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: Проектирование корпоративной сети с использованием протокола динамической маршрутизации Open Shortest Path First для УГГК №12 и ГК №10 города Алматы

Специальность Вычислительная техника и программное обеспечение

Выполнил (а) Кудайбергенов Т.С. ВТп-10-4
(Фамилия и инициалы) группа

Научный руководитель Терегусупова А.С., старший преподаватель
(Фамилия и инициалы, ученая степень, звание)

Консультанты:

по экономической части:
Ержанова З.Ж., ст. преподаватель
(Фамилия и инициалы, ученая степень, звание)
Ержанова «14» 05 2014 г.
(подпись)

по безопасности жизнедеятельности:
Жиенбаев Н.Г., д-р т.н., профессор
(Фамилия и инициалы, ученая степень, звание)
_____ «04» 06 2014 г.
(подпись)

по применению вычислительной техники:
Терегусупова А.С., старший преподаватель
(Фамилия и инициалы, ученая степень, звание)
_____ «31» мая 2014 г.
(подпись)

_____
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____ 20__ г.
(подпись)

Нормоконтролер: Тусупов Д.М.
(Фамилия и инициалы, ученая степень, звание)
_____ «30» мая 2014 г.
(подпись)

Рецензент: _____
(Фамилия и инициалы, ученая степень, звание)
_____ «_____»_____ 20__ г.
(подпись)

Алматы 2014 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Факультет Информационных технологий

Специальность Вычислительная техника и программное обеспечение

Кафедра Компьютерных технологий

ЗАДАНИЕ

на выполнение дипломного проекта

Студент Кудайберген Толеген Серікұлы

(фамилия, имя, отчество)

Тема проекта Проектирование корпоративной сети с использованием протокола динамической маршрутизации Open Shortest Path First для ГКБ №12 и ГП №10 города Алматы

утверждена приказом ректора № 115 от «24» сентября 2013 г.

Срок сдачи законченной работы «10» июня 2014 г.

Исходные данные к проекту требуемые параметры результатов проектирования (исследования) и исходные данные объекта

Разработка корпоративной сети для Центральной городской клинической больницы №12 и Городской поликлиники №10 города Алматы. Применение протокола динамической маршрутизации Open Shortest Path First

Перечень подлежащих разработке дипломного проекта вопросов или краткое содержание дипломного проекта:

Проектирование корпоративной сети для Центральной городской клинической больницы №12 и Городской поликлиникой №10 города Алматы.

Перечень графического материала (с точным указанием обязательных чертежей)

Рисунок 3.3 – Топология сети первого этапа.

Рисунок 3.4 – Топология сети второго этапа ТП №10.

Рисунок 3.5 – Топология сети третьего этапа ТП №10.

Рисунок 3.6 – Топология сети четвертого этапа ТП №10.

Рисунок 3.7 – Обобщенная топология Городской поликлиники №10

Рисунок 3.8 – Архитектура локальной сети в Городской поликлинике №10

Рисунок 3.9 – Архитектура локальной сети в Центральной городской клинической больнице №12.

Рекомендуемая основная литература

1 Никитюк Л.А., Комарницкий Д.Л. Методическое руководство к выполнению КП „Проектирование корпоративной сети" – Одесса 2006

2 Леммле Т., Тинсли Б. Конфигурирование маршрутизаторов Cisco. – 2-е изд. – Москва: Издательство „Вильямс", 2004.

3 Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – 3-е изд. – Санкт – Петербург: Издательство „Питер", 2006.

4 М.А. Щербаков, М.П. Строганов. Информационные сети и телекоммуникации. – Москва: Издательство „Высшая школа", 2008

Консультанты по проекту с указанием относящихся к ним разделов

Раздел	Консультант	Сроки	Подпись
БЖД	Прохоренко Н.Г.	11.04 – 04.05.14	
Экономика	Брежнева З.О.	15.04 – 14.05.14	Брежнева
Нормоконтроль	Гусулов Д.М.	30.05.14 г.	
Научный руководит.	Терещенкова А.С	31.05.14	

ГРАФИК
подготовки дипломного проекта

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления руководителю	Примечание
1	Изучение протокола OSPF	01.04.2014	
2	Изучение основных протоколов		
	динамической маршрутизации	05.04.2014	
3	Настройка протокола удален-		
	ного доступа SSH	15.04.2014	
4	Разработка локальной сети		
	Центральной городской кли-		
	нической больницы №12	30.04.2014	
5	Разработка локальной сети		
	Городской поликлиники	11.05.2014	
	№10		
6	Проектирование отказоустой-		
	чивой корпоративной сети		
	для ЦГКБ №12 и ГП №10	20.05.2014	

Дата выдачи задания «03» марта 2014 г.

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

Руководитель _____ Терещенова А.С.
(подпись) (Фамилия и инициалы)

Задание принял к исполнению
студент _____ Кудайбергенов Т.С.
(подпись) (Фамилия и инициалы)

Андатпа

Бұл дипломдық жобада Open Shortest Path First № 12 Орталық қалалық клиникалық ауруханағы және № 10 Қалалық емханаға үдемелі бағдарғылаудың хаттамасын қолдану арқылы корпоративтік желіні жобалау үдерісі келтірілген.

Берілген дипломдық жобада Open Shortest Path First үдемелі бағдарғылаудың хаттамасы, корпоративтік желіні құру сұлбасы мен жабдық құрамы қарастырылған.

Сонымен қатар жобада өміртіршілік қауыпсіздігінің шаралары сипатталған.

Жобаны енгізудің технико-экономикалық негіздемесі келтірілген.

Аннотация

В данном дипломном проекте представлен процесс проектирования корпоративной сети с использованием протокола динамической маршрутизации Open Shortest Path First для Центральной городской клинической больницы № 12 и Городской поликлиники № 10.

В данном дипломном проекте рассмотрен протокол динамической маршрутизации Open Shortest Path First, схемы построения корпоративной сети и состав оборудования.

В проекте также описаны меры безопасности жизнедеятельности.

Разработано технико-экономическое обоснование внедрения данного проекта.

Annotation

This diploma project provides a process of designing a corporate network using dynamic routing protocol Open Shortest Path First for the Central municipal clinical hospital № 12 and the Municipal policlinic № 10.

This diploma project is considered a dynamic routing protocol Open Shortest Path First, the circuits of the corporate network and Hardware.

Safety of vital functions measures are also described in a project.

The feasability study of introduction of this project is worked out.

Содержание

Введение

Основой инфраструктуры современных предприятий являются корпоративные сети передачи данных, предоставляющие транспорт для передачи информации между разными приложениями информационных систем.

В последнее время мультисервисные корпоративные сети приходят на смену специализированным сетям. Для обеспечения потребностей требования к мультисервисной корпоративной сети, непрерывно возрастают, как к среде передачи информации для выполнения работы различных приложений. Высокое значение имеет время реакции, оно требует надлежащей организации корпоративной сети и приложений.

Работа в реальном времени стала жизненной необходимостью и одним из главных требований, предъявляемых к корпоративным сетям и приложениям.

Но при этом гарантировать хорошее время реакции особенно трудно – этому препятствует разнообразие потоков данных и их высокая интенсивность, потребность совершать поиск данных в базах большого объема, невысокая скорость глобальных линий связи между подразделениями, замедление скорости взаимодействия в шлюзах, согласующих неоднородные компоненты разных подсетей.

Поддержание работы учреждений, пользующихся данной сетью – одна из главных целей корпоративной сети. Пользователями корпоративной сети являются сотрудники данного предприятия, т.е. медицинские работники.

Сегодня трудно найти компанию или учебное заведение, которое не имело бы сетевой инфраструктуры. Практически все современные сети являются маршрутизируемыми. С ростом размеров сети компании для поддержания ее нормальной работоспособности сетевому администратору приходится переходить от статической маршрутизации к динамической и, следовательно, к использованию одного из протоколов динамической маршрутизации.

Наиболее универсальным и гибким в настройке протоколом динамической маршрутизации в корпоративных сетях на сегодняшний день является открытый протокол выбора первого кратчайшего пути (Open Shortest Path First Protocol – OSPF). Протокол изначально был ориентирован на работу в больших сетях со сложной топологией.

Существует несколько положительных факторов, почему мне стоило выбрать именно этот протокол. Он основан на алгоритме состояния каналов связи и обладает высокой устойчивостью к изменениям топологии сети и быстрой сходимостью. Передача данных в данном протоколе происходит по наиболее скоростным каналам связи, так как при выборе маршрута используется метрика пропускной способности составной сети.

Протокол также обладает и другими достоинствами, полезными в крупных современных сетях. К ним относятся возможность балансировки нагрузки между каналами с равными метриками и средства аутентификации как по нешифрованному паролю, так и по шифрованному. Нумерация пакетов исключает их повторяемость и таким образом возможность повторной атаки. Открытость протокола определяет его поддержку практически всеми производителями сетевого оборудования, реализации в ПО под все популярные операционные системы.

таким образом, актуальность темы дипломной работы обусловлена необходимостью создания надѐжной и полнофункциональной корпоративной сети для медицинских учреждений.

Целью данной дипломной работы является проектирование корпоративной сети для Центральной городской клинической больницы № 12 и Городской поликлиники № 10 с использованием протокола динамической маршрутизации OPSF.

1 Обзор развития, проектирования и параметры качества корпоративных сетей

1.1 Корпоративная сеть как объект исследования

Успешная деятельность промышленной, финансовой или иной организации во многом определяется наличием единого информационного пространства. Развитая информационная система позволяет эффективно справляться с обработкой потоков информации, циркулирующих между сотрудниками предприятия и принимать им своевременные и рациональные решения, обеспечивающие выживание предприятия в жесткой конкурентной борьбе.

Корпоративная сеть (КС) – это сложная система, обеспечивающая передачу данных широкого спектра между различными приложениями, используемыми в единой информационной системе организации.

КС позволяет создать единую для всех подразделений базу данных, вести электронный документооборот, организовать селекторные совещания и проводить видеоконференции с отдаленными подразделениями, обеспечить все потребности организации в высококачественной телефонной и факсимильной местной, международной и междугородной связи, доступе в Интернет и другие интерактивные сети. Все это уменьшает время реакции на изменения, происходящие в компании, и обеспечивает оптимальное управление всеми процессами в реальном масштабе времени. При этом, снижается зависимость организации от операторов фиксированной и мобильной связи. Частичный отказ от услуг этих операторов позволяет существенно сократит расходы организации. Появляется возможность передавать любую конфиденциальную информацию производственного и финансового характера с уверенностью, что никто, кроме уполномоченных сотрудников компании, не имеет к ней доступа. Обобщенная схема КС представлена на рисунке 1.1.

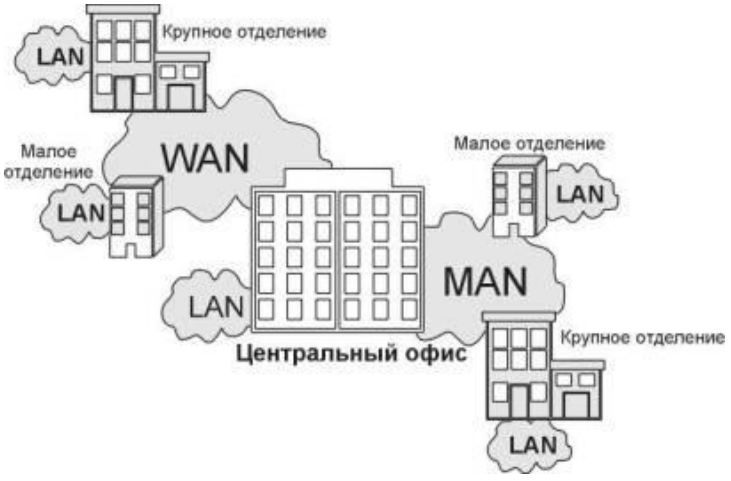

Рисунок 1.1 – Обобщенная схема корпоративной сети

Корпоративную сеть необходимо рассматривать с различных сторон: структурной, функциональной и системно-технической.

Со структурной точки зрения корпоративная сеть – сеть смешанной топологии, содержащая несколько локальных вычислительных сетей. Корпоративная сеть будет объединять филиалы ЛПУ, создавая общее информационное корпоративное пространство. С этой точки зрения корпоративная сеть отражает структуру медучреждения.

С функциональной точки зрения корпоративная сеть – это эффективная среда передачи актуальной информации необходимой для решения задач.

С системно-технической точки зрения корпоративная сеть представляет собой целостную структуру, состоящую из взаимосвязанных и взаимодействующих уровней, представленных на рисунке 1.2.

Рисунок 1.2 – Иерархия уровней корпоративной сети

таким образом, с системно-технической точки зрения корпоративная сеть – это сложная система, предоставляющая пользователям и программам набор полезных в работе услуг и сервисов, общесистемных и специализированных приложений, обладающая набором полезных качеств и свойств, и содержащая в

себе службы, гарантирующее нормальное функционирование корпоративной сети.

1.2 Роль корпоративных сетей в создании и развитии IT-инфраструктуры

В настоящее время IT-инфраструктура любого предприятия – это его ключевая инфраструктура, вне зависимости от вида деятельности. Для внедрения информационных технологий транспортную основу организуют корпоративные сети передачи данных.

Современная корпоративная сеть – это не только сеть передачи данных, а сложный комплекс, который способен предоставлять различные сервисы с прогнозируемыми характеристиками.

Благодаря корпоративным сетям результативно решаются задачи ключевых процессов. таких как:

- быстрый доступ к информационным массивам общего информационного пространства;
- анализ состояния и управление бизнес-процессами из единого аналитического центра;
- обмен информационными и расчетными документами;
- непрерывное автоматизированное наблюдение (мониторинг) и управление ресурсами инфокоммуникационной системы из единого центра.

1.3 Особенности проектирования корпоративных сетей

Основная цель проектирования корпоративных сетей состоит в том, чтобы определить структуру, состав аппаратно-программных средств и организацию корпоративной сети. И при заданных ограничениях на затраты ее проектирования, внедрения и обслуживания они будут выполнять основные требования к качеству информационных услуг, предоставляемых сетью. И строится это на основании характеристик корпоративных информационных потоков предприятия, параметров потребителей и производителей информации. При проектировании корпоративной сети сетевые администраторы и сетевые интеграторы стараются обеспечить выполнение следующих требований:

- расширяемость – возможность простой интеграции отдельных компонентов сети (пользователей, приложений, служб, компьютеров);
- масштабируемость – возможность добавления новых узлов и протяженность связей, а также производительности узлов и сетевого оборудования;
- производительность – обеспечение необходимых значений параметров производительности сетевых узлов и каналов связи (скорость передачи данных, время реакции, задержка передачи и ее вариация);
- управляемость – обеспечение возможностей централизованного

управления, планирования развития сети и мониторинга состояния сети;

- надежность – обеспечение бесперебойной работы узлов сети и каналов связи, согласованности, сохранности и доставки данных без изменений и ошибок узлу назначения;
- безопасность – обеспечение защиты данных от несанкционированного доступа.

Учитывая масштабность, использование глобальных связей, высокую степень разнородности проектирование корпоративных сетей является трудно формализуемым процессом. На сегодняшний день отсутствуют универсальные методики проектирования корпоративных сетей. Поэтому необходимо сформулировать некоторые типовые этапы выполнения сетевых проектов.

Процесс проектирования корпоративной сети состоит из следующих этапов:

1) анализ требований. На этом этапе формулируются основные цели предприятия (оперативный прием заказов, сокращение производственного цикла, повышение производительности труда и т.д.). Анализируются существующие аналогичные системы, обосновывается необходимость в собственных проектах системы;

2) разработка бизнес-модели предприятия. Бизнес-модель или функциональная модель производства излагает основные, административные и вспомогательные бизнес-процессы предприятия, иерархические взаимоотношения и информационные потоки между подразделениями. также передает структурированное отображение функций производственной системы, информации среды и объектов, связывающих эти функции;

3) разработка технической модели корпоративной сети (структурный синтез). техническая модель представляет собой совокупность технических средств, необходимых для реализации проекта корпоративной сети. На данном этапе определяются технические параметры компонентов сети, такие как полный функциональный набор необходимых программных и аппаратных средств, но без конкретизации оборудования (марок и моделей);

4) разработка физической модели корпоративной сети (параметрический синтез). Физическая же модель корпоративной сети представляет подробное описание программных и технических средств, их количества, технических параметров и способов взаимодействия. таким образом, это конкретизацией технической модели сети, в которой выбраны протоколы, конкретные сетевые устройства и прочие сетевые технические средства. Выбираются они же в соответствии с техническими параметрами, задаваемыми в технической модели. Параметры, структурная схема и алгоритмы функционирования сети, как результаты выполнения данного этапа, используются для последующего анализа;

5) моделирование и оптимизация корпоративной сети. Моделирование производится на данном этапе с целью оценки характеристик функционирования корпоративной сети и их оптимизации;

6) установка и наладка корпоративной сети. На этом этапе

подразумевается управление конфигурированием, координирование поставок от субподрядчиков, инсталляцию и наладку оборудования, обучение персонала;

7) тестирование корпоративной сети. На этом этапе должны проводиться необходимые испытания, описанные в контракте с интегратором;

8) сопровождение и эксплуатация корпоративной сети. Последний этап не имеет четко определенных временных границ, он предполагает непрерывный процесс.

1.4 Параметры качества корпоративной сети

В настоящее время постоянно растущие требования корпоративных пользователей корпоративных приложений к пропускной способности сети привели к появлению новых высокоскоростных технологий и новых механизмов качества обслуживания, учитывающих различные характеристики трафика: относительная скорость передачи данных и чувствительность к задержкам, потерям и искажением пакетов. Рассмотрим основные параметры качества корпоративной сети:

- пропускная способность сети – интегральный параметр характеризует объем информации, передаваемой сетью в единицу времени;
- реакция на характеристики профиля трафика – параметр, характеризующий изменения нагрузки на сеть в зависимости от характеристик профиля трафика. Например, изменение числа искаженных или потерянных пакетов, пропускной способности при пульсирующем или плавном изменении трафика; количество искаженных или потерянных пакетов (согласно экспертным оценкам, для протокола TCP 1-5% потерянных пакетов находится в пределах нормы, предельное значение при котором сеть практически не работает – 40% потерянных или искаженных пакетов);
- время доставки – время двойного хода (в прямом и обратном направлении). Этот параметр может изменяться в диапазоне от 0 до 2000 MS, оказывая влияние на производительность работы одного потока;
- неравномерность времени доставки пакетов – параметр, влияющий на работу отдельных приложений, например, приложения, управляющие техническим объектом в реальном времени или передающие мультимедийную информацию.

1.5 трехуровневая иерархическая модель

При проектировании корпоративной сети весь процесс разработки был разбит на три части, т.к. компьютерные сети удобно представлять в виде трехуровневой иерархической модели (Рисунок 1.3), которая содержит следующие уровни:

- уровень ядра;
- уровень распределения;

- уровень доступа.

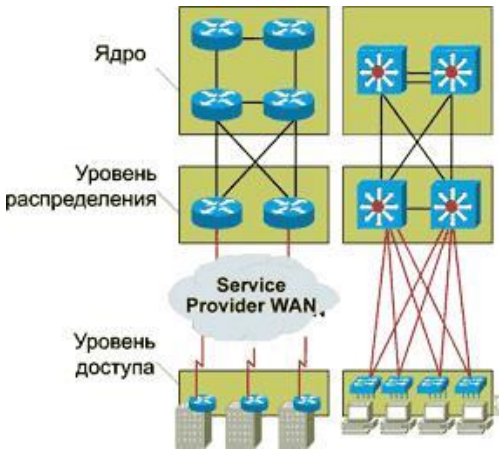

Рисунок 1.3 – трехуровневая модель

Уровень ядра предназначен для высокоскоростной передачи сетевого трафика и скоростной коммутации пакетов. Поэтому на сетевых устройствах этого уровня не вводятся дополнительные технологии (списки доступа или маршрутизация по правилам), отвечающие за маршрутизацию и фильтрацию пакетов.

Уровень ядра или базовый уровень представим несколькими поликлиниками, расположенными в разных городах. Маршрутизаторы этих узлов – маршрутизаторы ядра – соединены между собой, образуя кольцевое ядро сети с избыточными путями. Этот уровень предназначен для оперативной и надежной коммутации больших объемов трафика. На базовом уровне трафик передается совместно для нескольких пользователей. Здесь обрабатываются большие объемы трафика, поэтому не менее важно учитывать скорость и задержки. Обычно используются быстродействующие сети Multi-Gigabit Ethernet и Gigabit Ethernet.

С помощью протокола Ethernet к каждому из маршрутизаторов подключается через коммутатор маршрутизатор и группа серверов, которые вместе образуют демилитаризованную зону и обеспечивают доступ в Интернет. Группа корпоративных серверов подключается также к каждому узловому маршрутизатору. Каждый из маршрутизаторов ядра с помощью технологии глобальных сетей, например Frame Relay, соединен виртуальными каналами с маршрутизаторами районных поликлиник. Frame Relay ("Передача кадров") – технология передачи данных, активно применяющаяся в корпоративных сетях различного масштаба. Основной принцип этой технологии состоит в создании нескольких виртуальных каналов на одном физическом, при этом для каждого виртуального канала резервируется гарантированная полоса пропускания. Этот принцип дает ряд существенных преимуществ и перед выделенными цифровыми каналами, и перед протоколами X.25 и TCP/IP.

Уровень распределения используется для суммирования маршрутов. Суммирование проводится для уменьшения сетевого трафика на верхних

уровнях сети. Оно представляет собой объединение нескольких сетей в одну большую общую. Основными функциями уровня распределения являются фильтрация, маршрутизация и доступе к региональным сетям. Если необходимо, то и определение правил доступа пакетов к уровню ядра. На уровне распределения необходимо устанавливать наиболее быстрый способ обработки запросов к службам, такой как метод файлового обращения к серверу. Маршрутизаторы уровня распределения соединены с маршрутизаторами ядра. На уровне доступа производится контроль доступа к сети и формируется сетевой трафик. В основном используются сети 100-Mbps Fast Ethernet и 1000-Mbps Gigabit Ethernet.

Маршрутизаторы уровня доступа служат для подключения к глобальной вычислительной сети отдельных пользователей (серверы доступа) или отдельных локальных сетей. На этом уровне реализовано управление пользователями и рабочими группами при обращении к ресурсам объединенной сети. Иногда уровень доступа называют уровнем настольных систем. Наибольшая часть необходимых пользователям сетевых ресурсов должна быть доступна локально. На уровне распределения выполняется перенаправление трафика к удаленным службам. Скорость сети – Ethernet 10 Mbps или 100-Mbps Fast Ethernet.

Самым простым коммутирующим оборудованием уровня доступа являются коммутаторы рабочих групп. В свою очередь, к ним присоединяются автоматизированные рабочие места сотрудников организации (АРМы). По причине большого количества АРМов в сети коммутаторы уровня рабочих групп необходимо разделить на два уровня. Коммутаторы рабочих групп верхнего (второго) уровня объединяются в единую сеть с помощью коммутаторов зданий, которые в рамках одного кампуса соединяются в кольцо оптоволоконными линиями связи.

