ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
(Н И У « Б е л Г У »)

ИНСТИТУТ ИНЖЕНЕРНЫХ И ЦИФРОВЫХ ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

РАЗРАБОТКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ ДЛЯ ФИЛИАЛОВ КОМПАНИИ ТЕХНОСВЯЗЬСТРОЙ

Выпускная квалификационная работа
обучающегося по направлению подготовки 11.03.02
Инфокоммуникационные технологии и системы связи
заочной формы обучения, группы 12001452
Дубровина Романа Сергеевича

Научный руководитель
канд. техн. наук, доцент
кафедры
Информационно-
телекоммуникационных
систем и технологий
НИУ «БелГУ» Ушаков Д.И.

Рецензент
Ведущий инженер электросвязи
участка систем коммутации №1 г.
Белгорода Белгородского
филиала ПАО «Ростелеком»
Уманец С.В.

БЕЛГОРОД 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Построение телекоммуникационных сетей связи в крупных компаний является актуальной задачей. В связи с внедрением в структуру крупных предприятий новых информационных технологий растет потребность в выборе и построении оптимальной сети связи масштаба предприятия, удовлетворяющей его потребностям.

По мере развития компании у руководства обязательно возникают вопросы: создание максимально гибкой и эффективной системы управления предприятием, офисными площадками, создание единой системы документооборота, оперативного сбора информации и отчетов со складов и производственных площадок, централизация информационно-финансовых потоков и т.д. Правильное решение этих вопросов позволяет успешно управлять компанией в целом, делает её гибкой и динамично развивающейся.

Компания ТехноСвязьСтрой - успешно работающая проектно-монтажная организация в области строительной инженерии. Приоритетное направление деятельности - производство полного цикла электромонтажных и слаботочных работ, включая проектирование, согласования, монтаж. Кроме того компания выполняет работы по монтажу сантехнических систем, систем автоматического пожаротушения и оповещения о пожаре; также выполняет ремонтно-строительные и отделочные работы.

Штат сотрудников компании составляет более 500 сотрудников, имеет распределенную сеть филиалов в центральном регионе в таких городах как Москва, Воронеж, Орел, Курск, Липецк. На сегодняшний день возникает необходимость в единой сетевой инфраструктуре для территориально-распределенных филиалов с целью оптимизации документооборота, обеспечения безопасности передаваемых данных, единого call-центра, и различных корпоративных сервисов (эл. Почта, централизованная аутентификация, видеоконференцсвязь и т.п.).

Таким образом, выпускная квалификационная работа в которой предлагается построение современной мультисервисной сети связи для территориально - распределенных объектов ТехноСвязьСтрой является актуальной. Реализация предложенного проекта в компании ТехноСвязьСтрой позволит уменьшить эксплуатационные затраты, оптимизировать рабочий процесс, сократить бумажный документооборот внутри компании, повысить производительность труда, сократить время на получение и обработку информации, выполнять точный и полный анализ данных, обеспечивать получение любых форм отчетов по итогам работы. Как следствие, образуются дополнительные временные ресурсы для разработки и реализации новых проектов.

Целью выпускной квалификационной работы является организация выделенной сети связи, позволяющей объединить все информационные ресурсы ТехноСвязьСтрой в единое информационное пространство. Разрабатываемая сеть должна соответствовать принятым международным стандартам и обеспечить передачу всех видов информации (данные, голос, видео и т.п.) с учетом перспектив развития современных информационных технологий.

Для решения поставленной цели решаются следующие задачи:

1. Анализ существующей сети связи филиалов компании ТехноСвязьСтрой.
2. Выбор варианта реализации сети связи для территориально - распределенных дилерских центров.
3. Расчет нагрузок трафика.
4. Технико-экономическое обоснование проекта.

Данная выпускная квалификационная работа состоит из 6 глав, посвященных решению поставленных задач. Имеет приложения, в которых в виде графических схем изображены проектируемая схема организации сети связи, схема организации сети связи в филиалах компании, схема движения голосового трафика и сигнальных сообщений, схема размещения станционного

оборудования.

1 ЭКСПЛИКАЦИЯ ОБЪЕКТА ПРОЕКТИРОВАНИЯ

1.1 Общие сведения

ТехноСвязьСтрой — клиентоориентированный бизнес и надежный партнер, гибко реагирующий на изменения рыночной ситуации, привносящий отработанные методики в свою бизнес-практику.

Для того, чтобы предлагаемые услуги в новой проектируемой сети имели актуальность и были конкурентоспособными, необходимо в начале проектирования проанализировать существующую сеть связи: определить действующих операторов связи и набор предоставляемых ими услуг, а также выяснить технологии, на основе которых действующие операторы предоставляют свои услуги абонентам сети.

Территориальное расположение филиалов указано на рисунке 1.

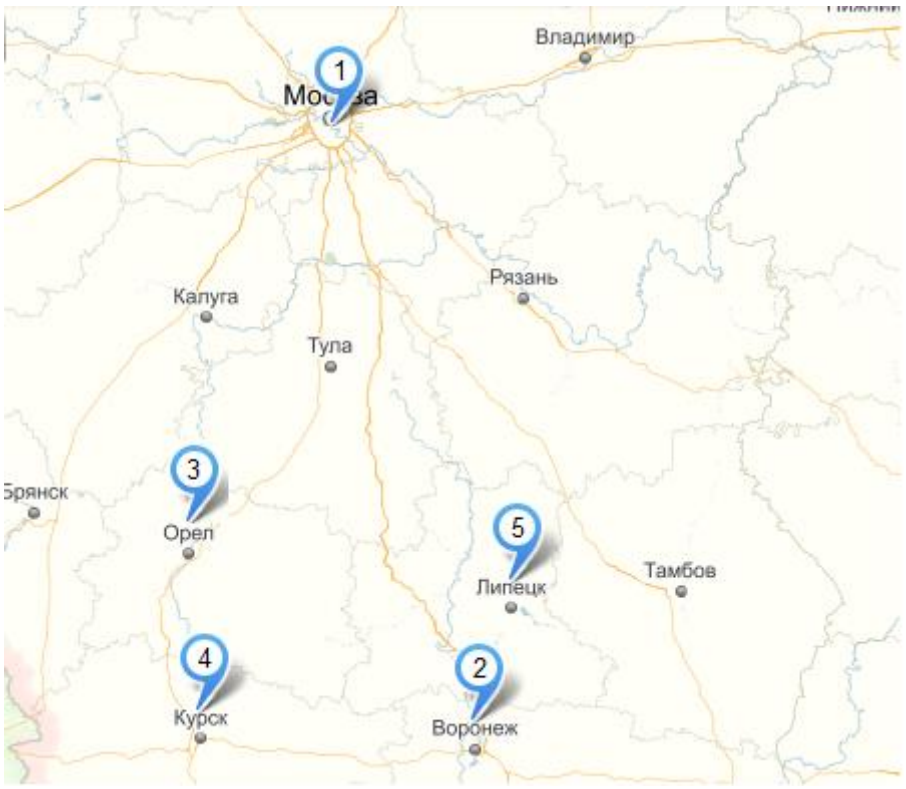


Рисунок 1. Расположение региональных филиалов компании ТехноСвязьСтрой.

В западной части России находится 5 удаленных друг от друга офисов компании ТехноСвязьСтрой. Количество абонентов в этих офисах рассмотрено в таблице 1.1.

Таблица 1.1 – Характеристика региональных филиалов компании

Удаленные офисы компании ТехноСвязьСтрой	Количество абонентов, чел.
Московский офис	50
Воронежский офис	40
Орловский офис	40
Курский офис	40
Липецкий офис	40

В настоящее время в офисах компании ТехноСвязьСтрой в качестве УПАТС (учережденческо-производственной АТС) используется мини АТС.

1.2 Анализ сетевой инфраструктуры

Распределение входящих звонков. Для каждой внешней линии мини АТС можно установить, на какие внутренние линии и в какое время она будет транслировать входящий звонок. При этом возможен перехват вызова. Для внутренних абонентов которые уже ведут разговор по другой линии при внешнем звонке будет поступать предупреждающий сигнал (при включении этой функции на этапе программирования). Звонки с внешних линий отличаются от звонков внутренних абонентов по длительности паузы.

Переадресация. Входящий звонок или исходящее соединение может быть переадресовано на любую другую внутреннюю или внешнюю линию мини АТС путем набора двузначного номера. Есть возможность наведения справки во время разговора. При этом внешний (или внутренний) абонент мини АТС переключается на музыкальную заставку.

Управление исходящей связью. Для любого телефона можно разрешить / запретить выход на городскую линию, доступ к междугородней связи (разрешить / запретить звонки через 8). Для разных групп абонентов можно выделить разные внешние линии. Назначение внешних линий также можно распределить, например, одни линии для исходящей связи, другие для входящей.

Набор номера. Выйти на городскую линию можно с помощью набора "9", либо набрав внутренний номер линии, либо включив прямой выход. В последнем случае при поднятии трубки абонент сразу подключается к телефонной линии. Мини АТС может работать с телефонными аппаратами с импульсным и тоновым набором.

Конференц-связь. Возможен любой вариант соединения абонентов, как между внутренними, так и между внешними линиями мини АТС с разным количеством участников.

Схема мини АТС представлена на рисунке 1.2.

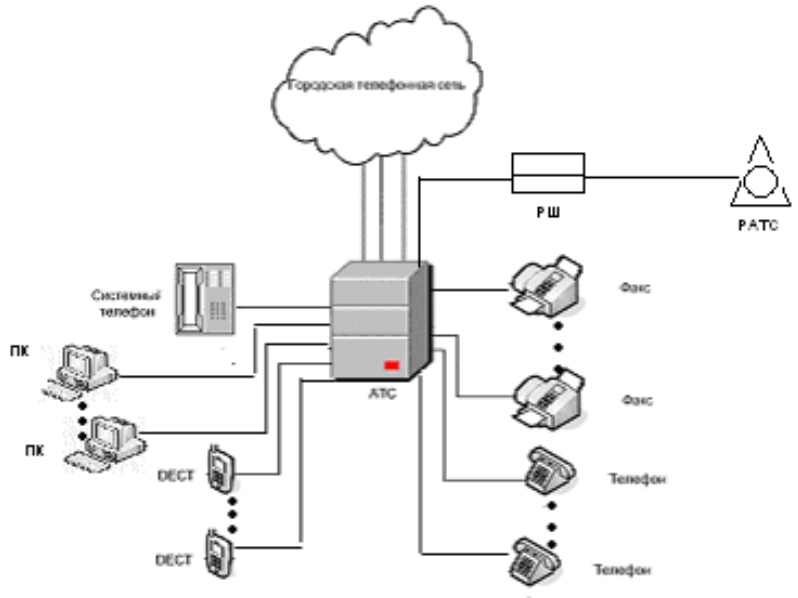


Рисунок 1.2 - Схема мини АТС ООО ТехноСвязьСтрой.

Для предоставления услуги доступ в Интернет используется технология ADSL по выделенной линии и дополнительных телефонных номеров. Клиент получает постоянный доступ в Интернет, скорость которого достигает 2 Мбит/с.

Преимущества ADSL следующие:

- Доступность, поскольку они организуются на обычных телефонных линиях;

- Невысокая стоимость;

- Быстрота и простота установки;

- Высокая скорость доступа

- Возможность одновременно работать в Интернете и пользоваться телефоном

- Постоянное соединение с Интернет

Одним из основных преимуществ ADSL перед другими технологиями высокоскоростной передачи данных является использование самых обычных витых пар медных проводов телефонных кабелей. Совершенно очевидно, что использование самой распространенной сети телефонной связи делает ADSL технологически доступной большому числу пользователей.

При создании этой технологии разработчики уделили большое внимание не только скорости на абонентском участке. В технологии определены высоко скоростные каналы для соединения каждого ADSL мультиплексора с городской сетью передачи данных и выхода в Интернет в частности. Все мультиплексоры подключены к сети передачи данных через волоконно-оптические линии связи (ВОЛС) на скорости 620 Мбит/секунду.

Тем не менее использование технологии ADSL для доступа в сеть Internet не позволяет организовать единую сетевую инфраструктуру компании, тем более, что каналы ADSL не достаточно скоростные и защищенные. При реализации единой сетевой инфраструктуры необходимо обеспечить высокий уровень конфиденциальности передаваемых данных и защищенности. При этом проектируемая система должна легко конфигурироваться и поддерживать централизованную систему IP телефонии.

Поэтому для создания новой телекоммуникационной инфраструктуры для территориально-распределенных офисов компании ТехноСвязьСтрой необходимо учесть все требования и использовать современные IT технологии.

2 ВЫБОР ВАРИАНТА РЕАЛИЗАЦИИ СЕТИ СВЯЗИ

2.1 Концептуальные положения

В настоящее время построение мультисервисных сетей с интеграцией различных услуг является одним из наиболее перспективных направлений развития телекоммуникационных сетей. Основная задача мультисервисных сетей заключается в обеспечении сосуществования и взаимодействия разнородных коммуникационных подсистем в единой транспортной среде, когда для передачи обычного трафика (данных) и трафика реального времени (голоса и видео) используется единая инфраструктура.

При создании мультисервисной сети связи для территориально-распределенных филиалов компании, можно получить следующие результаты:

1. Сократить расходы на междугородные и международные переговоры. Один из наиболее распространенных вариантов использования IP-телефонии. Связь через IP получается дешевле по ряду причин. Во-первых, в IP-телефонии используются широко распространенные (и дешевые) сети с коммутацией пакетов, (в отличие от более дорогостоящих сетей с коммутацией каналов, применяемых в традиционной телефонии). Во-вторых, благодаря использованию голосовых кодеков (вокодеров, voice coders) достигается существенное сжатие речевой информации. Так, при передаче голосового потока в системах цифровой телефонии требуется канал 64 кБит/с (ISDN). В системах IP-телефонии, при использовании наиболее популярных на сегодняшний день кодеков, требуется гораздо меньшая пропускная способность (6-13 кБит/с).

Можно выделить два наиболее популярных варианта подключения к провайдерам междугородной и международной телефонии:

- Через ССОП (Сеть Связи Общего Пользования) - при подключении пользователь набирает "городской" номер сервера IP-телефонии провайдера,

проходит аутентификацию (по pin-коду) и набирает нужный ему номер. Чтобы пользоваться IP-телефонией по этой схеме, достаточно иметь обычный городской номер.

- С помощью специальных "шлюзов" - в этом случае пользователь приобретает специальное устройство - шлюз IP-телефонии, с помощью которого получает возможность совершать звонки без использования ССОП (через интернет-канал, предоставляемый провайдером). В место шлюзов также можно применять программные (в том числе и бесплатные) и аппаратные IP-телефоны.

2. Построить корпоративную телефонную сеть. В данном случае для ведения телефонных разговоров в рамках предприятия используется внутренняя IP-сеть. Однако в минимальном варианте такие системы используются достаточно редко и как правило, корпоративные системы IP-телефонии также решают следующие задачи:

- обеспечение "мобильности" внутренних пользователей;
- организация связи между географически отдаленными филиалами;
- объединение телефонной емкости филиалов в единый номерной план;
- организация аудио - и видеоконференций;
- построение центров обработки вызовов (call-центров).

Данное направление систем IP-телефонии очень хорошо развито производителями оборудования. Наиболее известными поставщиками являются такие компании как, Cisco Systems, Avaya, Nortel Networks, Zyxel, D-Link.

3. Получить дополнительные возможности, не свойственные обычным телефонным сетям: click2Dial - возможность совершить звонок (например, менеджеру продаж или в службу тех. поддержки) прямо с веб-сайта компании, голосовые авто-информаторы на основе IVR (Interactive Voice Response), аудио- и видеоконференций, голосовую почту и историю пропущенных звонков через web, определение присутствия абонента в сети и т. д.

4. Обеспечить "дешевую связь" в пределах зон Wi-Fi. Пользователь, находящийся в пределах беспроводной точки доступа 802.11 может приме нять VOIP (вместо сотовой связи) .

5. Организовать сеансы аудиосвязи или связи типа точка-точка через Интернет. Используя стандартное оборудование IP-телефонии, можно организовать сеанс связи между пользователями Интернет (например, с использованием Microsoft NetMeeting) или соединить несколько географически отдаленных филиалов.

2.2 Требования к сети связи территориально-распределенных филиалов компании ТехноСвязьСтрой

Проектируемая мультисервисная сеть связи должна предоставлять абонентам следующие услуги связи:

- высокоскоростной доступ к сети Интернет и передача данных;
- организация IP – телефонии с подключением к сети общего пользования;
- конфиденциальность передаваемых данных;
- поддержка мобильности пользователей;
- защищенность от внешних атак.

В целом проект телекоммуникационной сети должен обеспечивать выполнение всех возлагаемых на неё функций:

- обмен всеми видами информации, включая передачу речевых, графических и видеоданных для проведения телеконференций;
- обеспечение информационной скрытности информации и исключение несанкционированного доступа к ней;
- интеграция с существующими телекоммуникационными системами за счет построения элементов сети на основе стандартных технических средств и методов передачи и обработки информации;

- возможность изменения конфигурации и легкость развития топологии (расширения) сети;
- возможность внедрения перспективных информационных и телекоммуникационных технологий в будущем.

2.3 Разработка стратегии проектирования сети связи компании ТехноСвязьСтрой

Анализ и выбор сетевых технологий

Создание корпоративной сети связи между территориально распределенными филиалами необходимо для объединения всех информационных ресурсов компании « ТехноСвязьСтрой» в единое информационное пространство. Это позволит сократить бумажный документооборот внутри компании, повысить производительность труда, сократить время на получение и обработку информации и выполнять точный и полный анализ данных. Данная сеть может организовываться на базе выделенных каналов связи или на базе существующей сети провайдера – услуга Virtual Private Network (VPN). Таким образом, принято проектное решение для организации связи Инженерных центров в филиалах компании использовать технологию VPN.

Анализ состояния существующей сети связи предприятия ТехноСвязьСтрой, показал, что для модернизации сети требуется решить следующие задачи:

1. Заменить коммутационное оборудование на более современно оборудование IP коммутации.
2. Провести расчет нагрузки на ССОП при модернизации сети
3. Организовать внешнюю связь с ССОП с использованием современной транспортной системы.

4. Внедрить на сети связи мультисервисные приложения для улучшения стратегии развития предприятия.

В сеть доступа инвестируется от 50% до 80% средств, поэтому правильный выбор технологий и вариантов построения сети чрезвычайно важен.

2.4 Выбор технологии для реализации сети связи

В данной выпускной квалификационной работе транспортная сеть связи будет объединять территориально распределенные филиалы компании. В связи с этим создание транспортной сети на базе собственных выделенных каналов связи между филиалами предприятия требует очень больших затрат на развертывание и сопровождение такой структуры.

Поэтому более предпочтительной альтернативой является создание виртуальной частной сети (VPN - Virtual Private Network) на базе общедоступной глобальной сети Internet.

2.4.1 Принцип работы технологии VPN

VPN-устройство располагается между внутренней сетью и Интернет на каждом конце соединения. Когда данные передаются через VPN, они исчезают «с поверхности» в точке отправки и вновь появляются только в точке назначения. Этот процесс принято называть «туннелированием». Это означает создание логического туннеля в сети Интернет, который соединяет две крайние точки. Благодаря туннелированию частная информация становится невидимой для других пользователей Интернета. Прежде чем попасть в интернет-туннель, данные шифруются, что обеспечивает их дополнительную защиту. Протоколы шифрования бывают разные. Все зависит от того, какой протокол туннелирования поддерживается тем или иным VPN-решением. Еще одной важной характеристикой VPN-решений является диапазон поддерживаемых протоколов аутентификации. Это означает, что, усилив свою виртуальную

частную сеть соответствующим протоколом аутентификации, можно гарантировать, что доступ к защищенным туннелям получат только известные вам люди.

