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 предприятия с удалёнными филиалами

Специальность 5В070400 ВТ и ПО

Выполнил (а) Чекмарёв К.А ВТ-10-4
(Фамилия и инициалы) группа

Научный руководитель Тайжанова А.К., ст. препод.
(Фамилия и инициалы, ученая степень, звание)

Консультанты:

по экономической части:
Ерешева З.Д., ст. преподаватель
(Фамилия и инициалы, ученая степень, звание)
Ерешева «02» 06 2014 г.
(подпись)

по безопасности жизнедеятельности:
Трунтаева Н.Г., д.х.н., профессор
(Фамилия и инициалы, ученая степень, звание)
«16» 05 2014 г.
(подпись)

по применению вычислительной техники:
Тайжанова А.К., ст. препод.
(Фамилия и инициалы, ученая степень, звание)
«10» 06 2014 г.
(подпись)

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

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

Рецензент: Нуркасымов А.С.
(Фамилия и инициалы, ученая степень, звание)
«5» июня 2014 г.
(подпись)

Алматы 2014 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Факультет_____

Специальность_____

Кафедра_____

ЗАДАНИЕ

на выполнение дипломного проекта

Студент _____

(фамилия, имя, отчество)

Тема проекта_____

_____

_____

утверждена приказом ректора № 115 от «24 » сентября 20___ г.

Срок сдачи законченной работы « ___ » _____ 20___ г.

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

_____

_____

_____

_____

_____

_____

_____

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

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Перечень графического материала (с точным указанием обязательных чертежей)

Рекомендуемая основная литература

Консультанты по проекту с указанием относящихся к ним разделов

Раздел	Консультант	Сроки	Подпись
БЖД	Туровцева Н.Г.	11.04 - 16.05.14	
Экономика	Ерешева З.Ю.	12.05 - 02.06.14	Ерешева
Нормоконтроль	Тусупов Д.М.	09.06.14 г.	
Основная часть	Тайжанова А.Ж.	10.06.14 г.	

Г Р А Ф И К
подготовки дипломного проекта

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления руководителю	Примечание

Дата выдачи задания «____»_____20___ г.

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

Руководитель _____ Гайнетдинова А.Ж.
(подпись) (Фамилия и инициалы)

Задание принял к исполнению
студент _____ _____
(подпись) (Фамилия и инициалы)

Андатпа

Бұл дипломдық жобада “Фаворит” компаниясының бас офисі мен филиалдарының корпоративтік желісін жобалау келтірілген.

Берілген дипломдық жобада корпоративтік желіні жобалаудығы қауіпсіздікті қамтамасыз ету және сәйкес шаралар қолдану.

Сонымен қатар жобада өміртіршілік қауыпсіздігінің шаралары сипатталған.

Жобаны енгізудің технико-экономикалық негіздемесі келтірілген.

Аннотация

В данной дипломной работе представлен процесс проектирования корпоративной сети для главного офиса предприятия “Фаворит” и его филиала.

В данном дипломном проекте были рассмотрены вопросы обеспечения безопасности проектируемой сети и приняты соответствующие меры.

В работе также были произведены расчеты по обеспечению безопасности жизнедеятельности на предприятии.

Проведено технико-экономическое обоснование разработки данного проекта.

Abstract

In this diploma project presents the process of designing a corporate network for the main office of the enterprise "Favorite" and its branch.

In this diploma project were considered questions of security network and taken appropriate action.

In the project also were calculated parameters to ensure safety of life at the company.

Feasibility study was carried out development of the project.

Содержание

Введение

В последнее время транспортировка корпоративной информации и документооборот внутри предприятий совершается в электронном виде тем или иным способом. Для этого уже существует множество протоколов и методов передачи данных. Немаловажную роль в передаче корпоративных данных на большие расстояния играет глобальная сеть Internet.

Информационные технологии нашего времени предоставляют большие возможности по улучшению работы предприятий, заменяя человеческий труд машинным, повышая рост производительности труда и снижая затраты на персонал и транспортировку данных. Работа в реальном времени стала одним из главных требований, предъявляемых к корпоративным сетям.

Благодаря компьютеризации и внедрению сетевых технологий стало возможным значительно повысить как оперативность, так и качество выполняемых работ на предприятиях. Автоматизация процесса обмена информацией на предприятии также отражается на качестве управления персоналом. К примеру, при использовании корпоративной сети отданный приказ администрацией предприятия будет моментально доводиться до подчиненных.

Но в то же время нельзя забывать про безопасность и надежность системы. Корпоративная информация, передаваемая через открытую сеть Интернет, может быть перехвачена злоумышленниками при помощи специальных программ-снифферов и использоваться в корыстных целях. Сюда относятся важнейшая информация, содержащаяся в конфиденциальных документах. Кроме этого могут быть извлечены логины и пароли от корпоративной почты или иных сервисов используемых на предприятии. Конфиденциальность передаваемых данных играет исключительную роль при проектировании корпоративной сети.

Для обеспечения нужной безопасности в корпоративных сетях применяются различные протоколы Virtual Private Network. С их помощью создаются виртуальные каналы связи поверх сети Интернет. Они позволяют соединять локальные сети различных технологий и их сегменты в одну корпоративную сеть. Одним из главных достоинств является шифрование всего трафика, проходящего по туннелю на канальном уровне модели OSI. Шифрование защищает от доступа к передаваемым данным, а инкапсуляция не позволяет злоумышленнику узнать адресат передаваемой информации.

Кроме всего прочего, поддержание функционирования удалённых филиалов предприятия, использующих данную сеть – одна из основных целей корпоративной сети. Пользователями корпоративной сети являются сотрудники данного предприятия.

Стратегическое планирование сети состоит в нахождении компромисса между потребностями предприятия в автоматизированной обработке

передаваемой информации, его финансовым положением и возможностями сетевых и информационных технологий сегодня и в ближайшем будущем.

Из сказанного выше можно заключить что, актуальность темы дипломного проекта обусловлена необходимостью создания надежной и полнофункциональной корпоративной сети для конкретного предприятия.

Целью данного дипломного проекта является проектирование корпоративной сети для главного офиса предприятия “Фаворит” и его удаленного филиала.

1 Теоретическая часть

1.1 Понятие корпоративной сети

Успех деятельности любой организации во многом определяется существованием единого информационного пространства. Развитая информационная система позволяет эффективно справляться с обработкой потоков информации, передаваемых между сотрудниками предприятия и принимать им своевременные и рациональные решения для обеспечения выживания предприятия в жесткой конкурентной борьбе на потребительском рынке.

Чаще всего под термином корпоративная сеть понимается объединение нескольких локальных вычислительных сетей (ЛВС), расположенных в различных структурных подразделениях одного предприятия, которые могут быть построены на различных технических, программных и информационных принципах.

Построение корпоративной сети обеспечивает:

- доступ сотрудников различных подразделений предприятия к общим корпоративным информационным ресурсам;
- единое централизованное управление, администрирование и техническое обслуживание информационно – коммуникационных ресурсов;
- эффективную защиту корпоративной информации от несанкционированного доступа;
- организацию единой системы электронной почты и электронного документооборота;
- взаимодействие корпоративной сети организации с бизнес - системами других предприятий, вычислительными сетями государственных учреждений и других органов, участвующих в информационном обмене на правах абонентов телекоммуникационной корпоративной системы.

Корпоративная сеть (КС) – это сложная система, включающая в себя множество разнообразных компонентов: компьютеры различных типов, сетевые адаптеры, маршрутизаторы и коммутаторы, системное и прикладное программное обеспечение (ПО), кабельную систему.

КС позволяет создать единую для всех отделов предприятия базу данных, вести электронный документооборот, организовать видеоконференции с удаленными филиалами, обеспечить высококачественную телефонной и факсимильной связи независимо от расстояния через доступ в Интернет и другие интерактивные сети. Все это повышает оперативность выполнения работ на предприятии и обеспечивает качественное управление персоналом в реальном времени. Появляется возможность передавать конфиденциальные данные производственного и финансового характера с минимальным риском того, что кроме уполномоченных сотрудников компании никто не имеет к ней

несанкционированного доступа. Обобщенная схема КС представлена на рисунке 1.1.

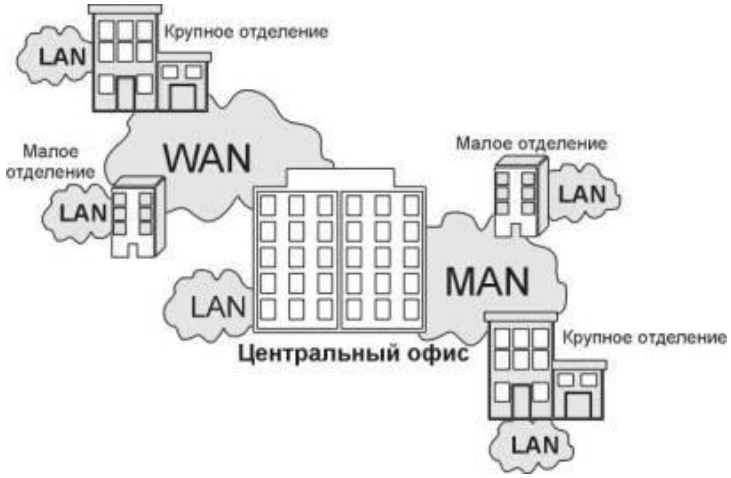

Рисунок 1.1 – Обобщенная схема корпоративной сети

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

Со структурной точки зрения корпоративная сеть – это сеть смешанной топологии, содержащая несколько ЛВС. Корпоративная сеть будет объединять подразделения предприятия, тем самым создавая общее информационное корпоративное пространство.

С функциональной точки зрения корпоративная сеть – это результативная среда передачи актуальной информации необходимой для выполнения 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 – Уровни корпоративной сети

Таким образом, с системно-технической точки зрения корпоративная сеть – это сложная система, предоставляющая пользователям и программам набор продуктивных 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 Обзор цикла проектирования корпоративной сети

Проектирование корпоративной сети состоит из следующих стадий:

1) анализ требований. Под анализом требований следует понимать определение проблем и деловых целей предприятия, а также формулировка задач и целей проектирования в соответствии с ними. Анализ требований к сети дает возможность оценки деловой значимости информационно-технологических решений. Четкое обозначение требований к функциям проектируемой сети даст избежать реализации ненужных свойств сети, что сэкономит средства предприятия. То есть, на данном этапе следует установить какие задачи будет решать проектируемая сеть, какими будут основные потоки трафика, как физически будут сосредоточены пользователи и ресурсы, нужно ли задание приоритетов видов трафика, как будет осуществлена защита информации внутри сети, как сеть будет подключена к сети Интернет, как будет реализовано управление правами доступа пользователей. Кроме всего перечисленного, на этапе анализа требований особо важно изучение состояния зданий и сооружений в месте развертывания сети, анализ уже существующей инфраструктуры. Эти данные жизненно необходимы как для постановки задачи проектирования, так и для самого проектирования;

2) разработка функциональной модели (бизнес-модели) производства отображает последовательность работ и технологических процессов предприятия, а также каждого из подразделений в отдельности, определяет набор сетевых задач, выполняемых в каждом из подразделений, на основании которых формулируются требования к проектируемой сети, предъявляемые к ней спецификой бизнес-процессов каждого из подразделений в отдельности и предприятия в целом;

3) разработка технической модели корпоративной сети (структурный синтез). Техническая модель описывает в достаточно общих терминах, какое компьютерное и сетевое оборудование нужно использовать, чтобы достичь поставленных целей. Для того чтобы построить техническую модель, нужно проанализировать существующее оборудование, определить системные требования, оценить состояния техники на сегодняшний день и провести прогнозирование ее состояния в будущем;

4) разработка физической модели корпоративной сети (параметрический синтез). На стадии физического моделирования проектировщик должен точно описать, какие компоненты нужны, в каком количестве, где они будут расположены, и как эти компоненты будут соединяться друг с другом в

корпоративную сеть;

5) моделирование и оптимизация корпоративной сети. Моделирование производится 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. Оценка эффективности работы сети (или тестирование сети) предполагает использование технических, организационных и программных решений и полностью согласуется со схемой администрирования системы. Оценка эффективности сети осуществляется в реальном режиме времени и может быть реализована с помощью встроенных инструментальных средств операционной системы и с помощью специальных программ типа анализаторов сети;

8) сопровождение и эксплуатация корпоративной сети. Этот этап не имеет четко определенных временных границ, а представляет собой непрерывный процесс.

1.3 Возможные топологии компьютерных сетей и их сравнение.

Топология сети – геометрическая форма и физическое расположение компьютеров по отношению друг к другу. Топология сети дает возможность сравнивать и классифицировать различные сети. Существует три основных вида топологии:

1) звезда;
2) кольцо;
3) шина.

В случае построения сети по шинной схеме каждый компьютер присоединяется к общему кабелю, на концах которого устанавливаются заглушки (терминаторы).

Сигнал проходит по сети последовательно через каждый компьютер, отражаясь от конечных терминаторов. Схема шинной топологии представлена на рисунке 1.3.

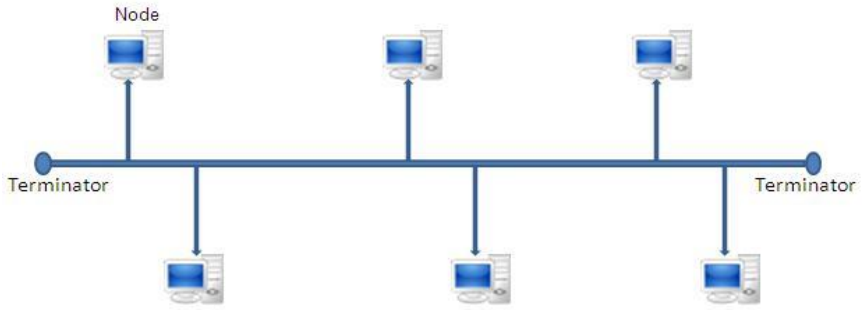

Рисунок 1.3 – Схема шинной топологии

Шина пропускает сигнал из одного конца сети к другому, при этом каждая рабочая станция проверяет адрес послания, и, если он совпадает с адресом рабочей станции, она его принимает. Если же адрес не совпадает, сигнал уходит дальше по линии. Если одна из подключённых рабочих станций не работает, это не окажет влияния на работу сети в целом, однако если соединение любой из подключенных машин нарушается из-за неисправности контакта в разъёме или обрыва кабеля, то весь сегмент сети (участок кабеля между двумя терминаторами) теряет целостность, что приводит к нарушению корректной работы всей сети.

Топология сети на основе шинной схемы имеет следующие достоинства:

- отказ любой из рабочих станций не оказывает влияние на дальнейшую работу всей сети;
- простота и гибкость соединений;
- низкая стоимость кабеля и разъемов;
- необходимо небольшое количество кабеля;
- простота прокладки кабеля.