Проектируемая сеть должна соответствовать требованиям избыточности и структурированности. Избыточность делает сеть устойчивой к нарушениям каналов передачи данных и их неполадкам, повышает надежность системы, однако и увеличивает трудоемкость администрирования сети.

1.6 Структура сети

территориальные компьютерные сети служат для обмена данными между поликлиниками, расположенными в разных регионах страны. Они обладают большой протяженностью и требуют больших затрат. В их стоимость входят кабели, работа по прокладке, затраты на коммутационное оборудование, промежуточную усилительную аппаратуру, обеспечивающую необходимую полосу пропускания канала и эксплуатационные затраты для поддержания в рабочем состоянии.

Глобальная сеть не может быть полностью создана для медицинских учреждений, поэтому предлагается промежуточный вариант: корпоративная сеть медицинских учреждений использует оборудование общественной

глобальной сети, их услуги, но часть дополняет своими собственными. Например, аренда каналов связи, на основе которой создать собственную территориальную сеть.

Локальные и глобальные сети состоит из периферийных подсетей и магистрали, которая связывает эти подсети. Структура крупной локальной сети приведена на рисунке 1.4, она состоит из подсетей, объединенных магистралью, включающих два кольца FDDI и четыре маршрутизатора. Каждая подсеть также может иметь иерархическую структуру, образованную своими маршуртизаторами, коммутаторами, концентраторами и сетевыми адаптерами. Все эти коммуникационные устройства связаны разветвленной кабельной системой. такая сеть может быть расположена на территории нескольких районов города.

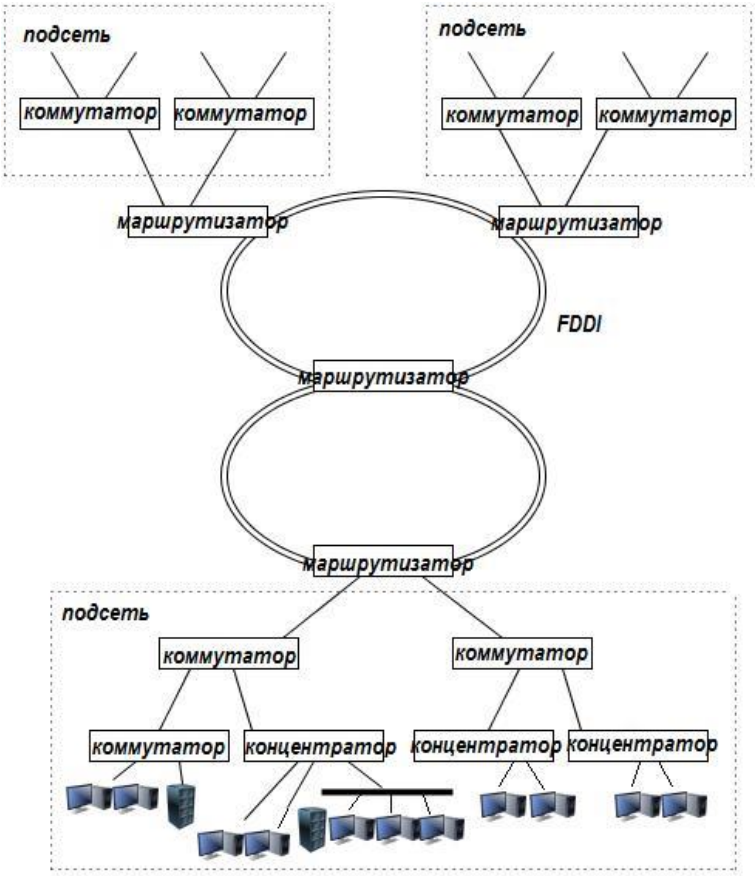

Рисунок 1.4 – Структура локальной сети

Глобальная сеть соединяет локальные сети, расположенные на большом расстоянии друг от друга. Она имеет иерархическую структуру с высокоскоростной магистралью, более медленными периферийными сетями и каналами доступа локальных сетей к глобальным.

Структура глобальной компьютерной сети приведена на рисунке 1.5. В основе лежат некоммутируемые каналы связи, которые соединяют коммутаторы глобальной сети. Коммутаторы называют также центрами

коммутации пакетов (ЦКП).

В местах, где требуется ответвление или соединение потоков данных или магистральных сетей устанавливаются коммутаторы. Выбор такого месторасположения коммутаторов определяется также возможностью обслуживания коммутаторов квалифицированным персоналом, наличием выделенных каналов связи в данном пункте, надежностью сети, определяемой избыточными связями между коммутаторами.

Конечные узлы глобальной сети показаны на рисунке 1.5. Основные типы конечных узлов глобальной сети: компьютеры (К), локальные сети, маршрутизаторы (R), мультиплексоры (MUX), используются для одновременной передачи по компьютерной сети данных и голоса (или изображения). Устройства типа DTE (Data Terminal Equipment) преобразуют пользовательскую информацию в данные для передачи по линии связи и осуществляющее обратное преобразование. Локальная сеть отделена от глобальной сети маршрутизатором или удаленным мостом.

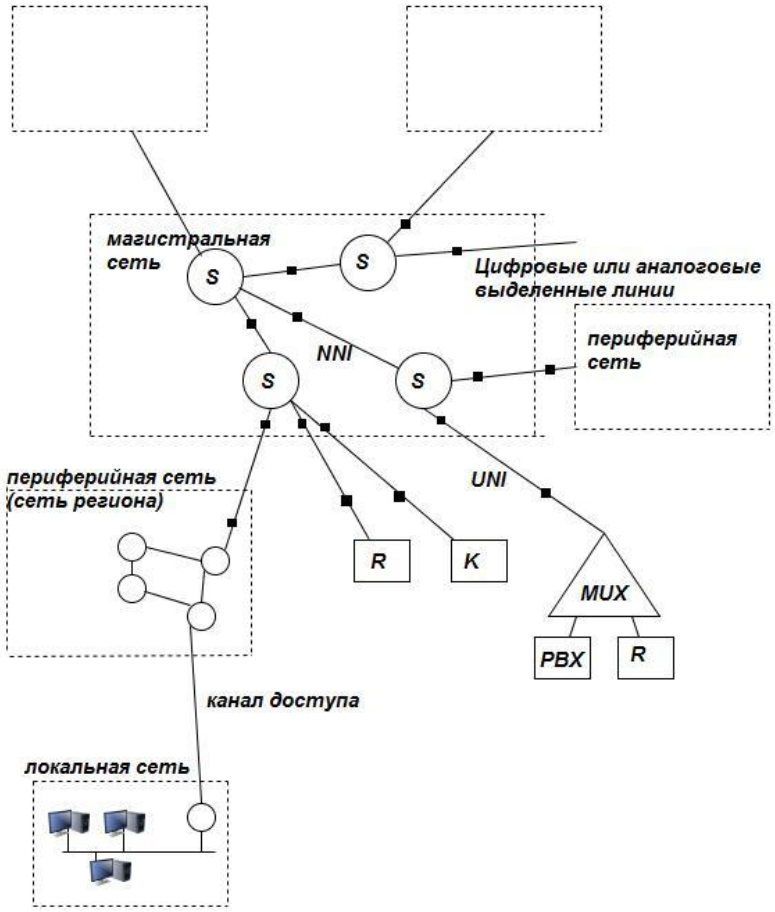

Рисунок 1.5 – Структура глобальной сети

На этом рисунке используются следующие обозначения:

- S (switch) – коммутаторы;
- К – компьютеры;
- R (router) – маршрутизаторы;

- MUX (multiplexor) – мультиплексор;
- UNI (User-Network Interface) – «интерфейс пользователь – сеть»;
- NNI (Network-Network Interface) – «интерфейс сеть – сеть»;
- офисная АтС – PBX;
- черные квадратики – устройства DCE.

При передаче данных через глобальную сеть мосты и маршрутизаторы работают в соответствии с той же логикой, что и при соединении локальных сетей. Мосты строят таблицу MAC-адресов на основании проходящего трафика, и по информации в этой таблицы принимают решение – предоставлять кадры в удаленную сеть или нет.

Маршрутизаторы принимают решение на основании номера сети пакета какого-либо протокола сетевого уровня (например, IP или IPX). Если же пакет нужно передать следующему маршрутизатору по глобальной сети упаковывают его в кадр этой сети, дополняют соответствующим аппаратным адресом следующего маршрутизатора и посылают в глобальную сеть.

так как конечные узлы глобальной сети должны передавать данные по каналу связи конкретного стандарта, то каждое устройство типа DTE необходимо оснастить устройством типа DCE (Data Circuit terminating Equipment) которое обеспечивает необходимый протокол физического уровня заданного канала. В зависимости от типа канала для связи с каналами глобальных сетей используются DCE трех основных типов: модемы для работы по выделенным и коммутируемым аналоговым каналам, устройства DSU/CSU для работы по цифровым выделенным каналам сетей технологии TDM и терминальные адаптеры (тА) для работы по цифровым каналам сетей ISDN. Устройства DTE и DCE обобщенно называют оборудованием, размещаемым на территории абонента глобальной сети – Customer Premises Equipment, CPE.

При использовании общественной сети очень важны предоставляемые сетью услуги правильное определение интерфейса взаимодействия с сетью. Оконечное оборудование программное обеспечение должны корректно сопрягаться с соответствующим оборудованием и программным обеспечением общественной сети, поэтому в глобальной сети строго прописан и стандартизован интерфейс «пользователь-сеть» (UNI – User-to-Network Interface). Это необходимо для того, чтобы пользователи могли без проблем подключаться к сети с помощью коммуникационного оборудования любого производителя, который соблюдает стандарт UNI данной технологии (например, X.25).

Протоколы взаимодействия коммутаторов внутри глобальной сети, называемые интерфейсом «сеть-сеть» (Network-to-Network Interface, NNI), стандартизуются не всегда. Если организация создает глобальную сеть, она должна иметь свободу действий, чтобы решать, как взаимодействовать внутренним узлам сети между собой. Поэтому внутренний интерфейс, в случае его стандартизации, носит название «сеть-сеть», а не «коммутатор-коммутатор», подчеркивая, что он должен использоваться в основном при взаимодействии двух территориальных сетей разных операторов.

2 Протокол динамической маршрутизации Open Shortest Path First

2.1 Библиографическая справка

Открытый протокол, базирующийся на алгоритме поиска наикратчайшего пути (Open Shortest Path Fisrt – OSPF) является протоколом маршрутизации, разработанным для сетей IP рабочей группой Internet Engineering Task Force (IETF), занимающейся разработкой протоколов для внутрисистемных роутеров (interior gateway protocol – IGP). Рабочая группа была образована в 1988 г. для разработки протокола IGP, базирующегося на алгоритме "поиска наикратчайшего пути" (shortest path first – SPF), с целью его использования в Internet, крупной международной сети, объединяющей научно-исследовательские институты, правительственные учреждения, университеты и частные предприятия. Как и протокол IGRP, OSPF был разработан по той причине, что к середине 1980 гг. непригодность RIP для обслуживания крупных гетерогенных объединенных систем стала все более очевидна.

OSPF явился результатом научных исследований по нескольким направлениям, включающим:

- алгоритм SPF компании Bolt, Beranek и Newman (BBN), разработанный для Arpanet (программы с коммутацией пакетов, разработанной BBN в начале 1970 гг., которая явилась поворотным пунктом в истории разработки сетей) в 1978 г;
- исследования Компании Radia Perlman по отказоустойчивости широкой рассылки маршрутной информации (1988);
- исследования BBN по маршрутизации в отдельной области (1986);
- одна из первых версий протокола маршрутизации IS-IS OSI.

Как видно из его названия, OSPF имеет две основных характеристики. Первая из них – это то, что протокол является открытым, т.е. его спецификация является общественным достоянием. Спецификация OSPF опубликована в форме Запроса для Комментария (RFC) 1247. Второй его главной характеристикой является то, что он базируется на алгоритме SPF. Алгоритм SPF иногда называют алгоритмом Дейкстры по имени автора, который его разработал.

2.2 Общие сведения о протоколе OSPF

OSPF – это открытый протокол маршрутизации, базирующийся на алгоритме поиска наикратчайшего пути (Open Shortest Path First – OSPF). OSPF имеет две основные характеристики: протокол является открытым, т. е. его спецификация является общественным достоянием, он базируется на алгоритме SPF.

OSPF является иерархическим протоколом маршрутизации с объявлением состояния о канале соединения (link-state). Он был спроектирован как протокол работы внутри сетевой области – AS (Autonomous System), которая представляет собой группу маршрутизаторов и сетей, объединенных по иерархическому принципу и находящихся под единым управлением и совместно использующих общую стратегию маршрутизации. В качестве транспортного протокола для маршрутизации внутри AS OSPF использует IP-протокол.

Обмен информацией о маршрутах внутри AS протокол OSPF осуществляет посредством обмена сообщениями о состояниях канала соединений между маршрутизаторами и сетями области (link-state advertisement – LSA). Эти сообщения передаются между объектами сети, находящимися в пределах одной и той же иерархической области – это может быть как вся AS, так и некоторая группа сетей внутри данной AS. В LSA-сообщения протокола OSPF включается информация о подключенных интерфейсах, о параметрах маршрутов и других переменных. По мере накопления роутерами OSPF информации о состоянии маршрутов области, они рассчитывают наикратчайший путь к каждому узлу, используя алгоритм SPF. Причем расчет оптимального маршрута осуществляется динамически в соответствии с изменениями топологии сети.

Для различных типов IP-сервиса (видов услуг высшего уровня, которые определяются значением поля TOS IP-пакета), OSPF может рассчитывать свои оптимальные маршруты на основании параметров, наиболее критичных для данного вида сервиса. Например, какая-нибудь прикладная программа может включить требование о том, что определенная информация является срочной. Если OSPF имеет в своем распоряжении каналы с высоким приоритетом, то они могут быть использованы для транспортировки срочных дейтаграмм.

OSPF поддерживает механизм, позволяющий работать с несколькими равноправными маршрутами между двумя объектами сети. Это позволяет существенно уменьшить время передачи данных и более эффективно использовать каналы связи.

Кроме того, OSPF-протокол поддерживает аутентификацию изменений маршрутов. Это означает, что только те маршрутизаторы, которые имеют определенные права, могут осуществлять маршрутизацию пакетов. Это позволяет, при соответствующей настройке прав системы маршрутизаторов, передавать по сети конфиденциальные сообщения, зная заранее, что они проходят только по определенным маршрутам.

2.3 Иерархия маршрутизации

В отличие от RIP, OSPF может работать в пределах некоторой иерархической системы. Самым крупным объектом в этой иерархии является автономная система (Autonomous System – AS) AS является набором сетей, которые находятся под единым управлением и совместно используют общую

стратегию маршрутизации. OSPF является протоколом маршрутизации внутри AS, хотя он и способен принимать маршруты из других AS и отправлять маршруты в другие AS.

Любая AS может быть разделена на ряд областей (area). Область – это группа смежных сетей и подключенных к ним хостов. Роутеры, имеющие несколько интерфейсов, могут участвовать в нескольких областях. такие роутеры, которые называются роутерами границы областей (area border routers), поддерживают отдельные топологические базы данных для каждой области.

топологическая база (topological database) данных фактически представляет собой общую картину сети по отношению к роутерам. топологическая база данных содержит набор LSA, полученных от всех роутеров, находящихся в одной области. т.к. роутеры одной области коллективно пользуются одной и той же информацией, они имеют идентичные топологические базы данных.

термин "домен" (domain) используется для описания части сети, в которой все роутеры имеют идентичную топологическую базу данных. термин "домен" часто используется вместо AS.

топология области является невидимой для объектов, находящихся вне этой области. Путем хранения топологий областей отдельно, OSPF добивается меньшего трафика маршрутизации, чем трафик для случая, когда AS не разделена на области.

Разделение на области приводит к образованию двух различных типов маршрутизации OSPF, которые зависят от того, находятся ли источник и пункт назначения в одной и той же или разных областях. Маршрутизация внутри области имеет место в том случае, когда источник и пункт назначения находятся в одной области; маршрутизация между областями – когда они находятся в разных областях.

Стержневая часть OSPF (backbone) отвечает за распределение маршрутной информации между областями. Она включает в себя все роутеры границы области, сети, которые не принадлежат полностью какой-либо из областей, и подключенные к ним роутеры. На рисунке 2.1 представлен пример объединенной сети с несколькими областями.

На рисунке 2.1 роутеры 4, 5, 6, 10, 11 и 12 образуют стержень. Если хост H1 Области 3 захочет отправить пакет хосту H2 Области 2, то пакет отправляется в роутер 13, который продвигает его в роутер 12, который в свою очередь отправляет его в роутер 11. Роутер 11 продвигает пакет вдоль стержня к роутеру 10 границы области, который отправляет пакет через два внутренних роутера этой области (роутеры 9 и 7) до тех пор, пока он не будет продвинут к хосту H2.

Сам стержень представляет собой одну из областей OSPF, поэтому все стержневые роутеры используют те же процедуры и алгоритмы поддержания маршрутной информации в пределах стержневой области, которые используются любым другим роутером. топология стержневой части невидима

для всех внутренних роутеров точно так же, как топологии отдельных областей невидимы для стержневой части.

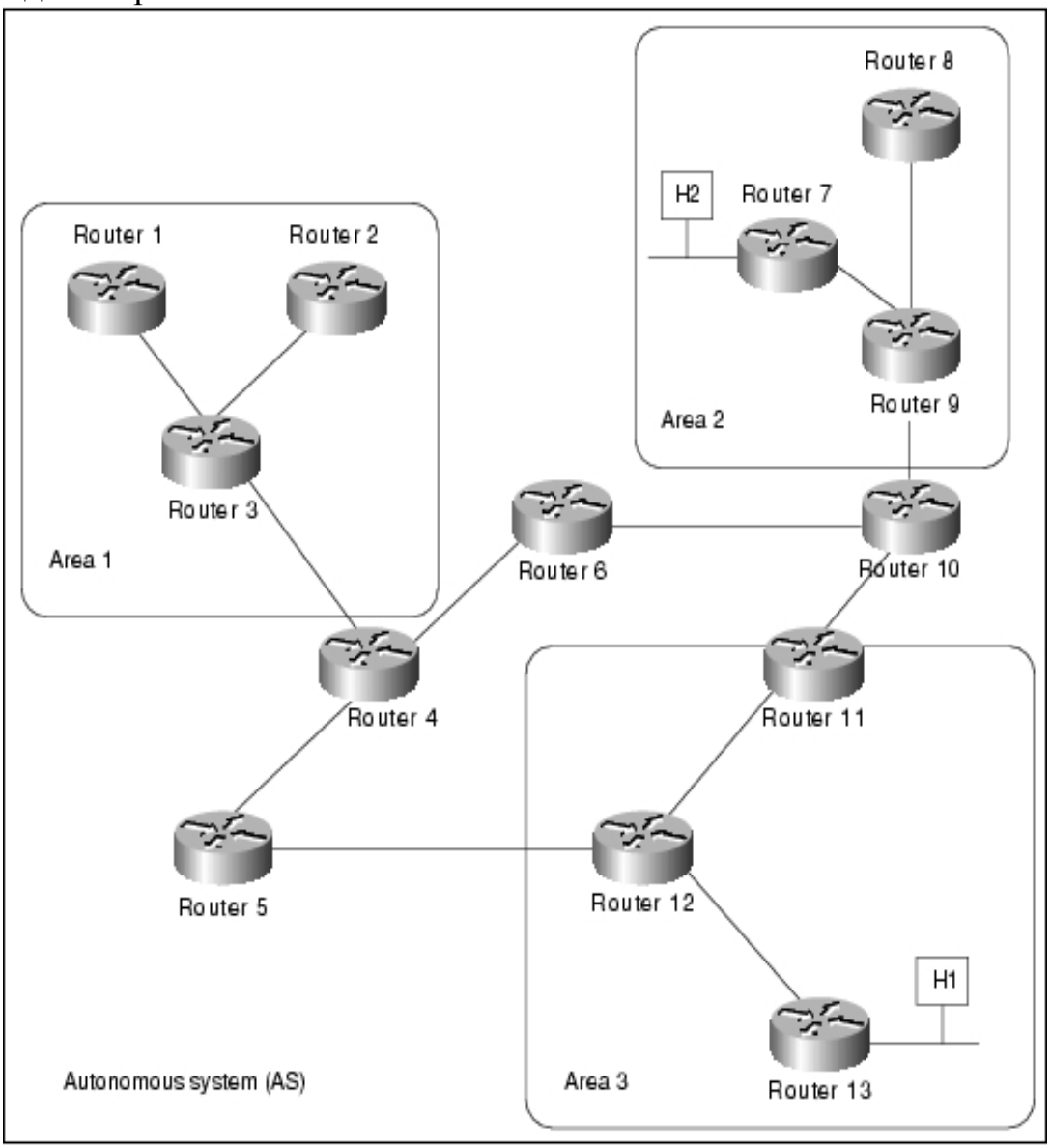

Рисунок 2.1 – Схема сети с несколькими областями

Область может быть определена таким образом, что стержневая часть не будет смежной с ней. В этом случае связность стержневой части должна быть восстановлена через виртуальные соединения. Виртуальные соединения формируются между любыми роутерами стержневой области, которые совместно используют какую-либо связь с любой из нестержневых областей, они функционируют так, как если бы они были непосредственными связями.

Граничные роутеры AS, использующие OSPF, узнают о внешних роутерах через протоколы внешних роутеров (EGPs), таких, как Exterior Gateway Protocol (EGP) или Border Gateway Protocol (BGP), или через информацию о конфигурации.

2.4 Процесс построения таблицы маршрутизации. Алгоритм Shortest Path First

1 Каждый маршрутизатор на всех интерфейсах изучает своих соседей и заносит их в таблицу «соседей» (Рисунок 2.2).

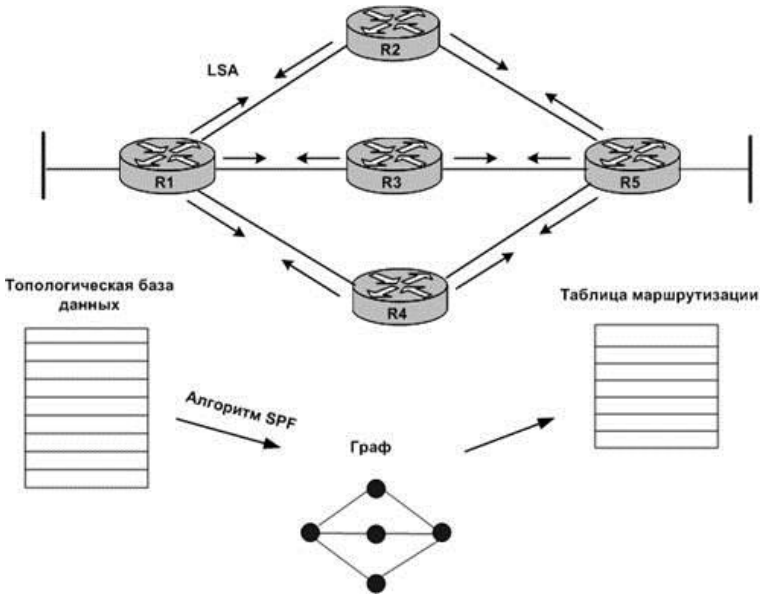

Рисунок 2.2 – Изучение своих соседей

2 Каждый маршрутизатор, используя LSA, строит топологическую базу данных состояния каналов (Рисунок 2.3), которая является картиной связи маршрутизаторов в одной области, обновляет ее и передает LSA всем соседним устройствам. Маршрутизаторы внутри одной области обладают общей информацией, у них одинаковые топологические базы данных.