VPN рисунок 2.1 представляет собой объединение отдельных машин или локальных сетей в виртуальной сети, которая обеспечивает целостность и безопасность передаваемых данных. Она обладает свойствами выделенной частной сети и позволяет передавать данные между двумя компьютерами через промежуточную сеть (internetwork), например Internet.

VPN отличается рядом экономических преимуществ по сравнению с другими методами удаленного доступа. Во-первых, пользователи могут обращаться к корпоративной сети, не устанавливая коммутируемое соединение, таким образом, отпадает надобность в использовании модемов. Во-вторых, можно обойтись без выделенных линий.

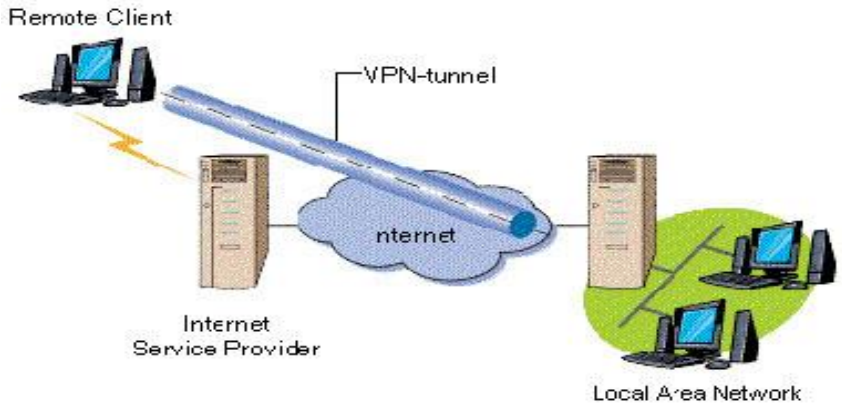


Рисунок 2.1 - VPN для двух офисных сетей

Имея доступ в Интернет, любой пользователь может без проблем подключиться к сети офиса своей фирмы. Следует заметить, что общедоступность данных совсем не означает их незащищенность. Система безопасности VPN - это броня, которая защищает всю корпоративную информацию от несанкционированного доступа. Прежде всего, информация передается в зашифрованном виде. Прочитать полученные данные может лишь

обладатель ключа к шифру. Наиболее часто используемым алгоритмом кодирования является Triple DES, который обеспечивает тройное шифрование (168 разрядов) с использованием трех разных ключей.

Подтверждение подлинности включает в себя проверку целостности данных и идентификацию пользователей, задействованных в VPN. Первая гарантирует, что данные дошли до адресата именно в том виде, в каком были посланы. Самые популярные алгоритмы проверки целостности данных - MD5 и SHA1. Далее система проверяет, не были ли изменены данные во время движения по сетям, по ошибке или злонамеренно. Таким образом, построение VPN предполагает создание защищенных от постороннего доступа туннелей между несколькими локальными сетями или удаленными пользователями.

Для построения VPN необходимо иметь на обоих концах линии связи программы шифрования исходящего и дешифрования входящего трафиков. Они могут работать как на специализированных аппаратных устройствах, так и на ПК с таки ми операционными системами как Windows, Linux или NetWare.

Прохождение пакета по сети MPLS VPN

Рассмотрев схему распространения маршрутной информации по сети MPLS VPN, можно проследить за тем как перемещаются данные между узлами одной VPN.

Пусть, например, из сайта 1 в VPN A узел с адресом 10.2.1.1/16 отправляет пакет узлу сайта 2 этой же VPN, имеющему адрес 10.1.0.3/16 рисунок 2.2.

Стандартными транспортными средствами IP пакет доставляется на пограничный маршрутизатор сайта CE1A, в таблице которого для номера сети 10.1.0.0 в качестве следующего маршрутизатора указан PE1. На маршрутизатор PE1 пакет поступает с интерфейса int2, поэтому для выбора дальнейшего продвижения пакета он обращается к таблице VRF1a, связанной с данным интерфейсом.

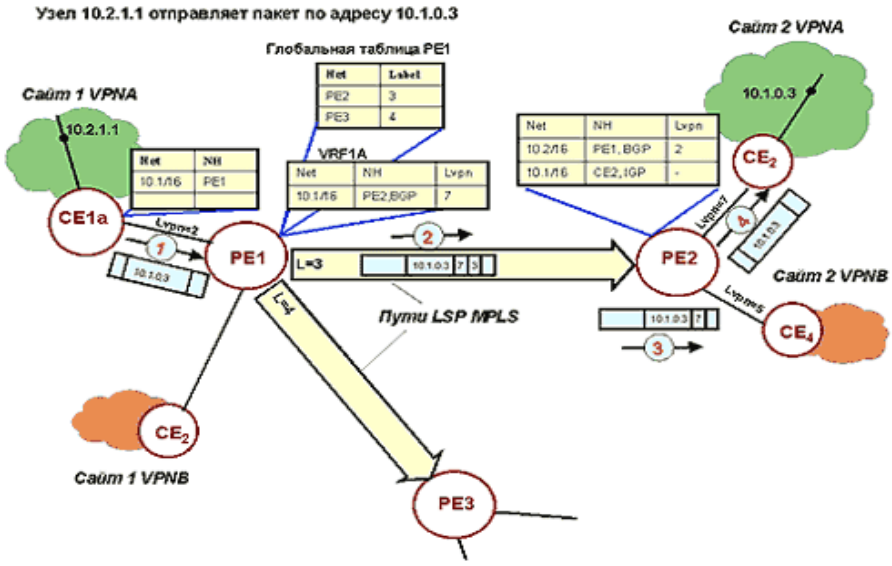


Рисунок 2.2 – Прохождение пакета по сети MPLS VPN

В таблице VRF1A адресу 10.1.0.0 соответствует запись протокола BGP, которая указывает, что очередным маршрутизатором для пакета определен PE2. Следующее поле записи содержит значение метки Lvpn=7, определяющей интерфейс выходного маршрутизатора PE, которое должно быть присвоено пакету для того, чтобы он попал в нужную VPN. Здесь также указывается, что запись была сделана протоколом BGP, а не IGP. На этом основании маршрутизатор PE «понимает», что очередной маршрутизатор не является непосредственным соседом, и путь к нему надо искать в глобальной таблице маршрутизации.

В глобальной таблице для адреса PE2 указывается начальное значение метки L пути LSP, равное 3. Способ его прокладки между маршрутизаторами PE1 и PE2 не имеет в данном случае принципиального значения — главное, чтобы такой путь существовал.

Технология MPLS VPN использует иерархические свойства путей MPLS, за счет чего пакет может быть снабжен несколькими метками, помещаемыми в стек. На входе во внутреннюю сеть провайдера, образуемую маршрутизаторами P, пакет будет снабжен двумя метками — внутренней Lvpn=7 и внешней L=3. Метка Lvpn интерпретируется как метка нижнего уровня — оставаясь на дне стека, она не используется, пока пакет путешествует по туннелю PE1-PE2.

Продвижение пакета происходит на основании метки верхнего уровня, роль которой отводится метке L. Каждый раз, когда пакет проходит очередной маршрутизатор P вдоль туннеля, метка L анализируется и заменяется новым значением. И только после достижения конечной точки туннеля маршрутизатора PE2 из стека извлекается метка Lvpn. В зависимости от ее значения пакет направляется на тот или иной выходной интерфейс маршрутизатора PE2.

Из таблицы VRF2A, связанной с данным интерфейсом и содержащей маршруты VPNA, извлекается запись о маршруте к узлу назначения, указывающая на CE2 в качестве следующего маршрутизатора. Заметим, что она была помещена в таблицу VRF2a протоколом IGP. Последний отрезок путешествия пакета от CE2 до узла 10.1.0.3 осуществляется традиционными средствами IP.

Несмотря на достаточно громоздкое описание механизмов MPLS VPN, процесс конфигурирования новой VPN или модификации существующей достаточно прост, поэтому он хорошо формализуется и автоматизируется. Для исключения возможных ошибок конфигурирования — например, приписывания сайту ошибочной политики импорта/экспорта маршрутных объявлений, что может привести к присоединению сайта к чужой VPN, — некоторые производители разработали автоматизированные программные системы конфигурирования MPLS. Примером может служить Cisco VPN Solution Center, который снабжает администратора средствами графического интерфейса для формирования состава каждой VPN, а затем переносит полученные конфигурационные данные в маршрутизаторы PE.

Повысить степень защищенности MPLS VPN можно с помощью традиционных средств: например, применяя средства аутентификации и шифрования IPSec, устанавливаемые в сетях клиентов или в сети провайдера. Услуга MPLS VPN может легко интегрироваться с другими услугами IP, например, с предоставлением доступа к Internet для пользователей VPN с защитой их сети средствами межсетевого экрана, установленного в сети

провайдера. Провайдер также может предоставлять пользователям MPLS VPN услуги, базирующиеся на других возможностях MPLS: в частности, услуги с предоставлением гарантированного качества обслуживания на основе методов MPLS Traffic Engineering. Механизм виртуального маршрутизатора полностью изолирует эти таблицы от глобальных таблиц маршрутизации провайдера, что обеспечивает необходимые уровни надежности и масштабируемости решений MPLS VPN.

2.4.2 Модели сети VPN MPLS

С помощью VPN можно осуществить соединения: сеть-сеть, узел-сеть или узел-узел. Такие свойства технологии VPN предоставляют возможность объединить территориально удаленные друг от друга локальные сети офисов компании в единую корпоративную информационную сеть. Необходимо отметить, что корпоративные вычислительные сети (КВС) можно организовывать и на базе выделенных (частных или арендованных) каналов связи. Такие средства организации используются для небольших КВС (предприятий с компактно расположенными офисами) с неизменяющимся во времени трафиком.

Известны основные виды VPN и их комбинации:

- Intranet VPN (внутрикорпоративные VPN);
- Extranet VPN (межкорпоративные VPN);
- Remote Access VPN (VPN с удаленным доступом);
- Client/Server VPN (VPN между двумя узлами корпоративной сети).

В настоящее время для построения корпоративных территориально распределенных сетей в разделяемой инфраструктуре сервис-провайдеров и операторов связи применяются следующие технологий:

- IP-туннели с использованием технологий GRE или IPSec VPN;
- SSL, к которой относятся OpenVPN и SSL VPN (SSL/TLS VPN) для организации безопасных каналов связи;

- MPLS в сети оператора (L3 VPN) или VPN в сети BGP/MPLS;
- Metro Ethernet VPN в сети оператора (L2 VPN). Наиболее перспективная технология, используемая в Metro Ethernet VPN, - это VPN на базе MPLS (MPLS L2 VPN) или VPLS.

Что касается применения выделенных линий и технологий Frame Relay, ATM для организации корпоративных территориально распределенных сетей, то они уже для этих целей практически не применяются. Сегодня, как правило, КВС строятся на основе оверлейных сетей (клиент-серверных и одноранговых сетей), которые работают в разделяемой инфраструктуре операторов, и являются «надстройками» над классическими сетевыми протоколами.

Для организации территориально распределенных корпоративных сетей провайдеры предоставляют заказчикам следующие основные модели VPN в среде Интернет:

- модель IP VPN (GRE, IPSec VPN, OpenVPN) через WAN сеть, в которой настройка VPN обеспечивается заказчиком;
- модель L 3 VPN или MPLS L3 VPN через WAN сеть, в которой настройка VPN обеспечивается сервис-провайдером или оператором связи;
- модель L2 VPN через MAN сеть, в которой настройка VPN обеспечивается провайдером или оператором связи:
  - point-to-point (AToM, 802.1Q, L2TPv3);
  - multipoint (VPLS и H-VPLS).

Технологии VPN можно классифицировать и по способам их реализации с помощью протоколов: аутентификации, туннелирования и шифрования IP-пакетов. Например, VPN (IPSec, OpenVPN, PPTP) основаны на шифровании данных заказчиков, VPN (L2TP и MPLS) базируются на разделении потоков данных между заказчиками VPN, а SSL VPN основана на криптографии и аутентификации трафика. Но, как правило, VPN используют смешанные варианты, когда совместно используются технологии: аутентификации, туннелирования и шифрования. В основном организация VPN-сетей

осуществляется на основе протоколов канального и сетевого уровней модели OSI.

Необходимо отметить, что для мобильных удаленных пользователей была разработана технология SSL VPN (Secure Socket Layer - уровень защищенных сокетов), которая основана на ином принципе передачи частных данных (данных пользователей) через Интернет. Для организации SSL VPN используется протокол прикладного уровня HTTPS. Для HTTPS используется порт 443, по которому устанавливается соединение с использованием TLS (Transport Layer Security - безопасность транспортного уровня).

TLS и SSL (TLS и SSL- протоколы 6 уровня модели OSI) - это криптографические протоколы, которые обеспечивают надежную защиту данных прикладного уровня, так как используют асимметричную криптографию, симметричное шифрование и коды аутентичности сообщений. Но поскольку в стеке TCP/IP определены 4 уровня, т.е. отсутствуют сеансовый и представительский уровни, то эти протоколы работают над транспортным уровнем в стеке TCP/IP, обеспечивая безопасность передачи данных между узлами сети Интернет.

2.4.3 Модель IP VPN, в которой настройка VPN обеспечивается заказчиком

Модель IP VPN может быть реализована на базе стандарта IPSec или других протоколов VPN (PPTP, L2TP, OpenVPN). В этой модели взаимодействие между маршрутизаторами заказчика устанавливается через WAN сеть сервис-провайдера. В этом случае провайдер не участвует в настройке VPN, а только предоставляет свои незащищённые сети для передачи трафика заказчика. Сети провайдеров предназначены только для инкапсулированного или наложенного (прозрачного) соединения VPN между офисами заказчика.

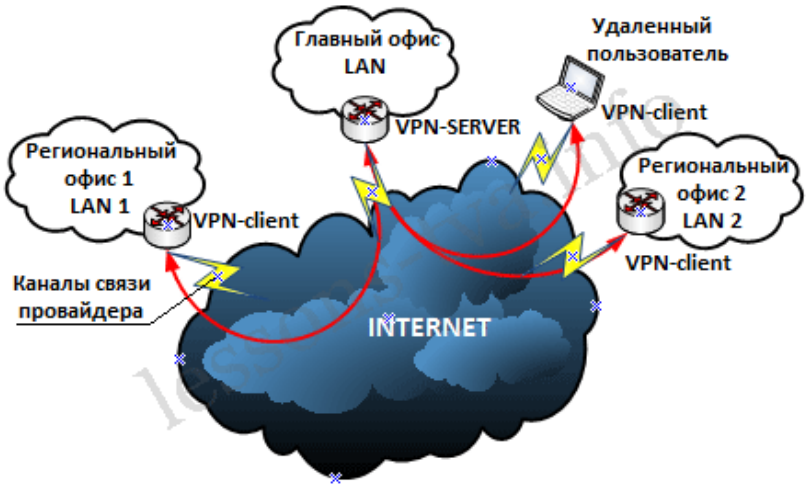
Настройка VPN осуществляется телекоммуникационными средствами заказчика, т.е. заказчик сам управляет маршрутизацией трафика. VPN соединение – это соединение поверх незащищённой сети типа точка-точка:

«VPN шлюз - VPN шлюз» для объединения удаленных локальных сетей офисов, «VPN пользователь - VPN шлюз» для подключения удаленных сотрудников к центральному офису.

Для организации VPN-сети в каждый офис компании устанавливается маршрутизатор, который обеспечивает взаимодействие сети офиса с VPN-сетью. На маршрутизаторы устанавливается программное обеспечение для построения защищённых VPN, например, бесплатный популярный пакет OpenVPN (в этом случае пакет OpenVPN надо сконфигурировать для работы в режиме маршрутизации). Технология OpenVPN основана на SSL стандарте для осуществления безопасных коммуникаций через Интернет.

OpenVPN обеспечивает безопасные соединения на основе 2-го и 3-го уровней OSI. Если OpenVPN сконфигурировать для работы в режиме моста - он обеспечивает безопасные соединения на основе 2 уровня OSI, если в режиме маршрутизации - на основе 3-го уровня. OpenVPN в отличие от SSL VPN не поддерживает доступ к VPN-сети через web-браузер. Для OpenVPN требуется дополнительное приложение (VPN-клиент).

Маршрутизатор головного офиса компании настраивается в качестве VPN-сервера, а маршрутизаторы удаленных офисов в качестве VPN-клиентов. Маршрутизаторы VPN-сервер и VPN -клиенты подключаются к Интернету через сети провайдера. Кроме того, к главному офису можно подключить ПК удаленного пользователя, настроив на ПК программу VPN-клиента. В итоге получаем модель IP VPN (скриншот представлен на рис. 2.3).



¶

Рисунок 2.3- Модель сети IP VPN (Intranet VPN + Remote Access VPN)

2.4.4 Модель MPLS L3 VPN или L3 VPN, в которой настройка VPN обеспечивается сервис-провайдером или оператором связи (поставщиком услуг)

Рассмотрим процесс организации VPN-сети для трех удаленных локальных сетей офисов заказчика услуг (например, корпорации SC-3), размещенных в различных городах, с помощью магистральной сети MPLS VPN поставщика услуг, построенной на базе технологии MPLS L3 VPN. Кроме того, к сети корпорации SC-3 подключен ПК удаленного рабочего места и ноутбук мобильного пользователя. В модели MPLS L3 VPN оборудование провайдера участвует в маршрутизации клиентского трафика через сеть WAN.

В этом случае доставка клиентского трафика от локальных сетей офисов заказчика услуг к магистральной сети MPLS VPN поставщика услуг осуществляется с помощью технологии IP. Для организации VPN-сети в каждый офис компании устанавливается периферийный или пограничный CE-маршрутизатор (Customer Edge router), который соединяется физическим каналом с одним из пограничных PE-маршрутизаторов (Provider Edge router) сети MPLS провайдера (оператора). При этом на физическом канале, соединяющем CE и PE маршрутизаторы, может работать один из протоколов канального уровня (PPP, Ethernet, FDDI, FR, ATM и т.д.).

Сеть поставщика услуг (сервис-провайдера или оператора связи) состоит из периферийных PE-маршрутизаторов и опорной сети (ядра сети) с коммутирующими по меткам магистральными маршрутизаторами P (Provider router). Таким образом, MPLS L3 VPN состоит из офисных локальных IP-сетей заказчика и магистральной сети MPLS провайдера (домена MPLS), которая объединяет распределенные локальные сети офисов заказчика в единую сеть.

Удаленные локальные сети офисов заказчика обмениваются IP-пакетами через сеть провайдера MPLS, в которой образуются туннели MPLS для передачи клиентского трафика по опорной сети поставщика. Скриншот модели сети MPLS L3 VPN (Intranet VPN + Remote Access VPN) представлен на рис. 2.4. С целью упрощения схемы сети приняты следующие начальные условия: все ЛВС офисов относятся к одной VPN, а опорная (магистральная) сеть является доменом MPLS (MPLS domain), находящаяся под единым управлением национального сервис-провайдера (оператора связи).

Необходимо отметить, что MPLS L3 VPN может быть организована с помощью нескольких доменов MPLS разных сервис-провайдеров. На рисунке 2.4 представлена полносвязная топология VPN.