Недостатками данной топологии являются:

- в случае разрыва кабеля или других неполадок в соединении может привести к неработоспособности всей сети;
- ограниченная длина кабеля и количество рабочих станций;
- сложность обнаружения дефектов соединений;
- низкая производительность;
- при большом объеме передаваемой информации главный кабель может не справляться с потоком данных, что в свою очередь приведет к задержкам.

Построение сети на основе кольцевой схемы представляет собой последовательное соединение компьютеров, но в отличие от шинной схемы последний компьютер соединён с первым. В данном случае сигнал проходит по кольцу от узла к узлу в одном направлении. Каждая рабочая станция сети работает как повторитель, усиливая сигнал и передавая его дальше. Поскольку сигнал проходит через каждую рабочую станцию, выход из строя или сбой в работе одной из них приведет к нарушению работы всей сети. Схема шинной топологии представлена на рисунке 1.4.

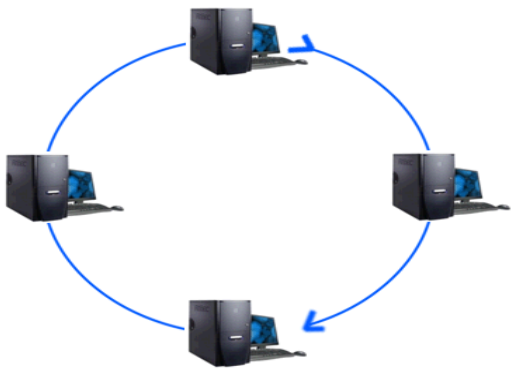

Рисунок 1.4 – Схема кольцевой топологии

Одной из базовых видов топологий является топология вида «Звезда». Она представляет собой схему соединения, в которой каждая рабочая станция подсоединена к сети при помощи отдельного кабеля. Один конец кабеля соединяется с гнездом сетевого адаптера компьютера, другой подсоединяется к центральному устройству, называемому концентратором (hub). Схема топологии вида «Звезда» представлена на рисунке 1.5.

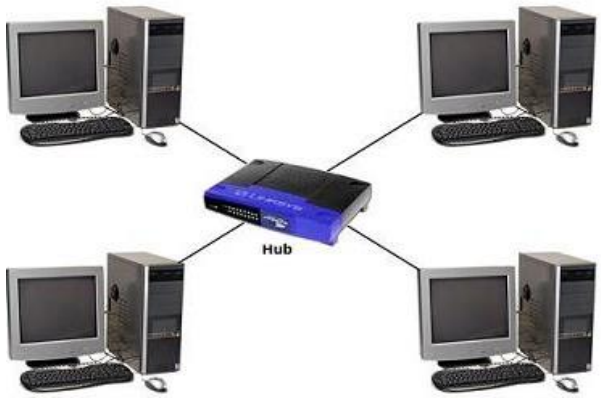

Рисунок 1.5 – Схема топологии вида «Звезда»

Прокладывать сеть топологии вида «Звезда» несложно и дешево. Количество рабочих станций, которые можно подключить к концентратору, зависит от числа портов на концентраторе, но имеются ограничения по числу узлов (максимум 1024). Рабочая группа, построенная по данной схеме, может работать независимо или может быть связана с другими рабочими группами.

Топология сети на основе схемы вида «Звезда» имеет следующие достоинства:

- подключение новых узлов не вызывает трудностей;
- возможность мониторинга сети;
- возможность централизованного управления сетью;
- при использовании централизованного управления сетью обнаружение дефектов соединений сильно упрощается;
- хорошая расширяемость и модернизация.

Недостатками данной топологии являются:

- отказ концентратора приводит к отключению всех узлов, подключенных к сети;
- требуется большое количество кабеля для реализации.

При комбинации базовых топологий можно получить новые виды топологий. Например, топология вида «Звезда-Шина», которая является комбинированной топологией. В ней несколько сетей построенных на топологии вида «Звезда» объединяются с помощью магистральной линейной шины.

В этом случае неисправность одного узла не повлечет за собой никакого влияния на сеть. Остальные рабочие станции по-прежнему будут взаимодействовать друг с другом. Нарушение работы концентратора приведет к остановке подключенных только к нему узлов и концентраторов. Схема топологии вида «Звезда-Шина» представлена на рисунке 1.6.

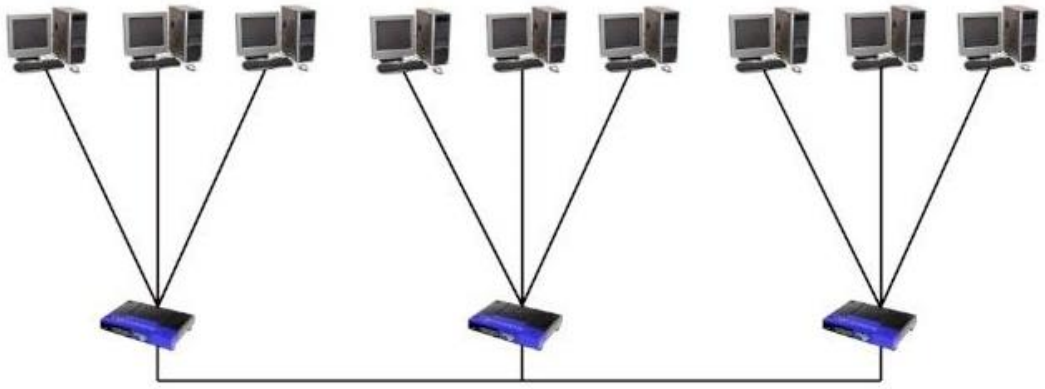

Рисунок 1.6 – Схема топологии вида «Звезда-Шина»

Нельзя не упомянуть о топологии вида «Дерево» (tree), которую можно рассматривать как комбинацию нескольких звезд. Такая топология может быть активной или пассивной. При активном дереве в центрах объединения линий связи находятся центральные рабочие станции. Схема топологии активного дерева представлена на рисунке 1.7.

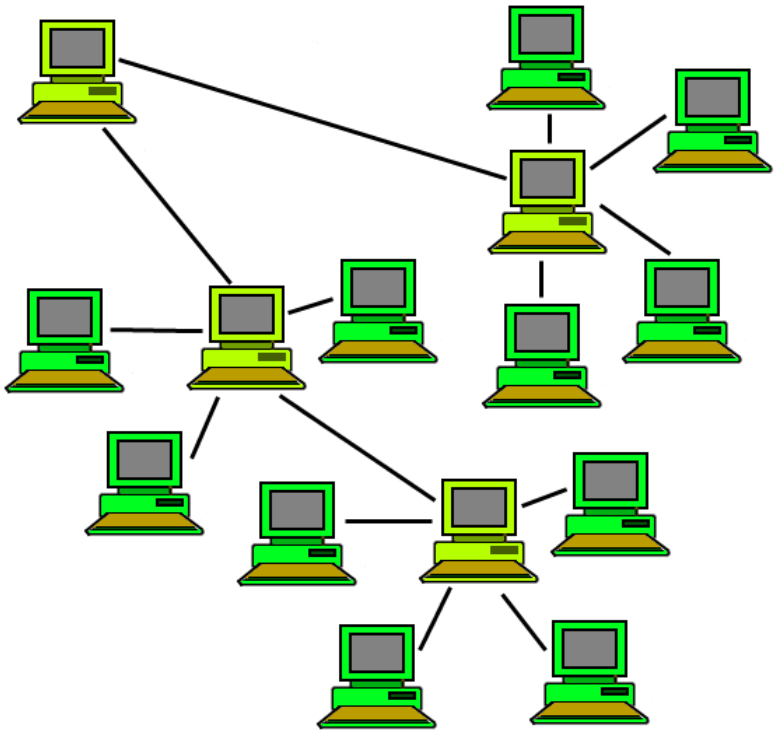

Рисунок 1.7 – Схема топологии активного дерева

Топология пассивного дерева отличается от активного тем, что в центрах объединения линий связи находятся не рабочие станции, а концентраторы. Схема топологии пассивного дерева представлена на рисунке 1.8.

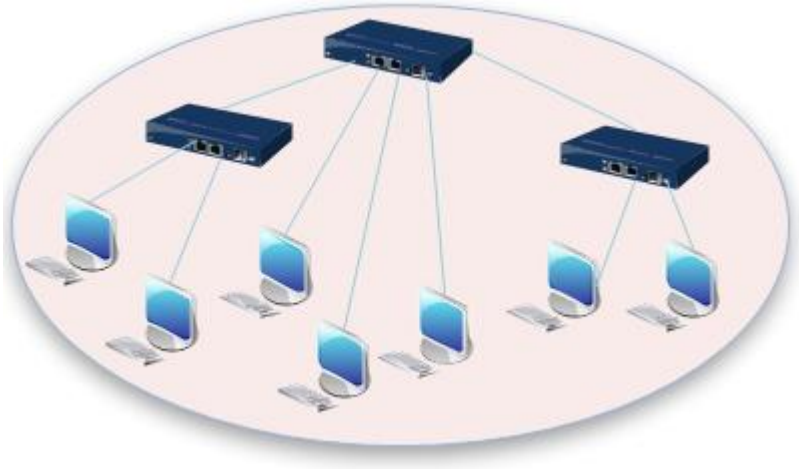

Рисунок 1.8 – Схема топологии пассивного дерева

Итак, топология сети определяет не только физическое расположение узлов, но и характер связей между ними, особенности передачи сигналов по сети. Именно характер связей определяет уровень отказоустойчивости сети, необходимую сложность сетевой аппаратуры, наиболее подходящий метод управления обменом, возможные типы сред передачи (каналов связи), допустимый размер сети (длина линий связи и количество абонентов), и много чего другого.

1.4 Технология виртуальных сетей VLAN

VLAN (Virtual Local Area Network) – это группа компьютеров, серверов и других сетевых ресурсов, трафик которой на канальном уровне полностью изолирован от других узлов. Это означает, что непосредственная передача кадров между разными виртуальными сетями невозможна, независимо от типа адреса. Внутри виртуальной сети кадры передаются в соответствии с технологией коммутации, т. е. только на тот порт, к которому приписан адрес назначения кадра.

В более широком понимании VLAN – это логическая («виртуальная») локальная компьютерная сеть, представляющая собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. Пример организации виртуальной локальной сети показан на рисунке 1.9.

Другими словами, физически сеть находятся в различных сегментах, но логически связана друг с другом. Распределенный по зданию персонал отдела,

объединенный в отдельную VLAN для совместного использования ресурсов, использует его как будто он подключен к одному общему сетевому сегменту.

Логическая группировка сетевых ресурсов в виртуальных локальных сетях освобождает сетевых администраторов от ограничений существующей сетевой топологии и кабельной инфраструктуры, и упрощает администрирование.

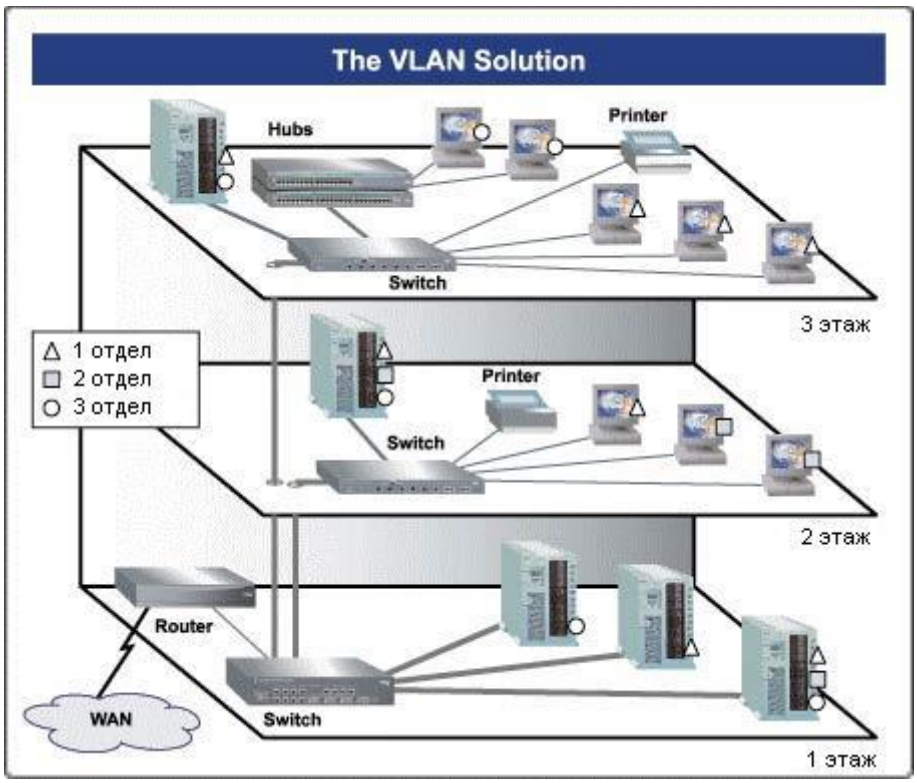

Рисунок 1.9 – Пример организации VLAN

Преимуществами технологии являются:

- гибкая сегментация. Другими словами это деление сети посредством сегментации более эффективно ограничивает распространение трафика между отдельными узлами по всей сети. Пользователи и ресурсы, наиболее часто взаимодействующие друг с другом, могут быть сгруппированы в общую виртуальную сеть, независимо от физического местоположения. Трафик каждой группы пользователей в значительной степени содержится в пределах виртуальных сетей, сокращая посторонний трафик в основной магистрали и улучшая производительность всей сети в целом;
- виртуальные сети на основе управляемого программного обеспечения (ПО) не требуют изменения существующей топологии и посещения комнат с коммуникационным оборудованием. Логические группировки позволяют быстро и легко изменять и реорганизовывать структуру сети с управляющей рабочей станции администратора сети;
- увеличение производительности. Виртуальные сети освобождают полосу пропускания в основной магистрали, ограничивая широковещательный

трафик от распространения по всей сети;

- более эффективное использование ресурсов сервера. Сетевой серверный адаптер с поддержкой VLAN, может принадлежать многим VLAN’нам, что уменьшает потребность в маршрутизации трафика к серверу и от него;
- расширение мер безопасности. Виртуальные сети создают виртуальные границы, которые могут пересекаться только при прохождении через маршрутизатор. Таким образом, стандартные технологии защиты, применяемые в маршрутизаторах, могут использоваться для ограничения доступа к различным виртуальным сетям.