Канал – это линия связи или интерфейс, соединяющий один маршрутизатор с другим или с сетью. Состояние канала – это описание интерфейса и его связей с соседними маршрутизаторами. Описание интерфейса может включать, например, IP-адрес интерфейса, маску, тип сети, к которой он подключен. Набор всех этих состояний каналов формирует базу данных состояния каналов.

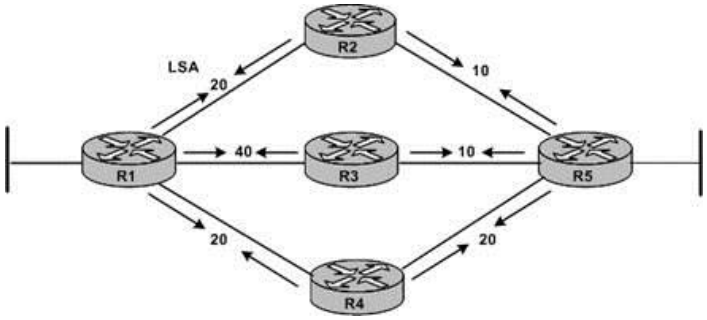

Рисунок 2.3 – Построение топологической таблицы

3 Как только маршрутизаторы OSPF соберут информацию о состоянии каналов, они начинают вычислять кратчайший путь к каждой сети (Рисунок 2.4). Каждый маршрутизатор считает себя корнем дерева и, используя базу данных состояний каналов, вычисляет наилучшие пути к сетям назначения, применяя алгоритм SPF (алгоритм Дейкстры) и выстраивая при этом SPF-дерево, основываясь на суммарной стоимости маршрута, который используется для достижения этих сетей.

Данный процесс может обнаруживать изменения в сетевой топологии, вызванные отказами оборудования и ростом сети.

Каждый маршрутизатор будет иметь свой собственный взгляд на топологию, несмотря на то, что все маршрутизаторы будут строить дерево кратчайших путей, используя одну и ту же базу данных состояния каналов.

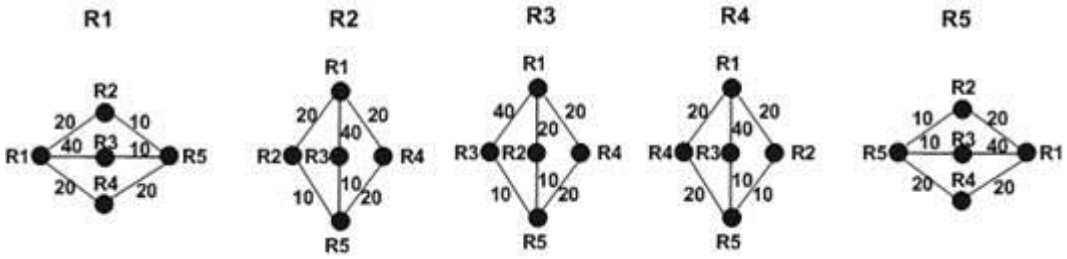

Рисунок 2.4 – Вычисление наикратчайшего пути

4 Затем из этого дерева к сетям назначения выбираются пути с наименьшей стоимостью и помещаются в таблицу маршрутизации (Рисунок 2.5). Стоимость или метрика интерфейса – это индикатор усилий, которые необходимы для отправки пакета через этот интерфейс. Стоимость интерфейса обратно пропорциональна полосе пропускания интерфейса, таким образом, большая полоса пропускания соответствует меньшей стоимости.

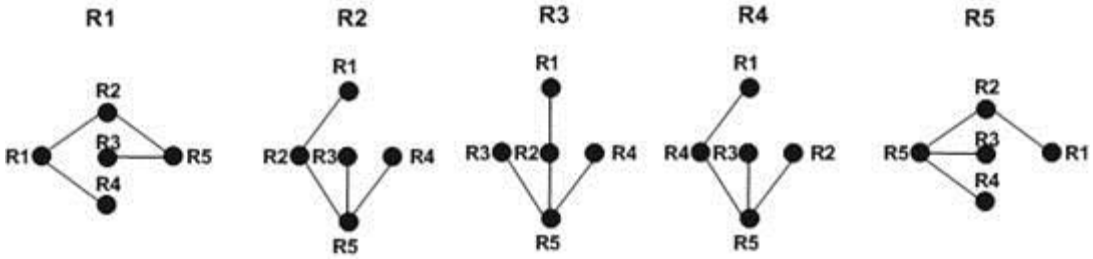

Рисунок 2.5 – Выбор пути с наименьшей стоимостью

5 После первоначального построения таблицы маршрутизации необходимо отслеживать изменения состояния сети и вносить коррективы в таблицу маршрутизации. Для контроля состояния связей и соседних маршрутизаторов они передают специальные короткие сообщения HELLO (Рисунок 2.6). Если состояние сети не меняется, то маршрутизаторы корректировкой своих таблиц маршрутизации не занимаются и не посылают

соседям объявления о связях. Сообщения HELLO отправляются через каждые 10 секунд, чтобы повысить скорость адаптации маршрутизаторов к изменениям, происходящим в сети. Небольшой объем этих сообщений делает возможной такое частое тестирование состояния соседей и связей с ними.

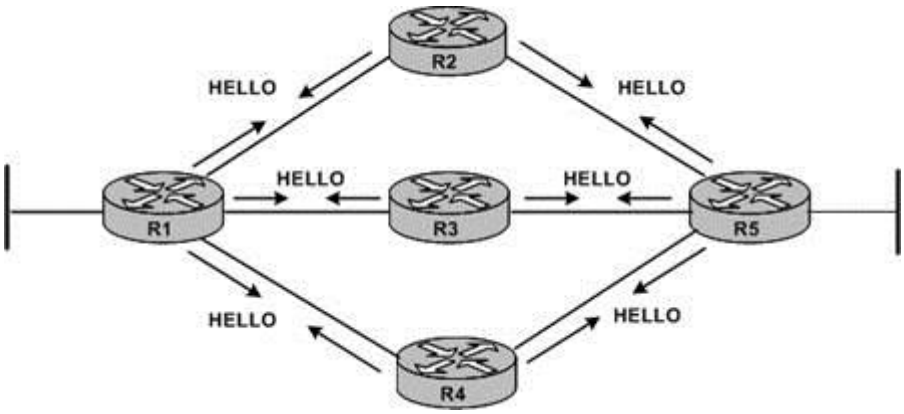

Рисунок 2.6 – Контроль состояния связей

Если же состояние связи изменилось, то начинается лавинная рассылка LSA по всей сети, касающаяся только данной связи, что, экономит пропускную способность сети. Получив новое объявление об изменении состояния связи, маршрутизатор пересчитывает дерево и заново ищет оптимальные маршруты (Рисунок 2.7). Одновременно маршрутизатор ретранслирует объявление каждому из своих ближайших соседей (кроме того, от которого он получил это объявление).

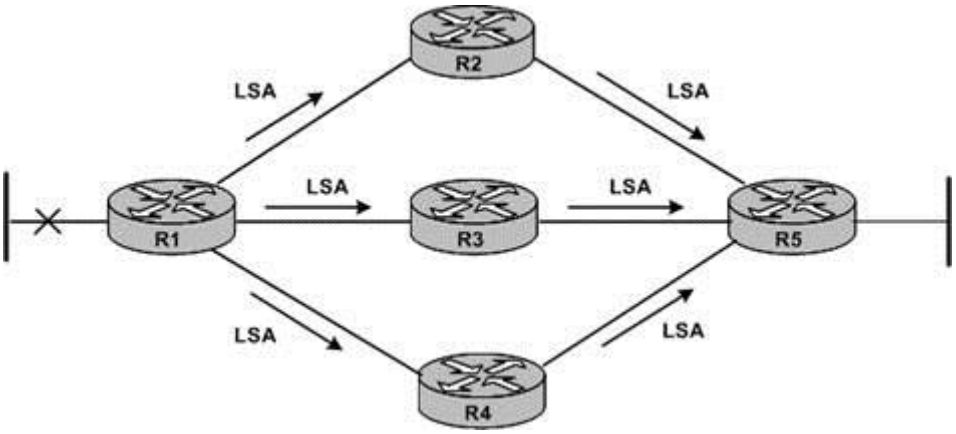

Рисунок 2.7 – Повторный поиск оптимального маршрута

В сетях с множественным доступом (сети, которые поддерживают больше двух маршрутизаторов на сегменте), например, сетях Ethernet, hello-протокол выбирает назначенный маршрутизатор (DR) и резервный назначенный маршрутизатор (BDR). В числе прочих задач, назначенный маршрутизатор отвечает за генерацию LSA-пакетов для всей сети с множественным доступом. Назначенные маршрутизаторы позволяют

уменьшить трафик при обновлениях маршрутной информации и управляют синхронизацией состояния каналов. DR и BDR выбираются на основании приоритетов OSPF и идентификатора маршрутизатора OSPF. В отсутствии множественного доступа, например, в сетях с последовательными соединениями типа точка-точка, DR или BDR не выбираются.

2.5 Достоинства и недостатки протокола OSPF

Открытый протокол выбора первого кратчайшего пути (Open Shortest Path First Protocol – OSPF) на сегодняшний день является наиболее универсальным и гибким в настройке протоколом динамической маршрутизации в корпоративных сетях. Протокол изначально был ориентирован на работу в больших сетях (до 65536 маршрутизаторов) со сложной топологией. Он основан на алгоритме состояния каналов связи и обладает высокой устойчивостью к изменениям топологии сети и быстрой сходимостью. При выборе маршрута используется метрика пропускной способности составной сети (т.е. передача данных по наиболее скоростным каналам связи). Протокол может поддерживать разные требования IP-пакетов на качество обслуживания (пропускная способность, задержка и надежность) посредством построения отдельной таблицы маршрутизации для каждого из этих показателей.

Протокол обладает и другими достоинствами, полезными в крупных современных сетях. К ним относятся возможность балансировки нагрузки между каналами с равными метриками и средства аутентификации как по нешифрованному паролю, так и по шифрованному (путем добавления к пакету дайджеста ключа и тела пакета по алгоритму MD5). Нумерация пакетов исключает их повторяемость и таким образом возможность повторной атаки. Открытость протокола определяет его поддержку практически всеми производителями сетевого оборудования, реализации в ПО под все популярные ОС (например, для Unix-подобных ОС – пакеты Zebra, Quagga и др.), а также непосредственную интеграцию в ряд ОС (например, Windows 2000 Server и выше, OpenBSD, Cisco IOS, Solaris 10 и т.д.).

К недостаткам прокола следует отнести высокую вычислительную сложность и, следовательно, высокие требования, предъявляемые к ресурсам маршрутизатора. Вычислительная сложность OSPF растет с увеличением размеров сети. Поэтому для увеличения масштабируемости протокола применяется разделение сети на логические области, соединенные магистральной областью. Внутренняя топологическая информация между областями не предается. Сокращению размеров таблиц маршрутизации и снижению служебного трафика при обновлении топологической информации служит возможность объединения нескольких адресов сетей в один при обнаружении у них общего префикса, и замена широковещательных рассылок мультикастинговыми. С целью экономии IP-адресов в соединениях типа «точка – точка» между маршрутизаторами назначать конечным точкам адреса не

обязательно. Платой за эти преимущества является сложность конфигурирования и необходимость тщательного предварительного планирования сети для ее оптимальной работы (разбивка на области, выделение магистрали, распределение функций между маршрутизаторами с учетом их вычислительной мощности: рядовые, выделенные в зоне, пограничные и т.д.).

2.6 Сравнительная характеристика основных протоколов динамической маршрутизации

Для определения эффективного протокола маршрутизации, который бы удовлетворял требованиям конкретной сети, необходимо провести сравнительный анализ наиболее известных протоколов динамической маршрутизации.

Протоколы маршрутизации делятся на два основных класса: протоколы внутренних шлюзов (Interior Gateway Protocols – IGP) и протоколы внешних шлюзов (Exterior Gateway Protocols – EGP). Протоколы класса IGP проектировались для обмена информацией о сетях и подсетях между внутренними маршрутизаторами одной автономной системы (Autonomous System – AS), т.е. между маршрутизаторами, находящимися под единым административным управлением, и использующими один протокол маршрутизации. такими сетями могут быть сети провайдеров услуг Internet, крупных правительственных и научно-исследовательских организаций, частных коммерческих концернов. Протоколы EGP проектировались для обмена маршрутной информацией между пограничными маршрутизаторами различных автономных систем. Доминирующим EGP-протоколом сегодня является протокол граничной маршрутизации версии 4 (Border Gateway Protocol version 4 – BGP-4). Это протокол используется для обмена маршрутной информацией между AS сети Internet.

По методу распространения маршрутной информации протоколы IGP делятся на дистанционно-векторные и состояния каналов связи. В методе вектора расстояний каждый маршрутизатор через равные промежутки времени посылает соседним маршрутизаторам обновления всей или части своей таблицы маршрутизации. По мере распространения маршрутной информации в сети каждый маршрутизатор может вычислить расстояния от него до всех сетей и подсетей в пределах внутрикорпоративной сети. Наиболее распространенными протоколами данного типа являются RIP (Routing Information Protocol) и IGRP (Interior Gateway Routing Protocol). В методе учета состояния каналов связи каждый маршрутизатор корпоративной сети посылает остальным маршрутизаторам информацию о своих непосредственных соединениях с сетями и маршрутизаторами. На основе полученной информации обо всех локальных соединениях в сети, каждый маршрутизатор способен построить ее полный топологический граф, а затем заполнить свою таблицу, используя сложный алгоритм выбора первого кратчайшего пути (Shortest Path First – SPF). Наиболее известными протоколами данного типа являются OSPF

(Open Shortest Path First) и IS-IS (Intermediate System to Intermediate System). Существуют также гибридные протоколы, сочетающие в себе преимущества обоих методов распространения маршрутной информации. Примером гибридного протокола является EIGRP (Enhanced Interior Gateway Routing Protocol).

Протоколы, основанные на методе вектора расстояния, требуют меньше вычислительных ресурсов маршрутизатора, чем протоколы с выбором по состоянию каналов связи с их сложными SPF-алгоритмами. С другой стороны, протоколы с выбором по состоянию каналов связи занимают меньшую часть полосы пропускания сети (кроме начального этапа изучения топологии сети) так, как они распространяют только информацию об изменениях, а не всю таблицу маршрутизации, что особенно важно для больших сетей.

Другие критерии сравнения протоколов динамической маршрутизации показаны ниже.

1) Скорость сходимости. Эта характеристика протокола определяет длительность временного интервала возможной нестабильной работы сети, в течении которого протокол выявляет недоступный маршрут, выбирает новый маршрут и распространяет новую информацию по сети. Быстрота реакции на изменения в сетевой топологии особенно важна при поддержке важных приложений, требующих высокой степени готовности сети. Протоколы, основанные на методе вектора расстояния, требуют большего времени для сходимости, чем протоколы с выбором по состоянию канала связи, так как информация о новом пути передается от одного маршрутизатора к другому косвенно без указания источника ее происхождения в процессе периодических рассылок.

2) Возможность учета в метрике (критерии) выбора наиболее рационального маршрута различных характеристик маршрута. Метрики могут рассчитываться на основе одной или нескольких характеристик пути. К наиболее употребительным характеристикам пути относятся:

- количество переходов (промежуточных маршрутизаторов в пути);
- пропускная способность каналов связи;
- задержка пакета в пути;
- надежность (частота возникновения ошибок каналах связи);
- нагрузка (загруженность маршрутизаторов и каналов связи);
- стоимость (произвольное значение, назначаемое администратором на основание как перечисленных выше, так и других соображений, например финансовых).

Метрики, вычисляемые на основе нескольких показателей, обеспечивают большую гибкость при выборе маршрута. Возможности протокола поддерживать одновременно несколько метрик позволяют удовлетворять требования QoS-трафика (Quality of Service) разных приложений.

3) Возможность балансировки нагрузки между несколькими маршрутами. Возможность хранения в таблицах маршрутизации нескольких маршрутов к одной сети (с равными или даже отличающимися метриками) дает возможность маршрутизатору снижать загрузку линий связи, путем попеременной отсылки пакетов по каждому из маршрутов. Следует обратить внимание на то, что балансировка нагрузки может вызвать проблемы в тех случаях, когда приложение использует дейтаграммные протоколы канального и транспортного уровней, которые не нумеруют и, следовательно, не восстанавливают порядок следования пакетов, как это делает, например, транспортный протокол с установлением соединения тСР.

4) Возможность объединения маршрутов на совпадающих участках. Наличие данной функции способствует снижению относительной сложности большой сети, сокращению количества записей в таблицах маршрутизаторов и ускорению поиска в них. Объединение маршрутов требует, чтобы протокол маршрутизации поддерживал маски подсетей переменной длины и был способен распространять информацию о сетевых масках вместе с информацией о сетевых маршрутах.

5) Максимальное количество маршрутизаторов в сети определяет возможности ее масштабирования. Это ограничение косвенно связано с другими характеристиками протокола маршрутизации, влияющими на его способность работать в большой сети (например, скоростью сходимости, долей полосы пропускания сети, требуемой для передачи служебных сообщений протокола).

6) Необходимость предварительной логической подготовки сети. Некоторые протоколы маршрутизации для достижения соответствующего уровня масштабирования (уменьшения потребления вычислительных ресурсов маршрутизаторов и полосы пропускания сети) подразумевают выделение в сети логических областей и связей между ними. Внедрение таких протоколов может потребовать серьезной инженерной проработки проекта сети (ее топологии и схемы адресации).

7) Обеспечение безопасности при обмене маршрутной информацией. Если сеть поддерживает обмен маршрутной информацией между подсетями, соединенными глобальными связями, то попадание такой информации в руки злоумышленников может представлять угрозу безопасности сети. В таких случаях поддержка протоколом маршрутизации методов аутентификации источника и шифрования маршрутной информации приобретает важное значение.

8) Доступность программного обеспечения (ПО) реализации протокола маршрутизации. Проколы могут быть отрытыми и поддерживаться различными производителями аппаратных маршрутизаторов и ПО для универсальных компьютеров, а могут быть закрытыми и реализоваться только определенными компаниями.

9) Перспективность – реализация в протоколе перспективных возможностей (например, протокола IP6, поддержка трафик инжиниринга).

Важной характеристикой протокола маршрутизации является скорость сходимости. Исходя из анализа самих алгоритмов и заявлений разработчиков компании Cisco Systems, можно сказать, что дистанционно-векторный протокол RIP уступает по этому параметру усовершенствованному протоколу IGRP. Еще большей скоростью сходимости обладает комбинированный протокол EIGRP, который приближается к наиболее скоростным протоколам OSPF и IS-IS, основанным на алгоритме учета состояния каналов связи.

В таблице 2.1 представлена сравнительная характеристика основных протоколов динамической маршрутизации.

т а б л и ц а 2.1 – Сравнительная таблица основных характеристик протоколов динамической маршрутизации

Критерии/ протоколы	RIP v.2	IS-IS	OSPF	EIGRP	BGP v.4
Безопасность	Открытый пароль или аутентификация по ключу MD5	–	Открытый пароль или аутентификация по ключу MD5	Аутентификация по ключу MD5	Разные методы аутентификации
тип алгоритма	Вектор расстояния	Состояние каналов связи	Состояние каналов связи	Комбинированный	Вектор расстояния
Балансировка нагрузки	–	Одинаковые метрики	Одинаковые метрики	Разные метрики	Разные метрики (полуавтоматически)
Объединение маршрутов	–	–	+	+	+
Маски подсетей переем длины	+	–	+	+	+
Максимальное количество машрутизаторов в сети	15	1024	65534	255	65534
Учет в метрике различных характеристик пути	Одна основная	Одна основная и три дополнительные	Одна основная и три дополнительные	Комбинированная	Произвольная
Поддержка QoS	–	+	+	+	–
Обновления маршрутной информации	Вся таблица	только изменения	только изменения	только изменения	только изменения
Необходимость логической подготовки сети	–	Выделение центральной области и связных областей	Выделение центральной области и связных областей	–	Разбитие сети на автономные системы и описание взаимодействия между ними

Окончание таблицы 2.1

Критерии/ протоколы	RIP v.2	IS-IS	OSPF	EIGRP	BGP v.4
Доступность реализации	Открытый	Открытый	Открытый	только на оборудова-нии Cisco Systems	Открытый
Поддержка IPv6	–	–	+	+	+

Сравнительная характеристика показывает, что наиболее совершенными внутренними протоколами динамической маршрутизации являются OSPF и EIGRP. Протокол IS-IS по сути является более ранней и менее функциональной версией протокола OSPF, поэтому в настоящее время редко используется в корпоративных сетях. Преимущества этих протоколов в полной мере проявляются в сложных больших сетях с сотнями и тысячами маршрутизаторов. Именно здесь необходима высокая скорость сходимости оптимальных маршрутов, гибкость при выборе путей (с учетом различных характеристик, составляющих маршруты каналов), поддержка требований QoS для разнородного трафика, экономия полосы пропускания каналов (за счет снижения служебного трафика), снижение размеров таблиц маршрутизации и скорости поиска в них информации. Эти требования оправдывают использование производительных аппаратных маршрутизаторов с большими объемами памяти и протоколов, требующих сложной настройки. Однако такие большие сети сегодня являются гетерогенными с точки зрения производителей сетевого оборудования, поэтому лидирующие позиции здесь занимает открытый протокол OSPF (EIGRP реализуется только на оборудовании Cisco Systems, и максимальное количество маршрутизаторов не более 255).

Для сетей среднего размера (десятки маршрутизаторов) при наличии соответствующих финансовых возможностей надежность и дополнительные технические преимущества оборудования фирмы Cisco Systems могут сыграть решающую роль в пользу построения однородной сети. тогда наибольший эффект даст использование протокола EIGRP. Поскольку лежащий в его основе алгоритм DUAL поддается гибкой настройке (комбинированная метрика, балансировка нагрузки путей с различными значениями метрики), это позволяет администратору сети обеспечивать ее максимальную производительность, поскольку хорошо известно, что перед сетью могут ставится самые разнообразные задачи, и только большие функциональные возможности и гибкость их использования помогут администратору решить любую поставленную задачу. Хотя вполне возможно, что и возможностей более простого в настройке протокола IGRP будет достаточно (например, если не предъявляются высокие требования ко времени сходимости оптимальных маршрутов, снижению уровня служебного трафика и его безопасности, не требуется поддержка масок подсетей переменной длины и функции агрегирования маршрутов).

