192.0	255.255.192.0	172.18.192.1	172.18.255.254	172.18.255.255	-	-

Приложение В

Таблица – В.1 – IPv6-адресация

Город	Отдел	Адрес сети	Маска	Первый ip-адрес	Последний ip-адрес	№ VLAN	Имя VLAN
Алматы	Кассовый отдел	4400:DB8:ACAD:1::0	/64	4400:DB8:ACAD:1::1	4400:DB8:ACAD:1::FFFF	11	CASH
Алматы	Фондовый отдел	4400:DB8:ACAD:4::0	/64	4400:DB8:ACAD:4::1	4400:DB8:ACAD:4::FFFF	21	STOCK
Алматы	Юрдический отдел	4400:DB8:ACAD:3::0	/64	4400:DB8:ACAD:3::1	4400:DB8:ACAD:3::FFFF	22	LAW
Алматы	Отдел кадров	4400:DB8:ACAD:2::0	/64	4400:DB8:ACAD:2::1	4400:DB8:ACAD:2::FFFF	23	HR
Алматы	Бухгалтерия	4400:DB8:ACAD:5::0	/64	4400:DB8:ACAD:5::1	4400:DB8:ACAD:5::FFFF	32	BOOK
Алматы	Администрация	4400:DB8:ACAD:6::0	/64	4400:DB8:ACAD:6::1	4400:DB8:ACAD:6::FFFF	31	MANAGERS
Алматы	Залы совещаний	4400:DB8:ACAD:7::0	/64	4400:DB8:ACAD:7::1	4400:DB8:ACAD:7::FFFF	41	TELEPRESS
Алматы	·зарезервирован·	4400:DB8:ACAD:8::0	/64	4400:DB8:ACAD:8::1	4400:DB8:ACAD:8::FFFF	-	-
Ташкент	Кассовый отдел	4400:DB8:ACAD:9::0	/64	4400:DB8:ACAD:9::1	4400:DB8:ACAD:9::FFFF	111	CASH
Ташкент	Финансовый отдел	4400:DB8:ACAD:A::0	/64	4400:DB8:ACAD:A::1	4400:DB8:ACAD:A::FFFF	211	STOCK
Ташкент	Администрация	4400:DB8:ACAD:B::0	/64	4400:DB8:ACAD:B::1	4400:DB8:ACAD:B::FFFF	212	MANAGERS
Ташкент	Залы совещаний	4400:DB8:ACAD:C::0	/64	4400:DB8:ACAD:C::1	4400:DB8:ACAD:C::FFFF	213	TELEPRESS
Ташкент	·зарезервирован·	4400:DB8:ACAD:D::0	/64	4400:DB8:ACAD:D::1	4400:DB8:ACAD:D::FFFF	-	-
Бишкек	Кассовый отдел	4400:DB8:ACAD:E::0	/64	4400:DB8:ACAD:E::1	4400:DB8:ACAD:E::FFFF	311	CASH
Бишкек	Финансовый отдел	4400:DB8:ACAD:F::0	/64	4400:DB8:ACAD:F::1	4400:DB8:ACAD:F::FFFF	311	STOCK
Бишкек	Администрация	4400:DB8:ACAD:F1::0	/64	4400:DB8:ACAD:F1::1	4400:DB8:ACAD:F1::FFFF	412	MANAGERS
Бишкек	Залы совещаний	4400:DB8:ACAD:F2::1	/64	4400:DB8:ACAD:F2::1	4400:DB8:ACAD:F2::FFFF	413	TELEPRESS
Бишкек	·зарезервирован·	4400:DB8:ACAD:F3::1	/64	4400:DB8:ACAD:F3::1	4400:DB8:ACAD:F3::FFFF	-	-

Приложение С

Конфигурация коммутатора SW-A3-1:

```
Building configuration...

Current configuration : 1622 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW-A3-1
!
!
!
spanning-tree mode rapid-pvst
spanning-tree vlan 32 priority 20480
spanning-tree vlan 31 priority 24576
!
interface FastEthernet0/1
switchport access vlan 31
switchport mode access
!
interface FastEthernet0/2
switchport access vlan 31
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 31
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 31
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 31
switchport mode access
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
```

```
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
switchport trunk allowed vlan 31-32
switchport mode trunk
!
interface FastEthernet0/24
switchport trunk allowed vlan 31-32
switchport mode trunk
!
interface GigabitEthernet0/1
switchport trunk allowed vlan 31-32
switchport mode trunk
!
interface GigabitEthernet0/2
switchport trunk allowed vlan 32
switchport mode trunk
shutdown
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
end
```