1.5 Протокол динамической конфигурации узла DHCP

DHCP (Dynamic Host Configuration Protocol – протокол динамической конфигурации узла) – это сетевой протокол, при помощи которого компютеры могут автоматически получать IP-адреса и другие параметры, необходимые для работы в сетях TCP/IP. Для этого компьютер отправляет запрос к специальному серверу, называемому сервером DHCP. Сетевой администратор может задать диапазон IP-адресов, распределяемых между узлами. Это позволяет автоматизировать настройки рабочих станций сети и уменьшает риск появления ошибок. Протокол DHCP применяется во множинстве крупных (и не очень) сетей TCP/IP. Общая схема работы DHCP представлена на рисунке 1.10.

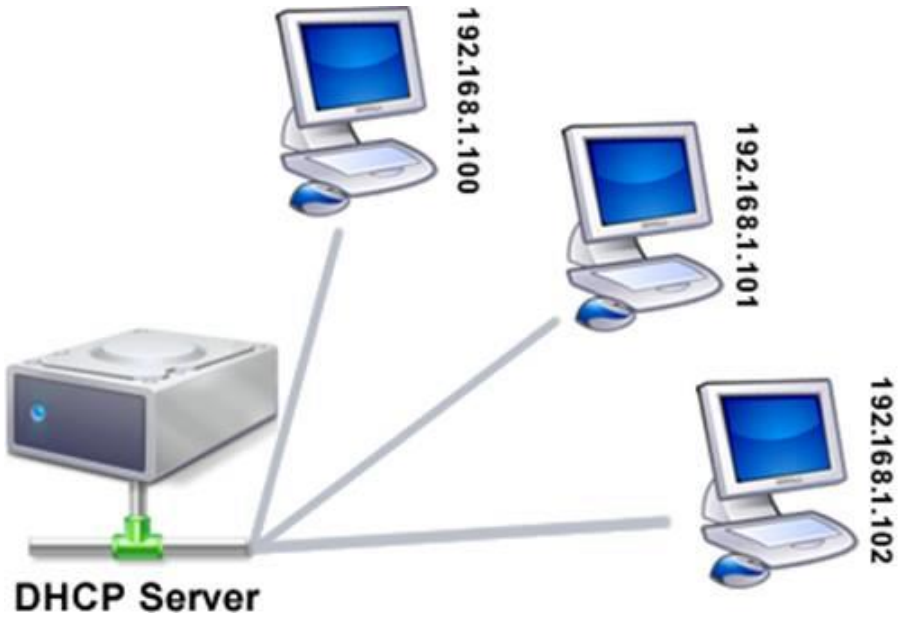

Рисунок 1.10 – Общая схема работы DHCP

Протокол DHCP предоставляет три способа распределения IP-адресов:

- ручное распределение. При этом способе сетевой администратор задает каждому компьютеру в сети определённый IP-адрес, привязывая его к MAC-адресу. Фактически, данный способ распределения адресов отличается от

ручной настройки каждого компьютера лишь тем, что сведения об адресах хранятся на сервере DHCP, и потому их легче изменять при необходимости;

- автоматическое распределение. При данном способе каждому узлу на постоянное использование выдается произвольный свободный IP-адрес из определённого администратором диапазона адресов;
- динамическое распределение. Этот способ похож на автоматическое распределение, за исключением того, что адрес выдаётся компьютеру не на постоянное пользование, а на некоторое время. Это называется арендой адреса. По истечении срока аренды IP-адрес вновь становится свободным, а клиент должен запросить новый.

Некоторые реализации службы DHCP способны автоматически обновлять записи DNS, соответствующие клиентским компьютерам, при выделении им новых адресов. Это производится при помощи протокола обновления DNS.

Рассмотрим процесс получения IP-адреса клиентом от сервера DHCP. Предположим, что клиент ещё не имеет собственного IP-адреса, но ему известен его предыдущий адрес – 192.168.1.101. Процесс состоит следующих этапов.

Первый этап – обнаружение DHCP. Сначала клиент выполняет широковещательный запрос по всей сети с целью обнаружить доступный DHCP-сервер. Он отправляет сообщение DHCPDISCOVER, при этом в качестве IP-адреса источника указывается 0.0.0.0 (так как компьютер ещё не имеет IP-адреса), а в качестве адреса назначения – широковещательный адрес 255.255.255.255.

Далее клиент заполняет несколько полей сообщения начальными данными. В поле xid помещается уникальный идентификатор транзакции, который позволяет отличать данный процесс получения IP-адреса от других, протекающих в это же время. В поле chaddr помещается MAC-адрес клиентской рабочей станции. В поле опций указывается последний известный клиенту IP-адрес. В данном примере это 192.168.1.101. Это необязательно и может быть проигнорировано сервером.

Сообщение типа DHCPDISCOVER может быть передано за пределы локальной физической сети при помощи специально настроенных агентов ретрансляции DHCP, перенаправляющих поступающие от клиентов сообщения DHCP серверам в других подсетях.

Второй этап – предложение DHCP. Получив сообщение от клиентского узла, сервер определяет конфигурацию клиента в соответствии с указанными сетевым администратором параметрами. В данном случае DHCP-сервер согласен с запрошенным клиентом адресом 192.168.1.101. Сервер отправляет ему ответ (сообщение типа DHCPOFFER), в котором предлагает конфигурацию узла. Предлагаемый клиенту IP-адрес указывается в поле yiaddr. Прочие параметры (такие, как адреса маршрутизаторов и DNS-серверов) указываются в виде опций в соответствующем поле.

Это сообщение сервер DHCP отправляет хосту пославшему DHCPDISCOVER на его MAC-адресс, при определенных обстоятельствах

может распространяться, как широковещательная рассылка. Клиент может получить сразу несколько различных предложений DHCP от разных серверов; из которых он должен выбрать то, которое его «устраивает».

Третий этап – запрос DHCP. Выбрав одну из предложенных конфигураций, клиент отправляет запрос DHCP (сообщение типа DHCPREQUEST). Он рассылается широковещательно, при этом к опциям, указанным клиентом в сообщении DHCPDISCOVER, добавляется специальная опция – идентификатор сервера, указывающая адрес DHCP-сервера, выбранного клиентом (в данном случае 172.16.1.1).

Четвертый этап – подтверждение DHCP. На данном этапе, сервер подтверждает запрос клиента и направляет это подтверждение (сообщение типа DHCPACK) ему. После этого клиент должен провести настройки своего сетевого интерфейса, используя предоставленные опции.

Пятый этап – отказ DHCP. Если после получения подтверждения (сообщение типа DHCPACK) от сервера клиент обнаруживает, что указанный сервером адрес уже кем-то зарезервирован, он рассылает широковещательное сообщение отказа DHCP (сообщение типа DHCPDECLINE), после чего процедура получения IP-адреса повторяется. Факт использования IP-адреса другим клиентом можно установить, выполнив запрос ARP.

Шестой этап – отмена DHCP. Если по каким-то причинам сервер не может предоставить клиенту запрошенный IP-адрес, или если аренда адреса удаляется администратором, сервер рассылает широковещательное сообщение отмены DHCP (сообщение типа DHCPNAK). При получении такого сообщения клиенту придется повторить процедуру получения IP-адреса.

Седьмой этап – освобождение DHCP. Клиент может явным образом прекратить аренду IP-адреса. Для этого он отправляет сообщение освобождения DHCP (сообщение типа DHCPRELEASE) тому серверу, который предоставил ему адрес в аренду. В отличие от других сообщений DHCP, сообщение типа DHCPRELEASE не рассылается широковещательно.

Восьмой этап – информация DHCP. Сообщение информации DHCP (DHCPINFORM) предназначено для определения дополнительных параметров TCP/IP (например, адреса маршрутизатора по умолчанию, DNS-серверов и т. п.) теми клиентами, которые не нуждаются в динамическом IP-адресе (то есть адрес которых настроен вручную). Серверы отвечают на такой запрос сообщением подтверждения (DHCPACK) без выделения IP-адреса.

1.6 Сетевой протокол SSH

SSH (Secure Shell – «безопасная оболочка») – сетевой протокол сеансового уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов). Схож по функциональным возможностям с протоколом Telnet, но, в отличие от него, шифрует весь передаваемый трафик, включая

пароли. SSH предоставляет возможность выбора различных алгоритмов шифрования.

SSH позволяет безопасно передавать через незащищенную среду практически любой другой сетевой протокол. Таким образом, можно не только удаленно выполнять работу на компьютере через командную оболочку, но и передавать по зашифрованному каналу потоки видео и звука (к примеру, с веб-камеры). Также SSH может сжимать передаваемые данные для последующего их шифрования. На рисунке 1.11 изображена общая схема использования SSH-протокола.

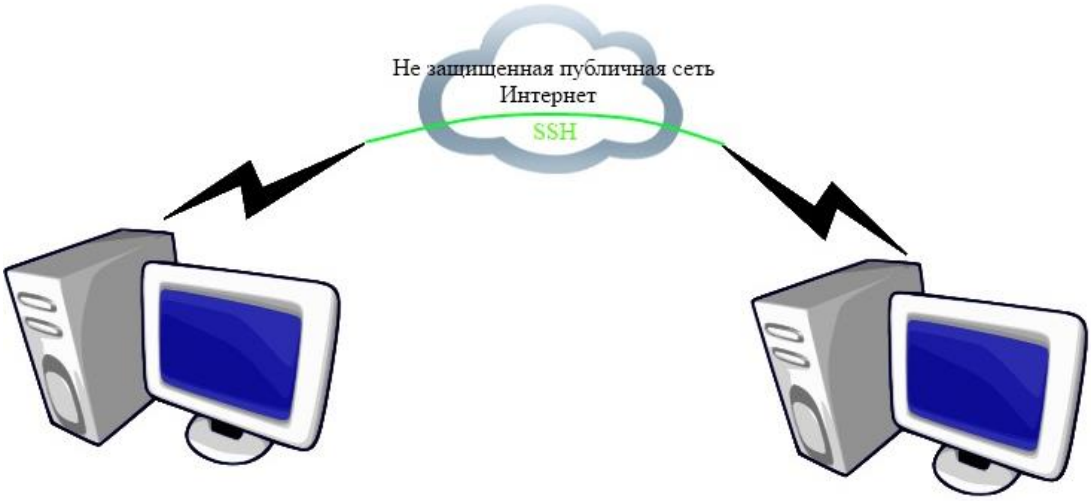

Рисунок 1.11 – Общая схема использования SSH

Для аутентификации сервера в SSH используется протокол аутентификации сторон на основе алгоритмов электронно-цифровой подписи (ЭЦП) RSA или DSA. Для аутентификации клиента также может использоваться ЭЦП RSA или DSA, но допускается также аутентификация при помощи пароля и даже ip-адреса хоста. Аутентификация по паролю наиболее распространена; она безопасна, так как пароль передается по зашифрованному виртуальному каналу (VPN). Аутентификация по ip-адресу наиболее небезопасна, эту возможность чаще всего исключают. Для создания общей секретности (сеансового ключа) используется алгоритм Диффи – Хеллмана (DH). Для шифрования передаваемых данных используется симметричные алгоритмы шифрования, такие как AES, Blowfish или 3DES.

Для сжатия данных может использоваться алгоритм LempelZiv (LZ77), который обеспечивает такой же уровень сжатия, что и архиватор ZIP. Сжатие SSH включено на опциональной основе.

Для создания VPN сетей используется так называемая технология SSH-туннелирования. SSH-туннель – это туннель, создаваемый посредством SSH-соединения и используемый для шифрования туннелированных данных. Используется для безопасной передачи данных в Интернете. Особенность состоит в том, что незашифрованный трафик какого-либо протокола шифруется на одном конце SSH-соединения и расшифровывается на другом.

Реализация SSH-туннеля может выполняться несколькими способами:

- использованием приложений, умеющих работать через SSH-туннель;
- созданием VPN-туннеля, подходит практически для любых приложений;
- если приложение работает с одним определённым сервером, можно настроить SSH-клиент таким образом, чтобы он пропускал через SSH-туннель TCP-соединения, приходящие на определённый TCP-порт рабочей станции, на которой запущен SSH-клиент. Например, клиенты терминального сервера подключаются по умолчанию на порт 3389. Тогда, чтобы настроить подключение к серверу через SSH-туннель, SSH-клиент конфигурируется на перенаправление подключений с любого порта локальной машины (например порт 5000) на удалённый сервер (например, server1.com и порт 3389). В данном случае клиент настраивается на подключение к серверу localhost (если SSH-клиент запущен на той же машине что и терминальный клиент) и порт 5000.

Преимущества этой технологии создания VPN сетей заключаются в том, что для реализации не нужно устанавливать и настраивать дополнительное программное обеспечение. Так же следует отметить, что настройка проходит намного проще, чем у любой другой схожей технологии. Эта технология, пусть немного и уступает по производительности, но для создания защищенных сетей подходит больше чем протокол IPsec, так как по масштабируемости и легкости настраивания каналов он в разы превосходит его.

1.7 Протокол динамической маршрутизации OSPF

OSPF (Open Shortest Path First) – это открытый протокол маршрутизации, базирующийся на алгоритме поиска наикратчайшего пути. OSPF имеет две основные характеристики: протокол является открытым и он базируется на алгоритме SPF. Алгоритм SPF иногда называют алгоритмом Дейкстры по имени его автора.

OSPF – иерархический протокол маршрутизации с объявлением состояния о канале соединения (link-state). Он был создан как протокол работы внутри сетевой области – AS (Autonomous System), которая представляет собой группу маршрутизаторов и сетей, объединенных по принципу иерархии и находящихся под единым управлением 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 при помощи обмена сообщениями о состояниях канала соединений между маршрутизаторами и сетями области LSA (link-state advertisement). 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 определяют наикратчайший путь к каждому узлу, используя алгоритм Дейкстры. Расчет наикратчайшего 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.

OSPF предлагает решение следующих задач:

- увеличение скорости сходимости (в сравнении с протоколом RIP2, т.к. нет необходимости выжидания многократных таймаутов по 30с);
- поддержка сетевых масок переменной длины (VLSM);
- достижимость сети (быстро обнаруживаются отказавшая аппаратура, и топология сети изменяется соответствующим образом;
- оптимальное использование пропускной способности (т.к строится минимальный остовный граф без ребер по алгоритму Дейкстры);
- метод выбора пути.

Теперь рассмотрим принцип работы протокола OSPF, который состоит из пяти этапов.

На первом этапе каждый маршрутизатор в сети определяет своих соседей и на всех интерфейсах изучает их. Изучив соседей, каждый из этих маршрутизаторов, заносит полученную информацию в таблицу «соседей» (Рисунок 1.12).