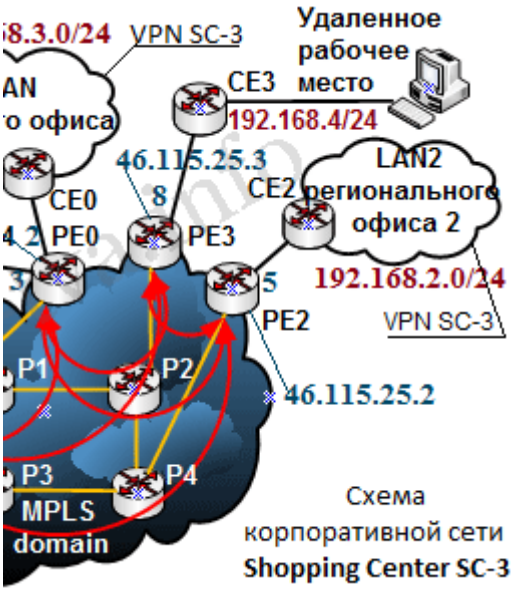


Рисунок 2.4 – Модель сети MPLS L 3 VPN (Intranet VPN + Remote Access VPN)

Функционирование PE-маршрутизаторов

Периферийные маршрутизаторы CE и PE (заказчика и провайдера) обмениваются друг с другом маршрутной информацией одним из внутренних протоколов маршрутизации IGP (RIP, OSPF или IS-IS). В результате обмена маршрутной информацией каждый PE-маршрутизатор создает свою отдельную (внешнюю) таблицу маршрутизации VRF (VPN Routing and Forwarding) для локальной сети офиса заказчика, подключенной к нему через CE-маршрутизатор. Таким образом, маршрутная информация, полученная от CE, фиксируется в VRF-таблице PE.

Таблица VRF называется виртуальной таблицей маршрутизации и продвижения. Только PE-маршрутизаторы знают о том, что в сети MPLS организована VPN для заказчика. Из модели сети MPLS L3 VPN следует, что между CE-маршрутизаторами заказчика не осуществляется обмен маршрутной информацией, поэтому заказчик не участвует в маршрутизации трафика через магистраль MPLS, настройку VPN (PE-маршрутизаторов и P-маршрутизаторов) осуществляет провайдер (оператор).

К PE-маршрутизатору могут быть подключены несколько VPN-сетей разных заказчиков (рис.2.5). В этом случае на каждый интерфейс (int1, int2 и т.д.) PE-маршрутизатора, к которому подключена локальная сеть офиса заказчика, устанавливается отдельный протокол маршрутизации. Для каждого интерфейса PE-маршрутизатора один из протоколов IGP создает таблицу маршрутизации VRF, а каждая таблица маршрутизации VRF соответствует VPN-маршрутам для каждого заказчика.

Например, для заказчика SC-3 и его сети LAN0 (главного офиса), подключенной через CE0 к PE0, на PE0 будет сформирована таблица VRF1 SC-3, для LAN1 заказчика SC-3 на PE1 будет создана VRF2 SC-3, для LAN2 на PE2 - VRF3 SC-3 и т.д., а принадлежат они одной VPN SC3. Таблица VRF1 SC-3 является общей для маршрутной информации CE0 и CE4. Необходимо отметить, что таблицы VRF пополняются информацией об адресах локальных сетей всех других офисов данного заказчика с помощью протокола MP-BGP (multiprotocol

BGP). Протокол MP-BGP используется для обмена маршрутами непосредственно между PE-маршрутизаторами и может переносить в маршрутной информации адреса VPN-IPv4.

Адреса VPN-IPv4 состоят из исходных адресов IPv4 и префикса RD (Route Distinguisher) или различителя маршрутов, который идентифицирует конкретную VPN. В итоге на маршрутизаторах PE будут созданы VRF-таблицы с идентичными маршрутами для одной сети VPN. Только те PE-маршрутизаторы, которые участвуют в организации одной и той же VPN-сети заказчика, обмениваются между собой маршрутной информацией по протоколу MP-BGP. Префикс RD конфигурируется для каждой VRF-таблицы.

Маршрутизация

Маршрутная информация, которой обмениваются PE-маршрутизаторы по протоколу MP-BGP через глобальный или внутренний интерфейс:

- Адрес сети назначения (VPN-IPv4);
- Адрес следующего маршрутизатора для протокола (next hop);
- Метка Lvpn – определяется номером интерфейса (int) PE - маршрутизатора, к которому подключена одна из ЛВС офиса заказчика;
- Атрибут сообщения RT (route-target) – это атрибут VPN, который идентифицирует все ЛВС офисов, принадлежащие одной корпоративной сети заказчика или одной VPN.

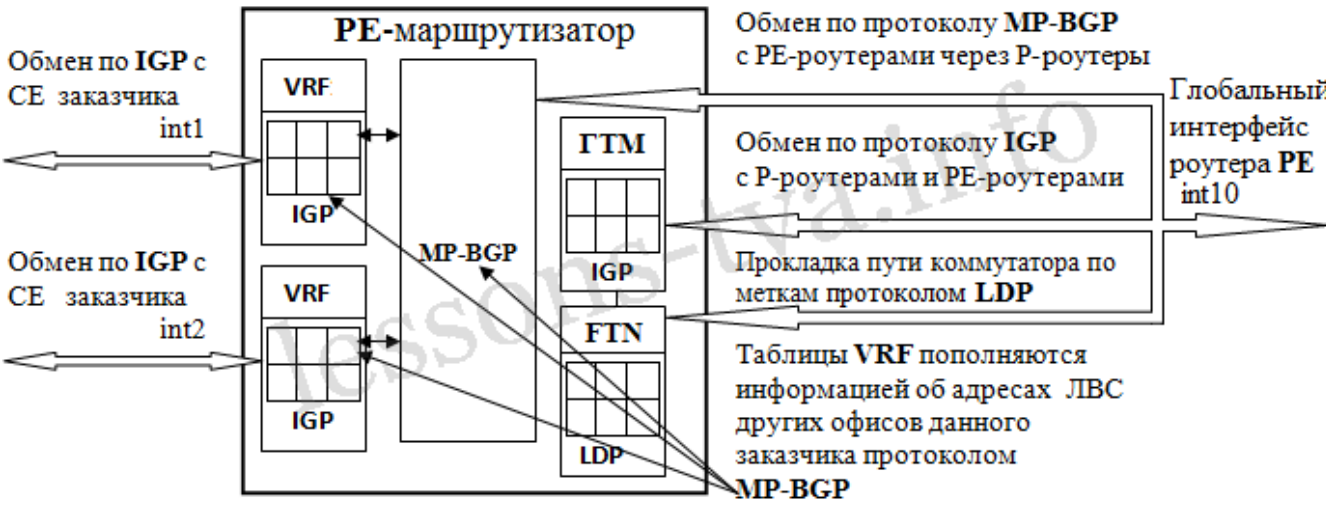


Рисунок 2.5 – Схема PE-маршрутизатора

Кроме того, каждый PE-маршрутизатор обменивается маршрутной информацией с магистральными P-маршрутизаторами одним из внутренних протоколов маршрутизации (OSPF или IS-IS) и создает также отдельную (внутреннюю) глобальную таблицу маршрутизации (GTM) для магистральной сети MPLS. Внешняя (VRF) таблица и внутренняя (GTM) глобальная таблицы маршрутизации в PE-маршрутизаторах изолированы друг от друга. P-маршрутизаторы обмениваются маршрутной информацией между собой и PE-маршрутизаторами с помощью традиционных протоколов внутренней IP-маршрутизации (IGP), например OSPF или IS-IS, и создают свои таблицы маршрутизации.

На основе таблиц маршрутизации с помощью протоколов распределения меток LDP или протоколов RSVP на основе технологии Traffic Engineering строятся таблицы коммутации меток на всех маршрутизаторах P (на PE создаются FTN), образующих определенный маршрут LSP (Label Switched Paths). В результате формируются маршруты с коммутацией по меткам LSP, по которым IP-пакеты продвигаются на основе значений меток заголовка MPLS и локальных таблиц коммутации, а не IP-адресов и таблиц маршрутизации.

Заголовок MPLS добавляется к каждому IP-пакету, поступающему на входной PE-маршрутизатор, и удаляется выходным PE-маршрутизатором, когда пакеты покидают сеть MPLS. В заголовке MPLS используется не метка, а стек из двух меток, т.е. входной PE назначает пакету две метки. Одна из них внешняя L, другая внутренняя Lvpn. Внешняя метка или метка верхнего уровня стека используется непосредственно для коммутации пакета по LSP от входного до выходного PE.

Необходимо отметить, что PE направляет входной трафик в определенный виртуальный путь LSP на основании FEC (Forwarding Equivalence Class – класса эквивалентности продвижения). FEC – это группа пакетов к условиям, транспортировки которых предъявляются одни и те же требования. Пакеты,

принадлежащие одному FEC, перемещаются по одному LSP. Классификация FEC может осуществляться различными способами, например: по IP-адресу сети (префиксу сети) назначения, типу трафика, требованиям инжиниринга и т.д.

Если использовать классификацию по IP-адресу сети назначения, то для каждого префикса сети назначения создается отдельный класс. В этом случае протокол LDP полностью автоматизирует процесс создание классов и назначение им значений меток (таблица 2.1). Каждому входящему пакету, который направляется маршрутизатором PE на определенный IP-адрес сети офиса, назначается определенная метка на основании таблицы FTN.

Таблица 2.1 – Таблица FTN (FEC To Next hop) на маршрутизаторе PE1

Признаки FEC	Метка
192.168.2.0/24	107
192.168.3.0/24	105
192.168.4.0/24	108
192.168.5.0/24	109

Из таблицы 2.1 следует, что значение внешней метки назначает входной маршрутизатор PE1 на основании IP-адреса локальной сети офиса. Внутренняя метка или метка нижнего уровня стека в процессе коммутации пакета по LSP от входного до выходного PE не участвует, а она определяет VRF или интерфейс на выходном PE, к которому присоединена ЛВС офиса заказчика.

Обмен информацией о маршрутах VPN по протоколу MP-BGP

Маршрутная информация (информация о маршрутах VPN), которую передает маршрутизатор PE1 маршрутизатору PE2 по протоколу BGP (красные линии):

- Адрес VPN-IPv4: 46.115.25.1:106:192.168.1.0;
- Next Hop = 46.115.25.1;
- Lvpn=3;
- RT= SC-3.

Различитель маршрутов RD=46.115.25.1:106 добавляется к IPv4-адресу сети LAN1 регионального офиса 1. Где 46.115.25.1 – это IP-адрес глобального интерфейса маршрутизатора PE1, через который PE1 взаимодействует с P-маршрутизаторами. Для данного маршрута VPN SC-3 администратор сети провайдера в маршрутизаторе PE1 или PE1 назначает метку (номер), например 106.

Когда маршрутизатор PE2 получает от PE1 адрес сети назначения VPN-IPv4, он отбрасывает разграничитель маршрутов RD, помещает адрес 192.168.1.0 в таблицу VRF3 SC-3 и отмечает, что запись была сделана протоколом BGP. Кроме того, он объявляет этот маршрут, подключенному к нему маршрутизатору заказчика CE2 для данной VPN SC-3.

Таблица VRF3 SC-3 также пополняется протоколом MP-BGP – об адресах сетей других ЛВС офисов данной VPN SC-3. Маршрутизатор PE1 направляет по протоколу MP-BGP маршрутную информация также другим маршрутизаторам: PE0 и PE3. В итоге, все маршруты в таблицах VRF маршрутизаторов (PE0, PE1, PE2 и PE3) содержат адреса всех сетей ЛВС офисов данного заказчика в формате IPv4.

Таблица 2.2 - Таблицы VRF маршрутизаторов (PE0, PE1, PE2 и PE3)

VRF1 SC-3		Router PE0		VRF2 SC-3		Router PE1	
Подсеть	Протокол	N	Lvn	Подсеть	Протокол	N	Lvn
192.168.24	BGP	PE	3	192.168.1/4	IGP	C1	3
192.168.24	BGP	PE2	5	192.168.2/4	BGP	P2	5
192.168.	IGP	CE0	2	192.168.3/	BGP	P	2

24				1		0	
192.168.24	BGP	PE3	8	192.168.4/1	BGP	P3	8
192.168.24	IGP	CE4	3	192.168.5/1	BGP	P0	3

VRF3 SC-3		Router PE2		VRF4 SC-3		Router PE3	
Подсеть	Протокол	N	Lvn	Подсеть	Протокол	N	Lvn
192.168.24	BGP	PE	3	192.168.1/1	BGP	P1	3
192.168.24	IGP	CE2	5	192.168.2/1	BGP	P2	5
192.168.24	BGP	PE0	2	192.168.3/1	BGP	P0	2
192.168.24	BGP	PE3	8	192.168.4/1	IGP	C3	8
192.168.24	BGP	PE0	3	192.168.5/1	BGP	P0	3

Маршрутная информация, которую передает маршрутизатор PE2 маршрутизатору PE1 по протоколу MP-BGP (красные линии):

- Адрес VPN-IPv4: 46.115.25.2:116:192.168.2.0;
- Next Hop = 46.115.25.2;
- Lvpn=5;
- RT=SC-3.

Передача данных между ПК в корпоративной сети организованной на базе технологии MPLS L3 VPN

Рассмотрим, как происходит обмен данными между ПК 2 (IP: 192.168.1.2) сети LAN1 и ПК 1 (IP: 192.168.3.1) сети LAN. Для доступа к файлам, размещенным в директориях или логических дисках ПК 1 (LAN) с общим доступом, необходимо на ПК 2 (LAN1) в строке "Найти программы и файлы"

ввести \\192.168.3.1 и нажать клавишу Enter. В результате на экране ПК 2 будут отображены директории с общим доступом (" расшаренные" директории или папки), которые размещены на ПК 1. Как это происходит?

При нажатии клавишу Enter в ПК 2 (LAN1) на сетевом уровне сформировался пакет с IP-адресом назначения 192.168.3.1. В первую очередь пакет поступает на маршрутизатор CE1 (рис. 2.6), который направляет его в соответствии с таблицей маршрутизацией на интерфейс int3 маршрутизатора PE1, так как он является следующим маршрутизатором для доступа к сети 192.168.3.0/24, в которой находятся ПК 1 (LAN ГО) с IP-адресом 192.168.3.1. С интерфейсом int3 связана таблица маршрутизации VRF2 SC-3, поэтому дальнейшее продвижение пакета осуществляется на основе ее параметров.

Как следует из таблицы VRF2 SC-3, следующим маршрутизатором для продвижения пакета к сети 192.168.3/24 является PE0 и эта запись была выполнена протоколом BGP. Кроме того, в таблице указано значение метки Lvpn=2, которая определяет интерфейс выходного маршрутизатора PE0. Отсюда следует, что дальнейшее продвижение пакета к сети 192.168.3/24 определяется параметрами глобальной таблицы маршрутизации ГТМ PE1.

В глобальной таблице (ГТМ PE1) адресу следующего маршрутизатора (NH - Next Hop) PE0 соответствует начальное значение внешней метки L=105, которая определяет путь LSP до PE0. Продвижение пакета по LSP происходит на основании L-метки верхнего уровня стека (L=105). Когда пакет проходит через маршрутизатор P3, а затем через маршрутизатор P1, метка L анализируется и заменяется новыми значениями. После достижения пакетом конечной точки LSP, маршрутизатор PE0 удаляет внешнюю метку L из стека MPLS.

Рисунок 2.6 – Передача данных между ПК2 (192.168.1.2) и ПК1 (192.168.3.1) сетей LAN1 и LAN главного офиса КС SC-3

Затем маршрутизатор PE0 извлекает из стека метку нижнего уровня стека Lvpn=2, которая определяет интерфейс int2, к которому присоединен маршрутизатор CE0 локальной сети главного офиса заказчика (LAN ГО). Далее из таблицы (VRF1 SC-3), содержащей все маршруты VPN SC3, маршрутизатор PE0 извлекает запись о значении метки Lvpn=2 и о связанном с ней маршруте к сети 192.168.3/24, который указывает на CE0 в качестве следующего маршрутизатора. Из таблицы следует, что запись о маршруте была помещена в таблицу VRF1 SC-3 протоколом IGP, поэтому путь движения пакета от PE0 до CE0 осуществляется по IP-протоколу.

Дальнейшее движение пакета от CE0 к ПК 1 с IP-адресом 192.168.3.1 осуществляется по MAC-адресу, так как CE0 и ПК 1 (192.168.3.1) находятся в одной ЛВС. После получения пакета-запроса от ПК 2 операционная система компьютера ПК 1 отправит копии своих директорий с общим доступом для ПК 2. Операционная система ПК 2, получив копии директорий с общим доступом от ПК 1, отображает их на экране монитора. Таким образом, через общественные сети MPLS провайдера по виртуальным каналам LSP осуществляется обмен данными между двумя ПК, принадлежащим разным ЛВС офисов одного заказчика.

Что касается подключения удаленного мобильного пользователя к ресурсам территориально распределенной корпоративной сети, то его можно реализовать с помощью одной из технологий Remote Access VPN (Remote Access IPSec VPN и SSL VPN). Необходимо отметить, что технология SSL VPN поддерживает два типа доступа: полный сетевой доступ и clientless. Технология clientless SSL VPN обеспечивает удаленный доступ к сети через стандартный веб-браузер, но в этом случае доступны только сетевые приложения с web-интерфейсом. Технология SSL VPN с полным сетевым доступом, после установки на ПК дополнительного приложения (VPN-клиента) обеспечивает доступ ко всем ресурсам территориально распределенной корпоративной сети.

Как правило, подключение удалённого пользователя к MPLS L3 VPN производится посредством сервера удаленного доступа (RAS), который подключается к одному из PE-маршрутизаторов MPLS сети. В нашем случае мобильный пользователь через сеть доступа (Интернет) подключен с помощью Remote Access IPSec VPN к RAS, который соединен с маршрутизатором PE0. Таким образом, мобильный пользователь через IPSec VPN подключается к своей корпоративной сети (корпорации SC-3), организованной на основе MPLS L3 VPN.

2.4.5 Модель MPLS L2 VPN, в которой настройка VPN обеспечивается провайдером или оператором связи (поставщиком услуг)

Организовать единое информационное пространство в трех офисах (например, корпорации SC-3), расположенных в пределах одного города можно на базе широкополосной Metro Ethernet сети оператора связи (L2 VPN). Одной из услуг сетей Metro Ethernet является организация корпоративных сетей через магистральные сети MAN (сети оператора связи в масштабах города). Для организации Metro Ethernet VPN (L2 VPN) используются различные технологии, например AToM (в основном EoMPLS), 802.1Q, L2TPv3 и так далее, но наиболее перспективной является технология MPLS L2 VPN или VPLS. В этом случае доставка клиентского трафика от локальных сетей офисов заказчика услуг к опорной сети MPLS VPN поставщика услуг осуществляется с помощью технологии второго уровня (Ethernet, Frame Relay или ATM).

Операторы связи предоставляют два типа услуг Ethernet сетей для организации виртуальных частных сетей на втором уровне модели OSI, которые формируются на базе технологии MPLS - это VPWS (Virtual Private Wire Services) и VPLS (Virtual Private LAN Services). Эти VPN строятся на базе псевдоканалов (pseudowire), которые связывают пограничные PE-маршрутизаторы сети провайдера (MPLS domain). Туннели LSP или логические каналы создаются при помощи меток, внутри которых прокладываются

псевдоканалы (эмулированные VC) и по этим псевдоканалам передаются пакеты MPLS. VPWS основана на Ethernet over MPLS (EoMPLS). Но в VPLS в отличие от сетей point-to-point (P2P) VPWS организация псевдоканалов осуществляется с помощью многоточечных соединений (P2M).

