

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ
КАЗАХСТАН

Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Кафедра «Электроника»

«Допущен к защите»
Зав. кафедрой «Электроника»

А.А. Копесбаева к.т.н., проф.
«__» _____ 2014г.

ДИПЛОМНЫЙ ПРОЕКТ

На тему: «Разработка MPLS сети для филиала Национальной Компании
«Казахстан Темиржолы» - ШЧ 19»

Специальность «5В071900 – Радиотехника, электроника и
телекоммуникации»

Выполнил _____ ст. гр. ЭСТ-10-1 С.С. Тастанова

Научный руководитель _____ С.Б. Абдрешова ,ст.преп.

Консультанты:

по экономической части:

Бекишева А.И., к.э.н., доцент

_____ « 27 » _____ 20 14 г.
(подпись)

по безопасности жизнедеятельности:

Санатова Т.С., к.т.н., доцент

_____ « 25 » _____ 20 14 г.
(подпись)

Нормоконтролер: С.Б. Абдрешова , ст.преп.

_____ « 2 » _____ 20 14 г.
(подпись)

Рецензент: З.М. Ярмухамедова к.т.н, проф.

_____ « _____ » _____ 20 ____ г.
(подпись)

Алматы 2014 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ
КАЗАХСТАН

Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Факультет «Радиотехники и связи»
Специальность «5В071900 – Радиотехника, электроника и телекоммуникации»
Кафедра «Электроника»

ЗАДАНИЕ
на выполнение дипломного проекта

Студента С.С.Тастанова

Тема проекта «Разработка MPLS сети для филиала Национальной Компании «Казахстан Темиржолы» - ШЧ 19» утверждена приказом ректора № 115 от 24 сентября 2013 г.

Срок сдачи законченной работы «15» мая 2014г.

Исходные данные к проекту (требуемые параметры результатов проектирования) и исходные данные: разработать сеть на основе технологии MPLS-VPN для филиала Национальной Компании «Казахстан Темиржолы», ШЧ 19 - Карагандинской дистанции сигнализации и связи, на участке которой находится более 20 станций.

Перечень подлежащих разработке в дипломном проекте вопросов или краткое содержание дипломного проекта

1. Технологическая часть (описание технологий MPLS – мультипротокольная коммутация по меткам).
2. Конструкторская часть (Разработка сети с использованием технологии MPLS-VPN для НК «КТЖ» ШЧ 19).
3. Программное обеспечение (написание программы в Cisco System IOS 12.3 для конфигурации оборудования).
4. Общие вопросы охраны труда (расчет освещения и вентиляции помещения, где осуществляется эксплуатация устройства).
5. Техничко–экономическая часть (расчет экономического эффекта от применения и производства устройства).

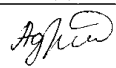

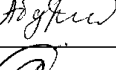

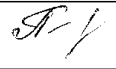
Перечень графического материала (с точным указанием обязательных чертежей): в данной работе содержится 20 рисунка и 13 таблиц.

Рекомендуемая основная литература:

- 1) Евстифеев А.В. Микроконтроллеры AVR семейства Mega. – М.: Додэка, 2008. – 558 с.
- 2) Шпак Ю.А. Программирование на языке С для AVR и PIC микроконтроллеров. – М.: МК-Пресс, 2011. – 546 с.

- 3) Берлин А.Н. Цифровые сотовые системы связи. – М.: Экотрендз, 2007. – 296 с.
- 4) Князевский Б.А. Охрана труда. – М.: Высшая школа, 2002. – 365 с.
- 5) Базылов К.Б., Алибаева С.А., Бабич А.А. Выпускная работа бакалавров. Экономический раздел. – Алматы: АИЭС, 2008. - 20 с.

Консультанты по проекту с указанием относящихся к ним разделов работы

Раздел	Консультант	Сроки	Подпись
Технологическая часть	Абдрешова С.Б.	30.03.14	
Разработка сети	Абдрешова С.Б.	15.04.14	
Программное обеспечение	Абдрешова С.Б.	30.04.14	
Безопасность жизнедеятельности	Санатова Т.С.	4.05.14	
Экономическая часть	Бекишева А. И.	10.05.14	

подготовки дипломного проекта

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления руководителю	Примечание
1	Договоры ЧОПОВ	23.03.14 - 01.04.14	
2	Сбор материалов по ИДН & VPN от	10.03.14 - 20.03.14	
3	Сбор информации	30.03.14 - 05.04.14	
4	Вопросы графика работ в программе Cisco System IOS 12.3 конфигурация маршрути- затора	14.04.14 - 28.04.14	
5	Безопасность передачи информации	05.05.14 - 27.05.14	
6	Аварийная ситуация	19.06.14 - 27.06.14	

Дата выдачи задания « 4 » мая 20 13 г.