Для гетерогенных сетей, особенно при наличии в них программных маршрутизаторов, лучшим выбором будет протокол OSPF. Поскольку при использовании EIGRP возникает проблема взаимодействия оборудования, то маршрутизаторам от других производителей остается использовать статические маршруты, либо иметь дело с комбинацией RIP и EIGRP, что представляется не очень осмысленным.

Если в соответствии с высокими требованиями к надежности, защищенности, производительности небольшой сети (до десятка маршрутизаторов) для нее будет выбрано оборудование Cisco, тогда, скорее всего, дополнительные возможности EIGRP, связанные с уменьшением времени сходимости и повышением масштабируемости, не понадобятся. И прокол IGRP решит задачи такой сети достаточно эффективно. Этот протокол наиболее понятен сетевым администраторам, уже знакомым с RIP, а также для достижения должной производительности требует от маршрутизаторов меньшего объема оперативной памяти и менее мощный процессор.

Здесь следует отметить существование большого количества организаций, для которых работа в сети не является непосредственным элементом их основной деятельности, а является скорее всего средством коммуникации.

Уровень трафика в таких сетях обычно не высок, поэтому возможности протокола, связанные с балансировкой нагрузки, снижением служебного трафика за счет иерархической организации и рассылки только обновлений скорее всего окажутся не востребованными. такие организации обычно не предъявляют высокие требования к сети, т.е. не требуют высокой скорости сходимости, поддержки QoS, учета в метрике характеристик разнородных каналов (как правило, все каналы типа Fast Ethernet), часто используют программные маршрутизаторы на не слишком производительных ПК, и не желают содержать высокооплачиваемые кадры квалифицированных администраторов. В этих случаях самый простой протокол RIPv2 будет вполне достаточным решением.

Протокол BGP разрабатывался как протокол взаимодействия между автономными системами Internet. Он имеет произвольную метрику и не высокую скорость сходимости. Его внедрение в корпоративную сеть в большинстве случаев не оправдается. Деление сети на автономные системы не дает существенного преимущества. Пограничные протоколы обычно нужны только в том случае, когда сеть организации связана с одной и той же внешней сетью (например Internet) несколькими каналами или, когда она работает как промежуточное звено между двумя или более сетями, при чем необходимо обеспечить резервные каналы связи (типичная ситуация для сервис-провайдера Internet).

таким образом, выбор конкретного протокола динамической маршрутизации зависит от размеров и требований, предъявляемых конкретной корпоративной сетью. Основываясь на данных таблицы, можно с уверенностью сказать, что на сегодняшний день наиболее совершенными внутренними

протоколами динамической маршрутизации являются OSPF и EIGRP. Их перспективность подтверждает и внедрение поддержки перспективного протокола IPv6.

2.7 Бесклассовая адресация

Бесклассовая адресация (англ. Classless Inter-Domain Routing, CIDR) – метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации. Использование этого метода позволяет экономно использовать ограниченный ресурс IP-адресов, поскольку возможно применение различных масок подсетей к различным подсетям.

Диапазоны адресов.

IP-адрес является массивом бит. Принцип IP-адресации – выделение множества (диапазона, блока, подсети) IP-адресов, в котором некоторые битовые разряды имеют фиксированные значения, а остальные разряды пробегают все возможные значения. Блок адресов задаётся указанием начального адреса и маски подсети. Бесклассовая адресация основывается на переменной длине маски подсети (англ. variable length subnet mask, VLSM), в то время, как в классовой (традиционной) адресации длина маски строго фиксирована 0, 1, 2 или 3 установленными октетами.

Пример записи идентификатора подсети 192.0.2.32/27 в бесклассовой нотации представлен в таблице 2.2.

т а б л и ц а 2.2 – Пример записи идентификатора подсети 192.0.2.32/27 в бесклассовой нотации

Октеты IP-адреса	192								0								2								32							
Биты IP-адреса	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0
Биты маски подсети	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0
Октеты маски подсети	255								255								255								224							

В данном примере видно, что в маске подсети 27 бит слева выставлены в единицу. В таком случае говорят о длине префикса подсети в 27 бит и указывают через косую черту (знак /) после базового адреса.

Пример записи IP-адреса 172.16.0.1/12 с применением бесклассовой адресации представлен в таблице 2.3.

т а б л и ц а 2.3 – Пример записи IP-адреса 172.16.0.1/12 с применением бесклассовой адресации

Октеты IP-адреса	172								16								0								1							
Биты IP-адреса	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Биты маски подсети	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Октеты маски подсети	255								240								0								0							

Множество всех адресов соответствует нулевой маске подсети и обозначается /0, а конкретный адрес IPv4 – маске подсети с длиной префикса в 32 бита, обозначаемой /32.

Для упрощения таблиц маршрутизации можно объединять блоки адресов, указывая один большой блок вместо ряда мелких. Например, 4 смежные сети класса C (4 × 255 адресов, маска 255.255.255.0 или /24) могут быть объединены, с точки зрения далёких от них маршрутизаторов, в одну сеть /22. И напротив, сети можно разбивать на более мелкие подсети, и так далее.

В Интернете используются только маски следующего вида: n единиц, дальше все нули (т.е. маска делится на два множества: набор единиц и набор нулей. Ноль не может встретиться среди единиц и единица не может встретиться среди нулей). Для таких (и только для таких) масок получающиеся множества IP-адресов будут смежными.

Возможные маски представлены в таблице 2.4.

т а б л и ц а 2.4 – Возможные маски

IPv4 CIDR				
IP/маска	До последнего IP в подсети	Маска	Количество адресов	Класс
a.b.c.d/32	+0.0.0.0	255.255.255.255	1	1/256 C
a.b.c.d/31	+0.0.0.1	255.255.255.254	2	1/128 C
a.b.c.d/30	+0.0.0.3	255.255.255.252	4	1/64 C
a.b.c.d/29	+0.0.0.7	255.255.255.248	8	1/32 C
a.b.c.d/28	+0.0.0.15	255.255.255.240	16	1/16 C
a.b.c.d/27	+0.0.0.31	255.255.255.224	32	1/8 C
a.b.c.d/26	+0.0.0.63	255.255.255.192	64	1/4 C
a.b.c.d/25	+0.0.0.127	255.255.255.128	128	1/2 C
a.b.c.0/24	+0.0.0.255	255.255.255.000	256	1 C
a.b.c.0/23	+0.0.1.255	255.255.254.000	512	2 C
a.b.c.0/22	+0.0.3.255	255.255.252.000	1024	4 C
a.b.c.0/21	+0.0.7.255	255.255.248.000	2048	8 C
a.b.c.0/20	+0.0.15.255	255.255.240.000	4096	16 C
a.b.c.0/19	+0.0.31.255	255.255.224.000	8192	32 C
a.b.c.0/18	+0.0.63.255	255.255.192.000	16 384	64 C
a.b.c.0/17	+0.0.127.255	255.255.128.000	32 768	128 C
a.b.0.0/16	+0.0.255.255	255.255.000.000	65 536	256 C = 1 B
a.b.0.0/15	+0.1.255.255	255.254.000.000	131 072	2 B

Окончание таблицы 2.4

IPv4 CIDR				
IP/маска	До последнего IP в подсети	Маска	Количество адресов	Класс
a.b.0.0/14	+0.3.255.255	255.252.000.000	262 144	4 B
a.b.0.0/13	+0.7.255.255	255.248.000.000	524 288	8 B
a.b.0.0/12	+0.15.255.255	255.240.000.000	1 048 576	16 B
a.b.0.0/11	+0.31.255.255	255.224.000.000	2 097 152	32 B
a.b.0.0/10	+0.63.255.255	255.192.000.000	4 194 304	64 B
a.b.0.0/9	+0.127.255.255	255.128.000.000	8 388 608	128 B
a.0.0.0/8	+0.255.255.255	255.000.000.000	16 777 216	256 B = 1 A
a.0.0.0/7	+1.255.255.255	254.000.000.000	33 554 432	2 A
a.0.0.0/6	+3.255.255.255	252.000.000.000	67 108 864	4 A
a.0.0.0/5	+7.255.255.255	248.000.000.000	134 217 728	8 A
a.0.0.0/4	+15.255.255.255	240.000.000.000	268 435 456	16 A
a.0.0.0/3	+31.255.255.255	224.000.000.000	536 870 912	32 A
a.0.0.0/2	+63.255.255.255	192.000.000.000	1 073 741 824	64 A
a.0.0.0/1	+127.255.255.255	128.000.000.000	2 147 483 648	128 A
0.0.0.0/0	+255.255.255.255	000.000.000.000	4 294 967 296	256 A

Количество адресов подсети не равно количеству возможных узлов. Нулевой адрес IP резервируется для идентификации подсети, последний – в качестве широковещательного адреса, таким образом в реально действующих сетях возможно количество узлов на два меньшее количества адресов.

2.8 Маски подсети переменной длины

Метод применения маски подсети переменной длины (англ. Variable Length Subnet Mask, VLSM) используется для получения адреса на основе класса и преобразования его в более масштабируемый и менее расточительный диапазон адресов. Недостатком адресов на основе классов является то, что они обычно предоставляют либо слишком большой, либо слишком маленький диапазон адресов для использования в большинстве ситуаций. Например, предположим, что организация имеет сеть со структурой, показанной на рисунке 2.8. После организации подсетей на основе адреса класса B с использованием 20-битовой маски (255.255.240.0) будет получено 14 подсетей и 4094 хостов в каждой подсети. Именно такие параметры необходимо создать в здании 1, поскольку в этом здании имеется 2500 хостов. Но в остальных местах потребность в размещении хостов значительно ниже и поэтому адреса используются неэффективно. Из всех прочих площадок ни на одной не используется свыше 500 IP-адресов, но все они имеют маску /20. Это означает, что данная организация не использует свыше 50 000 IP-адресов.

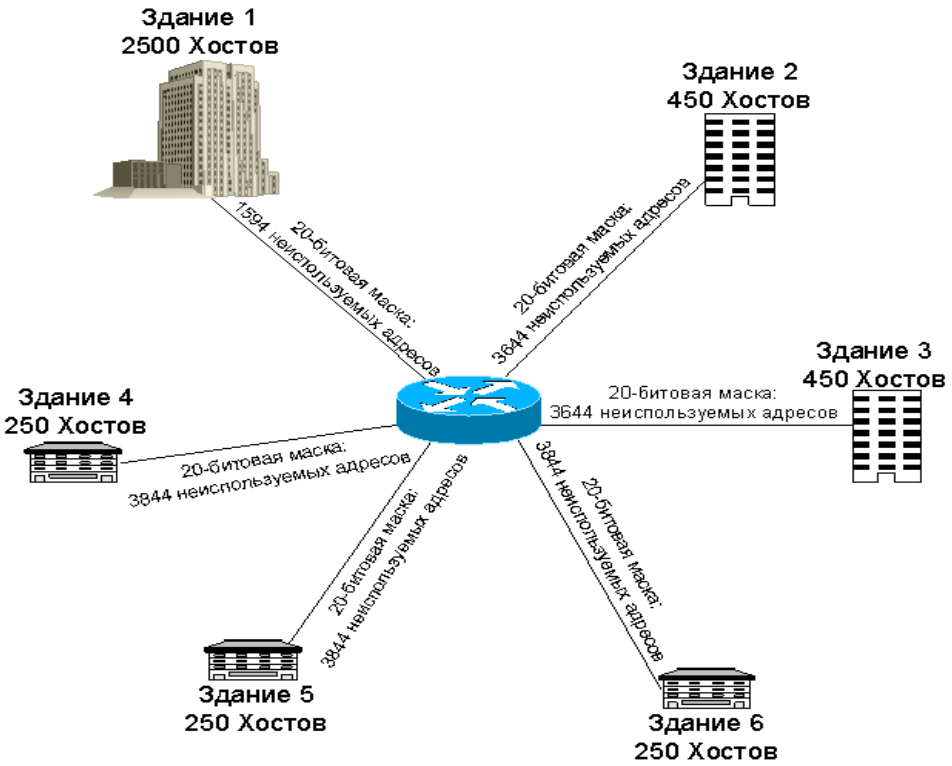

Рисунок 2.8 – Пример бесполезного расходования IP-адресов

Метод VLSM предусматривает разбивку на подсети адресного пространства, основанного на использовании классов, а затем разбивку подсетей на подсети до тех пор, пока не будет достигнуто требуемое количество хостов в каждой подсети.

При использовании метода VLSM вводится ряд новых правил распределения адресов, которые позволяют значительно уменьшить их непроизводительный расход. Во-первых, при использовании этого метода не требуется удалять подсети с номерами, состоящими из одних нулей или одних единиц. Эти подсети теперь разрешено использовать для размещения в них хостов. (Но удалять первый и последний IP-адреса из каждой подсети все равно необходимо.) Во-вторых, разрешено применять к разным частям сети разные маски. Это позволяет в случае необходимости разделять сеть на меньшие части как показано на рисунке 2.9. Единственное требование при этом состоит в том, чтобы диапазоны адресов в подсетях не перекрывали друг друга.

Единственный способ проверки того, что перекрытие адресов отсутствует, состоит в выполнении вычислений с помощью двоичной арифметики.

Предположим, что организации был выделен сетевой адрес 172.16.0.0/16 (IP-адрес класса B), и администратор планирует принять во внимание маски подсети переменной длины.

Во-первых, определим, какое количество хостов требуется для самых больших подсетей. В рассматриваемом случае для самой крупной подсети требуется, по меньшей мере, 2500 хостов, поэтому начнем с нее.

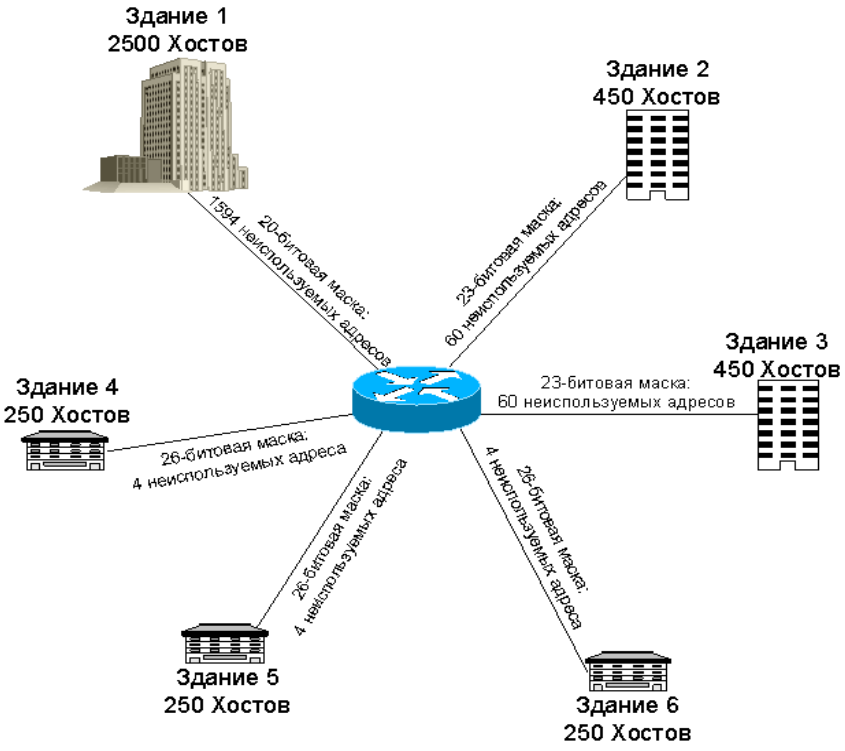

Рисунок 2.9 – Уменьшение непроизводительного расхода IP-адресов с использованием метода VLSM

Для поддержки этих хостов нужна 20-битовая маска, с помощью которой будет получено 16 подсетей (напомним, что при использовании метода VLSM не требуется отбрасывать первую и последнюю подсети) с 4094 хостами каждая (поскольку все еще необходимо отбрасывать первый и последний IP-адреса в каждой подсети).Одна из этих подсетей используются для здания 1 (172.16.0.0/20). Для всех остальных хостов требуется только менее 2000 IP-адресов, поэтому для поддержки этих подсетей необходимо взять одну из крупных 16 подсетей с количеством хостов 4094.

Возьмем одну подсеть (172.16.16.0) и разделим ее на восемь подсетей, используя для каждой из них 23-битовую маску. Добавим эти три бита к маске подсети (в результате чего они составят часть с обозначением адреса подподсети другой подсети), что позволяет создать восемь подсетей с 510 хостами каждая. Рассматривая двоичные значения адресов, приведенные на рисунке 2.7, можно заметить, что ни один из этих диапазонов не перекрывается.

Две из этих подсетей выделим зданию 2 (172.16.16.0/23) и 3 (172.16.18.0/23). Наконец, отметим, что для всех последних трех подсетей требуется меньше 254 хостов. В этом случае необходимо использовать 24-битовую маску, поэтому возьмем две из 23-битовых подсетей и разобьем их на меньшие подсети с применением этой маски. В результате будет получено 4 подсети, каждая из которых состоит из 254 хостов. три из этих диапазонов адресов будут использоваться для создания трех подсетей. В результате общий итог составляет 1 подсеть с 254 хостами, 4 подсети с 510 хостами и 14 подсетей с 4094 хостами, которые остаются в резерве для распределения в будущем.

На рисунке 2.10 показан пример вычислений диапазона IP-адресов с использованием метода VLSM.

Логическая структура созданного таким образом распределения адресов показана на рисунке 2.11.

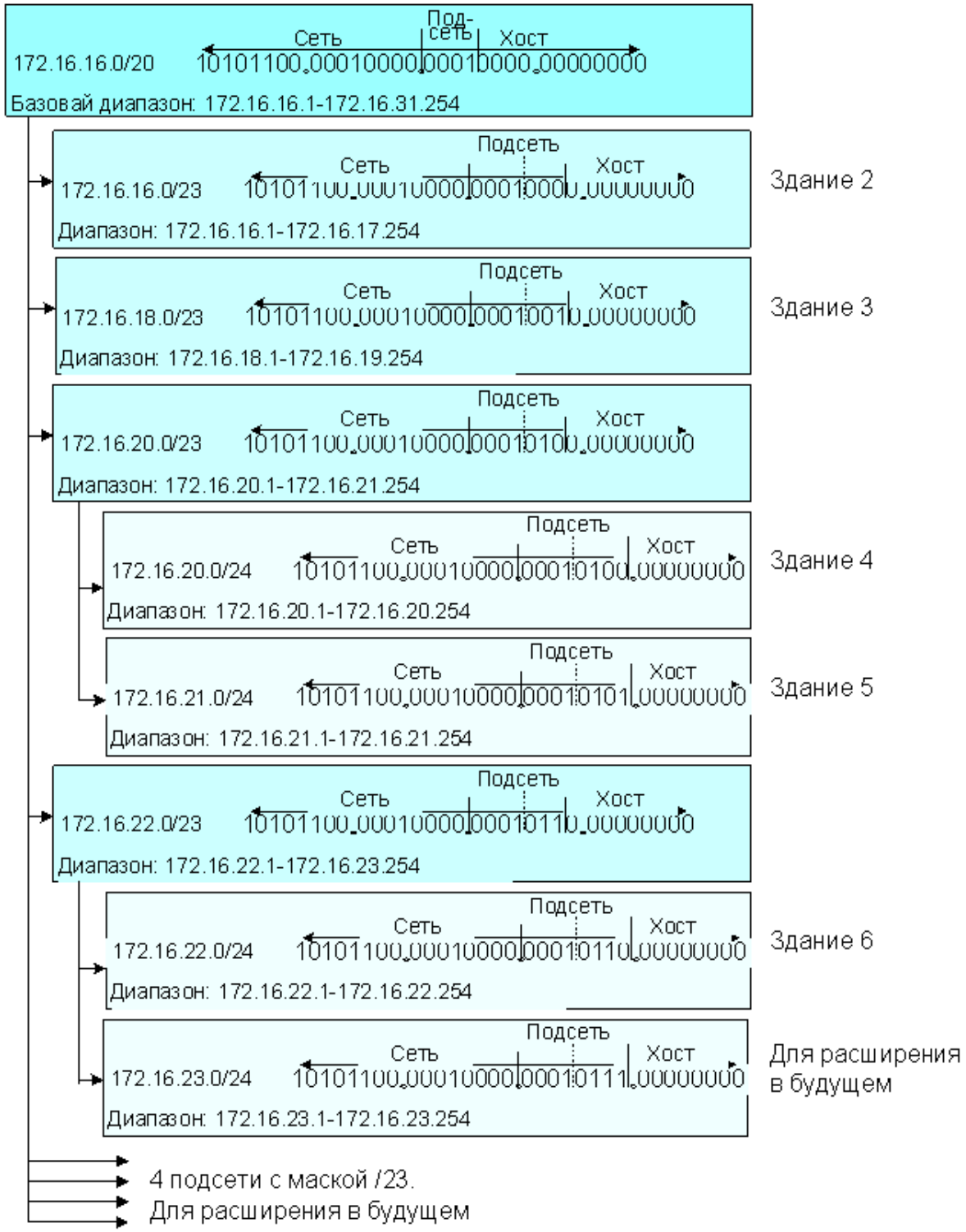

Рисунок 2.10 – Пример вычислений диапазона IP-адресов с использованием метода VLSM

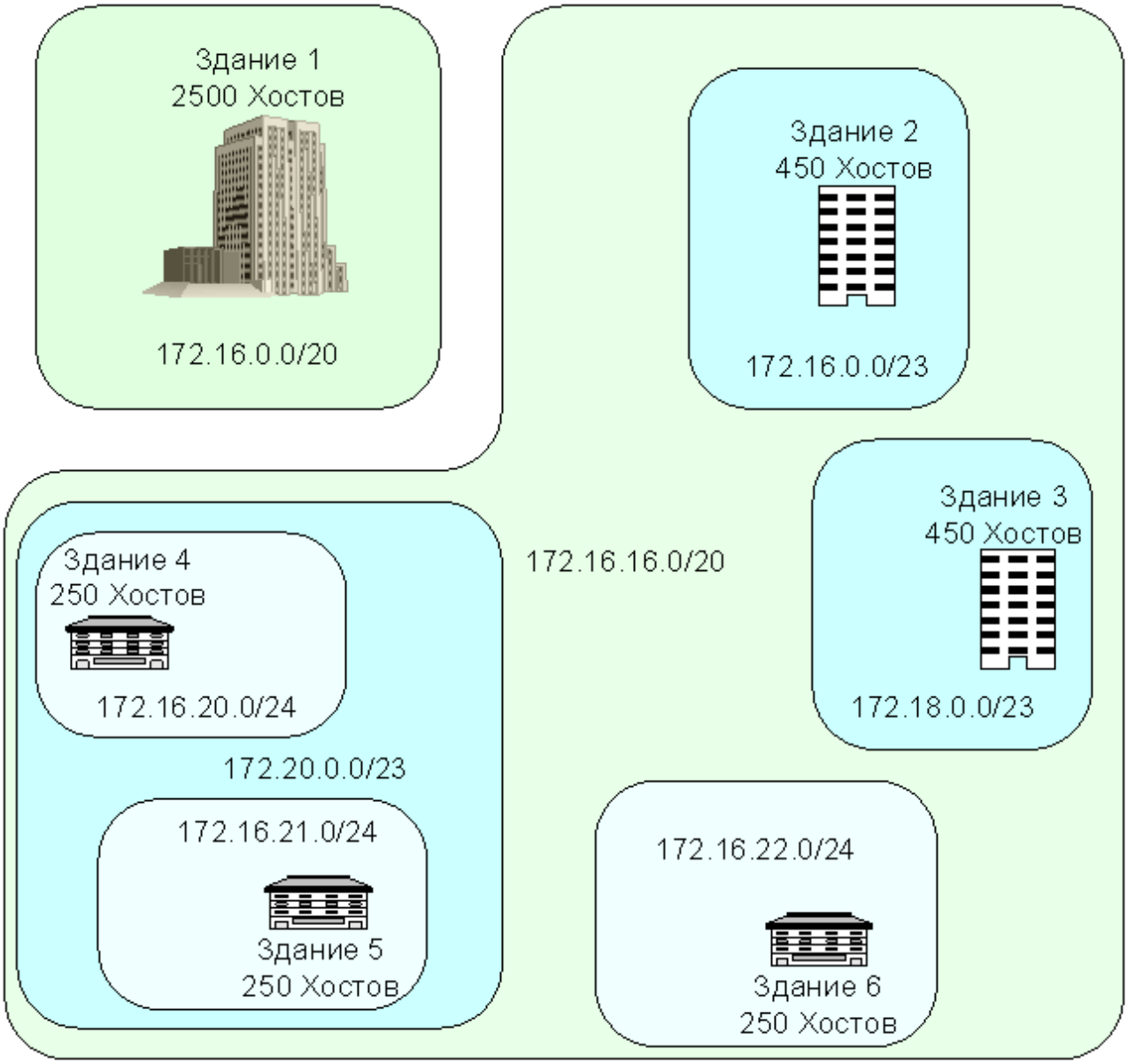

Рисунок 2.11 – Логическая структура созданного распределения адресов

Этот метод нельзя назвать слишком сложным, но для его применения требуется полное понимание того, какие манипуляции с двоичными числами лежат в основе адресации TCP/IP.