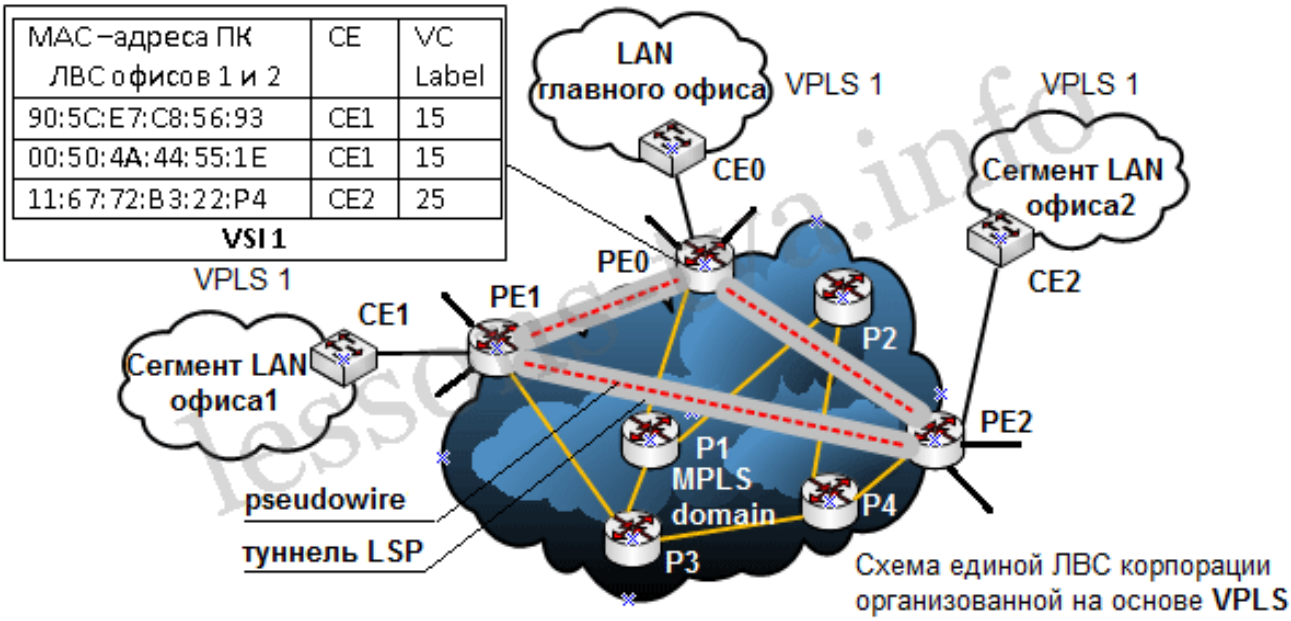
В VPLS существует два способа установления псевдоканалов между любыми двумя PE, которые входят в состав данной VPLS (с помощью протокола BGP и протокола рассылки меток LDP). Расширенный протокол BGP (MP-BGP) обеспечивает автоматическое определения PE, которые взаимодействуют при построении территориально распределенной ЛВС на основе сервиса VPLS, и сигнализацию меток (vc-labels) виртуальных каналов. Для сигнализации vc-labels можно использовать и расширенный протокол LDP. В этом случае выявление всех PE-маршрутизаторов, которые входят в состав данной VPLS, осуществляется в режиме ручной настройки.

Можно также использовать системы управления, которые автоматизируют поиск и настройку PE устройств для организации VPLS сервисов. Для передачи кадров использует стек меток, верхняя метка предназначена для туннелей LSP, которая используется для достижения выходного PE. Нижняя метка - это метка VC Label, которая используется для демультиплексирования виртуальных каналов (pseudowires), передаваемых внутри одного туннеля. В одном туннеле может быть проложено множество псевдоканалов для разных экземпляров VPLS.

Для каждого экземпляра VPLS на PE создаются отдельные виртуальные коммутаторы VSI. Коммутаторы VSI изучают MAC-адреса и строят таблицы продвижения MPLS-пакетов. На основании данных таблицы продвижения коммутаторы VSI, получив кадры, инкапсулированные в пакеты MPLS, направляют их в псевдоканалы ведущие к пограничным PE, к которым подключены пограничные коммутаторы CE сегментов ЛВС офисов заказчика.

На базе VPWS (point-to-point) можно объединить две подсети офисов корпорации в одиную сеть, с единой сквозной IP-адресацией. VPLS – это

технология, которая обеспечивает многоточечные соединения поверх пакетной сетевой инфраструктуры IP/MPLS. VPLS позволяет объединить несколько территориально распределенных локальных сетей офисов корпорации в единую локальную сеть. В этом случае магистральная сеть MPLS сервис-провайдера представляет собой виртуальный Ethernet-коммутатор (L2-коммутатор), который пересылает Ethernet-фреймы между сегментами ЛВС отдельных офисов заказчика. Схема территориально распределенной (в пределах города) локальной сети корпорации представлена на рис. 2.7.



¶Рисунок 2.7 – Схема территориально распределенной локальной сети корпорации

Суть концепции VPLS заключается в прозрачной передаче Ethernet-фреймов ПК локальных сетей офисов (сегментов сетей офисов заказчика) заказчика по магистральной сети MPLS провайдера. Пограничными устройствами на стороне заказчика VPLS 1 служат коммутаторы CE0, CE1, CE2, которые соединены с устройствами PE0, PE1, PE2. PE-маршрутизаторы взаимодействуют друг с другом, с целью выявления всех PE, подключенных к VPLS 1. Устройства PE и P строят таблицы маршрутизации, на основе которых создаются каналы LSP и псевдоканалы.

В качестве протоколов сигнализации могут использоваться как BGP, так и LDP. Виртуальные коммутаторы VSI 1 устройств PE0, PE1, PE2 строят таблицы продвижения MPLS-пакетов. Например, VSI 1 устройства PE0 формирует таблицу коммутации, представленную на рис. 2.7. При поступлении Ethernet-фрейма с одного из ПК сети LAN главного офиса на вход устройства PE0 он инкапсулирует Ethernet-фрейм в MPLS пакет и, используя таблицу коммутации, направляет его в туннель, по которому пакет поступает на выходное устройство PE1.

Для продвижения пакета через MPLS сеть (через псевдоканалы в туннелях LSP) используется стек меток, который состоит из метки туннеля LSP и метки псевдоканала VC Label, например, 15. На выходном устройстве PE1 пакеты MPLS преобразуются в Ethernet-фреймы и направляются на коммутатор C1, к которому подключен ПК назначения с MAC-адресом 90:5C:E7:C8:56:93. В документах RFC 4761 и RFC 4762 подробно изложены методы сигнализации на базе протоколов BGP и LDP для локальных сетей организованных с помощью услуг VPLS.

2.4.6 Маршрутизация в сети MPLS-VPN

Виртуальные частные сети на основе MPLS (MPLS VPN) привлекают сегодня всеобщее внимание. Количество ведущих провайдеров услуг, предлагающих своим клиентам воспользоваться новым видом сервиса для экономичного построения сетей Intranet и Extranet, постоянно растет, делая MPLS VPN доступными для пользователей все большего числа стран и регионов. От других способов построения виртуальных частных сетей, подобно VPN на базе ATM/FR или IPSec, MPLS VPN выгодно отличает высокая масштабируемость, возможность автоматического конфигурирования и естественная интеграция с другими сервисами IP, которые сегодня входят в обязательное меню любого успешного провайдера: доступом к Internet, Web и почтовыми службами, хостингом.

Из всего выше изложенного можно сделать вывод, что для построения сети для удаленных офисов компании ТехноСвязьСтрой подходит модель №2 Модель MPLS L3 VPN или L3 VPN, в которой настройка VPN обеспечивается сервис-провайдером или оператором связи (поставщиком услуг). Модель №3 не подходит так как подключения такого класса используется в масштабах одного города, что неприемлемо в случае с офисами компании ТехноСвязьСтрой.

2.5 Разработка общей схемы информационно телекоммуникационной сети ТехноСвязьСтрой

В каждом региональном офисе компании ТехноСвязьСтрой используется локальная сеть связи построенная на основе технологии Ethernet. Это существенно упрощает построение и конфигурирование общей сети филиалов, так как технологии на которых она реализуется также работают на базе протокола Ethernet.

Анализ сети связи филиалов ПАО «Ростелеком» дает нам возможность построить информационно телекоммуникационную сеть для корпорации центров ТехноСвязьСтрой на базе одного провайдера связи, для таких филиалов как: Московский, Орловский, Воронежский, Курский, Липецкий.

Общая схема будет основываться на построении MPLS VPN в каждом городе отдельной схемой. В Москве находится главный офис торгового объединения ТехноСвязьСтрой, куда и должна стекаться информация о работе филиалов, откуда можно вести контроль, управление работой персонала, поставками, обмен информацией, проведением видеоконференций и сотрудничество с партнерами, что можно увидеть на рисунке 2.8.

Для организации MPLS VPN филиалов ООО ТехноСвязьСтрой строится информационно телекоммуникационная сеть на базе местного оператора связи ПАО «Ростелеком». Маршрутизаторы для осуществления транспорта сети будут

сосредоточены в сети провайдера, на уровне клиента будут выбраны маршрутизаторы CE.

Доступ филиалов к услугам телефонии будет построен с использованием мультисервисного абонентского доступа, через который будет осуществляться передача речевых сообщений от аналоговых абонентов сети.

Установление соединения абонентов VoIP телефонии торгового объединения можно описать следующим образом. Если абонент Липецкого филиала ООО ТехноСвязьСтрой звонит абоненту в филиале г. Курск, то речевой трафик пойдет по протоколу MPLS VPN , а выход на ССОП осуществляется через медиа шлюз, при этом АМТС г. Липецка и г. Курск не задействованы. В данном случае сигнальные сообщения – должны пройти через X8004 г. Москва, т.к. управление установления соединения осуществляет платформа X8004.

Если абонент Липецкого филиала ООО ТехноСвязьСтрой звонит абоненту Курского филиала, задействованы будут ресурсы построенной сети без использования АМТС городов (рис. 2.9).

Таким образом, можно сэкономить на международных и междугородних соединениях (например г. Курска или г. Липецка).

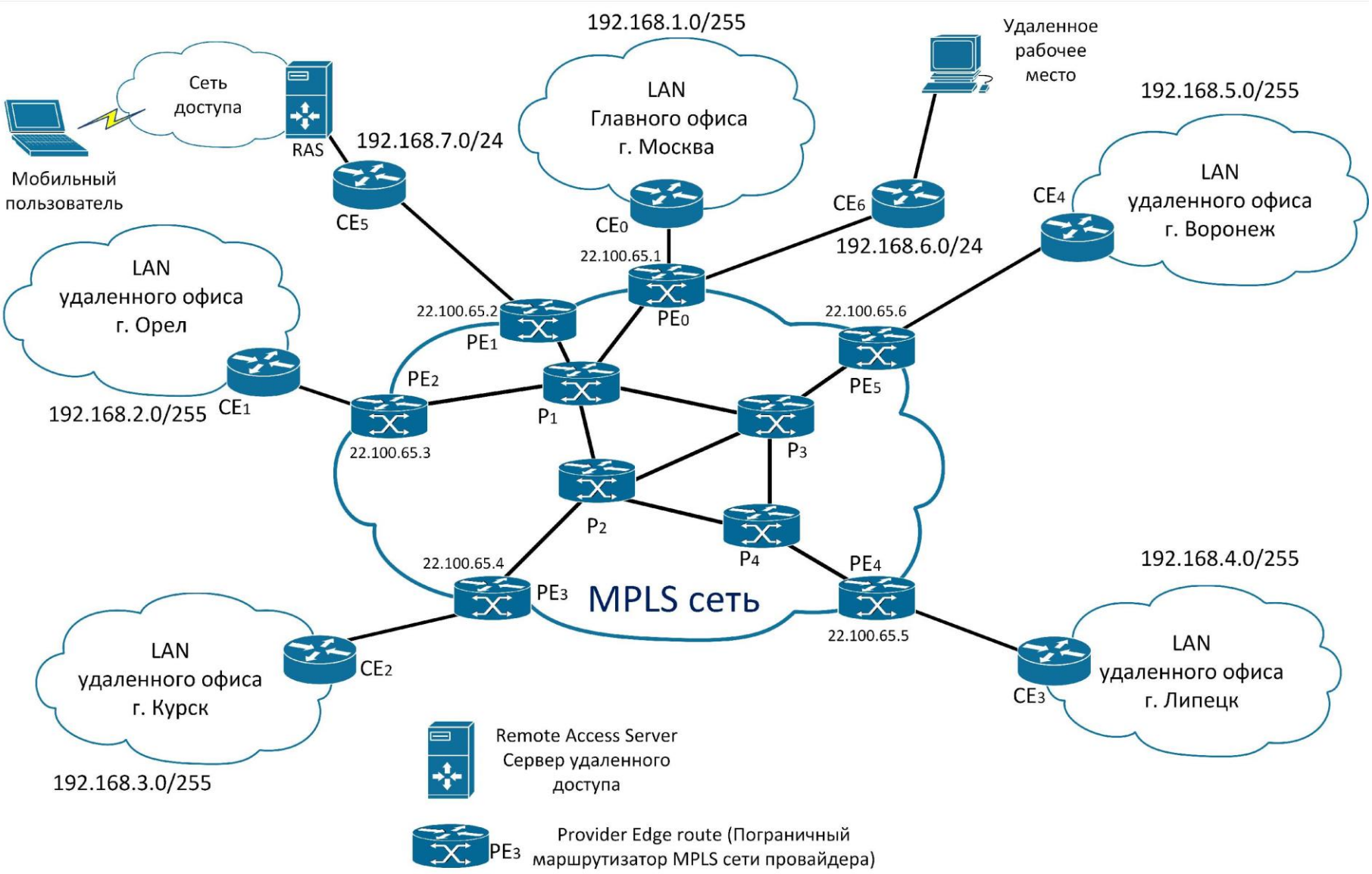


Рисунок 2.8 - MPLS VPN филиалов ООО ТехноСвязьСтрой.

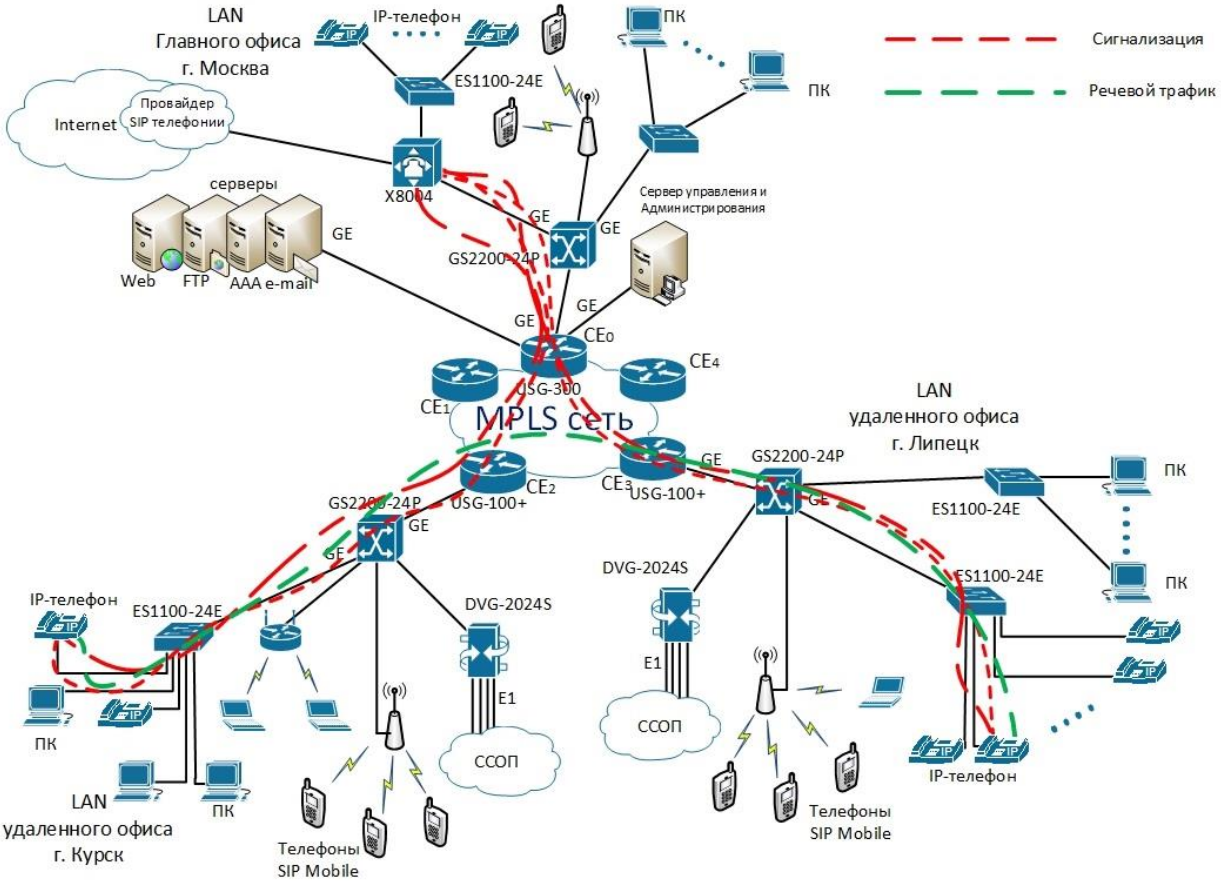


Рисунок 2.9 – Пути речевых и сигнальных пакетов при установлении голосовых соединений

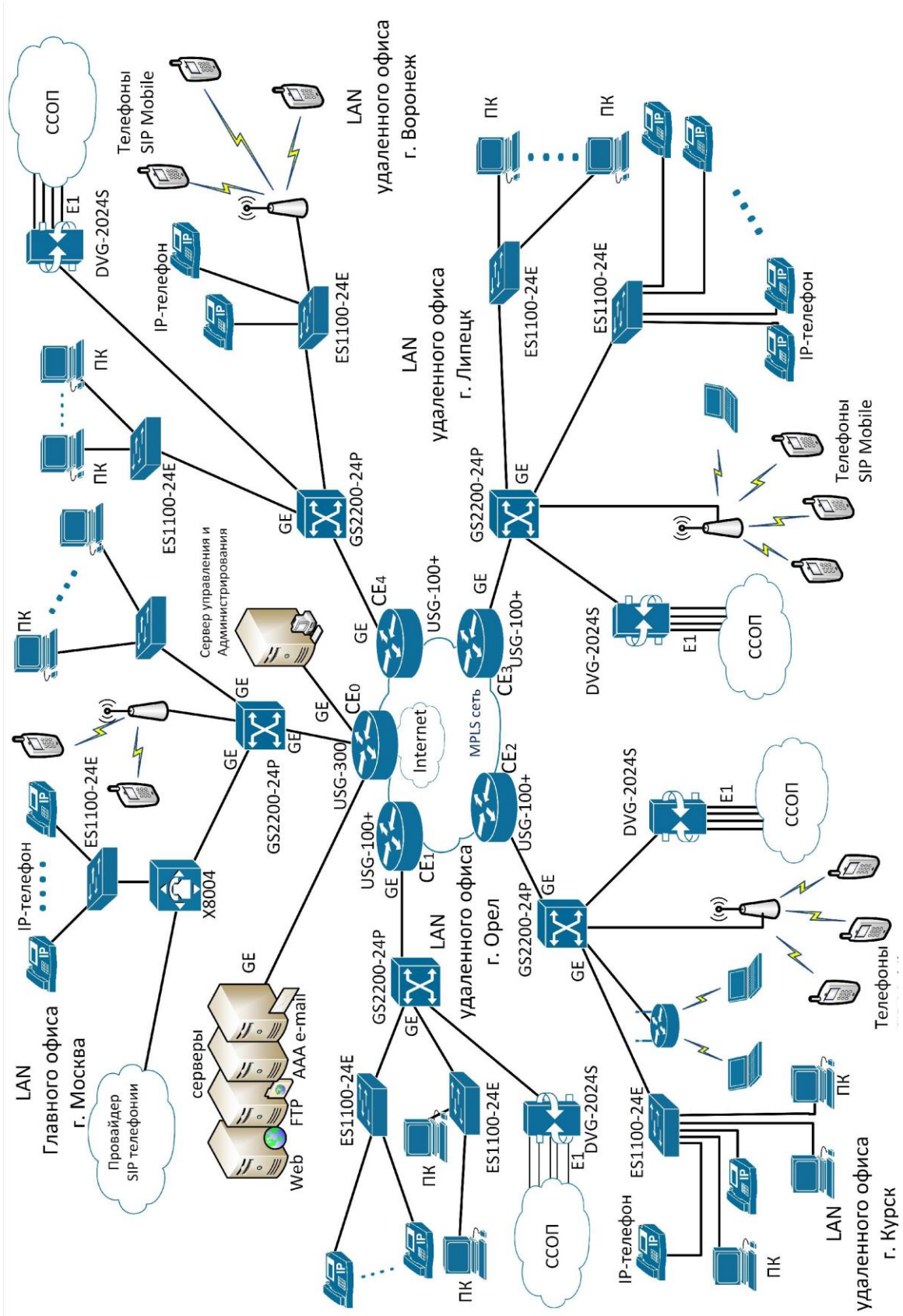


Рисунок 2.10 – Схема организации связи в филиалах ООО ТехноСвязьСтрой.