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

Руководитель Мухомов Мухомов Алексей Викторович
(подпись) (Фамилия и инициалы)

Задание принял к исполнению
студент Алиев Тимур Рамисович

АННОТАЦИЯ

В данном дипломном проекте представлен процесс проектирования сети с использованием технологии MPLS-VPN для филиала Национальной Компании «Казахстан Темиржолы», ШЧ 19 - Карагандинской дистанции сигнализации и связи, на участке которой находится более 20 станций.

В данном дипломном проекте показана технология MPLS-мультипротокольная коммутация по меткам, VPN-виртуальные частные сети, технология MPLS-VPN, схемы построения сети и состав оборудования.

В проекте также описаны меры безопасности жизнедеятельности.

Разработано технико-экономическое обоснование внедрения данного проекта.

АНДАТПА

Дипломдық жобада «Қазақстан Теміржолы» Ұлттық Компаниясының, 20-дан астам станциясы бар ШЧ 19 – Сигналдау және байланыстың Қарағандылық дистанциясы, филиалы үшін MPLS-VPN технологиясын пайдаланумен желіні жобалау процесі келтірілген.

Берілген жобада MPLS-белгі бойынша коммутациялау технологиясы, VPN – виртуалды жекеменшік желілері, желіні құру сұлбалары және жабдықтар құрамы келтірілген.

Сонымен қатар жобада өміртіршілік қауіпсіздігінің сұрақтары қарастырылады.

Жобаны енгізудің технико-экономикалық негізі келтірілген.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 8

1 ТЕХНОЛОГИЯ MPLS-VPN.....	9
1.1 Мультипротокольная коммутация по меткам (протокол MPLS).....	9
1.1.1 Архитектура и управление MPLS	12
1.1.2 Что такое - мультисервисные сети MPLS?.....	12
1.1.3 Сведения об использовании MPLS в мультисервисных сетях	13
1.1.4 Управление трафиком MPLS.....	13
1.2 VPN – виртуальные частные сети.....	15
1.2.1 Принцип работы технологии VPN.....	15
1.2.2 Достоинства VPN	17
1.3 Функции VPN по защите данных.....	18
1.3.1 Технологии создания виртуальных частных сетей.....	18
1.3.2 Варианты построения.....	19
1.4 MPLS VPN.....	20
1.4.1 Применение туннелей для VPN.....	22
1.4.2 Сравнительный анализ туннелей MPLS и обычных туннелей.....	22
1.4.3 Компоненты MPLS VPN.....	23
1.4.4 Путешествие пакета по сети MPLS VPN.....	25
1.4.5 Безопасность в сетях MPLS-VPN.....	27
2 РАЗРАБОТКА СЕТИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ MPLS-VPN ДЛЯ НК «КТЖ».....	29
2.1 Место реализации проекта.....	29
2.1.1 Разработка структурной схемы организации сети.....	30
2.2 Описание и характеристики выбранного оборудования.....	32
2.2.1 Set-top Box ADB3800 компании ADB.....	32
2.2.2 DIB-120 Цифровая телевизионная приставка высокого разрешения.....	33
2.2.3 DES-3526 Коммутатор управляемый 24x10XMbps, 2 SFP.....	35
2.2.4 Коммутаторы EX-серии.....	37
2.3 Этапы настройки.....	40
2.4 Организация VPN на базе MPLS.....	41
3 ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ	46
3.1 Код программы.....	46
4 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ.....	55
4.1 Анализ условий труда обслуживающего персонала при эксплуатации технического оборудования.....	55
4.1.1 Вид и характеристики используемого оборудования.....	55
4.1.2 Рабочее место, виды работ.....	56

4.1.3 Здание и помещение.....	57
4.1.4 Микроклимат рабочего помещения.....	59
4.1.5 Освещенность рабочего места.....	59
4.1.6 Пожарная безопасность.....	60
4.2 Технические решения вопросов охраны труда и окружающей среды.....	60
4.2.1 Расчет зануления.....	60
4.2.2 Расчет естественного освещения.....	64
4.2.3 Расчет системы автоматического пожаротушения.....	66
5 ЭКОНОМИЧЕСКАЯ ЧАСТЬ.....	70
5.1 Резюме.....	70
5.2 Компания и отрасль.....	70
5.3 Описание продукции (услуги).....	71
5.4 Анализ рынка сбыта. Изучение рынка услуг.....	72
5.5 Финансовый план.....	72
5.5.1 Расчет капитальных вложений.....	73
5.5.2 Расчет стоимости монтажа.....	75
5.5.3 Расчет затрат на проектирование сети.....	76
5.5.4 Расчет затрат на материалы для проектирования сети.....	76
5.5.5 Расходы по оплате труда.....	77
5.5.6 Расчет социальных отчислений.....	79
5.5.7 Расчет затрат на электроэнергию.....	79
5.5.8 Расчет амортизационных отчислений.....	80
5.5.9 Расчет накладных расходов.....	80
5.6 Эксплуатационные издержки.....	81
5.7 Экономический эффект от внедрения технологии MPLS.....	83
ЗАКЛЮЧЕНИЕ.....	86
СПИСОК ЛИТЕРАТУРЫ.....	87
ГЛОССАРИЙ.....	88
ПРИЛОЖЕНИЕ А1	
ПРИЛОЖЕНИЕ Б2	
ПРИЛОЖЕНИЕ В3	
ПРИЛОЖЕНИЕ Г4	
ПРИЛОЖЕНИЕ Д5	