3 Разработка корпоративной сети с использованием протокола динамической маршрутизации Open Shortest Path First для Центральной городской клинической больницы № 12 и Городской поликлиники № 10

3.1 Место реализации проекта

Центральная городская клиническая больница № 12 (Рисунок 3.1) – одна из самых крупных клиник в городе, все пострадавшие от тяжелых травм и сильнейших ожогов поступают в данную больницу. Уже много лет основными направлениями деятельности является травматология, ортопедия, а также оказание высокоспециализированной помощи ожоговым больным различной степени тяжести. В больнице имеются следующие отделения: отдел приема и регистрации пациентов, процедурный кабинет, кардиологическое отделение, физиотерапевтическое отделение, хирургическое отделение, терапевтическое отделение, гинекологическое отделение, неврологическое отделение, отделение травматологии и ортопедии, педиатрическое отделение, рентгенологическое отделение, отделение ультразвуковой диагностики, отделение функциональной диагностики, клинико-диагностическая лаборатория.

Рисунок 3.1 – Центральная клиническая больница № 12

На сегодняшний день государственное коммунальное предприятие (ГКП) «Центральная городская клиническая больница» на праве хозяйственного

ведения (ЦГКБ) – это многопрофильное лечебно-профилактическое учреждение, оказывающее высококвалифицированную, специализированную, экстренную, плановую, лечебно-диагностическую и консультативную медицинскую помощь жителям города Алматы, дальнего и ближнего зарубежья. В больнице функционирует более 40 структурных отделений и подразделений, в том числе стационар на 502 койки (335 бюджетных, 155 хозрасчетных коек и 12 коек отделения реанимации и анестезиологии), консультативно-диагностическое отделение с дневным стационаром на12 коек.

Клиника оснащена самой современной медицинской техникой, что позволяет выполнять уникальные малотравматичные урологические, гинекологические, травматологические и хирургические операции.

Многолетний опыт работы сотрудников, накопленный почти за 40 лет существования больницы и умелое решение организационных вопросов со стороны администрации больницы, позволяет постоянно, равномерно, без срывов оказывать пациентам необходимый объем медицинской помощи.

Городская поликлиника № 10 (Рисунок 3.2). В 1984 году распоряжением исполнительного Алма-Атинского городского совета народных депутатов была открыта поликлиника № 10 Алатауского района г.Алма-Аты. ГККП «Городская поликлиника № 10» Управления здравоохранения г. Алматы находится на страже здоровья 50 000 жителей микрорайонов Аксай 1, 2, 4 и Жетысу 1, 2 и 3. Причем 15000 из них дети. В данной поликлинике функционируют такие отделения, как: отдел приема и регистрации пациентов, кабинет рентгенографии, кабинет радиоактивного изображения, отделение тестирования сердечной функции, стоматологическое отделение, отделение ЭКГ, терапевтическое отделение, отделение офтальмологии, хирургическое отделение и т.д.

Рисунок 3.2 – Городская поликлиника № 10

Поликлиника тесно сотрудничает с ЮНИСЕФ ,«PSI», «СПИД Фондом Восток-Запад», НПО «Равный-Равному», Государственным фондом развития молодежной политики при акимате г.Алматы, Национальным центром здорового образа жизни, Алматинский городским центром формирования здорового образа жизни, Центром досуга Ауэзовского и Алатауского районов.

В 2011 г. в поликлинике открыт центр амбулаторной хирургии, получен государственный заказ на 600 медицинских услуг.

Центр укрепления здоровья поликлиники неоднократно награждался грамотами: за активное участие во внедрении программ формирования здорового образа жизни (2003 г.), за большую и активную работу по профилактике заболеваний и формированию здорового образа жизни (2004 г.), ценными подарками.

Разработка корпоративной сети между Центральной городской клинической больницей № 12 и Городской поликлиникой № 10 актуальна в связи с положительным социальным эффектом. Социальным эффектом внедрения корпоративной сети между данными медучреждениями является:

- улучшение качества работы врачей за счет создания электронной регистратуры больных, базы электронных карт пациентов, где будут храниться их истории болезней с момента первого обращения в медучреждения;
- уменьшение количества очередей в регистратуру и на прием к специалистам;
- любой специалист сможет за небольшой промежуток времени отследить всю динамику развития болезней пациента, оценить эффективность врачебного вмешательства на разных этапах лечения;
- при необходимости врачи могут немедленно отыскать необходимую справочную информацию по новейшим методикам лечения того или иного заболевания, а также характеристики новых и давно забытых лекарственных препаратов в базе данных этой корпоративной сети;
- улучшится взаимодействие между специалистами амбулаторного звена медучреждения и стационара, что позволит исключить большое количество врачебных ошибок при лечении того или иного пациента;
- улучшение качества управления врачебным персоналом и специалистами среднего звена, например, при получении того или иного приказа информация мгновенно будет доводиться до специалистов.

3.2 Разработка структурной схемы организации сети

В Городской поликлинике № 10 4 этажа. На каждом этаже установлен коммутатор, к которому подключены компьютеры из разных отделений.

На первом этаже к первому коммутатору подключены компьютеры из таких отделений, как отдел приема и регистрации пациентов, технический

отдел, медицинский архив, а также аптека. Помимо этого к коммутатору подключена точка доступа, которая находится в фойе первого этажа. К этой точке доступа будут подключаться ноутбуки, планшеты и смартфоны по беспроводной сети. топология сети первого этажа Городской поликлиники № 10 представлена на рисунке 3.3.

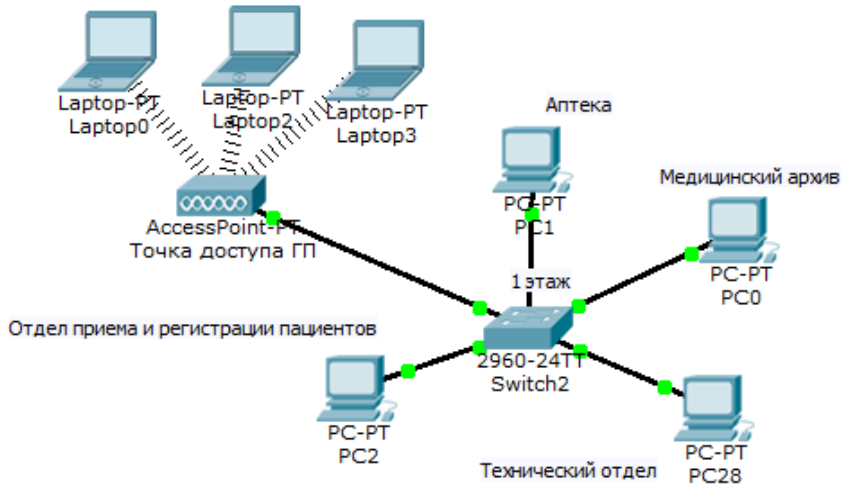

Рисунок 3.3 – топология сети первого этажа

На втором этаже ко второму коммутатору подключены компьютеры из таких отделений, как кабинет рентгенографии, кабинет радиоактивного изображения, судебное бюро медицинских расходов. топология сети второго этажа Городской поликлиники № 10 представлена на рисунке 3.4.

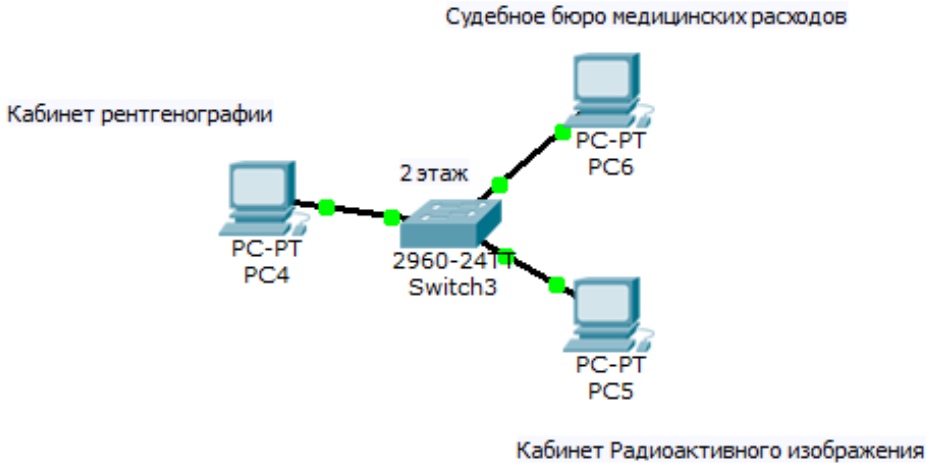

Рисунок 3.4 – топология сети второго этажа ГП № 10

На третьем этаже к третьему коммутатору подключены компьютеры из таких отделений, как Отделение тестирования сердечной функции, отделение

ЭКГ, стоматологическое отделение. топология сети третьего этажа представлена на рисунке 3.5.

Рисунок 3.5 – топология сети третьего этажа ГП № 10

На четвертом этаже соответственно к четвертому коммутатору подключены компьютеры из таких отделений, как Отделение тестирования сердечной функции, отделение ЭКГ, стоматологическое отделение. топология сети третьего этажа представлена на рисунке 3.6.

Рисунок 3.6 – топология сети четвертого этажа ГП № 10

Коммутаторы всех четырех этажей перекрестно подключены к еще двум коммутаторам для более отказоустойчивой сети. Затем эти два коммутатора подключаются к коммутатору третьего уровня, к которому, в свою очередь, подключен DHCP-сервер. DHCP-сервер служит нам для того, чтобы автоматически присваивать конечным устройствам IP-адреса. Для этого нам достаточно сконфигурировать сервер, ввести диапазоны адресов и настроить несколько дополнительных параметров.

Затем коммутатор третьего уровня подключается к маршрутизатору принадлежащему этой городской поликлинике. Маршрутизатор Городской

поликлиники № 10, в свою очередь, присоединен к двум модемам, каждый из которых отвечает за сеть разных провайдеров. Данная топология представлена на рисунке 3.7.

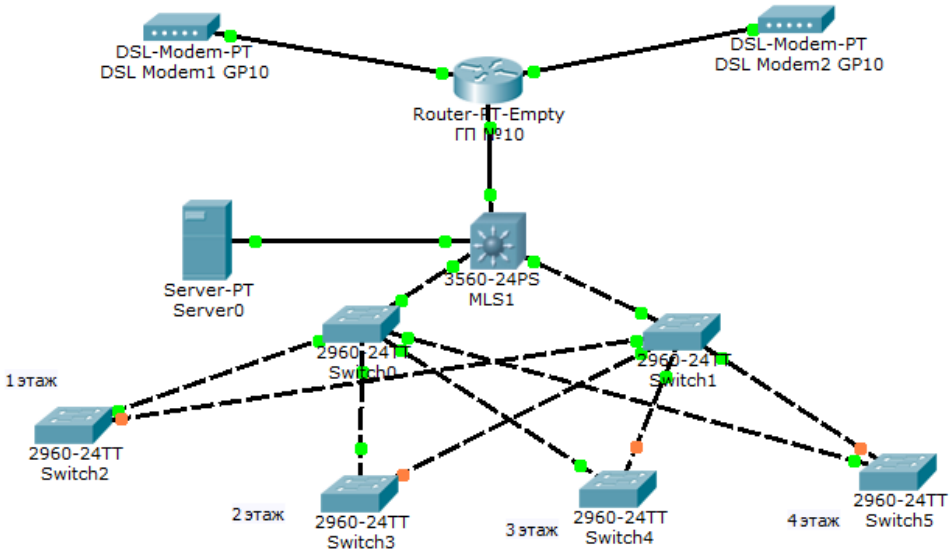

Рисунок 3.7 – Обобщенная топология Городской поликлиники № 10

Полная архитектура локальной сети Городской поликлиники № 10 представлена на рисунке 3.8.

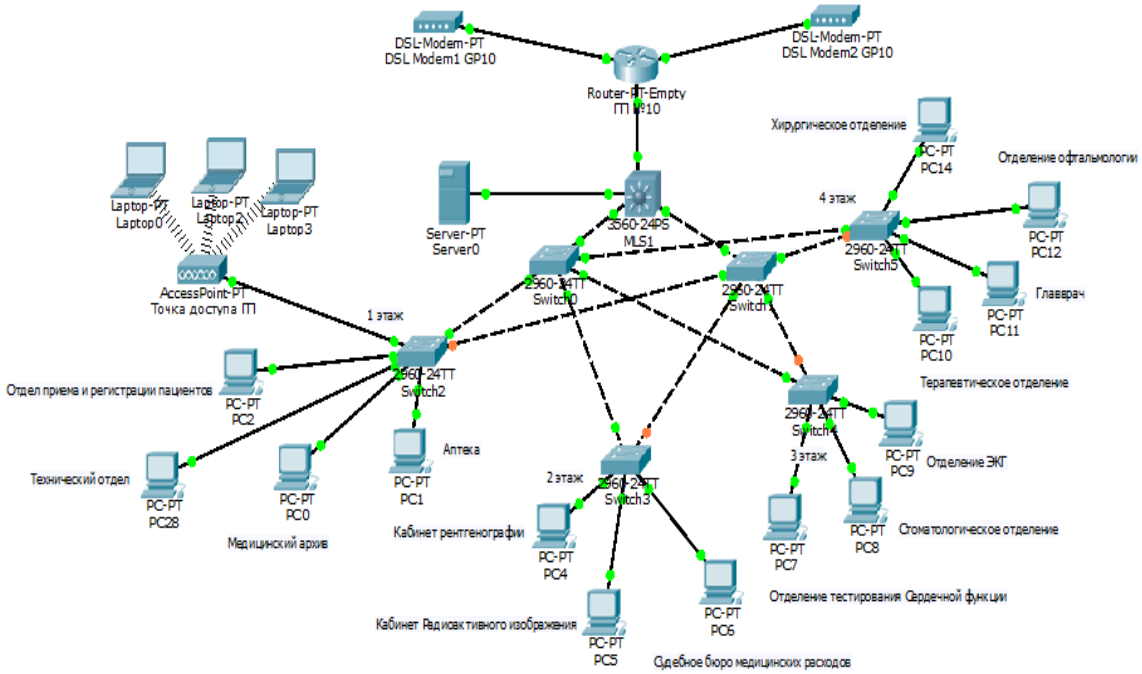

Рисунок 3.8 – Архитектура локальной сети в Городской поликлинике № 10

На рисунке 3.9 показана полная архитектура локальной сети Центральной городской клинической больницы № 12.

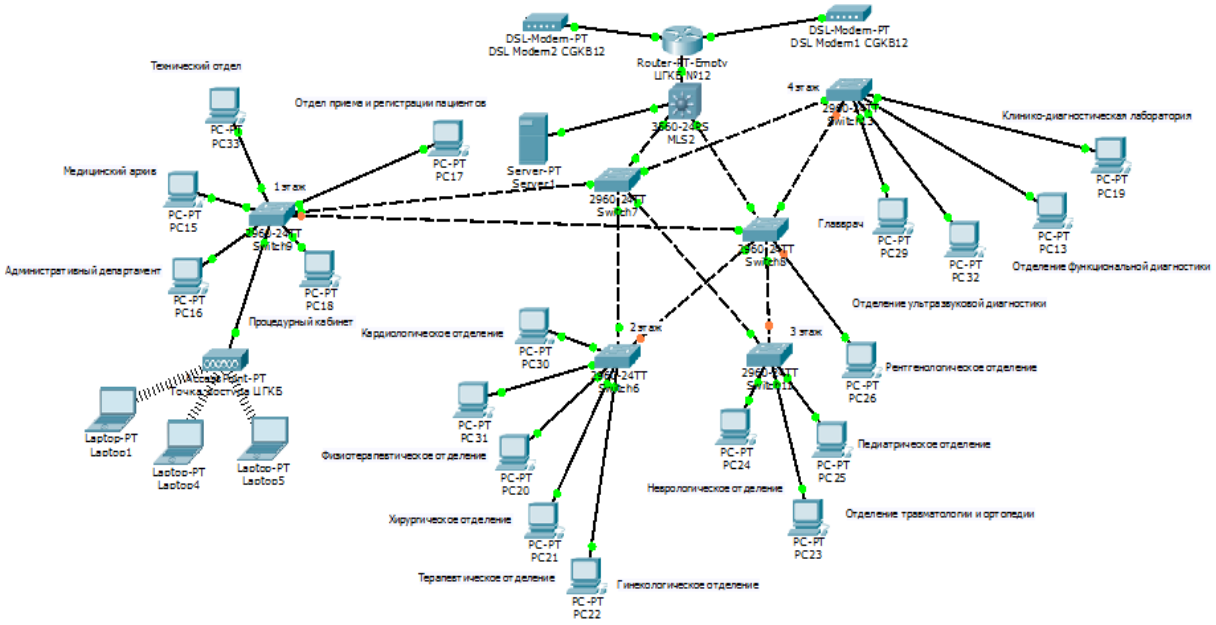

Рисунок 3.9 – Архитектура локальной сети в Центральной городской клинической больнице № 12

Архитектура локальной сети в ЦГКБ № 12 практически идентична архитектуре локальной сети в Городской поликлинике № 10. Различие лишь в том, что компьютеров, подключенных к коммутаторам на каждом этаже, больше и различие в отделениях.

Маршрутизатор Центральной городской клинической больницы № 12 также подключен к двум модемам к разным сетям провайдеров.

При проектировании сети для организации взаимодействия между Центральной городской клинической больницей № 12 и Городской поликлиникой № 10 был выбран способ предполагающий аренду каналов связи у провайдера в уже имеющихся сетях. так как из за такого относительно большого территориального расстояния данных медучреждений, прокладка собственных линий связи не целесообразна, в следствии очень высоких затрат на оборудование и монтаж сети.

Для обеспечения отказоустойчивости оба медучреждения подключены к двум сетям провайдеров, что позволяет организовать, независимые друг от друга, основной и резервный каналы связи. Задача выбора провайдера сегодня превращается в проблему нахождения надежного поставщика услуги, который владея достаточными техническими средствами, обеспечит комфортную и безопасную корпоративную сеть.

На рисунке 3.10 показана общая схема корпоративной сети между Центральной городской клинической больницей № 12 и Городской поликлиникой № 10 через сети двух провайдеров.

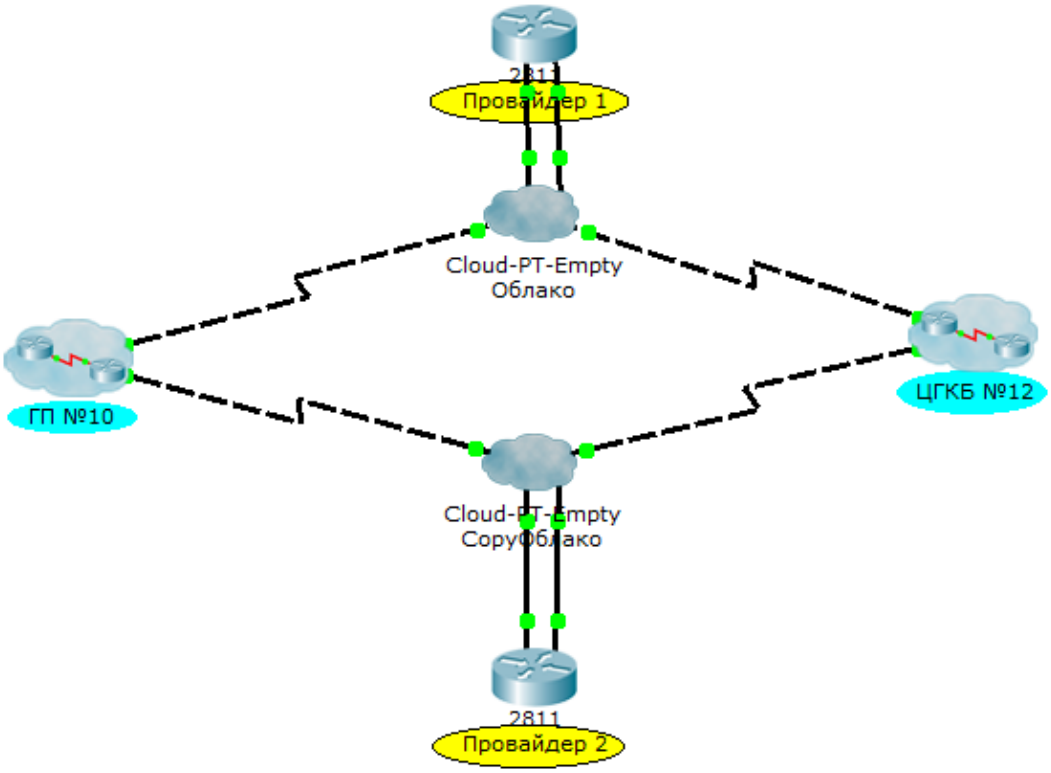

Рисунок 3.10 – Общая схема корпоративной сети между ЦГКБ № 12 и ГП № 10

Внутри облака ГП № 10 представлена топология локальной сети Городской поликлиники № 10, а в облаке ЦГКБ № 12 представлена топология локальной сети Центральной городской клинической больницы № 12 соответственно.