3 РАСЧЕТ ИНТЕНСИВНОСТИ НАГРУЗКИ СЕТИ СВЯЗИ ФИЛИАЛОВ ТЕХНОСВЯЗЬСТРОЙ

В проектируемой информационно телекоммуникационной сети ТехноСвязьСтрой основную полосу пропускания занимают услуги IP – телефонии, передачи данных внутри сети, доступ к глобальной сети Internet. Для предоставления остальных услуг требуется полоса пропускания существенно меньшая. Исходя, из этого рассчитаем требуемую полосу пропускания для услуг и учтем необходимый запас для предоставления оставшихся услуг.

Для правильной оценки характеристик и расчета требуемой пропускной способности для предоставления комплексных услуг используем параметры, предъявляемые сети со стороны пользователя. Проектируемая сеть должна быть надежной и на ней не должно быть перегрузок.

3.1 Расчет нагрузки информационно телекоммуникационной сети

Для проведения расчетов введем некоторые обозначения:

Московский филиал - №1;

Воронежский филиал - №2;

Орловский филиал - №3;

Курский филиал - №4;

Липецкий филиал - №5;

Расчет поступающих интенсивностей нагрузок (ИН)на каждый филиал производится по формуле:

$$Y_i = a \cdot N_i, \quad (3.1)$$

где $a=0,25$ Эрл – удельная поступающая ИН от абонентов филиалов;

N_i - емкость i-й филиала.

$Y_1 = a \cdot N_1 = 0{,}25 \cdot 50 = 12{,}5$ Эрл;

$Y_2 = a \cdot N_2 = 0{,}25 \cdot 40 = 10$ Эрл;

$Y_3 = a \cdot N_3 = 0{,}25 \cdot 40 = 10$ Эрл;

$Y_4 = a \cdot N_4 = 0{,}25 \cdot 40 = 10$ Эрл;

$Y_5 = a \cdot N_5 = 0{,}25 \cdot 40 = 10$ Эрл;

Для упрощения расчетов принимаем :

$$\frac{t_{вых\_i}}{t_{вх\_i}} = 1 \quad (3.2)$$

Нагрузка на выходе коммутационного поля (КП) определяется как:

$$Y_{вых\_i} = \frac{t_{вых\_i}}{t_{вх\_i}} \cdot Y_i \text{ , .. (3.3)}$$

где $t_{вх\_i}$ и $t_{вых\_i}$ – время занятия входа и выхода КП i-й ОТС.

$Yввы1 = Y1 = 12{,}5$ Эрл;

$Yввы2 = Y2 = 10$ Эрл;

$Yввы3 = Y3 = 10$ Эрл;

$Yввы4 = Y4 = 10$ Эрл;

$Yввы5 = Y5 = 10$ Эрл;

Интенсивность нагрузки в точке присоединения филиалов к сети ООО «Ростелеком», распределяется внутри филиалов.

Для определения внутристанционной нагрузки сначала рассчитывается общая исходящая ИН сети:

$$Y_{вых\_сети} = \sum_i Y_{вых\_i} \text{ , } (3.4)$$

где i – номер филиала;

$$Yввыхсет = 12{,}5 + 10 + 10 + 10 + 10 = 52{,}5 \text{ Эрл}$$

Затем вычисляем долю исходящей ИН для каждого филиала от общей исходящей ИН сети в процентах:

$$\eta_i = \frac{Y_{вых\_i}}{Y_{вых\_сети}} \cdot 100\% \quad , \quad (3.5)$$

$$\eta_1 = \frac{Yввы1}{Yввыхсет} \cdot 100\% = \frac{12{,}5}{52{,}5} \cdot 100\% = 23{,}81\% ;$$

$$\eta_2 = \frac{Yввы2}{Yввыхсет} \cdot 100\% = \frac{10}{52{,}5} \cdot 100\% = 19{,}05\% ;$$

$$\eta_3 = \frac{Yввы3}{Yввыхсет} \cdot 100\% = \frac{10}{52{,}5} \cdot 100\% = 19{,}05\% ;$$

$$\eta_4 = \frac{Yввы4}{Yввыхсет} \cdot 100\% = \frac{10}{52{,}5} \cdot 100\% = 19{,}05\% ;$$

$$\eta_5 = \frac{Yввы5}{Yввыхсет} \cdot 100\% = \frac{10}{52{,}5} \cdot 100\% = 19{,}05\% ;$$

Процент интенсивности внутрифилиальной нагрузки $K_{ВН\ \ i}$ от интенсивности исходящей нагрузки i-й филиала. По результатам наблюдений внутрифилиальная нагрузка составляет 10% и определяется производственной необходимостью.

$$Квн_1 = 10\% ;$$

$$Квн_2 = 10\% ;$$

$$Квн_3 = 10\% ;$$

$$Квн_4 = 10\% ;$$

$$Квн_5 = 10\% ;$$

Расчет внутристанционных ИН производим по формуле:

$$Y_{вн\_i} = \frac{K_{вн\_i} \cdot Y_{вых\_i}}{100} \quad , \quad (3.6)$$

$$Y_{вн1} = \frac{10 \cdot 12,5}{100} = 1,25 \text{ Эрл};$$

$$Y_{вн2} = \frac{10 \cdot 10}{100} = 1 \text{ Эрл};$$

$$Y_{вн3} = \frac{10 \cdot 10}{100} = 1 \text{ Эрл};$$

$$Y_{вн4} = \frac{10 \cdot 10}{100} = 1 \text{ Эрл};$$

$$Y_{вн5} = \frac{10 \cdot 10}{100} = 1 \text{ Эрл};$$

Результаты сводятся в таблицу (3.1):

Таблица 3.1 – Результаты расчетов нагрузок

номе филиала	Индекс илиала	Y , Эрл	$Y_{вых}$, рл	$K_{вн}$	$Y_{вн}$	$Y_{исх}$
1	1	12,5	12,5	10	1,2	11,25
2	2	10	10	10	1	11
3	3	10	10	10	1	11
4	4	10	10	10	1	11
5	5	10	10	10	1	11

При распределении ИН в направлении остальных филиалов пропорционально исходящим нагрузкам определим ИН от i-й филиалов к j-му :

$$Y_{ij} = \frac{Y_{исх\_i} \cdot Y_{исх\_j}}{\sum_{k=1}^{n} Y_{исх\_k} - Y_{исх\_i}}, \quad (3.7)$$

где n – число узлов.

$Y_{1-2} = 2,8$ Эрл;

$Y_{1-3} = 2,8$ Эрл;

$Y_{1-4} = 2,8$ Эрл;

$Y_{1-5} = 2{,}8$ Эрл;

Составляем матрицы телефонных нагрузок для каждого из методов распределения ИН и сводим в таблицу 3.2.

Таблица 3.2 – Матрица телефонных нагрузок филиалов

Номер зла (PBX)	1	2	3	4	5
1	-	2б8	7,3	10,2	13,2
2	7,4	-	5,26	7,4	9,6
3	7,4	5,26	-	7,4	9,6
4	10,2	7,3	7,3	-	13,2
5	12,97	9,2	9,2	12,97	-

3. 2 Расчет трафика телефонии информационно телекоммуникационной сети

Проектируемая сеть должна быть надежной и на ней не должно быть перегрузок. Поэтому все необходимые расчеты трафика будем производить для часа наибольшей нагрузки для одного оптического сетевого узла.

В начале рассчитаем трафик IP-телефонии. Для организации услуг IP-телефонии необходимо рассчитать требуемую полосу. Исходными данными для расчета являются:

1. количество источников нагрузки – абоненты, использующие терминалы SIP и подключаемые в пакетную сеть на уровне мультисервисного абонентского концентратора , N_{SIP}=300, человек;
2. тип кодека в планируемом к внедрению оборудовании, G.711;
3. длина заголовка IP-пакета, 58 байт.

Транспортный ресурс, который должен быть выделен для передачи в пакетной сети телефонного трафика, поступающего на концентратор, при условии использования кодека определяется следующим образом:

Полезная нагрузка голосового пакета G.711 CODEC составит

$$У_{полезн} = \frac{t_{звуч.голоса} \cdot \upsilon_{кодирования}}{8 \frac{бит}{байт}}, байт, \qquad (3.8)$$

где $t_{звуч.голоса}$ - время звучания голоса (мс), $\upsilon_{кодирования}$ - скорость кодирования речевого сигнала (Кбит/с).

Эти параметры являются характеристиками используемого кодека. В данном случае для кодека G.711 скорость кодирования – 8бит*8000Гц=64 Кбит/с, а время звучания голоса – 20 мс.

$$У_{полезн} = \frac{20мс \cdot 64Кбит/с}{8 \frac{бит}{байт}} = 160байт.$$

Каждый пакет имеет заголовок длиной в 58 байт. Структура заголовка IP пакета представлена на рисунке 3.1.

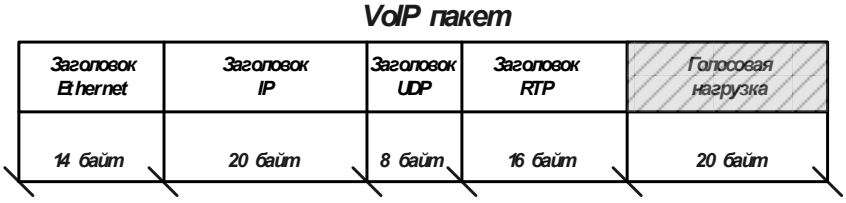


Рисунок 3.1 – Структура пакета VoIP

Общий размер голосового пакета составит

(3.9) $V_{пакета} = L_{Eth} + L_{IP} + L_{UDP} + L_{RPT} + Y_{полезн}, байт,$

где $L_{Eth,\ IP,\ UDP,\ RTP}$ – длина заголовка Ethernet, IP, UDP, RTP протоколов соответственно, (байт), $Y_{полез}$ – полезная нагрузка голосового пакета, (байт).

$V_{пакета} = 14 + 20 + 8 + 16 + 160 = 218, байт.$

Следовательно, полоса пропускания для одного вызова определится по формуле:

(3.10) $ППр_1 = V_{пакета} / t_{звучаниеголоса}, байт/с,$

где $V_{пакета}$ – размер голосового пакета, (байт).

$$ППр_1 = 218 байт / 20 мс = 87{,}2 Кбит / с.$$

В проектируемой информационно телекоммуникационной сети устанавливаются точки присутствия, в которых имеется 300 голосовых портов. Необходимая полоса пропускания для них составит

$$ППр_N = ППр_1 \cdot N \cdot Y_1, Кбит / с, \qquad (3.11)$$

где ППр $_1$ – полоса пропускания для одного вызова, (Кбит/с), N – количество голосовых портов в точках присутствия, (шт), Y_1– нагрузка от одного абонента (0,25 Эрл), это объясняется тем, что нагрузка, создаваемая в торговом секторе превышает нагрузку от одного абонента телефонной связи.

$$ППр_N = 87{,}2 Кбит / с \cdot 300 \cdot 0{,}25 Эрл = 6{,}54\ Мбит / с.$$

Результаты могли быть другими, если бы использовались другие средства кодирования/декодирования (CODEC), изменилась средняя продолжительность вызова.

3.3 Расчет трафика передачи данных

Компьютерные сети изначально предназначены для совместного доступа пользователя к ресурсам компьютеров: приложениям, файлам, принтерам и т.п. а так же для передачи мультимедийного трафика. Трафик, создаваемый этими традиционными службами компьютерных сетей, имеет свои особенности и существенно отличается от трафика сообщений в телефонных сетях или, например, в сетях кабельного телевидения. Трафик компьютерных данных характеризуется крайне неравномерной интенсивностью поступления сообщений в сеть. Так, коэффициент пульсации трафика отдельного пользователя сети, равный отношению средней интенсивности обмена данными к максимально возможной, может достигать 1:50 и даже 1:100. Но если число абонентов, обслуживаемых коммутаторами, достаточно велико, то пульсации отдельных абонентов в соответствии с законом больших чисел распределяются

во времени так, что их пики не совпадают и коэффициент пульсации на магистральных каналах значительно снижается.

Среди всех пользователей сети в час наибольшей нагрузки (ЧНН) в сети будет находиться и передавать данные только часть абонентов (активные абоненты). Даже в час наибольшей нагрузки количество активных абонентов может изменяться, поэтому для их подсчета используется пятиминутный временной интервал внутри ЧНН, и максимальное число активных абонентов за этот период времени определяется параметром Data Average Activity Factor (DAAF), в соответствии с этим количество активных абонентов составит

AS = TS*DAAF, аб, (3.12)

где TS – число абонентов на одном сетевом узле, (аб), DAAF – процент абонентов, находящихся в сети в ЧНН.

AS_1 = 50*0,8= 40 аб. (Московский филиал)

AS_2 = 40*0,8= 32 аб. (Воронежский филиал)

AS_3 = 40*0,8= 32 аб. (Орловский филиал)

AS_4 = 40*0,8= 32 аб. (Курский филиал)

AS_5 = 40*0,8= 32 аб. (Липецкий филиал)

Абоненты время от времени передают и принимают данные и, как правило, объем передаваемых данных значительно меньше объема принимаемых данных. Каждому абоненту необходимо обеспечить заявленную пропускную способность. Далее определим среднюю пропускную способность сети, требуемой для обеспечения нормальной работы пользователей.

Средняя пропускная способность для приема данных составит:

BDDA = (AS* ADBS)*(1 + OHD), Мбит/с, (3.13)

где AS - количество активных абонентов, (аб), ADBS – средняя скорость приема данных, (1.5 Мбит/с) [5], OHD – отношение длины заголовка IP пакета к его общей длине во входящем потоке .

$BDDA_1$ = (40*1, 5)*(1+0,1) = 66 Мбит/с. (Московский филиал)

$BDDA_2$ = (32*1, 5)*(1+0,1) = 52,8 Мбит/с. (Воронежский филиал)

$BDDA_3$ = (32*1, 5)*(1+0,1) = 52,8 Мбит/с. (Орловский филиал)

$BDDA_4$ = (32*1, 5)*(1+0,1) = 52,8 Мбит/с. (Курский филиал)

$BDDA_5$ = (32*1, 5)*(1+0,1) = 52,8 Мбит/с. (Липецкий филиал)

Средняя пропускная способность для передачи данных

BUDA = (AS* AUBS)*(1 + OHU), Мбит/с, (3.14)

где AS - количество активных абонентов, AUBS – средняя скорость передачи данных, (Мбит/с), OHU – отношение длины заголовка IP пакета к его общей длине во исходящем потоке .

$BUDA_1$= (40*0, 5)*(1+0,15) = 23 Мбит/с. (Московский филиал)

$BUDA_2$= (32*0, 5)*(1+0,15) = 18,4 Мбит/с. (Воронежский филиал)

$BUDA_3$= (32*0, 5)*(1+0,15) = 18,4 Мбит/с. (Курский филиал)

$BUDA_4$= (32*0, 5)*(1+0,15) = 18,4 Мбит/с. (Липецкий филиал)

$BUDA_5$= (32*0, 5)*(1+0,15) = 18,4 Мбит/с. (Орловский филиал)

Количество абонентов, передающих или принимающих данные в течении некоторого короткого промежутка времени, определяют пиковую пропускную способность сети. Количество таких абонентов в час наибольшей нагрузки определяется коэффициентом Data Peak Activity Factor (DPAF)

PS = A S*DPAF, аб, (3.15)

где DPAF – процент абонентов, одновременно принимающих или передающих данные в течении короткого интервала времени.

PS_1 = 40*0,7 = 28 аб. (Московский филиал)

PS_2 = 32*0,7 = 22,4≈23 аб. (Орловский филиал)

PS_3 = 32*0,7 = 22,4≈ 23 аб. (Курский филиал)

PS_4 = 32*0,7 = 22,4≈ 23 аб. (Липецкий филиал)

PS_5 = 32*0,7 = 22,4≈ 23 аб. (Воронежский филиал)

Пиковая пропускная способность измеряется за короткий промежуток времени (1 секунда), она необходима для приема и передачи данных в момент, когда одновременно несколько пользователей передают или принимают данные

по сети. Пиковая пропускная способность, требуемая для приема данных в час наибольшей нагрузки:

BDDP = (PS*PDBS)*(1 + OHD), Мбит/с, (3.16)

где PDBS – пиковая скорость приема данных, Мбит/с.

$BDDP_1$ = (28* 3)*(1+0,1) = 92,4 Мбит/с. (Московский филиал)

$BDDP_2$ = (23* 3)*(1+0,1) = 75,9 Мбит/с. (Орловский филиал)

$BDDP_3$ = (23* 3)*(1+0,1) = 75,9 Мбит/с. (Курский филиал)

$BDDP_4$ = (23* 3)*(1+0,1) = 75,9 Мбит/с. (Липецкий филиал)

$BDDP_5$ = (23* 3)*(1+0,1) = 75,9 Мбит/с. (Воронежский филиал)

Пиковая пропускная способность для передачи данных в ЧНН

BUDP = (PS* PUBS)*(1 + OHU), Мбит/с, (3.17)

где PUBS – пиковая скорость передачи данных, Мбит/с.

$BUDP_1$ = (28*1, 5)*(1+0,15) = 48,3 Мбит/с. (Московский филиал)

$BUDP_2$ = (23*1, 5)*(1+0,15) = 39,67 Мбит/с. (Орловский филиал)

$BUDP_3$ = (23*1, 5)*(1+0,15) = 39,67 Мбит/с. (Курский филиал)

$BUDP_4$ = (23*1, 5)*(1+0,15) = 39,67 Мбит/с. (Липецкий филиал)

$BUDP_5$ = (23*1, 5)*(1+0,15) = 39,67 Мбит/с. (Воронежский филиал)

Из расчета видно, что пиковая пропускная способность для передачи данных выше средней пропускной способности.

Для проектирования сети необходимо использовать максимальное значение полосы пропускания среди пиковых и средних значений для исключения перегрузки сети

BDD = Max [BDDA; BDDP], Мбит/ с, (3.18)

BDU = Max [BUDA; BUDP], Мбит/с, ... (3.19)

где BDD – пропускная способность для приема данных, (Мбит/с), BDU – пропускная способность для передачи данных, (Мбит/с).

BDD = Max [66; 92,4] = 92,4 Мбит/с, (Московский филиал)

BDU = Max [23;48,3] = 48,3 Мбит/с.

BDD = Max [52,8; 75,9] = 75,9 Мбит/с, (Орловский филиал)

BDU = Max [18,4; 39,67] = 39,67 Мбит/с.