ВВЕДЕНИЕ

Современное развитие информационных технологий и, в частности, сети Internet, приводит к необходимости защиты информации, передаваемой в рамках распределенной корпоративной сети, использующей сети открытого доступа. При использовании своих собственных физических каналов доступа эта проблема так остро не стоит, так как в эту сеть не имеет доступа никто из посторонних. Однако стоимость таких каналов высока, поэтому не каждая компания позволит себе использовать их. В связи с этим Internet является наиболее доступным. Internet является незащищенной сетью, поэтому приходится изобретать способы защиты конфиденциальных данных, передаваемых по незащищенной сети.

VPN - это технология, которая объединяет доверенные сети, узлы и пользователей через открытые сети, которым нет доверия». На мой взгляд, это наиболее яркий образ технологии, которая получает все большее распространение среди не только технических специалистов, но и среди рядовых пользователей, которым также требуется защищать свою информацию (например, пользователи Internet-банков или Internet-порталов).

Специалисты в области технологии VPN используют сугубо технические понятия, такие как «используемый алгоритм криптографического преобразования», «туннелирование», «сервер сертификатов» и т.д. Но для конечных пользователей эта терминология ничего не скажет. Скорее нас интересует несколько иная интерпретация вопросов - сколько лет можно не беспокоиться за сохранность своей информации и насколько медленнее будет работать сеть, защищенная с помощью VPN-устройства.

В данном дипломном проекте рассмотрен проект сети с использованием технологии MPLS-VPN для филиала Национальной Компании «Казахстан Темиржолы», ШЧ 19 - Карагандинской дистанции сигнализации и связи.

1 ТЕХНОЛОГИЯ MPLS-VPN

1.1 Мультипротокольная коммутация по меткам (протокол MPLS)

Протокол MPLS хорошо приспособлен для формирования виртуальных сетей (VPN) повышенного быстродействия (метки коммутируются быстрее, чем маршрутизируются пакеты, — это связано с меньшим размером маршрутных таблиц).

Принципиальной основой MPLS являются IP-туннели. Для его работы нужна поддержка протокола маршрутизации MP-BGP (RFC-2858). Протокол MPLS может работать практически для любого маршрутизируемого транспортного протокола (не только IP). После того как сеть сконфигурирована (для этого используются специальные, поставляемые производителем скрипты), она существует, даже если в данный момент через нее не осуществляется ни одна сессия. При появлении пакета в виртуальной сети ему присваивается метка, которая не позволяет ему покинуть пределы данной виртуальной сети. Никаких других ограничений протокол MPLS не накладывает. Протокол MPLS предоставляет возможность обеспечения значения QoS, гарантирующего более высокую безопасность.

Для обеспечения структурирования потоков в пакете создается стек меток, каждая из которых имеет свою зону действия. Формат стека меток представлен на рисунк 1.1 и 1.2 (смотри RFC-3032). В нормальной ситуации стек меток размещается между заголовками сетевого и канального уровней (соответственно L2 и L3). Каждая запись в стеке занимает 4 октета.



Рисунок 1.1 - Формат стека меток



Рисунок 1.2 - Размещение меток в стеке

Место заголовка MAC может занимать заголовок PPP. В случае работы с сетями ATM метка может занимать поля VPI и VCI. Смотри рисунок 1.3 Глубина стека в данном случае не может превышать 1.

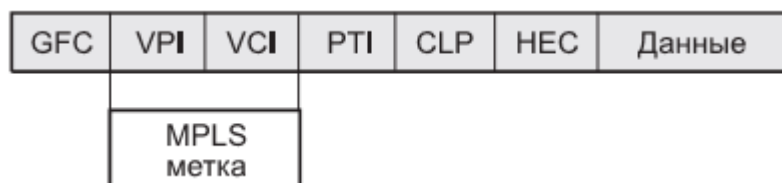


Рисунок 1.3 - Формат меток в ячейках ATM

На рисунке 1.1 поле CoS соответствует субполю приоритет поля ToS. Поле CoS имеет три бита, этого достаточно для поля приоритета IP-заголовка. 6-битовое поле кода дифференцированной услуги DSCP сюда записать нельзя. Можно попробовать разместить этот код в поле самой метки. S — флаг-указатель дна стека меток; TTL — время жизни пакета MPLS.