Конфигурация коммутатора MSW-A4-1

```
Building configuration...

Current configuration : 2283 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname MSW-A4-1
```

```
ip routing
!
spanning-tree mode rapid-pvst
spanning-tree vlan 32 priority 16384
spanning-tree vlan 21-23 priority 20480
!
interface Port-channel 1
!
interface FastEthernet0/1
channel-group 1 mode on
!
interface FastEthernet0/2
channel-group 1 mode on
!
interface FastEthernet0/3
!
interface FastEthernet0/4
switchport trunk allowed vlan 31-32
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
switchport trunk allowed vlan 32
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/23
switchport trunk allowed vlan 11
switchport trunk encapsulation dot1q
```

```
switchport mode trunk
!
interface FastEthernet0/24
switchport trunk allowed vlan 21-23
switchport trunk encapsulation dot1q
!
interface GigabitEthernet0/1
switchport trunk allowed vlan 11,21-23,31-32,51
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/2
switchport trunk allowed vlan 31-32
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Vlan1
no ip address
shutdown
!
interface Vlan11
ip address 172.16.31.254 255.255.224.0
!
interface Vlan21
ip address 172.16.63.254 255.255.224.0
!
interface Vlan22
ip address 172.16.79.254 255.255.240.0
!
interface Vlan23
ip address 172.16.95.254 255.255.240.0
!
interface Vlan31
ip address 172.16.159.254 255.255.224.0
!
interface Vlan32
ip address 172.16.127.254 255.255.224.0
!
interface Vlan51
ip address 172.16.223.254 255.255.224.0
!
ip classless
!
ip flow-export version 9
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```

Настройка IP-телефонов:

```
Router(config)#ip dhc
Router(config)#ip dhcp p
Router(config)#ip dhcp pool de
Router(config)#ip dhcp pool dev
Router(config)#ip dhcp pool device
Router(dhcp-config)#tele
Router(dhcp-config)#telepho
Router(dhcp-config)#telephony
Router(dhcp-config)#?
  default-router  Default routers
  dns-server      Set name server
  exit            Exit from DHCP pool configuration mode
  network         Network number and mask
  no              Negate a command or set its defaults
  option          Raw DHCP options
Router(dhcp-config)#exit
Router(config)#tele
Router(config)#telephony-service
Router(config-telephony)#au
Router(config-telephony)#aut
Router(config-telephony)#?
  auto              Define dn range for auto assignment
  auto-reg-ephone   Enable Ephone Auto-Registration
  create            create cnf for ethernet phone
  exit              Exit from telephony config mode
  ip                Define IP address and port for Telephony-Service/Fallback
  keepalive         Define keepalive timeout period to unregister IP phones
  max-dn            Maximum directory numbers supported
  max-ephones       Define max number of IP phones
  no                Negate or set default values of a command
Router(config-telephony)#auto-re
Router(config-telephony)#auto-reg-ephone
Router(config-telephony)#keep
Router(config-telephony)#keepalive 120
Router(config-telephony)#ep
Router(config-telephony)#eph
Router(config-telephony)#?
  auto              Define dn range for auto assignment
  auto-reg-ephone   Enable Ephone Auto-Registration
  create            create cnf for ethernet phone
  exit              Exit from telephony config mode
  ip                Define IP address and port for Telephony-Service/Fallback
  keepalive         Define keepalive timeout period to unregister IP phones
  max-dn            Maximum directory numbers supported
  max-ephones       Define max number of IP phones
  no                Negate or set default values of a command
Router(config-telephony)#ephone-dn 1
Router(config-ephone-dn)#exit
Router(config)#telephony-service
Router(config-telephony)#ephone-dn 3
Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 3.1, changed
state to up

Router(config-ephone-dn)#number 113
Router(config-ephone-dn)#number 54003
Router(config-ephone-dn)#exit
Router(config)#tele
Router(config)#telephony-service
Router(config-telephony)#cre
Router(config-telephony)#create cn
Router(config-telephony)#create cnf-files
```

```
Creating CNF files
CNF-FILES: Clock is not set or synchronized, retaining old versionStamp
Router(config-telephony)#ephone-dn 3
Router(config-ephone-dn)#number 54003
Router(config-ephone-dn)#exit
Router(config)#int
Router(config)#interface F
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip add
Router(config-if)#ip address 192.168.10.2
% Incomplete command.
Router(config-if)#ip address 192.168.10.2 255.255.255.0
% 192.168.10.0 overlaps with FastEthernet0/0
Router(config-if)#ip address 169.254.213.2 255.255.255.0
Router(config-if)#
%IPPHONE-6-REGISTER: ephone-3 IP:169.254.213.1 Socket:2 DeviceType:Phone has
registered.

%IPPHONE-6-REGISTER: ephone-3 IP:169.254.213.1 Socket:2 DeviceType:Phone has
registered.

%IPPHONE-6-REGISTER: ephone-3 IP:169.254.213.1 Socket:2 DeviceType:Phone has
registered.

%IPPHONE-6-REGISTER: ephone-3 IP:169.254.213.1 Socket:2 DeviceType:Phone has
registered.

%IPPHONE-6-REGISTER: ephone-3 IP:169.254.213.1 Socket:2 DeviceType:Phone has
registered.

Router#
%SYS-5-CONFIG_I: Configured from console by console


Настройка 6to4
Router#config t
Router(config#interface tunnel 0
Router(config-if)#ipv6 address 4400:DB8:ACAD:1::0/64
Router(config-if)#tunnel source 172.16.0.1
Router(config-if)#tunnel destination 172.16.32.1
Router(config-if)#tunnel mode ipv6ip

Switch#config t
Switch(config#interface tunnel 0
Switch(config-if)#ipv6 address 4400:DB8:ACAD:1::1/64
Switch(config-if)#tunnel source 172.16.0.2
Switch(config-if)#tunnel destination 172.16.32.2
Switch(config-if)#tunnel mode ipv6ip
```