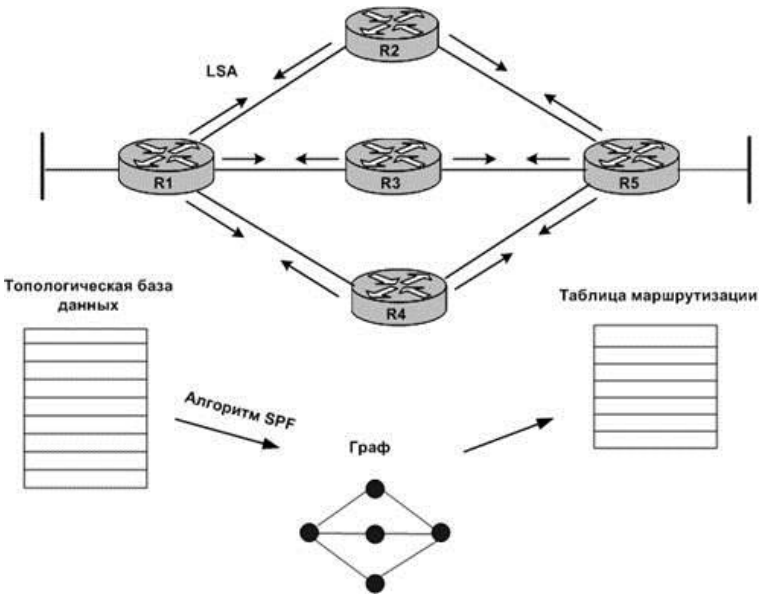

Рисунок 1.12 – Изучение своих соседей

На втором этапе каждый маршрутизатор, используя LSA, строит топологическую базу данных состояния каналов (Рисунок 1.13), 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.

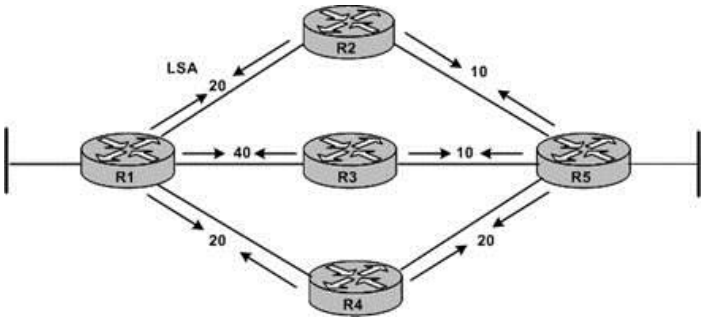

Рисунок 1.13 – Построение топологической таблицы

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.

На третьем этапе, как только маршрутизаторы OSPF соберут информацию о состоянии каналов, они начинают вычислять кратчайший путь к каждой сети (Рисунок 1.14). 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.

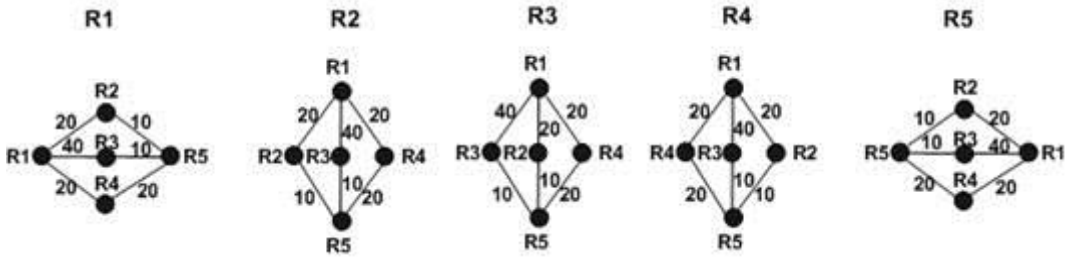

Рисунок 1.14 – Вычисление наикратчайшего пути

На четвертом этапе из построенного дерева к сетям назначения выбираются пути с наименьшей стоимостью и помещаются в таблицу маршрутизации (Рисунок 1.15). 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.

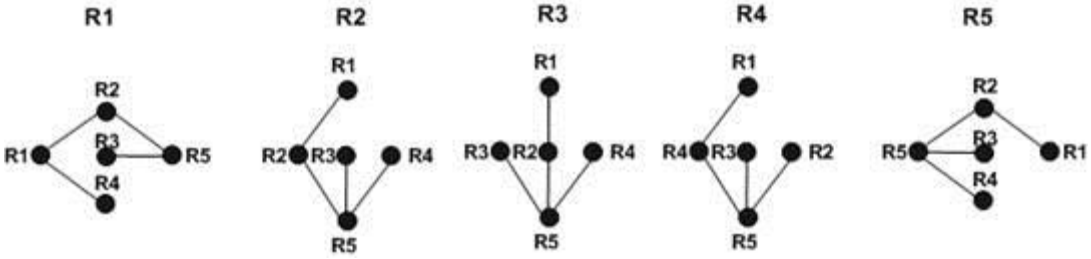

Рисунок 1.15 – Выбор пути с наименьшей стоимостью

На пятом этапе, 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 1.16). 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.

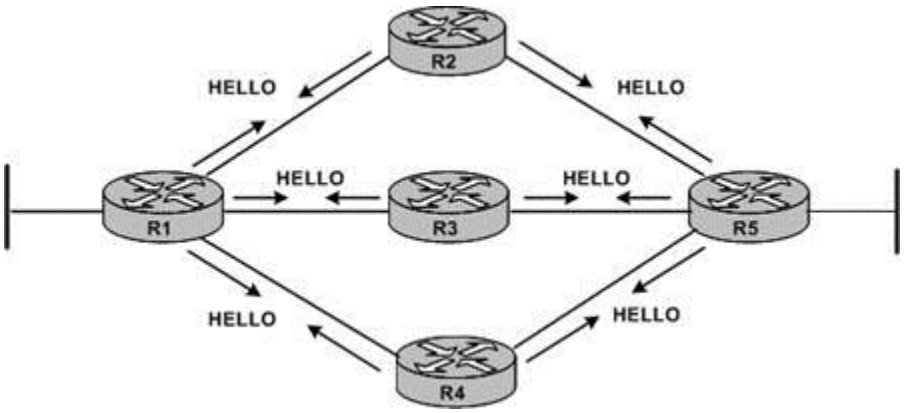

Рисунок 1.16 – Контроль состояния связей

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 1.17). Одновременно маршрутизатор ретранслирует объявление каждому из своих ближайших соседей (кроме того, от которого он получил это объявление).

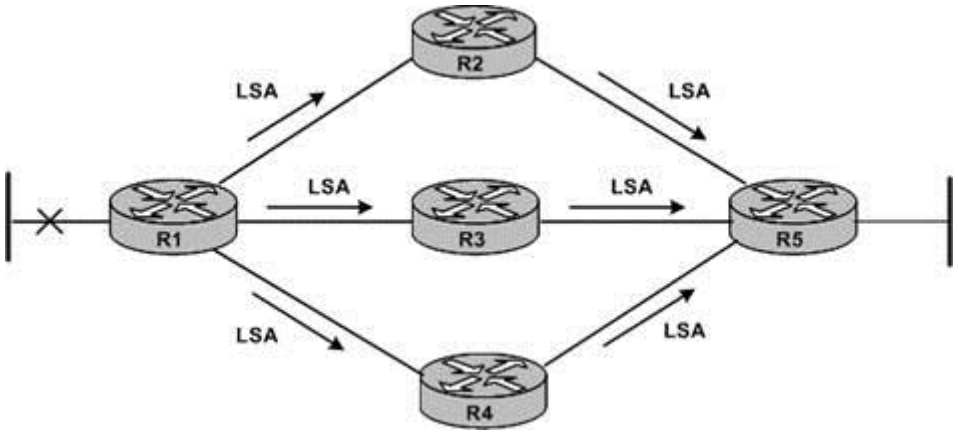

Рисунок 1.17 – Повторный поиск оптимального маршрута

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.

Разобравшись с принципом работы протокола OSPF, следует оговорить его плюсы и минусы.

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.).

1.8 Протокол мониторинга трафика сети NetFlow

NetFlow – проприетарный открытый протокол, разработанный Cisco для мониторинга трафика в сети. NetFlow предоставляет возможность анализа сетевого трафика на уровне сеансов, делая запись о каждой транзакции TCP/IP. Архитектура системы строится на сенсоре, коллекторе и анализаторе.

Сенсор собирает статистику по проходящему через него трафику. Сенсоры имеет смысл ставить в «узловых точках» сети, например, на граничных маршрутизаторах сегментов сети.

Коллектор осуществляет сбор информации от сенсоров. Полученные данные он сбрасывает в файл для дальнейшей обработки. Различные коллекторы сохраняют данные в различных форматах.

Анализатор, или система обработки, считывает эти файлы и генерирует отчеты в форме, более удобной для человека. Эта система должна быть совместима с форматом данных, предоставляемых коллектором. В современных системах коллектор и анализатор часто объединены в одну систему.

Обычно коллектор и анализатор являются частями одного программного комплекса, работающего на сервере. Разновидностей ПО коллектор/анализатор множество, платные и бесплатные, под Windows и Unix-системы. Нужно сразу уяснить, что коллектор и стоящий за ним анализатор являются «пассивными» элементами системы. Сенсор шлет на коллектор отчеты о трафике, коллектор принимает, анализатор анализирует, и заполняет свою базу данных на сервере. Пока сенсор шлет отчеты, коллектор их принимает, анализатор регистрирует.

Как правило, коллектор слушает порт 2055, 9555 или 9995 (или тот, который был указан при настройке коллектора и сенсора).

Сенсор выделяет из проходящего трафика потоки, характеризуемые следующими параметрами:

- адрес источника;
- адрес назначения;
- порт источника для UDP и TCP;
- порт назначения для UDP и TCP;
- тип и код сообщения для ICMP.

Потоком считается набор пакетов, проходящих в одном направлении. Когда сенсор определяет, что поток закончился (по изменению параметров пакетов, либо по сбросу TCP-сессии), он отправляет информацию в коллектор.

2 Техническая часть.

2.1 Место реализации проекта

Компания “Фаворит” одна из успешных компаний на территории города Талдыкорган, занимающаяся дистрибьюцией продукции Procter & Gamble, Gillette и прочих компаний. Основным ассортиментом предприятия является мыломоющая продукция и средства личной гигиены. Предприятие осуществляет продажи продукции как в городе Талдыкорган, так и в близлежащих населённых пунктах. В распоряжении предприятия находятся два здания: главный офис и филиал.

Разработка корпоративной сети между главным офисом предприятия “Фаворит” и его филиалом актуальна социальным эффектом. Социальным эффектом внедрения корпоративной сети на предприятии является:

- повышение скорости передачи данных и оперативности выполнения приказов;
- повышение качества труда;
- уменьшение затрат рабочего времени для передачи документов между главным офисом и филиалами;
- улучшится взаимодействие между специалистами предприятия;
- улучшение качества управления персоналом и специалистами среднего звена, например, при получении того или иного приказа информация мгновенно будет доводиться до специалистов.

2.2 Разработка структурной схемы организации сети

На территории компании “Фаворит”, где расположен главный офис, находятся два здания. В здании офиса два этажа, на каждом из которых установлен коммутатор, к которому подключены компьютеры из разных отделений.

На первом этаже к первому коммутатору подключены рабочие станции из таких подразделений, как отдел кадров, технический отдел, отдел закупок и продаж, а также отдел маркетинга. Топология сети первого этажа представлена на рисунке 2.1.

На втором этаже ко второму коммутатору подключены рабочая станция отдела финансов и компьютеры из кабинетов директора предприятия и его заместителя. Топология сети второго этажа представлена на рисунке 2.2.

Во втором здании на территории главного офиса предприятия к коммутатору подключены рабочие станции из двух складских помещений. Топология сети второго здания представлена на рисунке 2.3.

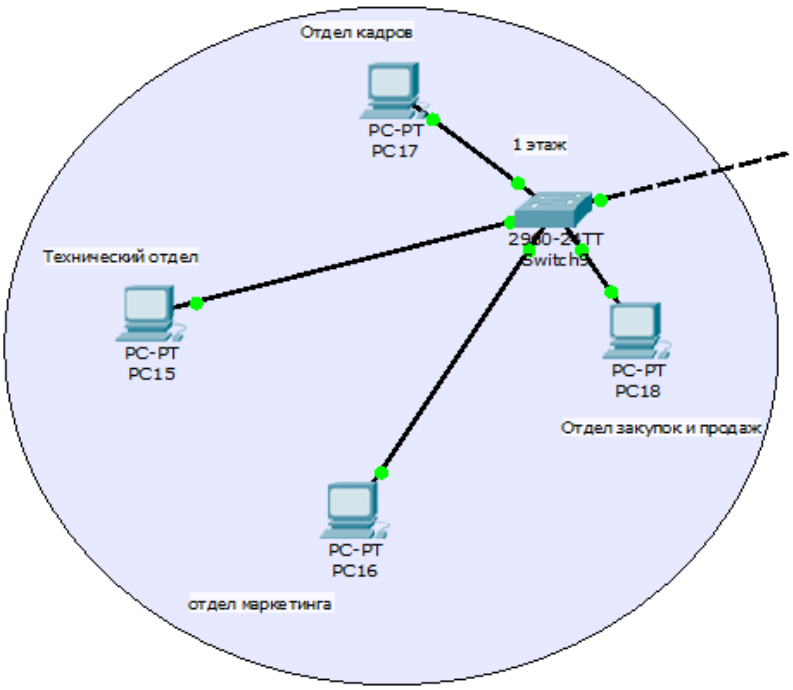

Рисунок 2.1 – Топология сети первого этажа

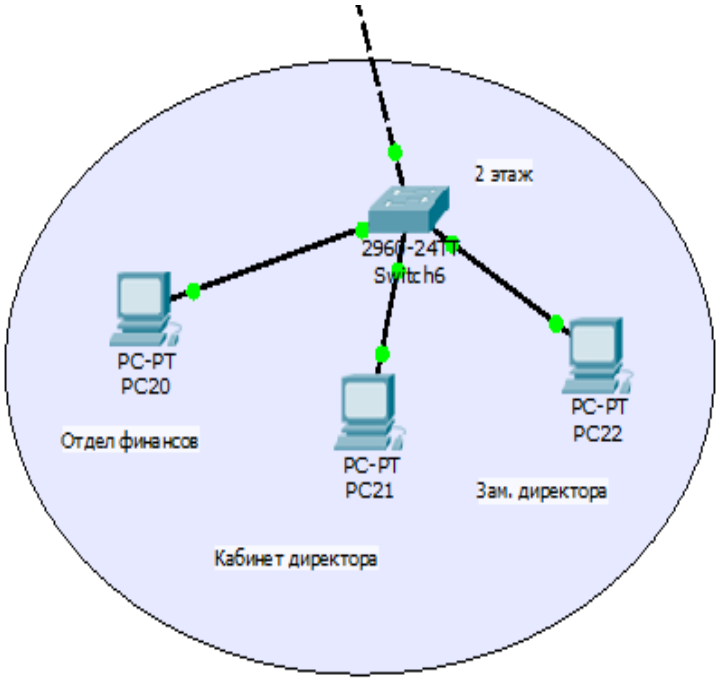

Рисунок 2.2 – Топология сети второго этажа

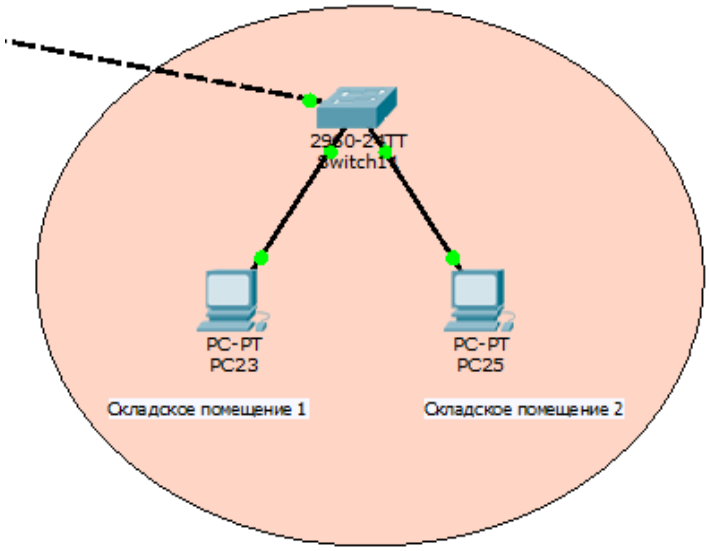

Рисунок 2.3 – Топология сети второго здания на территории главного офиса предприятия

Коммутаторы всех этажей здания главного офиса и здания отведенного под складские помещения подключены к коммутатору третьего уровня, к которому, в свою очередь, подключен DHCP-сервер. DHCP-сервер служит нам для автоматической раздачи IP-адресов рабочим станциям. Для этого сервер был сконфигурирован на раздачу адресов из заданного диапазона.