3.2 Планирование IP-адресаций

Планирование IP-адресаций указано в таблицах 3.1 – 3.7.

т а б л и ц а 3.1 – Планирование IP-адресации по медучреждениям

Медучреждение	IP-адрес
Центральная городская клиническая больница № 12	192.168.1.0
Городская поликлиника № 10	192.168.3.0

т а б л и ц а 3.2 – Планирование IP-адресации в ЦГКБ № 12 по этажам

Этаж	IP-адрес/Маска	Шлюз
1	192.168.1.2 – 32/27	192.168.1.1
2	192.168.1.34 – 64/27	192.168.1.33
3	192.168.1.66 – 96/27	192.168.1.65
4	192.168.1.98 – 128/27	192.168.1.97

т а б л и ц а 3.3 – Планирование IP-адресации в ГП № 10 по этажам

Этаж	IP-адрес/Маска	Шлюз
1	192.168.3.2 – 32/27	192.168.3.1
2	192.168.3.34 – 64/27	192.168.3.33
3	192.168.3.66 – 96/27	192.168.3.65
4	192.168.3.98 – 128/27	192.168.3.97

т а б л и ц а 3.4 – Планирование IP-адресации серверов в ЦГКБ № 12 и ГП № 10

Сервер	IP-адрес/Маска	Шлюз
ЦГКБ № 12	172.16.0.1/30	172.16.0.2
ГП № 10	172.16.1.1/30	172.16.1.2

т а б л и ц а 3.5 – Планирование IP-адресации маршрутизатора и коммутатора третьего уровня ЦГКБ № 12

Оборудование	IP-адрес/Маска
Маршрутизатор	192.168.0.1/24 1.1.1.2/24 1.2.1.2/24
Коммутатор третьего уровня	192.168.0.2/24

т а б л и ц а 3.6 – Планирование IP-адресации маршрутизатора и коммутатора третьего уровня ГП № 10

Оборудование	IP-адрес/Маска
Маршрутизатор	192.168.2.1/24 1.1.2.2/24 1.2.2.2/24
Коммутатор третьего уровня	192.168.2.2/24

т а б л и ц а 3.7 – Планирование IP-адресации провайдеров

Провайдер	IP-адрес/Маска
1	1.1.1.1/24 1.1.2.1/24
2	1.2.2.1/24

3.3 Настройка протокола Open Shortest Path First

Реализация протокола Open Shortest Path First выполняется на маршрутизаторах обоих сервис-провайдеров, на маршрутизаторе и коммутаторе третьего уровня Городской поликлиники № 10, а также на маршрутизаторе и коммутаторе третьего уровня Центральной городской клинической больницы № 12 соответственно.

Для начала настроим маршрутизаторы наших сервис-провайдеров. Перейдем на роутер первого сервис-провайдера и в режиме глобальной конфигурации введем следующую команду

```
Provider1(config)#router ospf 1
```

Единица – это номер процесса на роутере и на роутерах одной области может отличаться.

Далее получаем меню режима глобальной конфигурации на настройку протокола OSPF

```
Provider1(config-router)#
```

теперь здесь необходимо объявить все непосредственно подключенные сети. Если объявить не подключенную сеть (произвольную) то она не войдет в рассылаемую информацию о сетях этим маршрутизатором

```
Provider1(config-router)#network 1.1.1.0 0.0.0.255 area 0
```

0.0.0.255 – это wildcard mask (перевернутая маска), area 0 это номер области, и на всех маршрутизаторах одной области он должен быть одинаковый, как показано ниже

```
Provider1(config-router)#network 1.1.1.0 0.0.0.255 area 0
Provider1(config-router)#network 1.1.2.0 0.0.0.255 area 0
```

И по этой аналогии на всех маршрутизаторах данной схемы необходимо объявить все непосредственно подключенные сети.

тип сети, в которой работает протокол можно посмотреть командой

```
Provider1#show ip ospf interface
```

После слова interface нужно прописать название интерфейса, например

```
Provider1#show ip ospf interface fa0/0
```

Вывод команды

```
FastEthernet0/0 is up, line protocol is up
 Internet address is 1.1.1.1/24, Area 0
 Process ID 1, Router ID 1.1.2.1, Network Type BROADCAST,
Cost: 1
 Transmit Delay is 1 sec, State BDR, Priority 1
 Designated Router (ID) 192.168.0.1, Interface address 1.1.1.2
  Backup Designated Router (ID) 1.1.2.1, Interface address
1.1.1.1
```

```
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
 Hello due in 00:00:06
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1, Adjacent neighbor count is 1
 Adjacent with neighbor 192.168.0.1 (Designated Router)
 Suppress hello for 0 neighbor(s)
```

Далее представлены конфигурации маршрутизаторов и коммутаторов третьего уровня.

Конфигурация маршрутизатора Provider1

```
hostname Provider1
!
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/0
 ip address 1.1.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 1.1.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 1.1.2.0 0.0.0.255 area 0
 network 1.1.1.0 0.0.0.255 area 0
!
router rip
!
ip classless
!
line con 0
!
line aux 0
!
line vty 0 4
```

```
 login
!
end
```

Конфигурация маршрутизатора Provider2

```
hostname Provider2
!
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/0
 ip address 1.2.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 1.2.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 1.2.1.0 0.0.0.255 area 0
 network 1.2.2.0 0.0.0.255 area 0
!
ip classless
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
end
```

Конфигурация маршрутизатора Router-GP10

```
hostname Router-GP10
!
!
!
enable secret 5 $1$mERr$H/ic/D4UjHzrMLIm1rWfl/
```

```
!
aaa new-model
!
username admin privilege 15 secret 5
$1$mERr$bWEtFYbccSVsPV8Bnflfd0
!
ip ssh version 2
ip ssh authentication-retries 2
ip domain-name Router-GP10
!
interface Serial0/0
 no ip address
 shutdown
!
interface Serial1/0
 no ip address
 shutdown
!
interface FastEthernet2/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet3/0
 ip address 1.1.2.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet4/0
 ip address 1.2.2.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet5/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 1.1.2.0 0.0.0.255 area 0
 network 1.2.2.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
!
ip classless
!
no cdp run
!
line con 0
!
line aux 0
```

```
!
line vty 0 4
 logging synchronous
 transport input ssh
 privilege level 15
!
end
```

Конфигурация коммутатора третьего уровня MLS1

```
hostname MLS1
!
enable secret 5 $1$mERr$H/ic/D4UjHzrMLIm1rWfl/
!
aaa new-model
!
ip routing
!
username admin privilege 15 secret 5
$1$mERr$bWEtFYbccSVsPV8Bnflfd0
!
ip ssh version 2
ip ssh authentication-retries 2
ip domain-name MLS1
!
spanning-tree mode pvst
spanning-tree vlan 1-1000 priority 0
!
interface FastEthernet0/1
 no switchport
 ip address 192.168.2.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/2
 no switchport
 ip address 172.16.1.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
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
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 192.168.3.1 255.255.255.224
 ip helper-address 172.16.1.1
!
interface Vlan20
 ip address 192.168.3.33 255.255.255.224
 ip helper-address 172.16.1.1
!
interface Vlan30
 ip address 192.168.3.65 255.255.255.224
 ip helper-address 172.16.1.1
!
```

```
interface Vlan40
 ip address 192.168.3.97 255.255.255.224
 ip helper-address 172.16.1.1
!
router ospf 1
 log-adjacency-changes
 network 192.168.2.0 0.0.0.255 area 0
 network 172.16.1.0 0.0.0.255 area 0
 network 192.168.3.0 0.0.0.255 area 0
!
router rip
!
ip classless
!
line con 0
!
line aux 0
!
line vty 0 4
 logging synchronous
 transport input ssh
 privilege level 15
!
end
```

Конфигурация маршрутизатора Router-Cgkb12

```
hostname Router-CGKB12
!
!
!
!
enable secret 5 $1$mERr$H/ic/D4UjHzrMLIm1rWfl/
!
aaa new-model
!
username admin privilege 15 secret 5
$1$mERr$bWEtFYbccSVsPV8Bnflfd0
!
ip ssh version 2
ip ssh authentication-retries 2
ip domain-name Router-CGKB12
!
interface Serial0/0
 no ip address
 shutdown
!
interface Serial1/0
 no ip address
 shutdown
!
```

```
interface FastEthernet2/0
 ip address 192.168.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet3/0
 ip address 1.1.1.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet4/0
 ip address 1.2.1.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet5/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 192.168.0.0 0.0.0.255 area 0
 network 1.1.1.0 0.0.0.255 area 0
 network 1.2.1.0 0.0.0.255 area 0
!
ip classless
!
line con 0
!
line aux 0
!
line vty 0 4
 logging synchronous
 transport input ssh
 privilege level 15
!
end
```

Конфигурация коммутатора третьего уровня MLS2

```
hostname MLS2
!
!
!
!
enable secret 5 $1$mERr$H/ic/D4UjHzrMLIm1rWfl/
!
aaa new-model
!
```

```
ip routing
!
username admin privilege 15 secret 5
$1$mERr$bWEtFYbccSVsPV8Bnflfd0
!
ip ssh version 2
ip ssh authentication-retries 2
ip domain-name MLS2
!
spanning-tree mode pvst
spanning-tree vlan 1-1000 priority 0
!
interface FastEthernet0/1
 no switchport
 ip address 192.168.0.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/2
 no switchport
 ip address 172.16.0.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
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
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 192.168.1.1 255.255.255.224
 ip helper-address 172.16.0.1
!
interface Vlan20
 ip address 192.168.1.33 255.255.255.224
 ip helper-address 172.16.0.1
!
interface Vlan30
 ip address 192.168.1.65 255.255.255.224
 ip helper-address 172.16.0.1
!
interface Vlan40
 ip address 192.168.1.97 255.255.255.224
 ip helper-address 172.16.0.1
!
router ospf 1
 log-adjacency-changes
 network 192.168.0.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.0.255 area 0
!
ip classless
!
line con 0
!
line aux 0
!
```

```
line vty 0 4
 logging synchronous
 transport input ssh
 privilege level 15
!
!
end
```

3.4 Настройка протокола доступа SSH на маршрутизаторах и коммутаторах третьего уровня

SSH (Secure SHell) – сетевой протокол прикладного уровня, используется для удалённого управление различным оборудованием и операционными системами, а также для туннелирование TCP-соединений для просмотра, редактирования и передачи файлов, шифрует весь передаваемый трафик.

По умолчанию для управления оборудованием cisco используется протокол telnet, который является незащищённым и передаёт данные и пароли в открытом виде. Для обеспечения безопастности сетевого оборудования Cisco рекомендуется отключать протокол telnet, а для управления использовать протокол ssh. Далее будет показана настройка ssh доступа на маршрутизаторе Центральной городской клинической больницы № 12.

Заходим в привилегированный режим

```
router>enable
```

Настраиваем параметры необходимые для генерации ключа используемого ssh. Для начала входим в режим конфигурирования

```
cisco#configure terminal
```

Задаем домен

```
cisco(config)#ip domain name Router-CGKB12
```

Задаем имя роутера

```
cisco(config)#hostname Router-CGKB12
```

Генерируем rsa ключ для ssh

```
Router-CGKB12(config)#crypto key generate rsa
```

Задаем версию протокола ssh

```
Router-CGKB12(config)#ip ssh version 2
```

Задаем количество попыток подключения по ssh

```
Router-CGKB12(config)#ip ssh authentication-retries 2
```

Задаем хранение пароли в зашифрованном виде

```
Router-CGKB12(config)#service password-encryption
```

Включаем протокол aaa

```
Router-CGKB12(config)#aaa new-model
```

Создаем пользователя admin с паролем adm123 и максимальными уровнем привелегий 15

```
Router-CGKB12(config)#username admin 15 secret adm123
```

Задаем пароль qwerty для привилегированного режима

```
Router-CGKB12(config)#enable secret qwerty
```

Входим в режим конфигурирования терминальный линий

```
Router-CGKB12(config)#line vty 0 4
```

Разрешаем доступ только по ssh

```
Router-CGKB12(config-line)#transport input ssh
```

По умолчанию журнальные сообщения могут выводиться в независимости от того набирает пользователь какие либо команды или нет, прерывая исполнение текущих команд. Включая logging synchronous маршрутизатор начинает дожидаться завершения текущей команды и вывода ее отчета

```
Router-CGKB12(config-line)#logging synchronous
```

Позволяем входить сразу в привилегированный режим

```
Router-CGKB12(config-line)#privilege level 15
```

Выходим из режима конфигурирования

```
Router-CGKB12(config-line)#end
```

Сохраняемся

```
Router-CGKB12(config-line)#copy running-config startup-config
```

Далее аналогично настраиваем SSH доступ на остальных маршрутизаторах и коммутаторах третьего уровня.

3.5 Описание и характеристики выбранного оборудования

3.5.1 Коммутатор Cisco Catalyst 2960-24TT

Коммутаторы Cisco Catalyst 2960 – серия новых интеллектуальных коммутаторов Ethernet с фиксированной конфигурацией. Они обеспечивают потребность в передаче данных со скоростью 100 Мбит/сек и 1 Гбит/сек, позволяют использовать LAN сервисы, например, для сетей передачи данных, построенных в филиалах корпораций. Семейство Catalyst 2960 позволяет обеспечить высокую безопасность данных за счет встроенного NAC, поддержки QoS и высокого уровня устойчивости системы. Коммутатор Cisco Catalyst 2960-24TT изображен на рисунке 3.11. технические характеристики данного коммутатора приведены в таблице 3.8.

Рисунок 3.11 – Коммутатор Cisco Catalyst 2960-24TT

Серия коммутаторов Cisco Catalyst 2960 предлагает:

- высокий уровень безопасности, усовершенствованные списки контроля доступа (ACL);
- встроенные порты двойного назначения, функционирующие как для меди, так и оптоволокна. Каждый такой порт имеет встроенный порт 10/100/1000 Ethernet и порт SFP Gigabit Ethernet порт. При этом одновременно активным может быть только один из портов;
- организация контроля сети и оптимизация ширины канала с использованием QoS, дифференцированного ограничения скорости и ACL;
- для обеспечения безопасности сети коммутаторы используют широкий спектр методов аутентификации пользователя, технологии шифрации данных и

организации разграничения доступа к ресурсам на основании идентификатора пользователя, порта и MAC адресов;

- коммутаторы просты в управлении и конфигурировании;
- доступна функция авто конфигурации посредством Smart портов для некоторых специализированных приложений.

т а б л и ц а 3.8 – технические характеристики Cisco Catalyst 2960-24TT

тип коммутатора	Управляемый (Layer 2)
технология доступа	Ethernet
Количество LAN портов	24 шт
тип LAN портов	10/100/1000 Base-TX (1000 мбит/с)
Количество uplink-портов	2 шт
тип uplink-портов	10/100/1000 Base-TX (1000 мбит/с)
Внутренняя пропускная способность	16 ГБит/с
Производительность маршрутизации	3.6 mpps
Размер таблицы MAC-адресов	8000
Поддержка IPv6	Есть
Поддержка Auto-MDI/MDI-X	Есть
Поддержка IEEE 802.1d (Spanning Tree)	Есть
Поддержка IEEE 802.1p (Priority tags)	Есть
Поддержка IEEE 802.1q (VLAN)	Есть
Максимальное количество VLANs	255
Поддержка IEEE 802.1s (Multiple Spanning Tree)	Есть
Поддержка IEEE 802.3x (Flow control)	Есть
Поддержка PoE	Есть
Консольный порт	Есть
Объем оперативной памяти	64 МБ
Объем Flash памяти	32 МБ
Web-интерфейс	Есть
Telnet	Есть
DHCP-сервер	Есть
Поддержка IGMP (Multicast)	Есть
Поддержка SNMP	Есть
Рабочая температура	от -5°C до 45°C
температура хранения	от -25°C до 70°C

Окончание таблицы 3.8

тип коммутатора	Управляемый (Layer 2)
Влажность при эксплуатации	от 20% до 85% (без конденсации)
Влажность при хранении	от 10% до 90% (без конденсации)
Напряжение	220 В
ток	1.3 А
Потребляемая мощность	28 Вт
Поддержка операционных систем	MacOS, UNIX or Linux, Windows 98/NT/2000/XP/Vista/7/8
Возможность установки в стойку	Да
Габариты	445 x 44 x 236 мм
Вес нетто	3.6 кг
Вес брутто	4.8 кг

Сравнение конфигураций и аппаратных характеристик коммутаторов приведены в таблицах 3.9, 3.10.

т а б л и ц а 3.9 – Сравнение конфигурации коммутаторов серии Cisco Catalyst 2960

Наименование	Описание
Cisco Catalyst 2960-24TT	• 24 порта Ethernet 10/100, 2 порта с фиксированной конфигурацией – Ethernet 10/100/1000; • крепится в стойку 1RU, многоуровневый коммутатор; • интеллектуальные сервисы начального корпоративного уровня прединсталлированное ПО LAN BAse
Cisco Catalyst 2960-48TT	• 48 портов Ethernet 10/100, 2 порта с фиксированной конфигурацией – Ethernet 10/100/1000; • крепится в стойку 1RU, многоуровневый коммутатор; • интеллектуальные сервисы начального корпоративного уровня прединсталлированное ПО LAN BAse
Cisco Catalyst 2960-24TC	• 24 порта Ethernet 10/100, 2 порта двойного назначения; • крепится в стойку 1RU, многоуровневый коммутатор; • интеллектуальные сервисы начального корпоративного уровня прединсталлированное ПО LAN BAse
Cisco Catalyst 2960-48TC	• 48 портов Ethernet 10/100, 2 порта двойного назначения; • крепится в стойку 1RU, многоуровневый коммутатор; • интеллектуальные сервисы начального корпоративного уровня прединсталлированное ПО LAN BAse
Cisco Catalyst 2960G-24TC	• 24 порта Ethernet 10/100/1000, 4 из которых двойного назначения; • крепится в стойку 1RU; • интеллектуальные сервисы начального корпоративного уровня прединсталлированное ПО LAN BAse

т а б л и ц а 3.10 – Сравнение аппаратных характеристик коммутаторов серии Cisco Catalyst 2960

Аппаратные характеристики	WS-C2960-24TC-L	WS-C2960-24TT-L	WS-C2960-48TC-L	WS-C2960-48TT-L	WS-C2960G-24TC-L
Пропускная полоса (Gbps)	8.8	8.8	13.6	13.6	32
Максимальное кол-во коммутаторов в стеке	0	0	0	0	0
Кол-во пакетов в секунду (Mpps)	6.6	6.6	10.1	10.1	35.7
Число поддерживаемых MAC адресов	8000	8000	8000	8000	8000
Число поддерживаемых маршрутов	0	0	0	0	0
Встроенная память (DRAM)	64	64	64	64	64
Плотность портов Gigabit, GBIC/SFP	2	0	2	0	4
Порты 10/100/1000	2*	2	2	2*	24
Порты 10/100	24	24	48	48	0
Порты 100BASE-FX	0	0	0	0	0
Максимальное энергопотребление, Ватт	30	30	45	45	75
Порты PoE	0	0	0	0	0
Поддержка AC/DC	только AC	только AC	только AC	только AC	только AC
Размеры (ВхШхГ), см	4,4x44,5x23,6	4,4x44,5x23,6	4,4x44,5x23,6	4,4x44,5x23,6	4,4x44,5x32,8
Вес, кг	3,6	3,6	3,6	3,6	4,5

3.5.2 Коммутатор Cisco WS-C3560-24PS

Cisco Catalyst 3560 серия – это линейка коммутаторов промышленного класса с фиксированной конфигурацией, поддерживающая стандарт IEEE 802.3af и предварительный стандарт Cisco Power over Ethernet (PoE) в конфигурациях Fast Ethernet и Gigabit Ethernet. Cisco Catalyst 3560 является идеальным коммутатором уровня доступа для малого промышленного сетевого доступа или филиалов офисов, объединяя конфигурации 10/100/1000 и PoE для максимальной производительности и защиты инвестиций, одновременно

позволяя начать развертывание новых приложений, таких как IP-телефония, беспроводной доступ, видеонаблюдение, системы управления строительством, и удаленные видеостойки. Покупатели могут развернуть такие интеллектуальные службы, как улучшенное качество обслуживания (QoS), ограничение скорости, настраиваемые списки доступа (ACL), управление многоадресной передачей, и высокопроизводительная IP-маршрутизация и одновременное упрощение традиционной коммутации. Cisco Network Assistant является централизованным управляющим приложением, упрощающим задачи администрирования для коммутаторов Cisco, маршрутизаторов, и беспроводных точек доступа. Cisco Network Assistant обеспечивает мастера настройки, которые упрощают объединение нескольких сетей и интеллектуальных сетевых служб. Коммутатор Cisco WS-C3560-24PS изображен на рисунке 3.12. Характеристики коммутатора приведены в таблице 3.11.

Рисунок 3.12 – Коммутатор Cisco WS-C3560-24PS

т а б л и ц а 3.11 – технические характеристики Cisco WS-C3560-24PS

Характеристики	
Размеры (ширина x глубина x высота), см:	44.5 x 30 x 4.4 1RU
Вес, кг:	5.1
Параметры питания:	• потребляемая мощность: 485 Вт; • AC: 100 - 240 В (автоопределение), 5.5 - 2.8 А, 50 - 60 Гц; • DC (Cisco RPS 2300): + 12 В - 7.5 А; • PoE: 370 Вт
Индикаторы статуса:	• на каждом порте: целостность соединения, отключение, активность, скорость, полный дуплекс, функционирование PoE, ошибка PoE, отключение PoE; • состояние системы: система, RPS, состояние соединения, дуплекс, скорость, PoE
Оперативная память:	128 МБ
Флеш-память:	16 МБ
Медные интерфейсы:	• 24 x RJ-45 10/100 Fast Ethernet; • поддержка PoE на всех 24 портах
Оптические интерфейсы:	2 x SFP Gigabit Ethernet
Другие интерфейсы:	1 x консольный порт

3.5.3 Маршрутизатор D-Link DFL-800

Устройства серии DFL-800 (Рисунок 3.13, 3.14) представляют собой законченное решение в области безопасности, включающее встроенную поддержку межсетевого экрана, балансировки нагрузки, функций отказоустойчивости, механизма Zone-Defense, фильтрации содержимого, аутентификации пользователей, блокировки «мгновенных» сообщений и приложений P2P, защиты от атак «отказ в обслуживании» DoS и виртуальных локальных сетей VPN. Эти устройства соответствуют требованиям предприятий к безопасности и удаленному доступу, обеспечивая высокопроизводительное решение по разумной цене. В межсетевых экранах гармонично объединены расширенные функции, предоставляющие администраторам сетей решение безопасности «все в одном» business-класса. Характеристики D-Link DFL-800 показаны в таблице 3.12.