BDD = Max [52,8; 75,9] = 75,9 Мбит/с, (Курский филиал)

BDU = Max [18,4; 39,67] = 39,67 Мбит/с.

BDD = Max [52,8; 75,9] = 75,9 Мбит/с, (Липецкий филиал)

BDU = Max [18,4; 39,67] = 39,67 Мбит/с.

BDD = Max [52,8; 75,9] = 75,9 Мбит/с, (Воронежский филиал)

BDU = Max [18,4; 39,67] = 39,67 Мбит/с.

Общая пропускная способность для приема и передачи данных, необходимая для нормального функционирования оптического сетевого узла, составит

BD = BDD + BDU, Мбит/с, (3.20)

где: BDD – максимальная пропускная способность для приема данных, (Мбит/с), BDU – максимальная пропускная способность для передачи данных, (Мбит/с).

BD_1 = 92,4 +48,3 = 140,7 Мбит/с. (Московский филиал)

BD_2 = 75,9 +39,67 = 115,57 Мбит/с. (Орловский филиал)

BD_3 = 75,9 +39,67 = 115,57 Мбит/с. (Курский филиал)

BD_4 = 75,9 +39,67 = 115,57 Мбит/с. (Липецкий филиал)

BD_5 = 75,9 +39,67 = 115,57 Мбит/с. (Воронежский филиал)

Итак, для передачи данных между абонентами сети на одном сетевом узле необходимые полосы пропускания.

3.4 Определение трафика информационно телекоммуникационной сети ООО ТехноСвязьСтрой

Полоса пропускания для передачи и приема трафика телефонии, видео, данных и доступа к сети Internet на одном оптическом узле составит

ППр = $ППр_{WAN}$ +AB+ BD+BWData, Мбит/с, (4.21)

где $ППр_{WAN}$ – пропускная способность для трафика IP телефонии, (Мбит/с); AB – пропускная способность для видеопотоков, (Мбит/с); BD – пропускная способность для трафика данных, (Мбит/с); BWData - пропускная способность для предоставления услуги доступа к сети Internet, (Мбит/с).

$ППр_1$ =6,54+2+140,7=148,74 Мбит/с. (Московский филиал)

$ППр_2$ =6,54+2+115,57=124,11 Мбит/с. (Орловский филиал)

$ППр_3$ =6,54+2+115,57=124,11 Мбит/с. (Курский филиал)

$ППр_4$ =6,54+2+115,57=124,11 Мбит/с. (Липецкий филиал)

$ППр_5$ =6,54+2+115,57=124,11 Мбит/с. (Воронежский филиал)

Рассчитав нагрузку создаваемую филиалами компании ТехноСвязьСтрой можно утверждать, что каналы доступа по VPN со скоростью 200 Мбит/сек. вполне достаточно для бесперебойной работы сети в целом и гарантированной передачи данных и другой передаваемой информации по ней.

4 ВЫБОР ОБОРУДОВАНИЯ

Выбор оборудования является заключительным этапом построения информационно телекоммуникационной сети компании ТехноСвязьСтрой.

Сложности преследуют в выборе производителя оборудования, число производителей и номенклатура их продуктов, для организации доступа трафика, очень масштабны, поэтому ограничимся рассмотрением предложений лишь ключевых игроков рынка.

4.1 Оборудование VoIP телефонии

Шлюз выхода на ССОП

DVG-2024S представляет собой идеальное решение Интернет-телефонии для бизнеса. Этот шлюз преобразует голосовые данные в пакеты для передачи через Интернет и полностью совместим с сервисами Интернет-телефонии SIP. Шлюзы с высокой плотностью портов и низкой себестоимостью, обеспечивают удобство в работе и гарантируют экономию средств компаний, нуждающихся в частых междугородних и международных деловых звонках.

Снижение затрат и защита инвестиций. Шлюз DVG-2024S обеспечивает легкую и недорогую модернизацию для Интернет-телефонии, позволяя пользователям сохранить ранее приобретенные телефоны и факсимильные аппараты. Защита инвестиций компании достигается благодаря использованию существующей инфраструктуры и возможности ее поэтапной модернизации.

Гарантированное качество голоса. Шлюз DVG-2024S передает голос и факсимильные сообщения в соответствии с общепринятыми международными стандартами передачи голоса и данных. Поддержка функции качества обслуживания (QoS) обеспечивает качество связи, сравнимое с аналоговой телефонией.

Интерфейсы устройства

• 24 порта FXS с 1 разъемом RJ-21

• Порт 10/100BASE-TX RJ-45 WAN

• Порт 10/100BASE-TX RJ-45 LAN

Платформа IP PBX Zyxel X8004

Zyxel X8004 Premium Office предопределена для кабинетов с числом служащих до 256. Для связи с городской телефонной сетью работают транковые модули FXO, ISDN или же E1, а SIP- транки обеспечивают включение к оператору IP-телефонии.

IP-АТС **X8004** владеет всеми многофункциональными вероятностями классической офисной АТС и приглашает вспомогательные сервисы, присущие прогрессивным IP-АТС и повышающие совместную эффективность работы всякого работника и фирмы в целом.

В малой конфигурации (Base Office) IP-АТС X8004 гарантирует полновесную работу кабинета с числом служащих до 32 и вероятность последующего расширения до 256 юзеров на одно шасси. Функция « ZyStack» разрешает совместить в стек до 5 шасси и прирастить сплошное численность юзеров до 1280.

В качестве абонентских приборов возможно применить как аппаратные и программные IP-телефоны с помощью протокола SIP, например и обыденные аналоговые телефонные аппараты, которые подключают к портам FXS модулей M6FS4 или же VoIP-шлюзам корпоративной или, в случае удаленных служащих , хозяйственной сети. Удаленные работники охраняют доступ ко всем функциям IP-АТС и считаются ее равноправными абонентами, в том числе и находясь за почти все сотки км от кабинета .

Главные способности

Самодействующая обработка вызовов. X8004 автономно маршрутизирует телефонные вызовы на базе сконфигурированных правил, обеспечивая прохождение вызовов меж IP-телефонной, городской и корпоративной телефонными сетями. X6004 распределяет имеющие место быть городские телефонные части меж юзерами , в следствии этого возможно не арендовать у телефонной фирмы отдельную линию для всякого работника.

Мобильность. Кроме транковых модулей, X6004 поддерживает функцию «SIP trunk» для включения к оператору IP-телефонии. Включив IP-АТС к Онлайну и арендовав у оператора важное численность телефонных номеров, фирма обеспечит мобильность для себя и собственным работникам. Для развертывания телефонной сети при переезде в свежий кабинет понадобится лишь только Онлайн : все телефонные номера останутся давними , и фирма не потускнеет ассоциация с покупателями и партнерами по бизнесу. В случае присвоения SIP- транкам номерной емкости иных населенных пунктов X8004 обеспечит эффект наличествия фирмы в данных ареалах .

Единая корпоративная сеть телефонии. IP-АТС **Zyxel X8004** сводит телефонные сети удаленных кабинетов через Онлайн , делая коллективные вызовы буквально бесплатными. Районные звонки возможно создавать через городскую телефонную сеть, а ассоциация меж кабинетами воплотить в жизнь по IP-сети для экономии на междугородных вызовах, оперативности и обороны секретной инфы (используя передачу голоса по VPN-туннелям). Покупатели и партнеры по бизнесу имеют все шансы даром звонить для вас через Онлайн , применяя программные или же аппаратные IP-телефоны.

Система интерактивных голосовых рационы (IVR, Interactive Voice Response) X6004 продаст до 10 иерархических значений . Возможно сделать до 3 профилей автоответчика (например, с сообщениями на российском , британском и германском языках).

Автоматическое рассредотачивание вызовов (ACD, Automated Call Distribution) исполняется на базе стратегий (набора правил) и разрешает

размеренно распределять нагрузку по операторам, использующих IP- или же аналоговые телефонные аппараты . Входящие звонки выстраиваются в очередь, а вслед за тем распределяются по свободным операторам. Админ имеет возможность избирать различные методы рассредотачивания вызовов, что разрешает устроить работу Call-центра более действенной.

Аппаратная база

- Настольное исполнение, настенное крепление или установка в телекоммуникационную стойку 19" (высота 2U , возможность установки направляющих рельс)
- Индустриальная x86 платформа:
  - PICMG PCB
  - Intel E6300
  - 2 Гб RAM
  - 500 Гб HDD SATA
  - Поддержка USB 2.0
- Два порта Gigabit Ethernet (100/1000 Мбит/с) для подключения к Интернету и корпоративной сети.
- Четыре слота для установки голосовых модулей внешних и внутренних линий:
  - Модуль M8T1E1 - 1 порт T1/E1 PRI.
  - Модуль M8FO8 - 8 портов FXO для подключения внешних аналоговых телефонных линий.
  - Модуль M8FO4FS4 - 4 порта FXO для подключения внешних аналоговых телефонных линий и 4 порта FXS для подключения телефонных или факсимильных аппаратов.
- Четыре порта USB (HID, Mass Storage).
- Дополнительный отсек для установки жесткого диска.

Ёмкость системы

- Число внутренних телефонных линий (SIP, FXS, CTI)

- По умолчанию: лицензия на 128 пользователей
- Максимальное значение: 256 пользователей

• Число внешних телефонных линий (FXO, E1, SIP- транки)

- По умолчанию: лицензия на 46 линий
- Максимальное значение: 196 линий

• Максимальное число одновременных телефонных разговоров:

- С функцией перекодирования: 64
- Без перекодирования: 196

• Максимальное число участников конференц-связи: 196

• Ёмкость памяти для записи телефонных разговоров и хранения голосовой почты (количество часов): 48000

• Характеристики Contact-центра:

- Максимальное число активных оператора: 64
- Максимальное число проектов: 32
- Максимальное число задач в каждом проекте: 16

Другие характеристики

Физические размеры: 426 (Ширина) x 445 (Глубина) x 90 (Высота) мм

Электропитание от сети переменного тока 100-240В, 50/60Гц

Внутренний блок питания мощностью 300Вт, MTBF 100000+ часов

Максимальная потребляемая мощность (без модулей внешних и внутренних линий): 113 Вт

Диапазон рабочих температур: от 15 до 40 °C

Относительная влажность: от 20 до 95 %

Масса (без дополнительных модулей): 10 кг

Функциональные возможности

SIP v2 (RFC 3261)

SDP (RFC 2327)

RTP (RFC 1889)

Поддержка кодеков G .711 a/μ, G.729, GSM.

Поддержка видео H.264.

Поддержка DTMF (inband, RFC 2833, SIP Info).

Общая и частная записные книжки неограниченного объема.

Обработка и маршрутизация на базе визуальных сценариев с учетом Caller ID, Called ID, текущих значений времени и даты, состояний линий и направлений, статусов пользователей и внутренних номеров и т.д.

IVR-сценарии необходимой вложенности и ветвления.

Настраиваемые очереди на всех внутренних номерах.

Удержание звонка, перевод звонка.

MoH (Music on Hold) – проигрывание мелодии (определенной, из списка, из каталога) с указанием места в очереди и времени ожидания.

Многосторонние конференции различного уровня (закрытые, открытые, селекторное совещание).

Переадресация звонка на базе сценариев, глобальный поиск вызываемого абонента, информирование о пропущенном звонке (или голосовой почте) через IM, SMS, E- Mail, голосовое оповещение.

Hunt-группы для групповых звонков с различными алгоритмами обхода. Позволяет реализовать базовый функционал Call-центра без дополнительных лицензий.

Перехват звонков в группе или по набранному номеру.

База данных хранения детализированной информации о звонках. Возможность удаленного доступа. Построение статистики с графическим отображением. Экспорт в Excel.

Встроенная система внутреннего IM-чата с гарантированной доставкой сообщений в CTI-приложении.

Клиент внешних IM-чатов (ICQ, Jabber) с возможностью приема и отправки сообщений.

Почтовый клиент (smtp, pop3, imap) с возможностью приема и отправки почты в различной кодировке с вложениями.

Интеграция с провайдерами SMS-сервисов (Zanzara, MessageGroup) на прием и отправку SMS-сообщений с отслеживанием статуса доставки (например, для организации массовой рассылки SMS-сообщений клиентам).

Система глубокого протоколирования событий.

Contact-центр

Contact-центр входящих звонков.

Contact-центр исходящих компаний.

Динамическая привязка ресурсов к проектам Contact-центра.

Умные очереди с учетом приоритетов клиентов.

Исходящий обзвон с использованием прогрессивного и расчетного алгоритмов.

Интеграция с внешними БД клиентов.

Мониторинг в реальном времени загрузки ресурсов Contact-центра, проектов, задач.

Статистика, написание собственных выборок на SQL.

Графическое отображение статистики.

Контрольные события.

4.2 Оборудование для организации каналов VPN

ZyWALL USG 300 – это компактный скоростной шлюз доступа нового поколения, обеспечивающий комплексное решение задач сетевой безопасности и управления трафиком, включая потоковый антивирус, обнаружение и предотвращение вторжений, защиту от спама, контроль полосы пропускания для разнообразных объектов сети и безопасность удаленных подключений при помощи виртуальных частных сетей. Устройство имеет интуитивный пользовательский интерфейс с перекрестной системой навигации, встроенным справочником и графическим мониторингом состояния. Объектно-ориентированная модель управления позволяет максимально оптимизировать

настройку даже в сложных сетях. Поддержка LDAP/MS AD/RADIUS помогает структурировать политики безопасности на основе уже существующей методики организации сети. В устройстве предусмотрено 7 универсальных портов WAN/LAN/DMZ, реализуется множественное резервирование доступа в Интернет и балансировка нагрузки. Поддерживается резервирование подключения к провайдеру с помощью USB модемов 2,5/3G и резервирование самого ZyWALL, что позволяет обеспечить отказоустойчивость. Благодаря поддержке маршрутизируемых (IPSec VPN) и двухранговых (L2TP over IPSec и SSL VPN) виртуальных частных сетей, ZyWALL USG 300 может также быть применен в роли VPN-концентратора, для объединения территориально распределенных объектов в единую сеть или создания мобильных удаленных рабочих мест.

Параллельное использование трех типов VPN в одном устройстве

В дополнение к традиционной для МСЭ поддержке виртуальных частных сетей по технологии IPSec VPN, идеальной для создания постоянных подключений типа сеть-сеть, также поддерживаются L2TP over IPSec и SSL.

Технология SSL VPN особенно удобна для создания виртуальных рабочих мест для подключенных к Интернету сотрудников, поскольку не требует настройки промежуточного оборудования и установки клиента на удаленном компьютере

Технология L2TP over IPSec поддерживается операционными системами MS Windows, а так же операционными системами Android v3.00 и iPhone iOS4, что позволяет создавать мобильные рабочие места с использованием смартфонов и планшетных компьютеров.

Настраиваемые уровни безопасности сегментов сети

ZyWALL USG 300 поддерживает технологию виртуализации канального уровня VLAN 802.1q. Интерфейсы VLAN созданные на основе физических интерфейсов позволяют разделить корпоративную сеть на нужное количество сегментов и управлять уровнем безопасности различных подразделений,

назначать гранулированные политики контроля и вести наблюдение за активностью в сетях различного уровня сложности.

Средства обеспечения сетевой безопасности

ZyWALL USG 300 располагает впечатляющим арсеналом средств обеспечения сетевой безопасности, предназначенных для защиты сетевых ресурсов и интеллектуальной собственности предприятий от угроз из Интернета.

Потоковый антивирус основанный на современных технологиях ZyXEL и Лаборатории Касперского сканирует в реальном времени Интернет- трафик, препятствуя проникновению вредоносных программ в корпоративную сеть. Благодаря регулярному автоматическому обновлению баз сигнатур антивирус способен обнаруживать и уничтожать самые новые вирусы.

Для обновления сигнатур антивируса требуется приобретение и активация специальной карты.

Система обнаружения и предотвращения вторжений (Intrusion Detection&Prevention) нейтрализует сетевых червей, трояны, бэкдоры, атаки DoS и DDoS и эксплойты, использующие известные уязвимости операционных систем и прикладных программ. Использование автоматически обновляемой базы сигнатур позволяет эффективно бороться с новыми угрозами.

Для обновления сигнатур IDP требуется приобретение и активация специальной карты

Система обнаружения аномалий (Anomaly Detection and Prevention) анализирует проходящие через шлюз пакеты на 2 и 3 уровнях OSI, выявляя аномалии (несоответствия с RFC) протоколов HTTP, TCP,UDP и ICMP, а так же позволяет обнаружить аномалии трафика. Обнаружение аномалий трафика направлено на противодействие разведывательным действиям и атакам, использующим сканирование и флуд, таким как ICMP Flood Attack, Smurf, TCP SYN Flood Attack, LAND Attack, UDP Flood Attack, Port Scanning, Decoy Port Scans, Distributed Port Scans, Port Sweeps. Обнаружение аномалий протоколов позволяет обнаружить 32 типа атак, способных привести к краху

сетевых приложений и несанкционированному доступу злоумышленников к ресурсам сети.

Система фильтрации спама (Anti-Spam 2.0) способна оградить сотрудников от лавины бесполезных и потенциально опасных сообщений e- mail рассылаемых с целью распространения рекламы, вредоносных программ и хищения конфиденциальной информации. Использование облачных технологий компании Commtouch – ведущего в отрасли производителя решений для защиты корпоративных ресурсов в Интернете – позволяет обнаруживать во входящем трафике SMTP и POP3 до 99% спама. Антивирусная проверка, использующая базы сигнатур Commtouch эффективно обнаруживает и уничтожает вредоносные файлы во вложениях.

Для подключения сервиса Commtouch Anti-Spam требуется приобретение и активация специальной карты.

Контентная фильтрация (Content Filte 2.0) основанная на технологиях компаний Blue Coat и Commtouch позволяет исключить доступ сотрудников к потенциально опасным интернет-сайтам, а так же ограничить доступ к сайтам, не имеющим отношения к решению рабочих вопросов. Использование контентной фильтрации повышает уровень сетевой безопасности, сокращает бесполезный интернет-трафик и увеличивает продуктивность работы сотрудников.

Для подключения сервиса CF требуется приобретение и активация специальной карты.

Система End Point Security позволяет автоматически проверять соблюдение пользователями корпоративной политики безопасности. Критериями проверки являются тип операционной системы на компьютере сотрудника, наличие критичных обновлений, антивирусных средств, сетевого экрана, определенные запущенные/остановленные системные процессы, параметры реестра и наличие/размер/версия определенных файлов. В результате такой проверки можно исключить доступ в корпоративную сеть сотрудников

компьютеры которых не отвечают корпоративным требованиям сетевой безопасности.

Управление приложениями IM/P2P

Инструментарий управления пользовательскими приложениями позволяет регулировать обмен данными в широком спектре программ-клиентов и протоколов пиринговых сетей, потокового вещания, обмена мгновенными сообщениями и т. п. Гибкая объектно-ориентированная система настройки политик обработки трафика с интегрированным расписанием обеспечивает точную настройку правил для каждого пользователя сети, при этом, не обременяя администратора вводом лишних данных. По умолчанию поддерживается определение большинства современных популярных протоколов обмена данными (как например Bit Torrent, AIM, ICQ, MSN и Yahoo, протоколы VoIP), возможно добавление пользовательских сигнатур.

Многокритериальные политики доступа

Интеллектуальная система обработки правил реализованная в ZyWALL USG принимает решение о направлении пакетов в соответствии с политиками доступа основанными на множественных критериях объектного набора, в том числе, таких как пользователь/группа пользователей, IP-адрес источника/получателя, время активации/деактивации правила. Подобные политики действуют для правил межсетевого экрана, маршрутизации, контентной фильтрации и управления полосой пропускания.