Затем коммутатор третьего уровня подключается к маршрутизатору принадлежащему главному офису. Маршрутизатор главного офиса подключен к модему, которых отвечает за сеть провайдера. Данная топология представлена на рисунке 2.4.

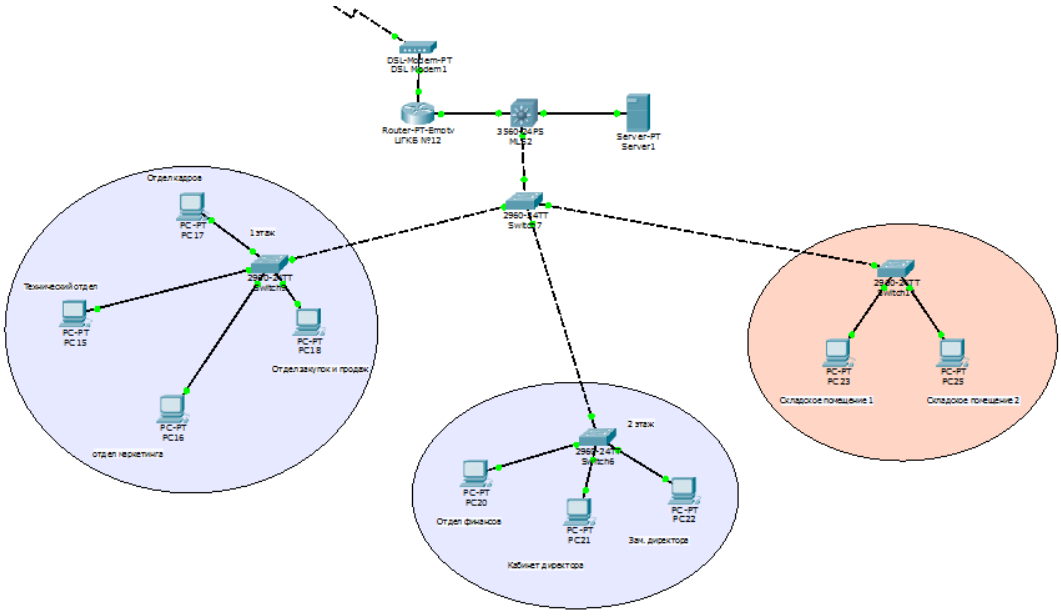

Рисунок 2.4 – Архитектура локальной сети главного офиса предприятия и здания отведенного под складские помещения.

В филиале предприятия одно двухэтажное здание. Архитектура локальной сети филиала схожа с архитектурой сети в главном офисе. Отличие заключается в том, что компьютеров, подключенных к коммутаторам на каждом этаже, меньше и различие в отделениях. На рисунке 2.5 показана полная архитектура локальной сети филиала предприятия “Фаворит”.

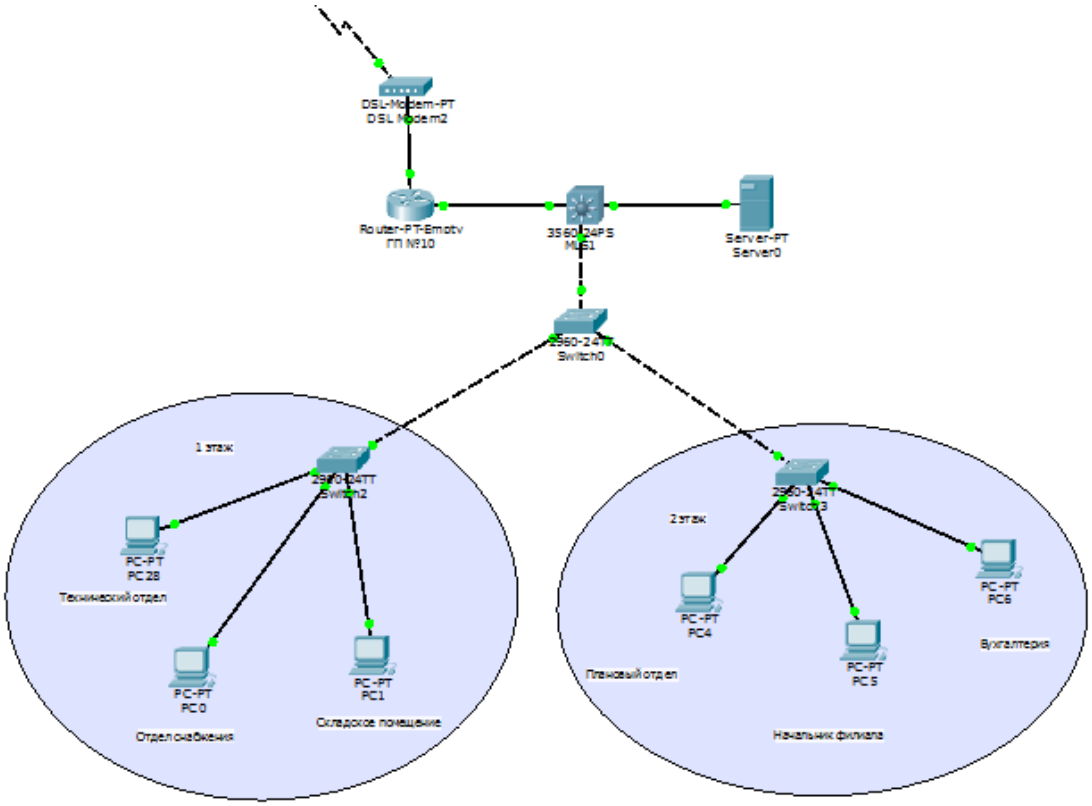

Рисунок 2.5 – Архитектура локальной сети филиала предприятия “Фаворит”

При построении сети для организации взаимодействия между главным офисом предприятия и филиалом был выбран способ предполагающий аренду каналов связи у провайдера. Из-за большого расстояния между главным офисом и филиалом предприятия прокладка кабеля не выгодна.

В качестве провайдера была выбрана компания ASTEL, занимающая лидирующую позицию на казахстанском рынке телекоммуникаций в наши дни. Основной деятельностью компании является построение корпоративных сетей передачи данных и голоса на базе современных технологий.

Выбор интернет-провайдера – важный и ответственный процесс. Ведь от правильности выбора зависит то, насколько удобно будет пользоваться Сетью и насколько эффективной будет работа и качественной выбранная услуга.

Используя оборудование ведущих мировых производителей, ASTEL предлагает своим клиентам широкий спектр высококачественных услуг, в числе которых: спутниковые коммуникации и беспроводной доступ, телерадиовещание и телефония, доступ в Интернет, а также разработка и реализация проектов любой сложности.

На рисунке 2.6 показана общая схема корпоративной сети между главным офисом и филиалом предприятия “Фаворит” через сеть провайдера.

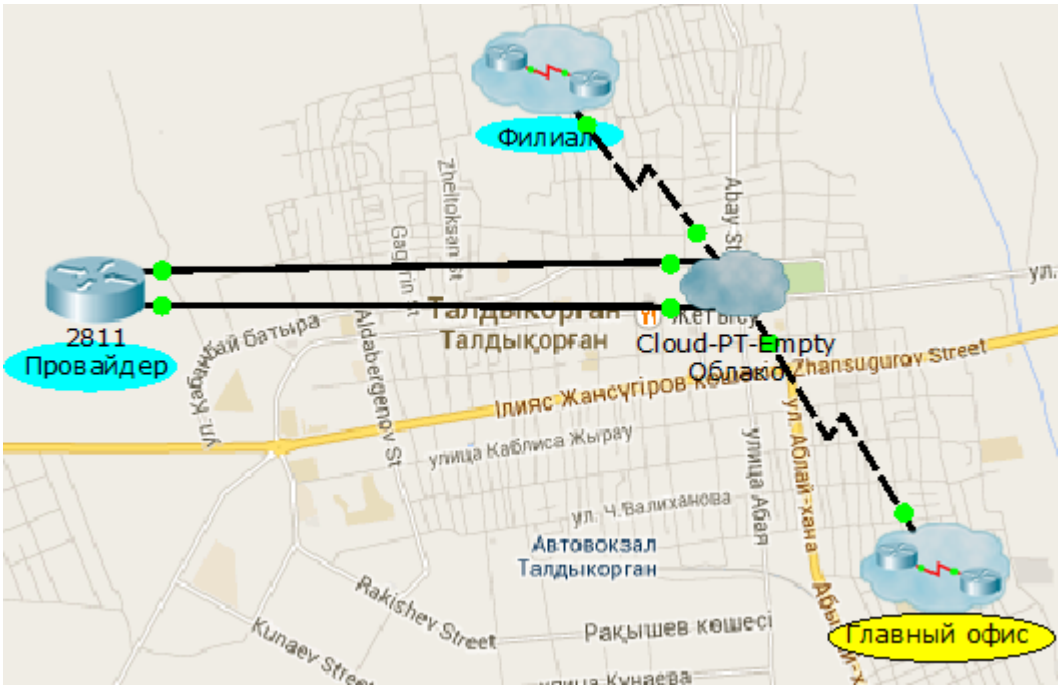

Рисунок 2.6 – Общая схема корпоративной сети между главным офисом и филиалом предприятия “Фаворит”

2.2 Планирование IP-адресаций

Планирование IP-адресаций указано в таблицах 2.1 – 2.7.

Т а б л и ц а 2.1 – IP-адресация на территориях предприятия

Подразделение предприятия	IP-адрес
Главный офис	192.168.1.0
Филиал	192.168.2.0

Т а б л и ц а 2.2 – IP-адресация в главном офисе

Подсети	IP-адрес/Маска	Шлюз
1 этаж в главном офисе	192.168.1.2 – 32/27	192.168.1.1
2 этаж в главном офисе	192.168.1.34 – 64/27	192.168.1.33
2-ое здание на территории главного офиса	192.168.1.66 – 96/27	192.168.1.65

Т а б л и ц а 2.3 – IP-адресация в филиале

Подсети	IP-адрес/Маска	Шлюз
1 этаж	192.168.3.2 – 32/27	192.168.3.1
2 этаж	192.168.3.34 – 64/27	192.168.3.33

Т а б л и ц а 2.4 – IP-адресация серверов в здании главного офиса и филиале

Территория	IP-адрес/Маска	Шлюз
Главный офис	172.16.0.1/30	172.16.0.2
Филиал	172.16.1.1/30	172.16.1.2

Т а б л и ц а 2.5 – IP-адресация маршрутизатора и коммутатора третьего уровня в филиале

Оборудование	IP-адрес/Маска
Маршрутизатор	192.168.0.1/27 1.1.1.2/27 1.2.1.2/27
Коммутатор третьего уровня	192.168.0.2/27

Т а б л и ц а 2.6 – IP-адресация маршрутизатора и коммутатора в главном офисе предприятия

Оборудование	IP-адрес/Маска
Маршрутизатор	192.168.2.1/27 1.1.2.2/27
Коммутатор третьего уровня	192.168.2.2/27

Т а б л и ц а 2.7 – Планирование IP-адресации провайдера

Провайдер	IP-адрес/Маска
ASTEL	1.1.1.1/27

2.3 Настройка SSH-протокола на маршрутизаторах и коммутаторах третьего уровня

SSH (Secure SHell) – сетевой протокол сеансового уровня, используется для удалённого управления узлами и другим оборудованием, а также для туннелирования TCP-соединений, для просмотра, редактирования и передачи файлов, шифрует все передаваемые данные.

Далее будет показана настройка SSH-протокола на маршрутизаторе в филиале предприятия “Фаворит”.

Входим в привилегированный режим

```
router>enable
```

Настроим нужные параметры для генерации ключа используемого ssh. Сначала войдем в режим конфигурации

```
cisco#conf t
```

Устанавливаем домен

```
router(config)#ip domain name RouterF
```

Устанавливаем имя роутера

```
router(config)#hostname RouterF
```

Генерируем RSA ключ для SSH

```
RouterF(config)#crypto key generate rsa
```

Устанавливаем версию протокола SSH

```
RouterF(config)#ip ssh version 2
```

Устанавливаем число попыток подключения по SSH

```
RouterF(config)#ip ssh authentication-retries 3
```

Устанавливаем хранение пароли в зашифрованном виде

```
RouterF(config)#service password-encryption
```

Включаем протокол Mod1

```
RouterF(config)#mod1 new-model
```

Создаем пользователя admkick с паролем adk1 и максимальными уровнем привелегий 15

```
RouterF(config)#username admkick 15 secret adk1
```

Устанавливаем пароль ticktack для привилегированного режима

```
RouterF(config)#enable secret ticktack
```

Входим в режим настройки терминальных линий

```
RouterF(config)#line vty 0 4
```

Даем доступ только по протоколу SSH

```
RouterF(config-line)#transport input ssh
```

Включим logging synchronous, после чего маршрутизатор начнет дожидаться завершения текущей команды и вывода ее отчета

```
RouterF(config-line)#logging synchronous
```

Даем доступ в привилегированный режим

```
RouterF(config-line)#privilege level 15
```

Выходим из режима настройки

```
RouterF(config-line)#end
```

Сохраняем настройки

```
RouterF(config-line)#wr mem
```

Далее тем же способом настраиваем SSH-протокол на остальных маршрутизаторах и коммутаторах третьего уровня.