Рисунок 3.13 – D-Link DFL-800

Рисунок 3.14 – D-Link DFL-800 (вид изнутри)

т а б л и ц а 3.12 – технические характеристики D-Link DFL-800

Характеристики	
Производитель	D-Link
Модель	DFL-800
тип оборудования	Межсетевой экран, маршрутизатор, коммутатор
Количество одновременных IPSec VPN соединений	До 300 туннелей
Firewall	Detect/Drop Intruding Packets, аутентификация пользователей на основе политик, встроенная база данных о пользователях (500 записей), RADIUS-клиент, поддержка нескольких виртуальных серверов, Intrusion Detection System (IDS)
Индикаторы	Power, System; для портов WAN, LAN и DMZ: Link/Activity
Защищенные VPN-протоколы	IPSec, PPTP, L2TP
Наличие консольного порта	Есть
Соответствие стандартам	802.1Q VLAN
VLAN	Есть
DMZ	Поддерживается. Есть 1 порт DMZ 10/100 Мбит/сек.
NAT	Поддерживается
DHCP-сервер	Есть
Управление	SNMP, веб-интерфейс, интерфейс командной строки
Порты Fast Ethernet	7 портов 10/100 Мбит/сек
Порты WAN	2 порта WAN 10/100 Мбит/сек
Безопасность	политики контроля полосы пропускания, блокировка по URL/ключевому слову, политики доступа
Блок питания	Внешний, 5В, 4А; входит в комплект поставки
Потребление энергии	20 ватт – максимальное
Размеры (ширина х высота х глубина)	27.9 х 4.4 х 21.4 см
Вес	1.27 кг
Рабочая температура	0 ~ 60°C

3.5.4 Сервер Asus TS100-E6-PI4 Xeon X3430

Сервер Asus TS100-E6-PI4 Xeon X3430 изображен на рисунке 3.15. технические характеристики данного сервера приведены в таблице 3.13.

Рисунок 3.15 – Сервер Asus TS100-E6-PI4 Xeon X3430

т а б л и ц а 3.13 – технические характеристики Xeon X3430

Характеристики	
Название продукта	Xeon X3430/ RAM 8 GB/ 4*HDD 500 Gb/
Модель	TS100-E6/PI4
Серверная платформа	Barebone server Asus TS100-E6-PI4, S1156 Xeon, i3420, 4 DDR3 ECC, 2xGLAN, VGA, DVD, 4 SATA, Tower

Окончание таблицы 3.13

Характеристики	
Цвета, использованные в оформлении	Серебристый, Черный
Частота шины	2500 МГц
Поддержка Hyper Threading	Да
Характеристики процессора	CPU Intel Xeon X3430, 2.40 GHz, (Lynnfield, 2.5 GT/s, 2.8), 4C/4T, 8MB L3, Socket 1156, oem
Гнездо процессора	Socket LGA1156
Поддержка типов процессоров	Intel Core i7 8xx, Core i5 7xx, Xeon L34xx, X34xx (Lynnfield, Clarkdale).
Видео	XGI Z9s, видеопамять 64 Мб DDR2.
Оперативная память	4x DIMM ECC DDR III 2 GB Silicon Power, (CL9), SP002GBRTE133S01, Registered, box
Количество разъемов DDR3	4 (2х канальный контроллер памяти).
тип поддерживаемой памяти	DDR3. Максимальная поддерживаемая пропускная способность памяти указана в описании процессора
Чипсет	Intel 3420
Жесткий диск	4x HDD SATA 500 Gb Western Digital, RE3, WD5002ABYS, 7200rpm, 16MB cache, SATA 3.0 Gb/s
Внутренних отсеков 3,5 дюйма	4
Отсеков 5,25 дюйма	3 (1 отсек занят оптическим приводом)
Охлаждение	Fan for case, 12cm, Thermaltake TurboFan, [A2492], 4 pin, 1400rpm, 50CFM, 17dBA
Оптический привод	DVD-RW встроенный полноразмерный SATA привод
Интегрированный RAID-контроллер	Встроен в чипсет, возможно построение RAID массивов уровней 0, 1, 10, 5 из Serial ATA устройств
Сеть	2 сетевых контроллера Marvell 88E8056 10/100/1000 Мбит/сек

3.5.5 точка доступа Cisco AIR-AP1262N-R-K9

точка доступа Cisco Aironet 1260 Series предоставляет пользователям надежные и предсказуемые беспроводные услуги с поддержкой 802.11n стандарта. Cisco Aironet 1260 в девять раз увеличивают пропускную способность сетей 802.11a/g для надежной и безопасной доставки мультимедийных приложений. Эти устройства были специально разработаны для сложных радиочастотных сред, таких как, например, производственные предприятия, склады или крупные центры розничной торговли, которые предъявляют особые требования к универсальности антенных устройств, а благодаря поддержке функционирования от внешних антенн, Cisco Aironet 1260 Series обеспечивает бесперебойную работу беспроводной сети в широком температурном диапазоне. Cisco AIR-AP1262N-R-K9 изображен на рисунках 3.16 и 3.17.

Рисунок 3.16 – Cisco AIR-AP1262N-R-K9 (вид спереди)

Рисунок 3.17 – Cisco AIR-AP1262N-R-K9 (вид сзади)

технические характеристики:

- внешние антенны (по три разъема RP-TNC на каждый радиомодуль);
- прочный металлический корпус для защиты от воздействий внешней среды;
- питание осуществляется от блока питания (приобретается отдельно), от инжектора питания или коммутатора с поддержкой стандарта PoE 802.3af;
- диапазон рабочих температур от -20° до +55° С;
- интерфейс подключения к сети 10/100/1000BASE-T Ethernet (RJ-45);

- поставляются в автономном и облегченном (для работы с беспроводным контроллером) вариантах;
- поддержка технологий ClientLink, BandSelect, VideoStream;
- эти беспроводные точки доступа класса предприятия имеют компактный дизайн с металлической оболочкой и жесткими компонентами;
- дизайн UL 2043 plenum-rated для установки над потолком, а также для того, чтобы предотвратить поломку от падения с потолка;
- устанавливаемое оборудование, которое легко подходить к монтируемым стойкам 1130 и 1240 Series для упрощения миграции на новое оборудование.

Построенная на высококлассных компонентах, серия 1260 поддерживает такие технологии, как:

- ClientLink – улучшение покрытия беспроводной сети путем динамического формирования диаграммы направленности для клиентских устройств со слабым сигналом;
- BandSelect – оптимизация использования диапазона 2.4 ГГц за счет принудительного переключения клиентов в диапазон 5 ГГц;
- VideoStream – технология, позволяющая улучшить передачу трафика с групповой адресацией (например, потоковое видео).

точки доступа Cisco Aironet 1260 Series поставляются с 10-дневным изменением оборудования.

Беспроводная точка доступа Cisco AIR-AP1262N-R-K9 предназначена для небольших офисных пространств. Работает в стандарте 802.11n, обеспечивает соединение до 300 Мб/сек и предусматривает автономное управление. Благодаря поддержке технологии MIMO, возможно увеличение дальности связи и пропускной способности каналов. Модель имеет 128 Мб оперативной памяти, 32 Мб флеш-памяти и один гигабитный порт Ethernet. Установлены передатчики мощностью 20 dBM и 23 dBM и предусмотрено подключение 6-ти антенн. Реализована возможность питания по медной паре PoE. Соответствует нормам и требованиям, предъявляемым к сетевому оборудованию на территории России.

технические характеристики Cisco AIR-AP1262N-R-K:

- артикул: AIR-LAP1262N-R-K9;
- производитель: Cisco Systems;
- габариты: 22.1 x 22.1 x 4.7 см;
- память: 128 MB RAM, 32 MB FLASH;
- сетевой контроллер: 10/100/1000BASE-T autosensing (RJ-45), Management console port (RJ-45);
- блок питания: 44 to 57 VDC;
- архитектура: IEEE 802.11a, 802.11b, 802.11g and 802.11n;
- частотный диапазон: 2.412–2.472 ГГц (13 channels), 5.180–5.320 ГГц (8 channels), 5745–5825 МГц (5 channels);
- ширина канала: 20/40 МГц;

- максимальная мощность: a-20 дБм, b-23 дБм, g-20 дБм, n-20 дБм;
- шифрование: AES-CCMP encryption (WPA2), TKIP (WPA), Cisco TKIP, WPA TKIP, IEEE 802.11 WEP keys of 40 bits and 128 bits;
- модуляция: 2x3 MIMO;
- максимальная скорость в радиоканале: до 300 Мбит/с;
- разъём для подключения антенны: 3 x RP-TNC (2.4 GHz), 3 x RP-TNC (5 GHz) Вес 1.04 кг;
- рабочие температуры: -20°C до +55°C;
- влажность: Влажность 10% – 90% без конденсации;
- ПО для настройки, мониторинга и управления: Веб-интерфейс.

3.5.6 Модем ADSL D-Link 2500U

DSL-2500U (Рисунок 3.18, 3.19, 3.20) – это доступный высокопроизводительный ADSL/Ethernet-маршрутизатор для сетей малых офисов и домашних сетей. Он позволяет быстро и просто получить широкополосный доступ к сети Интернет по технологии ADSL и организовать совместное использование канала связи несколькими пользователями.

DSL-2500U реализует все необходимые функции для создания безопасной, высокоскоростной проводной сети: поддержка стандартов ADSL/ADSL2/ADSL2+, поддержка стандарта Fast Ethernet, встроенный межсетевой экран, механизм обеспечения качественной передачи данных (QoS), а также множество дополнительных функций и Ethernet-порт, к которому можно подключить отдельный компьютер или коммутатор.

Рисунок 3.18 – D-Link DSL-2500U/BRU/D (Вид сверху)

Рисунок 3.19 – D-Link DSL-2500U/BRU/D (Вид спереди)

Рисунок 3.20 – D-Link DSL-2500U/BRU/D (Вид сзади)

Маршрутизатор DSL-2500U оснащен встроенным межсетевым экраном. Расширенные функции безопасности позволяют минимизировать последствия действий хакеров и предотвращают вторжения в Вашу сеть и доступ к нежелательным сайтам для пользователей Вашей локальной сети.

Для управления и настройки DSL-2500U используется простой и удобный встроенный web-интерфейс (доступен на двух языках – русском и английском). Характеристики данного модема показаны в таблице 3.14.

т а б л и ц а 3.14 – технические характеристики модема D-Link 2500U

Характеристики	
Интерфейсы	1 порт ADSL (RJ-11) 1 порт LAN 10/100BASE-TX (RJ-45)
Стандарты ADSL	ADSL: ANSI T1.413 Issue 2, ITU-T G.992.1 (G.dmt) Annex A, ITU-T G.992.2 (G.lite) Annex A, ITU-T G.994.1 (G.hs) ADSL2: G.992.3 (G.dmt.bis) Annex A/L/M, G.992.4 (G.lite.bis) Annex A ADSL2+: G.992.5 Annex A/L/M
Протоколы соединения с Интернетом	Мультипротокольная инкапсуляция поверх АтМ AAL5; Bridged and routed Ethernet encapsulation; Инкапсуляция LLC (управление логическим соединением) и мультиплексирование на основе виртуального канала (VC-based multiplexing); PPP over Ethernet (PPPoE); PPP over ATM (PPPoA); IP over ATM (IPoA)
Возможности ATM	4 виртуальных канала PVC;

	OAM F4/F5 loopback;

Окончание таблицы 3.14

Характеристики	
Сетевые протоколы и функции	Статическая IP-маршрутизация; NAT; Виртуальный сервер и переадресация портов; DHCP-сервер/клиент/relay; DNS relay, DDNS IGMP proxy, IGMP v.2 snooping для IP-TV; NTP
VPN	Поддержка множества одновременных туннелей IPSec/PPTP VPN/L2TP VPN pass-through, PPTP-клиент
Качество обслуживания (QoS – Quality of Service)	Приоритезация/классификация трафика на основе: очереди приоритетов 802.1p; виртуального канала PVC (3 очереди приоритетов PVC); протокола, определяемого пользователем (TCP/UDP/ICMP и т.д.); PVC/VLAN port mapping
Настройка и управление	Мастер быстрой установки; Web-интерфейс; Загрузка программного обеспечения через Web-интерфейс или по TFTP, настройка загрузки/пересылки; UPnP; SNMP v1 и v2c, встроенные агенты MIB-I, MIB-II
Питание	Внешний адаптер питания переменного тока 9 В / 1А; Переключатель питания ON/OFF; Отсылка пакета Dying Gasp при пропадании питания; Кнопка Reset
Размеры	119x104x32 мм
Вес	200 г
Рабочая температура	От 0 до 40 С
Электромагнитная совместимость (EMC/EMI)	FCC Part 15 Class B; CE (EN55022/EN55024/EN300 328/EN301 489)
Безопасность	CSA, LVD, RoHS совместимый

Плавные линии в дизайне и довольно компактные размеры корпуса модема-маршрутизатора D-Link DSL-2500U/BRU/D выдают в нем модель для домашнего и офисного использования. Корпус изготовлен из черного матового пластика без каких-либо вставок, но с крупным полированным логотипом D-Link сверху.

4 технико-экономическое обоснование

4.1 Резюме

Главной целью данного проекта является проектирование корпоративной сети для Центральной городской клинической больницы № 12 и Городской поликлиники № 10 с использованием протокола динамической маршрутизации Open Shortest Path First. Экономической эффективностью данного протокола является его открытость, то есть его поддержку практически всеми производителями сетевого оборудования, реализации в программном обеспечении под все популярные операционные системы. также данный протокол обладает высокой устойчивостью к изменениям топологии сети и быстрой сходимостью, что не маловажно в проектировании крупной современной сети.

4.2 Финансовый план

Этот раздел является расчётным. Финансовый план включает: расчет величины, определение источника инвестиций, прогноз объема реализации, доходы от продажи товаров или услуг, издержки, прибыль.

4.2.1 Расчет капитальных вложений

Для того, чтобы построить сеть необходимы существенные затраты как на оборудование, так и на монтажные работы по установке оборудования, и необходимы затраты на проектирование сети. Расчет капитальных затрат производится по формуле

$$\sum К_{кап} = К_{об} + К_{м} + К_{пр} + К_{т} \quad (4.1)$$

где $К_{м}$ – капитальное вложение на монтаж;

$К_{пр}$ – капитальное вложение на проектирование сети;

$К_{об}$ – капитальное вложение на приобретение оборудования;

$К_{т}$ – капитальные вложения на транспортные расходы;

$К_{кап}$ – сумма капитальных затрат.

транспортные расходы включены в стоимость оборудования.

На осуществление данного проекта необходимо задействовать 7 наименований оборудования и комплектующих, общей стоимостью 3 424 000 тенге без НДС.

Стоимость устанавливаемого оборудования и комплектующих сети отражены в таблице 4.1.

т а б л и ц а 4.1 – Затраты на оборудование и комплектующие

Наименование	Количество, шт.	Цена за ед., тенге	Сумма, тенге (без НДС)
1 точка доступа Cisco AIR-AP1262N-R-K9	2 шт	125 000	250 000
2 Модем ADSL D-Link 2500U	4 шт	10 000	40 000
3 Маршрутизатор D-link DFL-800	2 шт	100 000	200 000
4 Коммутатор Cisco Catalyst 2960-24TT	12 шт	140 000	1 680 000
5 Коммутатор Cisco WS-C3560-24PS-S	2 шт	420 000	840 000
6 Кабельная продукция UTP 5e	200 м	70	14 000
7 Сервер Asus TS100-E6-PI4 Xeon X3430	2 шт	200 000	400 000
Итого			3 424 000

4.2.2 Расчет стоимости монтажа

Для подключения оборудования необходимо провести монтажные работы. Общая стоимость монтажных работ составляет 352 800 тенге. Виды проведенных работ и их стоимость отражены 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 кабеля, метр	200	500	100 000
2 Измерение параметров сети, место	32	900	28 800
3 Монтаж кабельной системы передачи данных, место	32	7000	224 000
Итого			352 800

4.2.3 Расчет затрат на проектирование сети

В состав затрат на проектирование сети входят следующие статьи затрат:

- заработная плата разработчиков;
- социальный налог;

- расходы на материалы;
- накладные расходы.

Расходы на проектирование рассчитываются по формуле

$$К_{ПР} = ФОТ + О_С + Н + М \quad (4.2)$$

где ФОт – фонд оплаты труда;

$О_с$ – отчисления на социальные нужды;

Н – накладные расходы;

М – расходы на материалы.

4.2.4 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 22500 тенге. Виды материалов и их стоимость отражены в таблице 4.3.

т а б л и ц а 4.3 – Затраты на материалы

Наименование материала	Марка	Единица измерения	Кол-во	Цена за единицу, тенге	Сумма, тенге
Бумага (Ватман)	А1	шт.	50	100	5000
Бумага писчая	«SvetoCopy» A4 96% 80 г/м	пачка	10	650	6500
CD диски	CD-R Philips	шт.	20	50	1000
Картридж принтера	Cartridge for HP 1030	шт.	2	5000	10000
Итого					22500

4.2.5 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 определяется как сумма оплаты труда всех исполнителей вычисляется по формуле

$$З_{ОСН} = \sum_{i=1}^{n} З_i \cdot Т_i \qquad (4.4)$$

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

$Т_i$ – затраты времени i-го работника, дней.

Дополнительная заработная плата составляет 10% от основной заработной платы и вычисляется по формуле

$$З_{ДОП} = 0,1 \cdot З_{ОСН} \qquad (4.5)$$

труд разработчиков оплачивается согласно штатному расписанию. Количество исполнителей и размер месячной заработной платы представлены 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
Инженер	2	300 000
Руководитель проекта	1	200 000
Итого		500 000

Стоимость человека-дня вычисляется по формуле

$$Д = \frac{З_{Пм}}{Д_р} \qquad (4.6)$$

где $З_{Пм}$ – заработная плата за месяц, тенге;

$Д_р$ – среднемесячное количество рабочих дней.

Среднемесячное количество рабочих дней – 24. тогда, исходя из формулы (4.6), дневная зарплата для инженера будет равна

$$Д = \frac{150000}{24} = 6250 \text{ тенге}$$

Исходя из формулы (4.6), дневная зарплата для руководителя проекта будет равна

$$Д = \frac{200000}{24} = 8333 \text{ тенге}$$

На основе данных стоимости одного человека дня и продолжительности выполнения каждого этапа рассчитываем 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	6250	30	187 500
Руководитель проекта	8333	30	249 990

Исходя из формулы (4.4), основная заработная плата будет равна

$$З_{осн} = 187\,500 + 187\,500 + 249990 = 624990 \text{ тенге}$$

Исходя из формулы (4.5), дополнительная заработная плата будет равна

$$З_{доп} = 0{,}1 \cdot 624990 = 62499 \text{ тенге}$$

Исходя из формулы (4.3), суммарный фонд оплаты труда (ФОт) составит

ФОт = 624990+ 62499 = 687 489 тенге

4.2.6 Расчет социальных отчислений

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

$$О_С = 0{,}11 \cdot (ФОТ - ПО) \quad (4.7)$$

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

$$ПО = 0{,}1 \cdot ФОТ \quad (4.8)$$

Исходя из формулы (4.8), пенсионные отчисления будут равны

$$ПО = 0,1 \cdot 687489 = 68748,9 \text{ тенге}$$

тогда, исходя из формулы (4.7), социальный налог будет равен

$$О_с = 0,11 \cdot (687489 - 68748,9) = 68061,411 \text{тенге}$$

4.2.7 Расчет накладных расходов

Накладные расходы составляют 70% от общей суммы понесенных расходов и рассчитываются по формуле

$$Н = 0,7 \times (ФОТ + О_с + М) \quad (4.9)$$

тогда, исходя из формулы (4.9), накладные расходы составят

$$Н = 0,7 \times (687489 + 68061,411 + 22500) = 544635 \text{ тенге}$$

Результаты расчетов затрат по проектированию сети представлены в таблице 4.6.

т а б л и ц а 4.6 – Расходы по проектированию сети

Показатель	Сумма, тенге
ФОт, тенге	687 489
Отчисления на социальные нужды, тенге	68 061
Затраты на материалы, тенге	22 500
Накладные расходы, тенге	544 635
Итого	1 322 685

Суммарные затраты на разработку и в соответствии с приведенной формулой (4.2) и расчетами составляют

$$К_{ПР} = 1374978 + 136123 + 544635 + 22500 = 1322685 \text{ тенге}$$

так как транспортные расходы включены в стоимость оборудования общая сумма капитальных затрат в соответствии с произведенными расчетами и согласно формуле (4.1) составит

$\sum К_{кап}$ = 3424000 + 352800 + 1322685 = 5 099 485 тенге

4.3 Оценка эффективности внедрения корпоративной сети с использованием протокола динамической маршрутизации Open Shortest Path First для ЦГКБ № 12 и ГП № 10

Социальный эффект – это повышение материального и культурного уровня жизни граждан, более полное удовлетворение их потребностей в услугах, улучшение условий и техники безопасности труда, снижение доли ручного труда и др.

Данный проект не относится к коммерческим и не преследует получение прибыли. так как объектами внедрения являются медучреждения, речь идет о социальном эффекте.

Социальным эффектом внедрения корпоративной сети между ЦГКБ № 12 и ГП № 10 является:

- улучшение качества работы врачей за счет создания электронной регистратуры больных, базы электронных карт пациентов, где будут храниться их истории болезней с момента первого обращения в медучреждения;
- уменьшение количества очередей в регистратуру и на прием к специалистам;
- любой специалист сможет за небольшой промежуток времени отследить всю динамику развития болезней пациента, оценить эффективность врачебного вмешательства на разных этапах лечения;
- при необходимости врачи могут немедленно отыскать необходимую справочную информацию по новейшим методикам лечения того или иного заболевания, а также характеристики новых и давно забытых лекарственных препаратов в базе данных этой корпоративной сети;
- улучшится взаимодействие между специалистами амбулаторного звена медучреждения и стационара, что позволит исключить большое количество врачебных ошибок при лечении того или иного пациента;
- улучшение качества управления врачебным персоналом и специалистами среднего звена, например, при получении того или иного приказа информация мгновенно будет доводиться до специалистов.