Централизованное управление и мониторинг

ZyWALL USG 300 поддерживает работу с современной системой централизованного управления сетевыми шлюзами Vantage CNM и инструментом мониторинга и создания отчетов Vantage Report.

Аппаратные характеристики:	
Порты WAN RJ45 GbE	
Порты LAN/DMZ RJ45 GbE	

Порты WAN/LAN/DMZ RJ45 GbE	7
Консольный порт RS-232, DB9F	Да
Порты USB 2.0	2
Объем оперативной памяти, Байт	256M
Объем памяти flash, Байт	256M
Светодиодные индикаторы	PWR, SYS, AUX, ARD1, CARD2, ORTS
Кнопка сброса настроек	Да
Кнопка включения	Да
Производительность	
Пропускная способность МСЭ (UDP, размер кета 1,518 байт), Мбит/с	350
Пропускная способность IPSec VPN (AES, размер кета 1,424 байт), Мбит/с	130
Пропускная способность UTM (FW+AV+IDP, TTP, размер пакета 1,460 байт), Мбит/с	80
Максимальное количество одновременных сессий AT	60000
Максимальное количество новых сессий NAT в кунду	1500
Максимальное количество одновременных ннелей IPSec VPN	200
Максимальное количество одновременных ннелей SSL VPN в базовой комплектации	2
Максимальное количество одновременных	25

ннелей SSL VPN при активации специальной цензии	
Максимальное количество виртуальных терфейсов VLAN 802.1q	64
Максимальное количество интерфейсов-евдонимов (IP Alias) на одном интерфейсе	4

4.3 Оборудование уровня агрегации

Серия гигабитных управляемых коммутаторов GS2200 предназначена для развертывания сетевой инфраструктуры малых и средних предприятий. Широкий набор функций защиты пользовательского трафика, приоритезация голоса и видео, управление по защищенным протоколам SSH, SSL с поддержкой IPv6 позволяет использовать эту линейку коммутаторов для различных задач передачи трафика, включая подключение серверов, настольных компьютеров, видеокамер или Wi-Fi точек доступа.

GS2200-24P предназначен для установки в 19” стойку, его высота составляет 1U. Он имеет 24 RJ-45 порта для скорости 100/1000 Мбит/с и 4 совмещенных SFP-слота для оптических интерфейсов, обеспечивает неблокируемую коммутацию со скоростью до 56 Гбит/с и скоростью передачи 41,67 миллионов пакетов в секунду, что соответствует параметрам высокоэффективной сети.

Коммутатор GS2200-24P поддерживает одновременную работу до 24 портов Gigabit Ethernet в режиме PoE для передачи данных и питания, например, для беспроводных точек доступа и настольных IP-телефонов. Встроенный адаптер питания PoE в коммутаторе GS2200-24P обеспечивает питание PoE в объеме 225Вт. Используя внешний источник питания PPS250, можно увеличить бюджет мощности питания PoE до 400 Вт для обеспечения всех 24 портов доступа питанием PoE. Полное соответствие стандарту PoE-питания 802.3af.

Для удовлетворения постоянно растущих требований мультимедиа-приложений и обеспечения высокого качества обслуживания коммутаторы серии GS2200-24P обладают мощной системой управления трафиком. Пошаговая установка скорости на портах позволяет контролировать полосу пропускания и повысить эффективность работы всей сети. Коммутаторы используют протокол авторизации 802.1x, что исключает незаконное использование ресурсов сети.

Для облегчения процесса администрирования имеется возможность предоставлять привилегии доступа только определенным MAC-адресам, что исключает неавторизованный доступ к закрытым материалам. Серия GS2200 использует технологию кластерного администрирования, iStacking™ при работе с другими коммутаторами ZyXEL, поддерживающими эту технологию. Это дает возможность объединить в кластер по одному IP-адресу до 24 коммутаторов.

Кроме того, серия GS2200 поддерживает такие современные технологии коммутации 2-го уровня как использование до 4094 идентификаторов VLAN, протоколы IGMP Snooping и RSTP, улучшающие стабильность, надежность и производительность сети. Приоритезация и безопасность трафика может быть выполнена либо посредством соответствующих правил на каждом порту доступа либо с помощью списка управления доступа ACL.

Основные преимущества

24 порта Gigabit Ethernet для агрегации и коммутации трафика в корпоративных сетях

Доступная мощность для PoE технологии равна 220 Вт, что позволяет подключить до 13 устройств с максимальной мощностью 15.4 Вт по стандарту 802.3af. При использовании дополнительного источника питания PPS250 с дополнительной мощностью 225, общая мощность увеличится до 445 Вт, что позволит подключить 24 устройства с максимальной мощностью 15.4 Вт. Для подключения доступны любые порты доступа коммутатора с 1 по 24

Безопасное подключение по протоколу 802.1x гарантирует защиту от несанкционированного доступа неавторизованных пользователей к ресурсам сети

Продвижение кадров jumbo frame размером до 9216 байт ускоряет передачу больших объемов информации и сокращает время обработки пакетов

Авторизация по протоколу TACACS+ и RADIUS

Возможность ограничения скорости по портам для обеспечения требуемой пропускной способностью сети, генерации тарифных планов и оптимизации работы мультимедийных приложений

Администрирование коммутаторов как по вэб-интерфейсу и SNMP так и по командной строке

4.4 Беспроводные SIP телефоны

Компания Escene одна из первых представила на рынке настольных IP-телефонов модели с поддержкой Wi-Fi. Это полнофункциональный профессиональный IP-телефон, который не требует проводов. Телефон Escene WS320-N ориентирован на корпоративных потребителей, которые предъявляют высокие требования к внешнему виду устройства, качеству изготовления и удобству использования при сохранении привлекательной стоимости.

При разработке аппаратов, инженеры и дизайнеры компании Escene использовали единый подход к дизайну, функциональным характеристикам, а так же к интерфейсам управления. Линейка включает модели от базовых до продвинутых телефонов, но всех их объединяет схожие черты — они отвечают высоким требованиям и обладают всеми необходимыми функциями IP-телефонов корпоративного уровня.

Рассматриваемый телефон — продвинутая модель в ряду корпоративных IP-телефонов Escene. По сравнению с базовой моделью WS220-N аппарат имеет улучшенный экран с большим разрешением, более строгий корпоративный

дизайн, встроенную двенадцати кнопочную программируемую панель, регулируемую подставку и дополнительные возможности для подключения гарнитуры. К телефону можно подключить гарнитуру, причем тремя способами.

Рисунок 4.1 – Внешний вид телефона Escene WS320-N

Линейка Wi-Fi телефонов Escene на данный момент включает три модели — базовую WS220-N, которую мы рассматривали в предыдущем обзоре, продвинутую WS320-N, которую мы рассмотрим в данном обзоре и самую «заряженную» с большим цветным экраном WS620-E. Эти модели объединяют схожие черты — они отвечают высоким требованиям и обладают всеми необходимыми функциями IP телефонов корпоративного уровня.

Особенности

Часть единого модельного ряда корпоративного уровня.

Поддержка беспроводной сети Wi-Fi

Высокое качество материалов корпуса.

Большой и четкий графический экран.

Высокая эргономичность.

Регулируемая подставка.

Подходит для оснащения рабочего места секретаря.

Подходит для работы в контакт-центре.

Простота настройки за счет понятного интерфейса.

Русифицированные web-интерфейс и экранное меню.

Возможность полностью настроить телефон при помощи экрана и кнопок, включая учетные записи SIP.

Возможность адаптации телефона для работы с SIP-совместимым оборудованием.

Функциональности больше, чем поддерживают большинство IP-АТС и операторов связи в настоящий момент.

Функциональные возможности

Прямое подключение по SIP к Виртуальным IP АТС (например, Broadworks, МФИ РТУ) и к офисным IP АТС (например Asterisk, 3CX IP PBX, Avaya IP Office).

Порт LAN с беспроводным контроллером Wi-Fi IEEE b/g/n

Возможностью работать в режиме коммутации или маршрутизации между портами PC и LAN(подключение по Wi-Fi)

Простота установки и эксплуатации, возможность расширенной настройки (включая функции SIP и ДВО) через экранное меню или через web-интерфейс.

Поддержка двух одновременных вызовов на двух независимых учетных записях SIP.

Адаптация для работы оператора в контакт-центре (эргономика, дополнительный разъем RJ11 для гарнитуры оператора контакт-центра).

Полнодуплексная громкая связь, определитель номера, удержание вызова, перевод и переадресация вызова, а так же и другие дополнительные функции.

Поддержка звука высокой четкости Voice HD (кодек G.722).

Встроенный VPN клиент.

Шифрование сигнального SIPS и медиа SRTP трафика.

Поддержка корпоративной записной книжки по протоколу LDAP или XML или личной записной книги.

Русифицированное экранное меню и web-интерфейс телефона.

Технические характеристики

VoIP

RFC 3261 стандарт SIP-сервер, Asterisk, Avaya, Cisco, Broadsoft, РТУ МФИ, 3CX IP PBX, Panasonic SIP-АТС и другие.

Шифрование сигнального трафика SIPS и медиа трафика SRTP.

Аудио кодеки : G.711 u/a, G.722(HD Voice), G.729a, G.723.

QoS: TOS, Jiffer Buffer, VAD, CNG, G.168 (32ms).

Поддержка DNS SRV.

Две учетных записи SIP с возможностью регистрации на двух независимых SIP серверах и возможностью автоматического переключения в случае потери регистрации.

Два одновременных вызова на телефон с любой из двух учетных записей SIP.

Передача данных

Беспроводной контроллер Wi-Fi (IEEE b/g/n, WPA/WPA2 и 64/128 bit WEP) на LAN порт

1*RJ45 10/100M Ethernet (порт PC)

Поддержка VLAN/ QoS.

IP адресация: DHCP клиент или назначение статического IP.

Встроенный VPN клиент L2TP или SSL VPN.

Сетевые протоколы HTTP, BOOTP, FTP, TFTP, IEEE 802.1Q, IEEE 802.1X.

Физические параметры

Монохромный LCD экран с подсветкой и размером 128*64 символов с белой подсветкой.

3 дополнительных разъёма для гарнитуры — поддерживается подключение одним из трех способов: с разъёмом USB, при помощи гнёзд Jack 3.5 мм или разъема RJ11.

Индикатор статуса линии (двухцветный LED).

Полнодуплексный динамик и микрофон громкой связи.

Две кнопки выбора линии 1 и линии 2 со световой индикацией состояния линии.

Кнопки для регулировки громкости телефона/вызывного сигнала.

4 многофункциональные кнопки под экраном.

Дополнительные виды обслуживания (дополнительные функции)

Ожидание второго вызова, очереди (если поддерживает IP АТС), перевод вызова, переадресация вызова, удержание вызова, перехват вызова, обратный вызов, повтор вызова, автоответ.

Быстрый набор номера, кнопка начала записи разговора по стар коду (если поддерживает IP АТС).

BLF(Busy Lamp Field)

Многосторонняя конференция (если поддерживает IP АТС), 3х-сторонняя конференция на телефоне.

Не беспокоить (DND).

Голосовая почта (если функция поддерживается IP АТС).

5 ТЕХНИКО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ ПРОЕКТА

5.1Оценка капитальных вложений в проект

К капитальным вложениям относятся все затраты, вносимые на первоначальном этапе строительства сети, и имеющие единовременный характер. Сюда входят все затраты, предшествующие запуску системы в работу. Для определения капитальных вложений для данного дипломного проекта составим смету затрат на используемое оборудование и материалы, составляющие инвестиции в проект.

Инвестиции в оборудование по проекту и на ввод оборудования в эксплуатацию складываются из следующих составляющих:

1 стоимость оборудования;

2 установка и монтаж оборудования;

3 стоимость кабеля;

4 прокладка кабеля в грунт;

5 прокладка кабеля в канализации;

6 транспортные расходы (тара и упаковка, таможенные расходы);

7 прочие затраты (техническая документация, обучение специалистов, страховка);

8 прочие непредвиденные расходы .

Затраты на строительство проектируемых информационно телекоммуникационной сети, а также организацию и построение ВОЛС составляются согласно сметной стоимости строительства данного объекта.

Затраты на приобретение и монтаж станционного оборудования, а также стоимость волоконно – оптического кабеля определяются на контрактной и договорной основе с заказчиком и подрядчиком, что является коммерческой тайной предприятия, поэтому используются ориентировочные цены.

5.2 Расчет капитальных вложений на оборудование и строительно-монтажные работы

Размещение оборудования производится на существующих площадях, поэтому затраты на строительство новых зданий не предусмотрены.

Расчет капитальных вложений в оборудование и материалы представлен в таблице 5.1.

Таблица 5.1 – Капитальные вложения в оборудование и материалы для г. Москва

Наименование	Кол-во единиц	Стоимость (руб.)	
		за единицу	всего
Zyxel USG-300	1	84 000	84 000
Zyxel GS2200-24P	1	57 000	57 000
Zyxel ES1100-24E	2	4 200	8 400
Zyxel X8004	1	250 000	250 000
Сервер	5	54 000	270 000
IP телефон Escene WS320-N	35	8 000	380 000
IP телефон беспроводной RTX 8630 Handset	4	10 000	40 000
Кабель UTP, 24 AWG, PVC, 4 пары, Cat.5e	1000	5	5 000
Точка доступа Wi-Fi Zyxel NBG318S EE	3	6 500	19 500
Патчкорд 1 GB/s, 0.5м.	20	150	3 000
ПО для серверов и её инсталляция [19]	6	5000	30 000
Аренда VPN каналов 100 Мбит/с Оператора	5	50 000	250 000
Пуско-наладочные работы [20] (кол-во элементов)	6	2 000	12 000

Стоимость СМР по прокладке кабеля [20]	100 м	50	50 000
Итого			**1 358 00**

Таблица 5.2 – Капитальные вложения в оборудование для г. Орел

Наименование	Кол-о единиц	Стоимость (руб.)	
		за диницу	всего
Zyxel USG- 100+	1	84 000	84 000
Zyxel GS2200-24P	1	57 00	57 000
Zyxel ES1100-24E	2	4 200	8 400
VoIP шлюз DWG-2024S	1	80 00	80 000
IP телефон Escene WS320-N	20	8 000	160 00
IP телефон беспроводной RTX 8630 Handset	4	10 00	40 000
Кабель UTP, 24 AWG, PVC, 4 пары, Cat.5e	1000 .	5	5 000
Точка доступа Wi-Fi Zyxel NBG318S EE	1	6 500	6 500
Патчкорд 1 GB/s, 0.5м.	15	150	2 250
Подключение к сети Internet MPLS Провайдера	1 анал	20 00	20 000
Пуско-наладочные работы [19] (кол-во элементов)	5	2 000	10 000
Стоимость СМР по прокладке кабеля [20]	1000	50	50 000
Итого			**523 50**

Таблица 5.3 – Капитальные вложения в оборудование и материалы для г. Курск

Наименование	Кол-во единиц	Стоимость (руб.)	
		за единицу	всего
Zyxel USG- 100+	1	84 000	84 000
Zyxel GS2200-24P	1	57 000	57 000
Zyxel ES1100-24E	2	4 200	8 400
VoIP шлюз DWG-2024S	1	80 000	80 000
IP телефон Escene WS320-N	20	8 000	160 000
IP телефон беспроводной RTX 8630 Handset	4	10 000	40 000
Кабель UTP, 24 AWG, PVC, 4 пары, Cat.5e	1000	5	5 000
Точка доступа Wi-Fi Zyxel NBG318S EE	2	6 500	13 000
Патчкорд 1 GB/s, 0.5м.	15	150	2 250
Подключение к сети Internet MPLS Провайдера	1 канал	20 000	20 000
Пуско-наладочные работы [19] (кол-во элементов)	5	2 000	10 000
Стоимость СМР по прокладке кабеля [20]	1000	50	50 000
Итого			**529 650**

Таблица 5.4 – Капитальные вложения в оборудование и материалы для г. Липецк

Наименование	Кол-во единиц	Стоимость (руб.)	
		за единицу	всего

Zyxel USG- 100+	1	84 000	84 000
Zyxel GS2200-24P	1	57 00	57 000
Zyxel ES1100-24E	2	4 200	8 400
VoIP шлюз DWG-2024S	1	80 00	80 000
IP телефон Escene WS320-N	15	8 000	120 00
IP телефон беспроводной RTX 8630 Handset	5	10 00	50 000
Кабель UTP, 24 AWG, PVC, 4 пары, Cat.5e	1000	5	5 000
Точка доступа Wi-Fi Zyxel NBG318S EE	1	6 500	6 500
Патчкорд 1 GB/s, 0.5м.	15	150	2 250
Подключение к сети Internet MPLS Провайдера	1 анал	20 00	20 000
Пуско-наладочные работы [19] (кол-во элементов)	5	2 000	10 000
Стоимость СМР по прокладке кабеля [20]	1000	50	50 000
Итого			**493 50**

Таблица 5.5 – Капитальные вложения в оборудование и материалы для г. Воронеж

Наименование	Кол-во единиц	Стоимость (руб.)	
		за единицу	всего
Zyxel USG- 100+	1	84 000	84 000
Zyxel GS2200-24P	1	57 000	57 000
Zyxel ES1100-24E	2	4 200	8 400
VoIP шлюз DWG-2024S	1	80 000	80 000
IP телефон Escene WS320-N	20	8 000	160 000

IP телефон беспроводной RTX 8630 Handset	4	10 000	40 000
Кабель UTP, 24 AWG, PVC, 4 пары, Cat.5e	1000 м.	5	5 000
Точка доступа Wi-Fi Zyxel NBG318S EE	2	6 500	13 000
Патчкорд 1 GB/s, 0.5м.	15	150	2 250
Подключение к сети Internet MPLS Провайдера	1 канал	20 00	20 000
Пуско-наладочные работы [19] (кол-во элементов)	5	2 000	10 000
Стоимость СМР по прокладке кабеля [20]	1000 м	50	50 000
Итого			**529 650**

Таблица 5.6 - Капитальные вложения, не вошедшие в таблицы 5.1-5.5

N	**Наименование**	**Кол-во единиц**	**Цена в руб**	**Стоимость**
1	Аренда каналов E1 у местного оператора ССОП	5	5 000	25 000
2	Разработка документации сети	1	43 000	43 000
3	Оборудование для обслуживания сети	1	10 000	10 000
4	ПО ZyXEL E- Vantage CNM 100 Devices для управления сетью [21]	1	270 000	270 000
5	СТОЙКА 19” 33U	5	20 000	100 000
6	**Программный IPSec VPN-клиент для Windows (50 лицензий) [21]**	1	90 000	90 000
	Итого:	**538 000**		
	Итого по всем филиалам:	**3 972 500**		

Капитальные затраты на оборудование рассчитываются по формуле:

$$K_{обор} = K_{пр} + K_{тр} + K_{смр} + K_{т/у} + K_{зср} + K_{пнр} \text{ руб. (5.1)}$$

где $К_{пр}$ – Капитальные затраты на приобретение оборудования; $К_{тр}$ – транспортные расходы в т.ч. таможенные расходы (4% от $К_{пр}$); $К_{смр}$ – строительно-монтажные расходы (20% от $К_{пр}$); $К_{т/у}$ – расходы на тару и

упаковку (0,5% от $К_{пр}$); $К_{зср}$ – заготовительно-складские расходы (2% от $К_{пр}$); $К_{пнр}$ – прочие непредвиденные расходы (5% от $К_{пр}$).

$$K_{обор} = 3972500 + 158900 + 794500 + 19862,5 + 79450 + 198625 = 5223837,5 \ руб.$$

5.3 Калькуляция эксплуатационных расходов

Эксплуатационными расходами называются текущие расходы предприятия на производство услуг связи. В состав эксплуатационных расходов входят все расходы на содержание и обслуживание сети. Эти расходы имеют текущий характер.