2.4 Настройка протокола OSPF

Реализация протокола OSPF выполняется на маршрутизаторе провайдера, на маршрутизаторах и коммутаторах третьего уровня всего предприятия.

Для начала настроим маршрутизатор провайдера. Перейдем на роутер провайдера и в режиме глобальной конфигурации введем следующую команду

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

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

Далее входим в меню режима глобальной конфигурации на настройку протокола OSPF

```
RouterPR(config-router)#
```

Теперь здесь необходимо указать все непосредственно подключенные сети. Если указать не подключенную сеть, то она не войдет в рассылаемую информацию о сетях этим маршрутизатором

```
RouterPR(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, на маршрутизаторах единой области он должен быть идентичен

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

И по аналогии на маршрутизаторах данной схемы необходимо указать все непосредственно подключенные сети.

Тип сети, в которой работает протокол можно посмотреть с помощью команды

```
RouterPR#show ip ospf interface
```

После слова interface нужно прописать название интерфейса, например

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

Вывод команды

```
FastEthernet 0/0 is up, line protocol is up
 Internet address is 1.1.1.1/27, 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) 192.168.1.1, 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 30, Wait 30,
Retransmit 5
 Hello due in 00:00:04
 Index 1/1, flood queue length 1
 Next 0x0(0)/0x0(0)
 Last flood scan length is 2, maximum is 2
 Last flood scan time is 1 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 на маршрутизаторе RouterPR

```
hostname RouterPR
!
!
!
!
Spanning tree mode pvts
!
interface FastEthernet 0/0
 ip address 1.1.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan1
```

```
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 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 на маршрутизаторе RouterMO

```
hostname RouterMO
!
!
enable secret 5 $1$mERr$H/ic/D4UjHfGhTMLIm1rWfl/
!
aaa new-model
!
User name admin privilege 15 secret 5
$1$moRr$bWAtFYbcGSVsPV8Bnttlfd0
!
ip ssh version 2
ip ssh authentication retries 2
ip domain name RouterMO
!
interface Serial0/0
 no ip address
 shutdown
!
interface Serial0/0
 no ip address
 shutdown
!
interface FastEthernet 1/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet 2/0
 ip address 1.1.1.2 255.255.255.0
 duplex auto
```

```
 speed auto
!
!
interface FastEthernet 5/0
 no ip address
 duplex auto
 speed auto
 no shutdown
!
router ospf 1
 log-adjacency-changes
 network 1.1.2.0 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 ssh 2
 privilege level 15
!
end
```

Конфигурация на коммутаторе третьего уровня MLS-1

```
hostname MLS-1
!
enable secret 5 $1$mERr$H/ic/De9FUjHzRMLImhzrWfl/
!
Mod1 new-model
!
ip route
!
username admkick privilege 15 secret 5
$1$tERr$bSEtFYbc7aSVGPV8Rnflfd0
!
ip ssh v 2
ip ssh authentication retries 2
ip domain name MLS-1
!
spanning-tree mode pvst
spanning-tree vlan 1-900 priority 0
!
interface FastEthernet 0/1
 no switchport
```

```
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet 0/2
 no switchport
 ip address 172.16.1.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet 0/3
!
interface FastEthernet 0/4
!
interface FastEthernet 0/5
!
interface FastEthernet 0/6
!
interface FastEthernet 0/7
!
interface FastEthernet 0/8
!
interface FastEthernet 0/9
!
interface FastEthernet 0/10
!
interface FastEthernet 0/11
!
interface FastEthernet 0/12
!
interface FastEthernet 0/13
!
interface FastEthernet 0/14
!
interface FastEthernet 0/15
!
interface FastEthernet 0/16
!
interface FastEthernet 0/17
!
interface FastEthernet 0/18
!
interface FastEthernet 0/19
!
interface FastEthernet 0/20
!
interface FastEthernet 0/21
!
interface FastEthernet 0/22
!
interface FastEthernet 0/23
!
```

```
interface FastEthernet 0/24
!
interface GigabitEthernet 0/1
!
interface GigabitEthernet 0/2
!
interface Vlan 1
 no ip address
 shutdown
!
interface Vlan 10
 ip address 192.168.3.1 255.255.255.224
 ip helper-address 172.16.1.1
!
interface Vlan 20
 ip address 192.168.3.33 255.255.255.224
 ip helper-address 172.16.1.1
!
interface Vlan 30
 ip address 192.168.3.65 255.255.255.224
 ip helper-address 172.16.1.1
!
interface Vlan 40
 ip address 192.168.3.97 255.255.255.224
 ip helper-address 172.16.1.1
!
router ssh 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 на маршрутизаторе RouterF

```
hostname RouterF
!
```

```
!
!
!
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 RouterF
!
interface Serial0/0
 no ip address
 shutdown
!
interface Serial1/0
 no ip address
 shutdown
!
interface FastEthernet 2/0
 ip address 192.168.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet 3/0
 ip address 1.1.1.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet 4/0
 ip address 1.2.1.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet 5/0
 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 на коммутаторе третьего уровня MLS-2

```
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 FastEthernet 0/1
 no switchport
 ip address 192.168.0.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet 0/2
 no switchport
 ip address 172.16.0.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet 0/3
!
interface FastEthernet 0/4
!
interface FastEthernet 0/5
!
```

```
interface FastEthernet 0/6
!
interface FastEthernet 0/7
!
interface FastEthernet 0/8
!
interface FastEthernet 0/9
!
interface FastEthernet 0/10
!
interface FastEthernet 0/11
!
interface FastEthernet 0/12
!
interface FastEthernet 0/13
!
interface FastEthernet 0/14
!
interface FastEthernet 0/15
!
interface FastEthernet 0/16
!
interface FastEthernet 0/17
!
interface FastEthernet 0/18
!
interface FastEthernet 0/19
!
interface FastEthernet 0/20
!
interface FastEthernet 0/21
!
interface FastEthernet 0/22
!
interface FastEthernet 0/23
!
interface FastEthernet 0/24
!
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
```

Настройки коммутатора второго уровня в складском помещении

```
hostname Switch
!
!
!
!
spanning-tree mode pvst
spanning-tree vlan 1-1000 priority 8192
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/4
 switchport access vlan 20
```

```
 spanning-tree portfast
!
interface FastEthernet0/5
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/6
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/7
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/8
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/9
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/10
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/11
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/12
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/13
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/14
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/15
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/16
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/17
 switchport access vlan 20
```

```
 spanning-tree portfast
!
interface FastEthernet0/18
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/19
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/20
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/21
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/22
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/23
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/24
 switchport access vlan 20
 spanning-tree portfast
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface Vlan1
 no ip address
 shutdown
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```

Настройки маршрутизатора провайдера

```
Building configuration...
```

```
Current configuration : 853 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
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 1.1.1.1 255.255.255.0
 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 192.168.0.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.3.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.0.255 area 0
 network 172.16.1.0 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
```

2.5 Настройка протокола мониторинга трафика NetFlow

Сконфигурируем сенсор

```
RouterFIL# configure terminal
RouterFIL(config)# ip flow-export destination 192.168.1.2 9996
RouterFIL(config)# ip flow-export destination 10.10.1.2 9996
RouterFIL(config)# ip flow-export version 9
```

В режиме конфигурации указываем адреса коллектора и порты, куда будем перенаправлять статистику мониторинга, указываем версию протокола NetFlow. В сложноустроенной сети возможно иметь два интерфейса коллектора, если есть какие-либо ограничения на маршрутизацию между сегментами сети.

Устанавливаем частоту обновления кэша активной сессии NetFlow

```
RouterFIL(config)# ip flow-cache timeout active 1
!
```

Определяем время, на тот случай если в течение некоторого времени в существующем потоке не передаются данные. Поток будет закрываться и информация о нем записывается в кэш, а затем передается на коллектор

```
RouterFIL(config)# ip flow-cache timeout inactive 15
```

Настраиваем анализатор мониторинг интерфейса, VLAN и Port-channel

```
RouterFIL(config)# ip flow-export source FastEthernet 0/0
RouterFIL(config)# ip flow-export source vlan4
RouterFIL(config)# ip flow-export source Port-channel1.2
```

Добавим ACL для более гармоничной работы

```
!
ip access-list standard iacl-snmp
remark ACL for SNMP access to device
permit 192.168.1.2
permit 10.10.1.2
deny any log
!
```

Настраиваем snmp для правильного распознавания имен интерфейсов

```
!
snmp-server group snmp v1 access iacl-snmp
snmp-server group snmp v2c access iacl-snmp
snmp-server community ****** **** iacl-snmp
snmp-server ifindex persist
snmp-server trap-source Loopback0
snmp-server enable traps tty
!
```

Указываем, какой трафик будет учитываться, входящий в интерфейс или исходящий из него. Если исходящий, то ip flow egress, если входящий, то ip flow ingress

```
RouterFIL(config)# interface FastEthernet 0/0
RouterFIL(config-if)# ip flow egress
RouterFIL(config-if)# ip flow ingress
```

2.6 Описание и характеристики выбранного оборудования

2.6.1 Коммутатор Cisco Catalyst WS-C2960-24TT-L

Cisco Catalyst WS-C2960-24TT-L относится к серий коммутаторов 2960, и позволяет работать в сетях второго уровня, что повышает уровень их доступности.

Cisco WS-C2960-24TT-L поддерживает отличный интерфейс командной строки для тонкой настройки и программное обеспечение CiscoNetworkAssistant, предназначенное для быстрой настройки на основе предварительно установленных шаблонов. Кроме того, система сетевого управления CiscoWorks поддерживает коммутаторы CiscoCatalyst серий 2960 при управлении всей сетью организации.

В линейке Catalyst 2960, Cisco обеспечивает оптимальный уровень потребления электроэнергии, благодаря интеграции сервисов и непрерывному процессу внедрения инноваций, таких как технология CiscoEnergyWise. Средства поддержки этой технологии на коммутаторах Cisco Catalyst

позволяют обеспечить существенное снижение затрат на энергопитание и повысить устойчивость бизнеса.

Модели CiscoCatalyst серии 2960 с технологией PoE поддерживают новейшие устройства, включая IP-телефоны Cisco и точки доступа к беспроводной сети CiscoAironet, а также любые конечные устройства, совместимые с IEEE 802.3af, за счет обеспечения выходной мощности до 15,4 Вт на один порт.

Коммутаторы Cisco WS-C2960-24TT-L серии 2960 поддерживают технологии, которые позволяют предприятиям надежно защитить их сети, данные и ресурсы.

Все модели 2960 предоставляют интеллектуальные сервисы, обеспечивающие эффективность и слаженность работы. Ведущие в отрасли механизмы маркировки, классификации и планирования обеспечивают высокую производительность передачи трафика данных, голоса и видео на скорости проводного соединения.

Коммутатор Cisco WS-C2960-24TT-L изображен на рисунке 2.7. Технические характеристики данного коммутатора приведены в таблице 2.8.

Рисунок 2.7 – Коммутатор Cisco WS-C2960-24TT-L

Т а б л и ц а 2.8 – Технические характеристики Cisco WS-C2960-24TT-L

Характеристики коммутатора Cisco WS-C2960-24TT-L	
Технология доступа	Ethernet
Число портов LAN	24 шт
Тип портов LAN	10/100/1000 Base-TX (1000 мбит/с)
Число uplink-портов	2 шт
Тип uplink-портов	10/100/1000 Base-TX (1000 мбит/с)
Внутренняя пропускная способность	15 ГБит/с
Производительность маршрутизации	3.5 mpps
Размер таблицы MAC-адресов	8000
Поддержка IPv6	Присутствует
Поддержка Auto-MDI/MDI-X	Присутствует

Окончание таблицы 2.8

Характеристики коммутатора Cisco WS-C2960-24TT-L	
Поддержка IEEE 802.1d (Spanning Tree)	Присутствует
Поддержка IEEE 802.1p (Priority tags)	Присутствует
Поддержка IEEE 802.1q (VLAN)	Присутствует
Максимальное количество VLAN’ов	255
Поддержка IEEE 802.1s (Multiple Spanning Tree)	Присутствует
Поддержка IEEE 802.3x (Flow control)	Присутствует
Поддержка PoE	Присутствует
Консольный порт	Присутствует
Объем оперативной памяти	64 МБ
Объем Flash памяти	32 МБ
Web-интерфейс	Присутствует
Telnet	Присутствует
DHCP-сервер	Присутствует
Поддержка IGMP (Multicast)	Присутствует
Поддержка SNMP	Присутствует
Рабочая температура	от -5°C до 45°C
Температура хранения	от -25°C до 70°C
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	Есть
Габариты	450 x 46 x 238 мм
Вес нетто	3.2 кг
Вес брутто	4.4 кг

Серия коммутаторов Cisco Catalyst 2960 обладает рядом особенностей:

- на коммутаторах серии 2960 довольно высокий уровень безопасности;
- по сравнению с предыдущими сериями списки контроля доступа (ACL) значительно улучшены;
- встроенные порты двойного назначения, которые функционируют как для медных соединений, так и для оптоволоконных. Каждый из таких портов уже имеет встроенный порт 10/100/1000 Ethernet и порт SFP Gigabit Ethernet. При этом одновременно активным может быть только один из этих портов;
- на коммутаторах этой серии есть возможность организации 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 этой серии просты не только в управлении, но и в конфигурировании;
- доступна функция автоматической конфигурации посредством Smart портов для некоторых специализированных приложений.

Сравнение конфигураций и аппаратных характеристик коммутаторов приведены в таблицах 2.9, 2.10.

Таблица 2.9 – 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

Таблица 2.10 – 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 свитчей в стеке	0	0	0	0	0
Объем оперативной памяти	32	64	64	64	128

Окончание таблицы 2.10

Аппаратные характеристики	WS-C2960-24TC-L	WS-C2960-24TT-L	WS-C2960-48TC-L	WS-C2960-48TT-L	WS-C2960G-24TC-L
Кол-во пакетов в секунду (Mpps)	6.8	6.8	10.2	10.2	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	4,2x46,5x24,6	4,4x46,5x23,6	4,4x44,5x24,6	4,3x44,5x23,6	4,3x44,5x32,8
Вес, кг	3,6	3,6	3,6	3,6	4,5

2.6.2 Коммутатор Cisco Catalyst WS-3560-24TS

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-3560-24TS изображен на рисунке 2.8. Характеристики коммутатора приведены в таблице 2.11.