Вывод

В данной части дипломного проекта было представлено технико-экономическое обоснование, в котором рассматривается вопрос о проектировании корпоративной сети для Центральной городской клинической больницы № 12 и Городской поликлиники № 10.

В финансовой части технико-экономического раздела был рассчитан объём капитальных вложений, который составил 5 099 485 тенге.

Социальным эффектом внедрения корпоративной сети между ЦГКБ № 12 и ГП № 10 является:

- улучшение качества работы врачей за счет создания электронной регистратуры больных, базы электронных карт пациентов, где будут храниться их истории болезней с момента первого обращения в медучреждения;
- уменьшение количества очередей в регистратуру и на прием к специалистам;
- любой специалист сможет за небольшой промежуток времени отследить всю динамику развития болезней пациента, оценить эффективность врачебного вмешательства на разных этапах лечения;
- при необходимости врачи могут немедленно отыскать необходимую справочную информацию по новейшим методикам лечения того или иного заболевания, а также характеристики новых и давно забытых лекарственных препаратов в базе данных этой корпоративной сети;
- улучшится взаимодействие между специалистами амбулаторного звена медучреждения и стационара, что позволит исключить большое количество врачебных ошибок при лечении того или иного пациента;
- улучшение качества управления врачебным персоналом и специалистами среднего звена, например, при получении того или иного приказа информация мгновенно будет доводиться до специалистов.

5 Безопасность жизнедеятельности

5.1 Анализ потенциально опасных и вредных факторов, воздействующих на обслуживающий персонал при эксплуатации технического оборудования

Главной целью данного проекта является организация корпоративной сети Центральной городской клинической больницы № 12 и Городской поликлиники № 10, с целью предоставления современных услуг связи: высокоскоростной доступ в Интернет, компьютерная сеть, на базе протокола Open Shortest Path First, который имеет неплохую масштабируемость и обладает высокой отказоустойчивостью.

В настоящее время все предприятия, учреждения или организации не могут функционировать достаточно эффективно без использования компьютерной техники. Постоянное развитие любого предприятия, учреждения или организации, а как следствие объёмов и сложности информации требует расширения компьютерных сетей и автоматизированных информационных систем. Но кроме очевидных выгод компьютерная техника несет в себе опасность здоровью и поэтому актуальной становится проблема охраны труда человека в процессе работы, сохранение его здоровья и работоспособности.

Существует несколько вредных факторов, воздействующих на работников, занятых на работе с видеодисплейными терминалами (ВДт) и персональными компьютерами (ПК):

1) воздействие электромагнитных полей (радиочастот), статического электричества;
2) неудовлетворительный микроклимат помещений;
3) недостаточная освещенность;
4) психоэмоциональное напряжение.

Без строгого учёта правил техники безопасности и производственной санитарии, неточного выполнения требований техники безопасности может привести к аварии, либо к профессиональным заболеваниям и производственному травматизму. Охрана труда обеспечивается системой законодательных актов, социально-экономических, организационных, технических, гигиенических и лечебно-профилактических мероприятий и средств, направленных на создание таких условий труда, при которых исключено воздействие на работающих опасных и вредных производственных факторов. Создание наиболее благоприятных, комфортных условий труда, улучшение охраны труда и техники безопасности, без сомнения, ведет к более высокой производительности труда, социальному развитию и повышению благосостояния.

Согласно ГОСт 12.1.005-88 «ССБт. Оптимальные и допустимые нормы микроклимата, в зависимости от категории работ», работа людей в помещении относится к работе лёгкой тяжести (1а), так как управление оборудованием осуществляется дистанционно с помощью компьютеров.

С целью создания нормальных условий для работников предприятий связи установлены нормы производственного микроклимата. В помещениях при работе с ЭВМ должны соблюдаться следующие климатические условия:

1) холодный период года:

- оптимальная температура 22-24 С˚, допустимая температура 18-26 С˚;
- относительная влажность 40-60 %, допустимая влажность 75%;
- скорость движения воздуха относительная и допустимая 0,1 м/с;

2) тёплый период года:

- 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.

5.2 Планировка рабочего места

Эргономика – прикладная наука целью, которой является приспособление труда к физиологическим и психическим возможностям человека для обеспечения наиболее эффективной работы, которая не создаёт угрозы здоровью человека.

Практика показывает, что планировка рабочего места должна удовлетворять требованиям удобства выполняемых работ и экономии энергии, и времени оператора, рационального использования производственных площадей и удобства обслуживания устройств ПК.

При планировке рабочего места необходимо учитывать удобство расположения дисплеев, принтеров, пульта ПК, а также зоны досягаемости рук оператора. Эти зоны, установленные на основании антропометрических данных тела человека, дают возможность рационально разместить компьютер, его клавиатуру и дисплей.

Высота рабочей поверхности стола должна регулироваться в пределах 680-800 мм (Рисунок 5.1), при отсутствии такой возможности должна составлять 725 мм.

Дисплей должен удовлетворять следующим требованиям:

1) важнейшие элементы конструкции должны быть расположены в центре поля зрения (клавиатура);

2) элементы должны быть сгруппированы по функциональному признаку;

3) рабочие поверхности должны быть расположены наклонно, по возможности перпендикулярно взгляду оператора;

4) экран видеомонитора должен находиться от глаз пользователя на оптимальном расстоянии 600-700 мм (Рисунок 5.1), но не ближе 500 мм с учётом размеров знаков и символов.

Рисунок 5.1 – План рабочего места на ПК

Важнейшими характеристиками зрительного восприятия оператора являются: яркость, контрастность между объектами и фоном, и острота зрения. Контрастность по отношению к фону влияет на восприятие цветов. так, например, лучше воспринимаются комбинации цветов: черный на желтом, черный на белом, зеленый на черном, белый на черном. Отсюда следует оптимальность выбора цветов:

1) для экрана: белый на черном;

2) для клавиатуры: черный на белом.

Наиболее удобно сиденье, имеющее выемку, соответствующую форме бедер и наклон назад. Спинка стула должна быть изогнутой формы, обнимающей поясницу. Рабочий стул (кресло) должен быть снабжен подъёмно-поворотным механизмом, обеспечивающим регуляцию высоты сидения и спинки. Рабочее кресло должно иметь подлокотники. Регулировка каждого параметра должна легко осуществляться, быть независимой и иметь надёжную фиксацию. На рабочем месте необходимо предусматривать подставку для ног.

Клавиатура должна располагаться на поверхности стола таким образом, чтобы соответствовать локтю сидящего оператора. Его рука должна быть

согнута на 90 градусов в локтевом суставе, а предплечье – лежать горизонтально.

5.3 Расчет вентиляции помещения

В помещении, где находятся ЭВМ, системы отопления и системы кондиционирования следует устанавливать так, чтобы ни теплый, ни холодный воздух не направлялся на людей. На производстве рекомендуется создавать динамический климат с определенными перепадами показателей. температура воздуха у поверхности пола и на уровне головы не должна отличаться более чем на 5 градусов. В производственных помещениях помимо естественной вентиляции предусматривают приточно-вытяжную вентиляцию. Основным параметром, определяющим характеристики вентиляционной системы, является кратность обмена, т.е. сколько раз в час сменится воздух в помещении.

$V_{вент}$ – объем воздуха, необходимый для обмена;

$V_{пом}$ – объем рабочего помещения.

Для расчета примем следующие размеры рабочего помещения (Рисунок 5.2):

- длина А = 6 м;
- ширина В = 4 м;
- высота Н = 3 м.

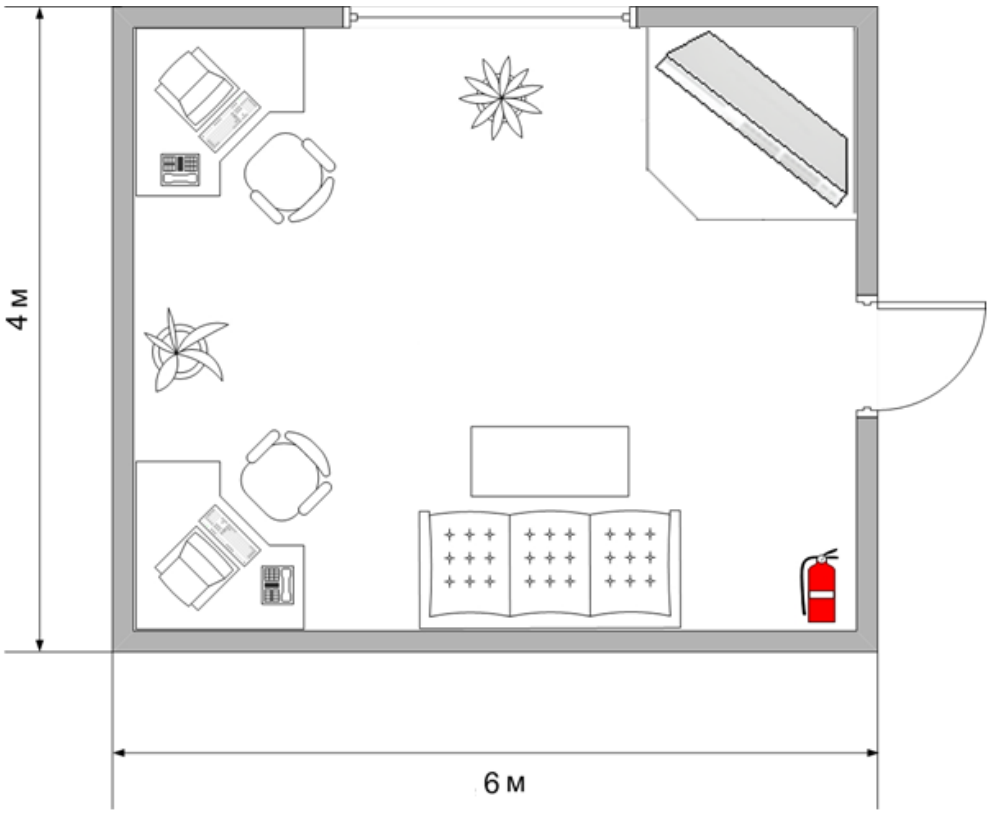

Рисунок 5.2 – План рабочего помещения

Объем помещения рассчитывается по формуле

$$V_{пом} = A \cdot B \cdot H \quad (5.1)$$

тогда, исходя из формулы (5.1), объем помещения будет равен

$V_{пом} = A \cdot B \cdot H = 72\ м^3$

Необходимый для обмена объем воздуха $V_{вент}$ из уравнения теплового баланса определяется по формуле

$$V_{вент} = C \cdot (t_{уход} - t_{приход}) \cdot Y \quad (5.2)$$

тогда, исходя из формулы (5.2), объем воздуха будет равен

$V_{вент} = C \cdot (t_{уход} - t_{приход}) \cdot Y = 3600 \cdot Q_{избыт}$

где $Q_{избыт}$ – избыточная теплота (Вт);
C = 1000 – удельная теплопроводность воздуха (Дж/кгК);
Y = 1,2 – плотность воздуха (мг/см).

температура уходящего воздуха определяется по формуле

$$t_{уход} = t_{р.м.} + (H - 2) \cdot t \quad (5.3)$$

где t = 1-5 градусов – превышение t на 1м высоты помещения;
$t_{р.м.}$ = 25 градусов – температура на рабочем месте;
H = 3 м – высота помещения;
$t_{приход}$ = 18 градусов.

тогда, исходя из формулы (5.3), температура уходящего воздуха будет равна

$t_{уход} = 25 + (3 - 2) \cdot 2 = 27$

Общий избыток тепла рассчитывается по формуле

$$Q_{избыт} = Q_{изб.1} + Q_{изб.2} + Q_{изб.3} \quad (5.4)$$

где $Q_{изб.1}$ – избыток тепла от электрооборудования и освещения;
$Q_{изб.2}$ – теплопоступление от солнечной радиации;
$Q_{изб.3}$ – тепловыделения людей.

$$Q_{изб.1} = E \cdot p \quad (5.5)$$

где E – коэффициент потерь электроэнергии на теплоотвод (E = 0,55 для освещения);

P – мощность (P = 300 Вт).

Исходя из формулы (5.5), избыток тепла от электрооборудования и освещения будет равно

$$Q_{изб.1} = 0{,}55 \cdot 300 = 165 \text{ Вт}$$

теплопоступление от солнечной радиации рассчитывается по формуле

$$Q_{изб.2} = m \cdot S \cdot k \cdot Q_c \qquad (5.6)$$

где m – число окон, примем m = 2;

S – площадь окна, $S = 2{,}3 \cdot 2 = 4{,}6$ м^2;

K – коэффициент, учитывающий остекление. Для двойного остекления k = 0,6;

Q_c = 127 Вт/м – теплопоступление от окон.

тогда, исходя из формулы (5.6), теплопоступление от солнечной радиации равно

$$Q_{изб.2} = 4{,}6 \cdot 2 \cdot 0{,}6 \cdot 127 = 701 \text{ Вт}$$

$$Q_{изб.3} = n \cdot q \qquad (5.7)$$

где q = 80 Вт/чел.;

n – число людей (n = 2).

Исходя из формулы (5.7), тепловыделения людей будут равны

$$Q_{изб.3} = 2 \cdot 80 = 160 \text{ Вт}$$

Исходя из формулы (5.4), общий избыток тепла будет равен

$$Q_{избыт} = 165 + 701 + 160 = 1026 \text{ Вт}$$

Исходя из формулы (5.2), $V_{вент}$ будет равен

$$V_{вент} = 3600 \cdot 1026 / (1000 \cdot (27 - 18)) = 410{,}4 \text{ м}^3$$

Необходимо тщательно продумать месторасположение кондиционера в офисе. Можно установить канальный кондиционер за подвесным потолком и развести воздух в разные точки комнаты через воздуховоды. Это обеспечит равномерное распределение воздуха и температуры. Если высота подшивных

потолков не позволяет установить канальный кондиционер (как в данном случае), можно предусмотреть два или даже три внутренних блока, расположенных в разных точках помещения. такой вариант особенно оправдан в комнатах неправильной или вытянутой формы. Полупромышленные кондиционеры допускают подсоединять до трех внутренних блоков разного вида к одному наружному блоку. Это снизит стоимость всей системы и сохранит стену здания от множества блоков.

5.4 Расчет пожарной безопасности

Здание по степени опасности развития пожара, от функционального назначения и пожарной нагрузки горючих материалов, относится к 1-ой группе категории D.

Причинами возникновения пожара могут быть:

- возгорание элементов аппаратуры;
- возгорание отделочных материалов от неисправных выключателей, розеток;
- несоблюдение режимов эксплуатации оборудования, неправильное действие персонала.

При возникновении пожара может пострадать не только помещение, но и дорогостоящая аппаратура, привести к человеческим жертвам. Поэтому необходимо чтобы были приняты меры по раннему выявлению и ликвидации пожаров. Источниками зажигания могут оказаться электронные схемы ЭВМ, приборы, применяемые для технического обслуживания, устройства электропитания, кондиционеры воздуха, где в результате различных нарушений образуются перегретые элементы, и др.

В соответствии с требованиями правил пожарной безопасности помещение оборудованы углекислотными огнетушителями ОУ-5 с учетом – один огнетушитель на 100 м^2. Общая площадь помещения управления составляет 24 м^2 таким образом устанавливаются 1 огнетушитель. В качестве огнетушащего вещества применяется комбинированный углекислотно-хладоновый состав. Расчетная масса комбинированного углекислотно-хладонового состава m_d, кг, для объемного пожаротушения определяется по формуле

$$m_d = k \cdot g_n \cdot V \qquad (5.8)$$

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

g_n – нормативная массовая концентрация углекислотно-хладонового состава (g_n = 0,04);

V – объем помещения.

$$V = A \cdot B \cdot H \qquad (5.9)$$

где A = 6 м – длина помещения;
B = 4 м – ширина помещения;
H = 3 м – высота помещения.

Исходя из формулы (5.9), объем составит

$$V = 6 \cdot 4 \cdot 3 = 72 м^3$$

Исходя из формулы (5.8), масса комбинированного углекислотно-хладонового состава будет равна

$$m_д = 1{,}2 \cdot 0{,}04 \cdot 72 \approx 3{,}5 кг$$

Расчетное число баллонов определяется из расчета вместимости в 20-литровый баллон 12 кг углекислотно-хладонового состава.

Внутренний диаметр магистрального трубопровода d_i, мм, определяется по формуле

$$d_i = 12 \cdot \sqrt{2} \qquad (5.10)$$

Исходя из формулы (5.10), внутренний диаметр магистрального трубопровода будет равен

$$d_i = 12 \cdot \sqrt{2} = 17 \text{ мм}$$

Эквивалентная длина магистрального трубопровода l_2, м, определяется по формуле

$$l_2 = k_1 \cdot l_1 \qquad (5.11)$$

где k_1 = 1,2 – коэффициент увеличения длины трубопровода для компенсации не учитывающих местных потерь;
l_1 = 3м – длина трубопровода по проекту тогда.

Исходя из формулы (5.11), эквивалентная длина магистрального трубопровода равна

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

Расход углекислотно-хладонового состава Q, кг/с, в зависимости от эквивалентной длины и диаметра трубопровода равна 1,4 кг/с.

Расчетное время подачи углекислотно-хладонового состава t, мин, определяется по формуле

$$t = \frac{m_d}{60 \cdot Q} \tag{5.12}$$

тогда, исходя из формулы (5.12), время подачи углекислотно-хладонового состава будет равно

$$t = \frac{3,5}{60 \cdot 1,4} = 0,041 \text{мин}$$

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

$$m = 1,1 \cdot m_d \cdot \left(1 + \frac{k_2}{k}\right) \tag{5.13}$$

где k_2 = 0,2 – коэффициент учитывающий остаток углекислотно-хладонового состава в баллонах и трубопроводах.

тогда, исходя из формулы (5.13), масса основного запаса углекислотно-хладонового состава будет равна

$$m = 1,1 \cdot 3,5 \cdot \left(1 + \frac{0,2}{1,2}\right) = 4,49 \text{кг}$$

таким образом из полученных результатов можно сделать вывод, что для обеспечения нормального функционирования системы автоматического пожаротушения потребуется 1 баллон углекислотно-хладонового состава вместимостью 20 литров, с массой смеси 3,5 кг. Автоматические установки газового пожаротушения имеют устройства для автоматического пуска в соответствии с ГОСт 12.4.009-83. Принципиальная схема установки автоматического пожаротушения показана на рисунке 5.3. Схема включает:

1) аппарат для хранения огнетушащего вещества;
2) устройство для подачи огнетушащего вещества;
3) устройство включения системы;
4) устройство для обнаружения пожара и оповещения о ней;
5) устройство выпуска огнетушащего вещества;
6) очаг горения.

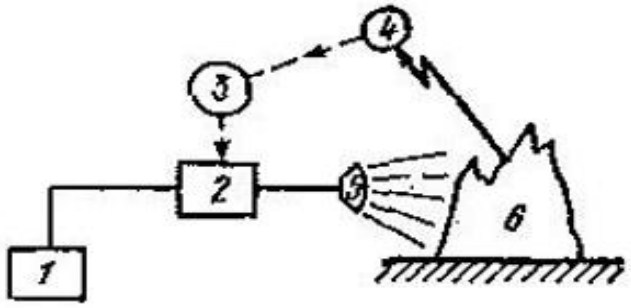

Рисунок 5.3 – Принципиальная схема установки автоматического пожаротушения

Вывод

В данном разделе был произведён анализ условий труда в рабочем помещении. Уровень условий труда признан допустимым, и данные, полученные из расчетов, полностью удовлетворяют требованиям стандартов безопасности жизнедеятельности.

также мы рассчитали все необходимые параметры для кондиционирования воздуха в помещении, т.е. автоматическое поддержание его состояния в помещении в соответствии с определенными требованиями независимо от изменения состояния наружного воздуха и условий в самом помещении.

Электротехническое оборудование в помещении является потенциальным источником возникновения пожара.

Из расчетов получили, что для обеспечения нормального функционирования системы автоматического пожаротушения потребуется 1 баллон углекислотно-хладонового состава вместимостью 20 литров, с массой смеси 3,5 кг.

Заключение

В данном дипломном проекте приводится описание разработки корпоративной сети для Центральной городской клинической больницы № 12 и Городской поликлиники № 10 с использованием протокола динамической маршрутизации Open Shortest Path First (OSPF).

В проекте имеется обзор развития, проектирования и параметры качества корпоративных сетей. также в проекте описан протокол динамической маршрутизации OSPF. Показан сравнительный анализ характеристик основных протоколов динамической маршрутизации.

В графической части работы показана структурная схема корпоративной сети с использованием протокола динамической маршрутизации OSPF, общая схема корпоративной сети между Центральной городской клинической больницей № 12 и Городской поликлиникой № 10 через сети двух провайдеров.

В технико-экономическом расчёте определены затраты на реализацию проекта и был определен социальный эффект от внедрения проекта.

В проекте был произведён анализ условий труда в рабочем помещении, рассчитаны все необходимые параметры для кондиционирования воздуха в помещении, а также был произведен расчет пожарной безопасности.

Список использованной литературы

1 Структура и реализация сетей на основе протокола OSPF. – 2-е изд. – Москва: Издательство «Вильямс», 2004.

2 М.А. Щербаков, М. П. Строганов. Информационные сети и телекоммуникации. – Москва: Издательство «Высшая школа», 2008.

3 Никитюк Л.А., Комарницкий Д.Л. Методическое руководство к выполнению КП «Проектирование корпоративной сети». – Одесса, 2006.

4 Леинванд А., Пински Б. Конфигурирование маршрутизаторов Cisco. – 2-е изд. – Москва: Издательство «Вильямс», 2004. – 368 с.

5 Cisco Systems. Руководство Cisco по междоменной многоадресной маршрутизации. – Москва: Издательство «Вильямс», 2004. – 320 с.

6 Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – 3-е изд. – Санкт-Петербург: Издательство «Питер», 2006. – 958 с.

7 Сайт http://www.citforum.ru

8 Сайт http://www.rfc-editor.org

9 Сайт http://www.wikipedia.org

10 Сайт http://www.cisco.com

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

12 Горфинкель В.Я., Швандара В.А. Экономика предприятия. – 4-е изд. – Москва: Издательство «Юнити», 2007.

13 Аманбаев У.А. Экономика предприятия. – Алматы: Издательство «Бастау», 2012.

14 Роберт т. Фатрелл, Дональд Ф. Шафер, Линда И. Шафер. Управление программными проектами. Достижение оптимального качества при минимуме затрат. – Москва: Издательство «Вильямс», 2008.

15 Белов С.В., Девисилов В.А., Ильницкая А.В. Безопасность жизнедеятельности. – 8-е изд. – Москва: Издательство «Высшая школа», 2009.

16 Арустамова Э.А. Безопасность жизнедеятельности. – 12-е изд. – Москва: Издательство «Дашков и К», 2007.

17 Хван т.А., Хван П.А. Безопасность жизнедеятельности. – Ростов-на-Дону: Издательство «Феникс», 2007.