Эксплуатационные расходы по своей экономической сущности выражают себестоимость услуг связи в денежном выражении.

Для определения эксплуатационных расходов по проекту используем следующие статьи:

1. Затраты на оплату труда.
2. Единый социальный налог.
3. Амортизация основных фондов.
4. Материальные затраты.
5. Прочие производственные расходы.

5.3.1 Расходы на оплату труда

Для расчета годового фонда заработной платы необходимо определить численность штата производственного персонала. Данное оборудование не требует постоянного присутствия обслуживающего персонала на всех узлах сети.

Планируется для поддержания работы IT инфраструктуры предприятия содержать отдел IT, который будет возглавлять руководитель отдела. Рекомендуемый состав персонала по обслуживанию станционного оборудования

приведен в таблице 5.7.

Таблица 5.7 – Состав персонала по обслуживанию станционного оборудования

Наименование должности	**Оклад**	**Количество, чел.**	**Сумма з/ пл, руб.**
Руководитель отдела IT	30 000	1	30 000
Инженер	20 000	1	20 000
Электромонтер	15 000	2	30 000
Системный администратор	28 000	1	28 000
Итого		**5**	**108 000**

Годовой фонд оплаты труда составит:

для линейного персонала

ФОТгод = СЗП*12*1,04*1,25(5.2)

где 12 – количество месяцев в году;

1,04 – коэффициент, учитывающий доплату за работу с вредными условиями труда;

1,25 – размер премии (25 %);

ФОТгод = СЗП*12*1,04*1,25= 108 000*12*1,04*1,25 = 1 684 800 руб.

$$ФОТ^{год} = ФОТ^{год}_{\text{вр. усл.}} \quad (5.3)$$

$ФОТ^{год}$ = 1 684 800 руб.

5.3.2 Страховые взносы

Каждое предприятие обязано выплачивать **страховой взнос** и его ставка составляет порядка 30% от заработной платы.

СВ =0,3 * ФОТгод = 0.3 *1 684 800 = 505 440 руб., (5.4)

5.3.3 Амортизационные отчисления

Под амортизацией понимается процесс постепенного возмещения стоимости основных фондов, в целях накопления средств для реконструкции и приобретения основных средств. Самым распространенным способом оценки амортизации является учет амортизации, составленный исходя из общего срока службы основных фондов, в этом случае:

$$AO = T / F \text{ , руб}$$

где Т – стоимость оборудования, F – срок службы этого оборудования.

АОгод = 2872500/5 =574 500 руб., (5.5)

5.3.4 Материальные затраты

Величина материальных затрат включает в себя оплату электроэнергии для производственных нужд, затраты на материалы и запасные части и др. Эти составляющие материальных затрат определяются следующим образом:

а) затраты на оплату электроэнергии определяются в зависимости от мощности станционного оборудования:

$З_{ЭН}$ = Т*24 *365*Р(5.6)

где Т = 3,14 руб./кВт час – тариф на электроэнергию;

Р =5*3=15 кВт - мощность установок.

Тогда, затраты на электроэнергию составят

$З_{ЭН}$ =3,14*24*365*15=412 596 руб.

б) затраты на материалы и запасные части составляют 3,5% от ОПФ:

Затраты на материалы и запасные части рассчитываем по формуле

$$З_М = \frac{ОПФ \cdot 3{,}5\%}{100\%}, \qquad (5.7)$$

где *ОПФ* - это основные производственные фонды (капитальные вложения)

В итоге материальные затраты составляют:

Зм =5223837.5* 3,5 % = 182834,3125 руб.

Таким образом, общие материальные затраты равны

$З_{ОБЩ} = З_{ЭН} + З_{М}$ (5.8)

$З_{ОБЩ}$=412 596 +182834,3125=595430,3 руб.

5.3.5Прочие расходы

Прочие расходы предусматривают общие производственные ($З_{пр.}$) и эксплуатационно- хозяйственные затраты ($З_{эк.}$):

$Зпр = 0,15 * ФОТ^{год}$ (5.9)

$Зэк = 0,25 * ФОТ^{год}$ (5.10)

Подставив значения в формулы (5.9) и (5.10) , получаем

Зпр = 0,15 *1 684 800 = 252 720 руб.

Зэк = 0,25 *1 684 800 = 421 200 руб.

Таким образом, вычислим прочие расходы:

Зпрочие = Зпр+ Зэк (5.11)

$З_{прочие}$=252 720 + 421 200=673920 руб.

Результаты расчета годовых эксплуатационных расходов сведены в таблицу 5.8

Таблица 5.8 – Результаты расчета годовых эксплуатационных расходов

Наименование затрат	**Сумма затрат, руб.**
2. ФОТ	1 684 800
3. Страховые взносы	505 440
4. Амортизационные отчисления	574 500
5. Материальные затраты	595 430,3
6. Прочие расходы	673 920
Итого:	**4 034 090,3**

Таким образом, суммарные годовые затраты на содержание и обслуживание проектируемой сетевой инфраструктуры составляют 4 034 090,3

рублей.

6 МЕРЫ ПО ОХРАНЕ ОКРУЖАЮЩЕЙ СРЕДЫ, ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ И ОХРАНЕ ТРУДА

6.1 Обеспечение мер по охране окружающей среды на предприятиях связи

Эксплуатация электроустановок без устройств, обеспечивающих соблюдение установленных санитарных норм и правил и природоохранных требований или с неисправными устройствами, не обеспечивающими соблюдение этих требований, не допускается.

При эксплуатации электроустановок в целях охраны водных объектов от загрязнения необходимо руководствоваться действующим законодательством, государственными и отраслевыми стандартами по охране водных объектов от загрязнения.

Так как выбранное оборудование имеет соответствующие сертификаты и документы, разрешающие его использование на территории Российской Федерации, то все нормы по экологической безопасности соблюдены.

Применяемые при строительстве МСС волоконно-оптические кабели связи не наносят вред окружающей среде, не являются радиоактивными элементами и не распространяют горения. Находясь в грунте в специальной защитной оболочке, волоконно-оптические кабели не способствуют ухудшению характеристик почвы.

6.2 Техника безопасности предприятия связи и охрана труда

Работа по охране труда должна осуществляться в соответствии с действующим Положением об организации работы по охране труда на

предприятиях, в учреждениях и организациях, подведомственных Министерству связи Российской Федерации, утвержденным Приказом Минсвязи России от 24.01.94 N 18, и Рекомендациями по организации работы службы охраны труда на предприятиях, в учреждениях и организациях от 27.02.95 N 34-у.

Монтаж и эксплуатация производственного оборудования должны осуществляться в соответствии с требованиями Правил эксплуатации электроустановок потребителей, Правил устройства электроустановок (ПУЭ). Производственное оборудование по безопасности, должно соответствовать требованиям ГОСТ 12.2.003, требованиям технических условий на оборудование, требованиям отраслевых стандартов и стандартов предприятия на отдельные группы и виды оборудования.

Все оборудование, включая оборудование иностранных фирм, должно иметь сертификат соответствия, содержащий требования безопасности, выданный, в зависимости от вида оборудования, Министерством связи РФ или Госстандартом России. Блоки и части оборудования, являющиеся источниками опасных излучений, вредных испарений, представляющие опасность для обслуживающего персонала, должны иметь знаки безопасности или сигнальную окраску в соответствии с требованиями ГОСТ 12.4.026. Размещение и установка оборудования должны осуществляться в соответствии с ведомственными нормами технологического проектирования, ведомственными строительными нормами (ВСН 332-93) и ОСТ 45.86-96.

На предприятиях связи к самостоятельной работе допускаются работники, имеющие профессиональную подготовку, соответствующую характеру работы, прошедшие обязательное медицинское освидетельствование, вводный инструктаж, первичный инструктаж на рабочем месте, обучение безопасным методам труда и имеющие соответствующую группу по электробезопасности.

Работник связи обязан соблюдать правила внутреннего трудового распорядка. Соблюдать требования по охране труда и обеспечению безопасности

труда, предусмотренные действующими законами и иными нормативными актами.

Использовать все средства индивидуальной или коллективной защиты от неблагоприятного воздействия факторов производственной среды и потенциальных производственных рисков.

Содержать в исправном состоянии оборудование, инструменты и другую выделенную ему технику для выполнения работы и соответствующего ухода за ней. О любой неполадке немедленно сообщить своему непосредственному руководителю. Использовать выделенное ему оборудование по назначению. Запрещается его эксплуатация в личных целях.

Сообщать работодателю или его представителю о любой рабочей ситуации, которая, по его мнению, создает угрозу жизни или здоровью. Работодатель не может требовать от работника возобновления работы, если такая опасность продолжает сохраняться. О любом повреждении здоровья, какой бы степени тяжести оно ни было, незамедлительно сообщать непосредственному или вышестоящему руководителю.

Знать и уметь оказывать первую медицинскую помощь пострадавшим от электрического тока и при других несчастных случаях. Соблюдать меры пожарной безопасности, знать маршруты эвакуации.

При обслуживании конкретных узлов и станций руководствоваться указаниями мер безопасности, изложенными в технических описаниях.

Проверить состояние общего и рядового освещения, наличие и исправность переносных светильников, работу сигнализации. На всех кожухах оборудования, щитах и розетках с напряжением 42 кВ и выше переменного тока, должен быть нанесен знак электрического напряжения для предупреждения обслуживающего персонала. При внешнем осмотре электроинструмента и приборов обратить внимание на целостность изоляции, отсутствие оголенных токоведущих частей.

При других чрезвычайных ситуациях проявить собранность и используя персонал служб предприятия или аварийных служб города действовать быстро и оперативно, руководствуясь инструкцией при чрезвычайных ситуациях.

По окончании смены необходимо привести в порядок рабочее место, инструмент, приспособления, спецодежду. Если нужно, отключить оборудование, электроприборы от электрической сети. Сообщить сменщику обо всех неисправностях, замеченных во время работы, и мерах, принятых к их устранению.

В целях предупреждения несчастных случаев и профессиональных заболеваний обязан выполнять общие и специальные правила по охране труда, действующие в организации; их нарушение влечет за собой применение мер дисциплинарного взыскания в соответствии с действующим законодательством.

Обязан проходить обучение, инструктаж, проверку знаний правил, норм и инструкций по охране труда в порядке и в сроки, которые установлены для определенных видов работ и профессий.

Условия труда - это совокупность факторов производственной среды, оказывающих влияние на здоровье и работоспособность человека в процессе труда. Условия труда должны быть комфортными и исключать предпосылки для возникновения травм и профессиональных заболеваний.

При техническом обслуживании станционного оборудования возможны воздействия следующих опасных и вредных производственных факторов:

Физические:

- опасное напряжение в электрической цепи, замыкание которой может произойти через тело человека, электрического удара, ожога электродугой;
- недостаточной освещенности рабочей зоны;
- опасности возникновения пожара;
- падение с высоты персонала при работах на стремянках и лестницах;
- падение предметов с высоты (инструмента, элементов оборудования);
- лазерное излучение;

- повышенное напряжение органов зрения;

- расположение рабочего места на значительной высоте относительно поверхности пола (земли);

Психофизиологические:

- физические перегрузки.

Инженер руководствуется знаками безопасности и надписями установленного содержания, которыми обозначаются опасные зоны, во избежание травмы работник не допускает посторонних лиц за пределы защитного и специального ограждения.

Инженер должен различать сигнальные цвета, которые оповещают об опасности:

Красный – запрещение, непосредственная опасность, средство пожаротушения;

Желтый – предупреждение, возможная опасность;

Зеленый – предписание об опасности;

Синий – указания, информация.

При определении условий труда необходимо рассмотреть следующие вопросы:

1. производственный микроклимат помещения;
2. производственное освещение;
3. воздействие шума и вибрации;
4. электромагнитное излучение;
5. электропожаробезопасность.

ЗАКЛЮЧЕНИЕ

Одним из важнейших условий успешного развития бизнеса является эффективное управление информационными потоками. Особенно это актуально для крупных предприятий и территориально распределенных холдингов, таких как компания ТехноСвязьСтрой. И одним из условий эффективного управления является развитая коммуникационная инфраструктура.

Создание выделенной сети позволяет компании сократить затраты на услуги связи, обеспечить своим сотрудникам доступ к общекорпоративным ресурсам, защитить передаваемые данные от несанкционированного доступа и получить квалифицированную сервисную поддержку.

В результате выполнения данного дипломного проекта была разработана выделенная сеть связи для компании ТехноСвязьСтрой, филиалы которой расположены в пяти городах России. Данная сеть организована на базе технологии IP/MPLS. VPN-решение привлекательно, так как оно предлагает безопасность при значительном снижении расходов по сравнению с арендой выделенных каналов или построения собственных. В качестве провайдера, предоставляющего услугу VPN, была выбрана компания ПАО «Ростелеком».

В результате выполнения проекта предложена сетевая инфраструктура, которая обеспечивает передачу всех видов информации (данные, голос, видео) с учетом перспектив развития современных информационных технологий. Кроме того, данная сеть обеспечивает интеграцию и работоспособность всех элементов и систем. Проектируемая сеть построена на оборудовании компании Zyxel.

При проектировании были рассчитаны капитальные затраты на реализацию проекта, которые складывались из затрат на приобретение оборудования и строительства кабельных сооружений. Капитальные затраты составили 5 223 837.5 руб.

СПИСОК АББРЕВИАТУР И СОКРАЩЕНИЙ

ADSL ***Asymmetric Digital Subscriber Line*** – Ассиметричная ифровая абонентская линия. В ходит в число технологий ысокоскоростной передачи данных, известных как технологии SL и имеющих общее обозначение xDSL. К другим ехнологиям DSL относятся HDSL, VDSL и другие.

ATM ***Asynchronous Transfer Mode*** – Режим Асинхронной ередачи. Информация в сети ATM передается ячейками (cell) иксированной длины (~53байта).

BRAS ***Broadband Remote Access Server*** – Широкополосный ервер удаленного доступа

DSL ***Digital Subscriber Line*** - Цифровая абонентская линия

DSLAM ***Digital Subscriber Line Access Multiplexer*** – Мультиплексор цифровой абонентской линии

HDSL ***High data rate Digital Subscriber Line*** - Высокоскоростная ифровая абонентская линия

IP ***Internet Protocol*** – Интернет Протокол. Задачей протокола **P** является перемещение дейтаграмм через множество оединенных между собой сетей. Модули **IP** размещаются на остах и шлюзах (маршрутизаторах) Internet. Маршрутизация от дного модуля к другому на основе интерпретации адресов **IP**.

ISDN ***Integrated Services Digital Network*** - Интегральная ифровая сеть связи .

LAN ***Local Area Network*** – Локальная вычислительная сеть.

POTS ***Plain Old Telephone System*** – Телефонная Сеть (ТФОП)

PPPoE ***Point-to-Point Protocol over Ethernet*** - Протокол передачи в ежиме " точка-точка" поверх Ethernet

Router ***Router*** – Маршрутизатор. Определяет и перемещает пакеты соответствии с IP адресом. Содержит множество интерфейсов азличного типа (Ethernet, RS232, V35, G.703 и т.п.)

Splitter ***Splitter*** – Частотный разделитель

Switch ***Switch*** – Коммутатор. Предназначен для коммуттации акетов **Ethernet** или ячеек **ATM**.

TCP ***Transmission Control Protocol*** **–** Протокол Управления ередачей. Протокол TCP предназначен для надежной и арантированной доставки данных между хостами в омпьютерных сетях с коммутацией пакетов и между сетями ерез промежуточные системы. Т СР располагается в ногоуровневой модели непосредственно над базовым ротоколом Интернет (IP).

VDSL ***Very high data rate Digital Subscriber Line*** - верхвысокоскоростная цифровая абонентская линия

UDP ***User Datagram Protocol*** – Протокол пользовательских ейтаграмм. Предназначен для поддержки режима обмена ейтаграммами на основе коммутации пакетов в среде вязанных между собой компьютерных сетей. Предполагает спользование **IP** в качестве протокола нижележащего уровня.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Захватов М. Построение виртуальных частных сетей (VPN) на базе технологии MPLS [Текст] / М. Захватов – М.: Cisco Systems , 2004

2. РД 45.120. -2000 Руководящий документ отрасли. Нормы технологического проектирования. Городские и сельские телефонные сети. ЦНТИ, «ИНФОРМСВЯЗЬ», Москва, 2000 г.

3. Шмалько, А.В. Цифровые сети связи: основы планирования и построения [Текст]/ А.В. Шмалько. – М.: Эко- Трендз, 2001. – 278 с.

4. Гольдштейн, Б.С. Протоколы сети доступа [Текст]. Том 2. 2-е изд., перераб, и доп. - М.: Радио и связь, 2002.

5. Константин Гласман. Системы видеокомпрессии: от MPEG-1 до AVC и VC-1."625". — №1. — 2006.

6. Официальный сайт компании Zyxel [Электронный ресурс] // ZyXEL Russia E. : URL: http://zyxel.ru/ (дата обращения 12.03.2015).

7. Официальный сайт компании «D- Link» [Электронный ресурс] // D-Link systems. URL: http://www.d-link.ru/ (Дата обращения 12.03.2015г.);

8. Коммутаторы локальных сетей D-Link: Учебное пособие. / D-Link systems . - М.: 2004.

9. Галкин, В.А. Телекоммуникации и сети [Текст] / В.А. Галкин – М.: МГТУ им. Н.Э. Баумана, 2003, 608 с.

10. Куни, Л. Ethernet [Текст]/ Л. Куни, Р. Рассел –М.: Издательская группа BHV, 1998, 448 с.

11. Бирюков, Н.Л. Транспортные сети и системы электросвязи. Системы мультиплексирования [Текст] / Н.Л. Бирюков, В.К. Стеклов – М.: 2003, 352 с.

12. Гольдштейн, Б.С. Интеллектуальные сети [Текст] / Б.С. Гольдштейн, И.М. Ехриель, Р.Д. Рерле -М.: Радио и связь, 2005, 504 с.

13. Шмалько, А.В. Цифровые сети связи: основы планирования и построения [Текст] / А.В. Шмалько – М.: Эко- Трендз, 2001. – 278 с.

14. Гольдштейн, Б.С. IP-телефония [Текст]/ Б.С. Гольдштейн, А.В. Пинчук, А.Л. Суховицкий -М.: Радио и связь, 2001, 336 с.

15. Конахович, Г.Ф. Сети передачи пакетных данных [Текст] / Г.Ф. Конахович, В.М. Чуприн -М.: МК-Пресс, 2006, 272 с.

16. Телекоммуникационные системы и сети: Учеб. пособие. В 3 томах. Том 3. Мультисервисные сети / под ред. В.П. Шувалова. - М.: Горячая линия – Телеком, 2005. – 592 с.

17. Росляков, А.В. IP-телефония [Текст] / А.В. Росляков, М.Ю. Самсонов, И.В. Шибаева -М.: Эко- Трендз, 2003, 252 с.

18. Официальный сайт компании PROFSERVICE [Электронный ресурс] // Компания-подрядчик по монтажу кабельных систем. URL: http://www.obcom.su/price/server/ (Дата обращения 20.04.2015г.).

19. Официальный сайт компании Фруктус [Электронный ресурс] / / Компания -подрядчик по проектированию и монтажу интегрированых мультисервисных сетей. URL: http://pcquality.ru/ceny-stoimost-rascenki-na-sks-lvs-prais/ (Дата обращения 20.04.2015г.).

20. Интернет магазин Zyxel [Электронный ресурс] // Магазин сетевого оборудования. URL: http://store.zyxel.ru/zyxel_e.html. (Дата обращения 25.04.2015г.).

21. ГОСТ 2.105 – 95. Межгосударственный стандарт. Общие требования к текстовым документам ЕСКД, Москва. 1995.