Рисунок 2.8 – Коммутатор Cisco WS-3560-24TS

Т а б л и ц а 2.11 – 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: 480 Вт; • AC: 100 - 240 В (автоопределение), 5 - 2.6 А, 55 - 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

2.6.3 Маршрутизатор D-Link DFL-800E

Устройства серии DFL-800E (Рисунок 2.9, 2.10) 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-800E показаны в таблице 2.12.

Рисунок 2.9 – D-Link DFL-800E

Рисунок 2.10 – D-Link DFL-800E (вид изнутри)

Т а б л и ц а 2.12 – Технические характеристики D-Link DFL-800E

Характеристики	
Производитель	D-Link
Модель	DFL-800E
Тип оборудования	Межсетевой экран, маршрутизатор, коммутатор
Число одновременных IPSec VPN соединений	До 340 туннелей

Окончание таблицы 2.12

Характеристики	
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	Да
Соответствие стандартам	802.1Q
VLAN	Да
DMZ	Поддерживается. Присутствует 1 порт DMZ 10/100 Мбит/сек.
NAT	Да
DHCP-сервер	Да
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	25 ватт – максимальное
Размеры (ширина x высота x глубина)	27.4 x 4.2 x 21.6 см
Вес	1.23 кг
Рабочая температура	0 ~ 65°C

2.6.4 Сервер Asus TS500-E6-PS4 Dual Xeon S1366

Asus TS500-E6-PS4 – единственный сервер формфактора 5U с двумя процессорами. Данный сервер поставляется в базовой конфигурации, поэтому его цена зависит от выбранных покупателем компонентов.

Как показали тесты производительности, сервер ASUS TS500-E6-PS4 подходит для выполнения большинства существующих деловых приложений.

В данной сервере технологии уменьшения шума охлаждающей системы, по сравнению с предыдущими моделями, значительно усовершенствованы.

ASUS TS500-E6/PS4 представляет собой идеальное решение для небольших предприятий, использующих в своей работе высокодоступные и критически важные компьютерные приложения.

Сервер Asus TS500-E6-PS4 Dual Xeon S1366 изображен на рисунке 2.11. Технические характеристики этого сервера приведены в таблице 2.13.

Рисунок 2.11 – Сервер Asus TS500-E6-PS4 Dual Xeon S1366

Т а б л и ц а 2.13 – Технические характеристики Asus Dual Xeon S1366

Характеристики	
Название продукта	Dual Xeon S1366/ 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 2.13

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

2.6.5 Модем ADSL D-Link 2500U

DSL-2500U (Рисунок 2.12, 2.13, 2.14) – это недорогой высокоскоростной ADSL/Ethernet-модем для сетей малых офисов и домашних сетей. С его помощью можно быстро и просто получить широкополосный доступ к сети Интернет по технологии ADSL и организовать использование канала связи несколькими пользователями одновременно.

DSL-2500U реализует все необходимые функции для создания безопасной, высокоскоростной проводной сети: поддержка стандартов ADSL, ADSL2, ADSL2+, поддержка стандарта Fast Ethernet, в нем присутствуют 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 2.12 – D-Link DSL-2500U (Вид сверху)

Рисунок 2.13 – D-Link DSL-2500U (Вид спереди)

Рисунок 2.14 – D-Link DSL-2500U (Вид сзади)

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

Для управления и настройки в DSL-2500U присутствует простой и удобный встроенный web-интерфейс (доступен на двух языках – русском и английском). Характеристики данного модема показаны в таблице 2.14.

Т а б л и ц а 2.14 – Технические характеристики модема D-Link 2500U

Характеристики	
Интерфейсы	1 порт ADSL (RJ-11) 1 порт LAN 10/100BASE-TX (RJ-45)
Поддерживаемые стандарты ADSL	ADSL: ANSI T2.412 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 ADSL2+ G.DMT.bis.plus
Поддерживаемые протоколы соединения с Интернетом	Мультипротокольная инкапсуляция поверх ATM 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;
Сетевые протоколы и функции	Статическая IP-маршрутизация; Протокол NAT; Виртуальный сервер и переадресация портов; DHCP-сервер/клиент/relay; DNS relay; DDNS; IGMP proxy, IGMP v.2 snooping для IP-TV; Протокол 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 не только через Web-интерфейс, но и по TFTP, настройка загрузки/пересылки; UPnP; SNMP v1 и v2c, встроенные агенты MIB-I, MIB-II
Размеры	118x104x30 мм
Вес	210 г

Окончание таблицы 2.14

Характеристики	
Питание	Внешний адаптер питания переменного тока 9 В / 1.3А; Переключатель питания Вкл/Выкл; Отсылка пакета Dying Gasp при остановке питания; Кнопка перезапуска
Рабочая температура	От 0 до 40 С
Электромагнитная совместимость (EMC/EMI)	FCC Part 15 Class B; CE (EN54022/EN54024/EN300 328/EN301 488)
Безопасность	CSA, LVD, RoHS совместимый

Красивый дизайн и довольно небольшие размеры корпуса модема D-Link DSL-2500U определяют в нем модель для домашней и офисной эксплуатации. Корпус изготовлен из пластика черного матового цвета без каких-либо вставок, но с крупным отполированным логотипом D-Link на верхней понели.

2.7 Проверка работоспособности корпоративной сети

Теперь, когда структура сети определена и проведены настройки оборудования, нужно удостовериться в работоспособности самой сети. Для этого мы будем отправлять с разных рабочих станций пинг-запросы.

Ping – утилита для проверки соединений в сетях на основе TCP/IP, а также обиходное наименование самого запроса.

Начнем с главного офиса предприятия “Фаворит”. Отправим пинг-запрос с рабочей станции отдела закупок и продаж, IP-адрес которой 192.168.1.1, на рабочую станцию отдела маркетинга с IP-адресом 192.168.1.5.Оба отдела находятся на первом этаже главного офиса. Как видно из рисунка 2.15, пинг-запрос прошел успешно.

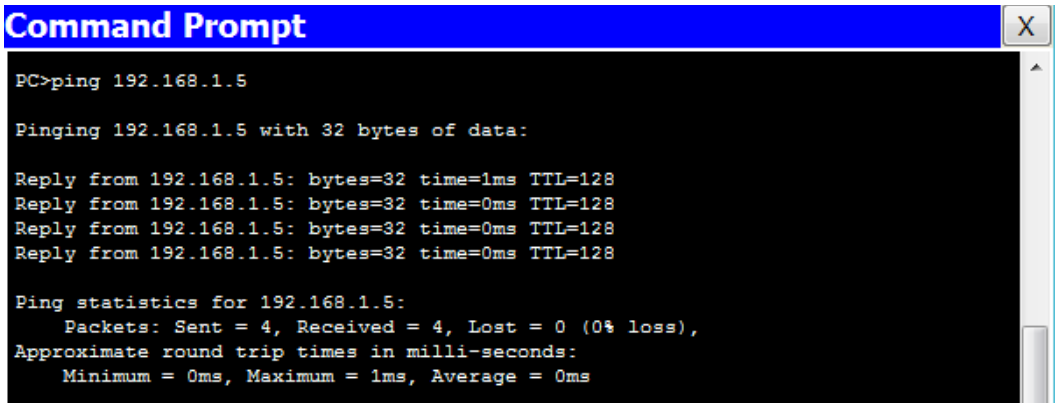

Рисунок 2.15 – Результат выполнения пинг-запроса между отделами первого этажа главного офиса

Далее, отправим пинг-запрос с рабочей станции отдела закупок и продаж, IP-адрес которой 192.168.1.1, на рабочую станцию с IP-адресом 192.168.1.67 расположенной в первом складском помещении соседнего здания. Как видно из рисунка 2.16, пинг-запрос прошел успешно.

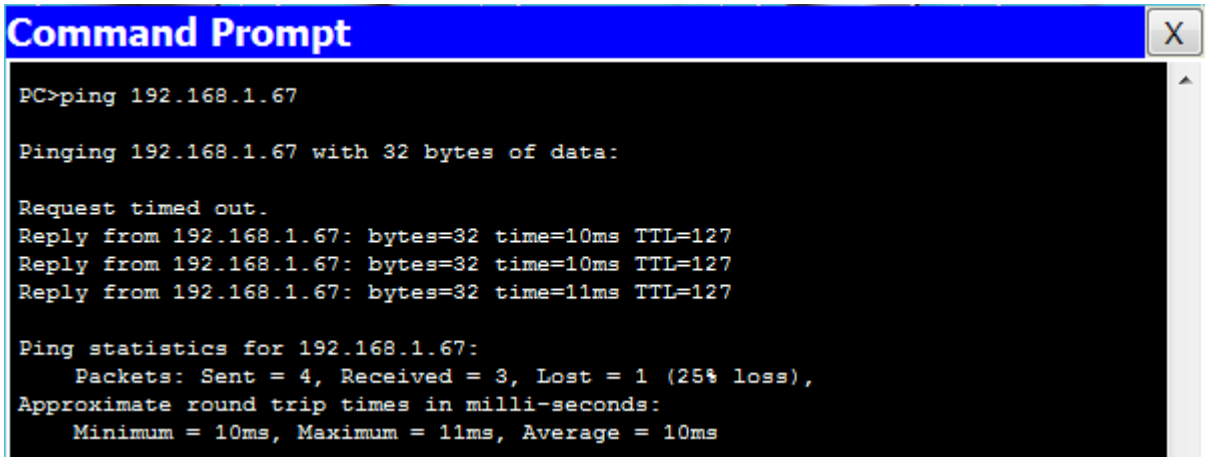

Рисунок 2.16 – Результат выполнения пинг-запроса между подразделениями соседних зданий на территории главного офиса

Теперь проверим локальную сеть в филиале предприятия. Для этого отправим пинг-запрос со станции планового отдела, IP-адрес которой 192.168.3.34, на рабочую станцию с IP-адресом 192.168.3.3 расположенной в отделе снабжения. Отделы находятся на разных этажах, а также в разных подсетях. Как видно из рисунка 2.17, пинг-запрос прошел успешно.

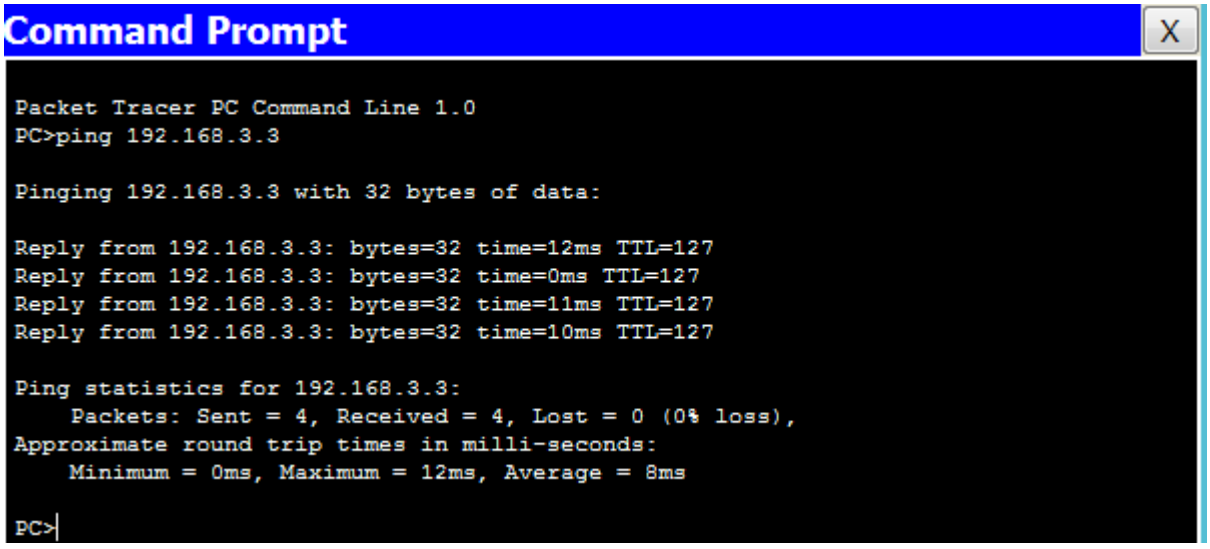

Рисунок 2.17 – Результат выполнения пинг-запроса между отделами разных этажей филиала

Убедившись в работоспособности локальных сетей в главном офисе и филиале предприятия, нужно проверить связь между этими локальными

сетями. Для этого отправим пинг-запрос со станции отдела закуп и продаж главного офиса, IP-адрес которой 192.168.1.1, на рабочую станцию с IP-адресом 192.168.3.3 расположенной в отделе снабжения здания филиала предприятия. Как видно из рисунка 2.18, пинг-запрос прошел успешно.

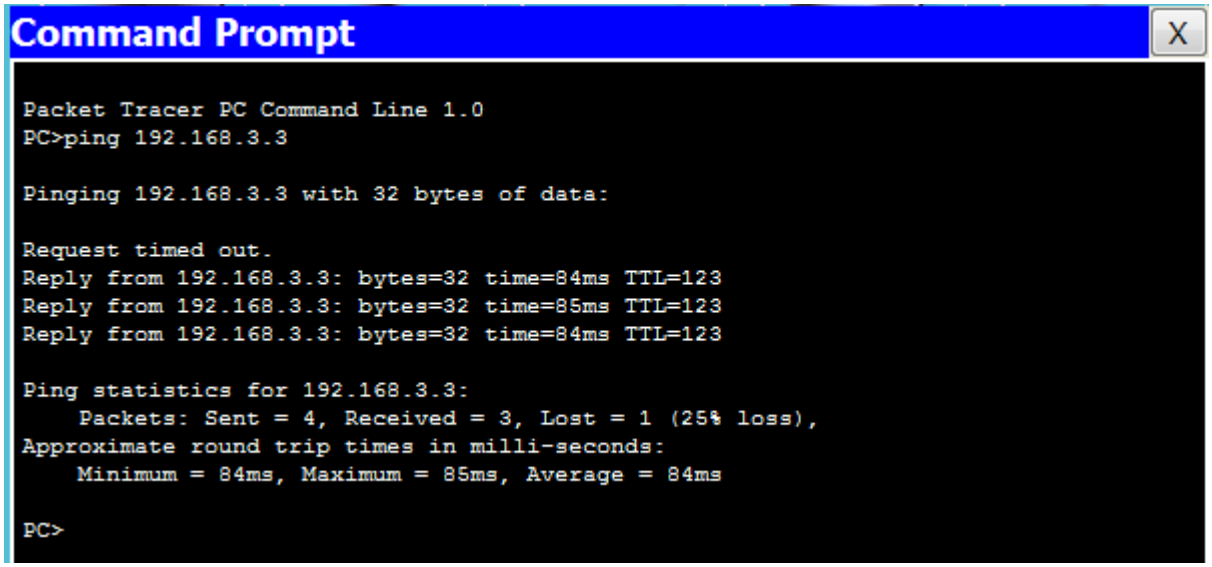

Рисунок 2.18 – Результат выполнения пинг-запроса между отделами главного офиса и филиала предприятия

Из полученных результатов проведенной проверки можно заключить, что вся корпоративная сеть функционирует исправно.

3 Технико-экономическое обоснование

3.1 Резюме

Главной целью данного проекта является проектирование корпоративной сети для главного офиса предприятия “Фаворит” и его филиала. При проектировании сети использовался протокол OSPF. Данный протокол обладает таким свойством как 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, оптимальным использованием пропускной способности (т. к. строится дерево кратчайших путей по алгоритму Дейкстры) и быстрой сходимостью, что не маловажно в проектировании крупной современной сети.

3.2 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.

3.2.1 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

$$\sum К_{кап} = К_{об} + К_{м} + К_{пр} + К_{т} \quad (3.1)$$

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 3.1.

Т а б л и ц а 3 .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	3 шт	125 000	150 000
2 Модем ADSL D-Link 2500U	3 шт	10 000	30 000
3 Маршрутизатор D-link DFL-800	3 шт	100 000	300 000
4 Коммутатор Cisco Catalyst 2960-24TT	4 шт	140 000	560 000
5 Коммутатор Cisco WS-C3560-24TS-S	3 шт	420 000	1 260 000
6 Кабельная продукция UTP 8e	100 м	70	7 000
7 Сервер Asus TS500-E6-PS4 Xeon X3430	3 шт	200 000	600 000
Итого			2 907 000

3.2.2 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 3.2.

Т а б л и ц а 3.2 – Данные по стоимости монтажа

Наименование оборудования и работ, ед. изм.	Кол-во	Цена тенге	Сумма тенге
1 Монтаж кабеля, метр	100	500	50 000
2 Измерение параметров сети, место	16	900	14 400
3 Монтаж кабельной системы передачи данных, место	16	7000	112 000
Итого			176 400

3.2.3 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

$$К_{ПР} = ФОТ + О_С + Н + М \quad (3.2)$$

где ФОТ – фонд оплаты труда;

$О_с$ – отчисления на социальные нужды;

Н – накладные расходы;

М – расходы на материалы.

3.2.4 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 3.3.

Т а б л и ц а 3.3 – 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	«SvetCopy» А4 95% 82 г/м	пачка	10	650	6500
CD диски	CD-RW Philips	шт.	20	50	1000
Картридж принтера	Cartridge for HP 1010	шт.	2	5000	10000
Итого					22500

3.2.5 Расходы по оплате труда

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

$$ФОТ = З_{ОСН} + З_{ДОП} \quad (3.3)$$

Заработная плата (оплата труда работника) – вознаграждение за труд в зависимости от квалификации работника, сложности, количества, качества и условий выполняемой работы.

Основная заработная плата определяется как сумма оплаты труда всех исполнителей вычисляется по формуле

$$З_{ОСН} = \sum_{i=1}^{n} З_i \cdot Т_i \quad (3.4)$$

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

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

Вознаграждения за труд сверх установленной нормы, за трудовые успехи и изобретательность и за особые условия труда. В нее входят доплаты, надбавки, гарантийные и компенсационные выплаты, предусмотренные действующим законодательством.

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

$$З_{ДОП} = 0,1 \cdot З_{ОСН} \quad (3.5)$$

Труд разработчиков оплачивается согласно штатному расписанию. Количество исполнителей и размер месячной заработной платы представлены в таблице 3.4.

Т а б л и ц а 3.4 – 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

$$Д = \frac{З_{Пм}}{Д_р} \quad (3.6)$$

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 (3.6), 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 3.5).

Т а б л и ц а 3.5 – Трудозатраты

Исполнитель	Дневная зарплата, тенге	Количество дней	Сумма, тенге
Инженер	6250	30	187 500
Руководитель проекта	8333	30	249 990

Исходя из формулы (3.4), основная заработная плата будет равна

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

Исходя из формулы (3.5), дополнительная заработная плата будет равна

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

Исходя из формулы (3.3), суммарный фонд оплаты труда (ФОТ) составит

ФОТ = 624990+62499 = 687 489 тенге

3.2.6 Расчет социальных отчислений

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

$$О_С = 0{,}11 \cdot (ФОТ - ПО) \qquad (3.7)$$

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

$$ПО = 0,1 \cdot ФОТ \quad (3.8)$$

Исходя из формулы (3.8), пенсионные отчисления будут равны

$ПО = 0,1 \cdot 687489 = 68749$ тенге

Тогда, исходя из формулы (3.7), социальный налог будет равен

$О_с = 0,11 \cdot (687489 - 68749) = 68061$ тенге

3.2.7 Расчет накладных расходов

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

$$Н = 0,7 \cdot (ФОТ + О_с + М) \quad (3.9)$$

Тогда, исходя из формулы (3.9), накладные расходы составят

$Н = 0,7 \cdot (687489 + 68061,411 + 22500) = 544635$ тенге

Результаты расчетов затрат по проектированию сети представлены в таблице 3.6.

Т а б л и ц а 3.6 – 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 капиталовложения на разработку корпоративной сети, в соответствии с приведенной формулой (3.2) и проведенными расчетами составляют

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

Так как транспортные расходы включены в стоимость оборудования общая сумма капитальных затрат в соответствии с произведенными расчетами и согласно формуле (3.1) составит

$$\sum К_{кап} = 2907000 + 176400 + 1322685 = 4\ 499\ 085 \text{ тенге}$$

3.3 Оценка эффективности внедрения корпоративной сети на предприятие “Фаворит”

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.

Социальным эффектом внедрения корпоративной сети между главным офисом предприятия “Фаворит” и его филиалами является:

- повышение скорости передачи данных и оперативности выполнения приказов;
- повышение качества труда;
- уменьшение затрат рабочего времени для передачи документов между главным офисом и филиалами;
- улучшится взаимодействие между специалистами предприятия;
- улучшение качества управления персоналом и специалистами среднего звена, например, при получении того или иного приказа информация мгновенно будет доводиться до специалистов.

Вывод по экономической части дипломного проекта

Общий объём капитальных вложений на проектирование корпоративной сети составил 4 499 085 тенге.

Социальным эффектом внедрения корпоративной сети между главным офисом предприятия “Фаворит” и его филиалами является:

- повышение скорости передачи данных и оперативности выполнения приказов;
- повышение качества труда;
- уменьшение затрат рабочего времени для передачи документов между главным офисом и филиалами;
- улучшится взаимодействие между специалистами предприятия;
- улучшение качества управления персоналом и специалистами среднего звена, например, при получении того или иного приказа информация мгновенно будет доводиться до специалистов.

4 Безопасность жизнедеятельности

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

Главной целью данного проекта является организация корпоративной сети главного офиса предприятия “Фаворит” и его филиалов, с целью предоставления современных услуг связи: высокоскоростной доступ в Интернет.

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.

4.2 Планирование 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 4.1), 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 4.1), но не ближе 500 мм с учётом размеров знаков и символов.

Рисунок 4.1 – 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.

4.3 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. Основным параметром, определяющим характеристики вентиляционной системы, является кратность обмена, т.е. сколько раз в час сменится воздух в помещении. Для ее определения нужны следующие параметры:

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

$V_{пом}$ – объем рабочего помещения.

Для расчета примем следующие размеры рабочего помещения (Рисунок 4.2):

- длина А = 7 м;
- ширина В = 6 м;
- высота Н = 3 м.

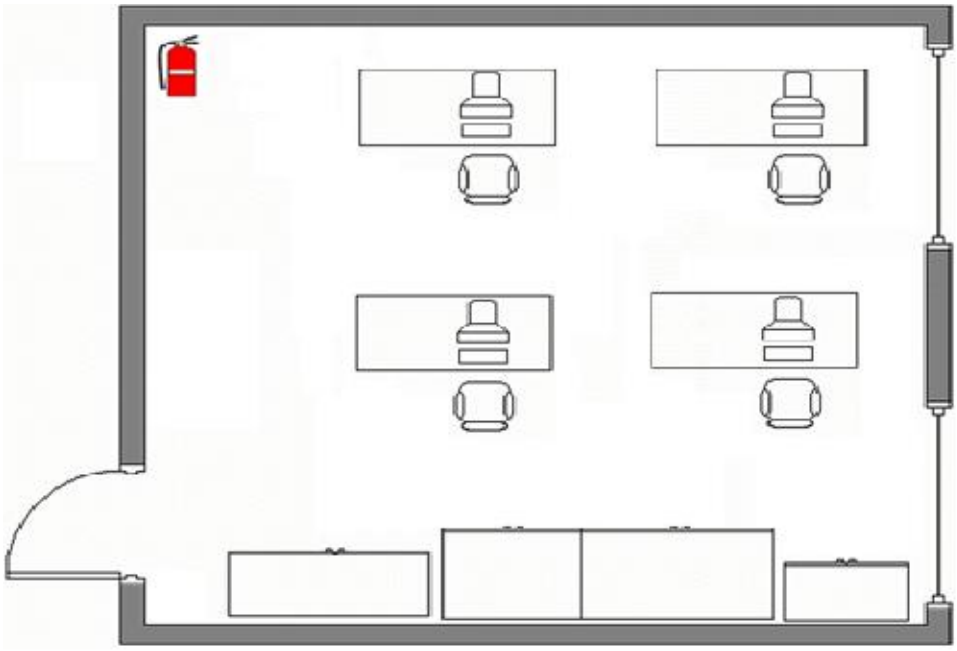

Рисунок 4.2 – План рабочего помещения

Объем помещения рассчитывается по формуле

$$V_{пом} = A \cdot B \cdot H \qquad (4.1)$$

Тогда, исходя из формулы (4.1), объем помещения будет равен

$V_{пом} = A \cdot B \cdot H = 126$ м^3

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

$$V_{вент} = C \cdot (t_{уход} – t_{приход}) \cdot Y \quad (4.2)$$

Тогда, исходя из формулы (4.2), 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

$$t_{уход} = t_{р.м.} + (H – 2) \cdot t \quad (4.3)$$

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 (4.3), температура уходящего воздуха будет равна

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

Общий избыток тепла рассчитывается по формуле

$$Q_{избыт} = Q_{изб.1} + Q_{изб.2} + Q_{изб.3} \quad (4.4)$$

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

$$Q_{изб.1} = E \cdot p \quad (4.5)$$

где E – коэффициент потерь электроэнергии на теплоотвод (E = 0,55 для освещения);
P – мощность (P = 300 Вт).

Исходя из формулы (4.5), избыток тепла от электрооборудования и освещения будет равно

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

Теплопоступление от солнечной радиации рассчитывается по формуле

$$Q_{изб.2} = m \cdot S \cdot k \cdot Q_c \quad (4.6)$$

где m – число окон, примем m = 2;

S – площадь окна, S = 2,3 · 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 (4.6), теплопоступление от солнечной радиации равно

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

$$Q_{изб.3} = n \cdot q \quad (4.7)$$

где q = 80 Вт/чел.;

n – число людей (n = 4).

Исходя из формулы (4.7), тепловыделения людей будут равны

$$Q_{изб.3} = 4 \cdot 80 = 320 \text{ Вт}$$

Исходя из формулы (4.4), общий избыток тепла будет равен

$$Q_{избыт} = 165 + 701 + 320 = 1186 \text{ Вт}$$

Исходя из формулы (4.2), $V_{вент}$ будет равен

$$V_{вент} = 3600 \cdot 1186 / (1000 \cdot (27 – 18)) = 474,4 \text{ м}^3$$

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.

4.4 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 и приборы, применяемые для технического обслуживания.

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

$$m_d = k \cdot g_n \cdot V \qquad (4.8)$$

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.

$$V = A \cdot B \cdot H \qquad (4.9)$$

где A = 7 м – длина помещения;

B = 6 м – ширина помещения;

H = 3 м – высота помещения.

Исходя из формулы (4.9), объем составит

$$V = 6 \cdot 4 \cdot 3 = 126 м^3$$

Исходя из формулы (4.8), масса комбинированного углекислотно-хладонового состава будет равна

$$m_д = 1{,}2 \cdot 0{,}04 \cdot 126 \approx 6 кг$$

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

$$d_i = 12 \cdot \sqrt{2} \qquad (4.10)$$

Исходя из формулы (4.10), 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

$$l_2 = k_1 \cdot l_1 \qquad (4.11)$$

где k_1 = 1,2 – коэффициент увеличения длины трубопровода для компенсации;

l_1 = 3м – длина трубопровода по проекту тогда.

Исходя из формулы (4.11), эквивалентная длина магистрального трубопровода равна

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

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

$$t = \frac{m_д}{60 \cdot Q} \qquad (4.12)$$

Тогда, исходя из формулы (4.12), время подачи углекислотно-хладонового состава будет равно

$$t = \frac{6}{60 \cdot 1{,}4} = 0{,}071 \text{мин}$$

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

$$m = 1{,}1 \cdot m_д \cdot \left(1 + \frac{k_2}{k}\right) \qquad (4.13)$$

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

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 6 кг. Принципиальная схема установки автоматического пожаротушения показана на рисунке 4.3. 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.

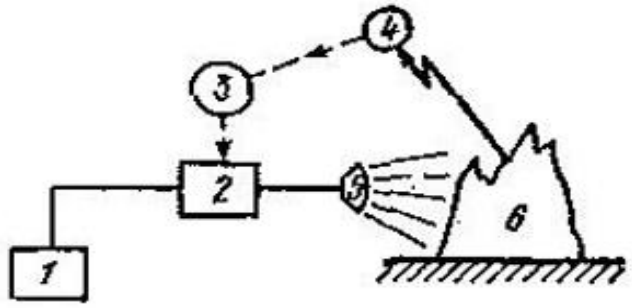

Рисунок 4.3 – Принципиальная схема установки автоматического пожаротушения

Вывод по разделу безопасность жизнедеятельности

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 6 кг.

Заключение

В данном дипломном проекте приводится описание разработки корпоративной сети для главного офиса и филиала компании “Фаворит”.

В проекте имеется обзор существующих топологий корпоративных сетей. Также в проекте описаны протоколы DHCP, SSH, NetFlow и OSPF. В работе были рассмотрены вопросы безопасности сетей. В ходе выполнения поставленных задач были настроены протоколы SSH и NetFlow.

В технической части работы показана структурная схема корпоративной сети между главным офисом и филиалом предприятия, а также предоставлены результаты проделанной работы.

В технико-экономическом расчёте определены капиталовложения на реализацию проекта и приобретения необходимого оборудования, а также был определен социальный эффект от разработки корпоративной сети.

В проекте был произведён анализ условий труда в рабочем помещении, рассчитаны все необходимые параметры микроклимата 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.