Существующие версии программного обеспечения Cisco IOS (например, Cisco IOS Release 12.0) содержат набор средств управления трафиком. Управление коммутацией по меткам основывается на базе данных LIB (Label Information Base). Пограничный маршрутизатор MPLS LER (Label Edge Router) удаляет метки из пакетов, когда пакет покидает облако MPLS, и вводит их во входящие пакеты. Схема работы с помеченными и обычными IP-пакетами показана на рисунке 1.4

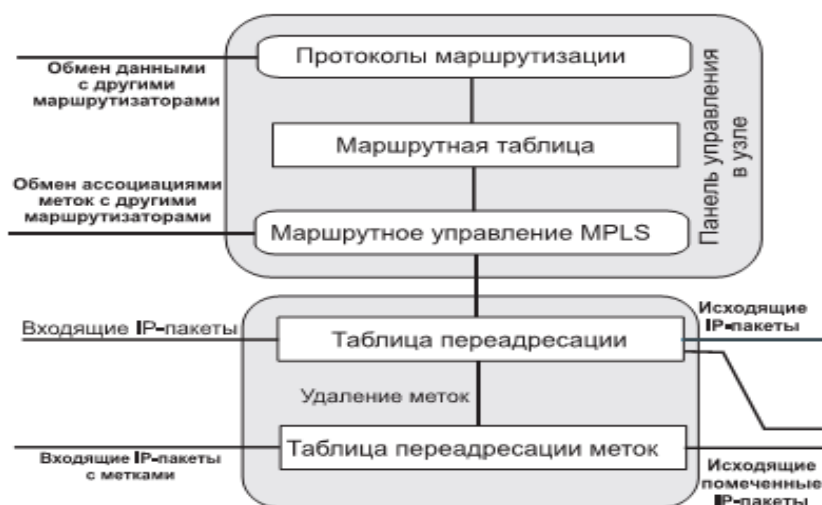


Рисунок 1.4 - Обработка помеченных и обычных IP-пакетов

Управление трафиком MPLS автоматически устанавливает и поддерживает туннель через опорную сеть, применяя возможности RSVP. Путь, используемый данным туннелем, в любой момент времени определяется на основе ресурсных требований и сетевых возможностей, таких, как полоса пропускания.[1]

Путь туннеля вычисляется, основываясь на сформулированных требованиях и имеющихся ресурсах (constraintbased routing). IGP автоматически маршрутизирует трафик через эти туннели. Обычно пакет, проходящий через опорную сеть MPLS, движется по одному туннелю от его входной точки к выходной. Управление трафиком MPLS основано на следующих механизмах IOS (Input/output System):

- туннелях LSP (Labelswitched path), которые формируются посредством RSVP, с расширениями системы управления трафиком. Туннели LSP представляют собой туннельные двунаправленные интерфейсы IOS с известным местом назначения;

- протоколах маршрутизации IGP, базирующихся на состоянии канала (таких, как IS-IS) с расширениями для глобальной рассылки ресурсной информации, и расширениями для автоматической маршрутизации трафика по LSP-туннелям;

- модуле формирования пути MPLS, который определяет пути для LSP туннелей;

- модуле управления трафиком MPLS, который обеспечивает доступ и запись ресурсной информации, подлежащей рассылке;

- переадресации согласно меткам, которая предоставляет маршрутизаторам возможности, сходные с уровнем L2, — перенаправлять трафик через большое число узлов согласно алгоритму маршрутизации отправителя.

Для реализации MPLS управления трафиком сеть должна поддерживать следующие возможности Cisco IOS:

- мультипротокольную переадресацию пакетов с использованием меток (MPLS);

- IPпереадресацию CEF (Cisco Express Forwarding);

- протокол маршрутизации ISIS (Intermediate System to Intermediate System; см. RFC-1142, 1195, 2763, 2966 и 2973)

1.1.1 Архитектура и управление MPLS

В архитектуре MPLS можно выделить несколько уровней. Магистральный уровень: является универсальной высокоскоростной платформой передачи информации, реализованной на базе цифровых телекоммуникационных каналов (MPLS, DWDM, SDH). Уровень распределения включает узловое оборудование сети оператора, а уровень агрегирования выполняет задачи агрегации трафика с уровня доступа и подключения к магистральной (транспортной) сети.

Уровень доступа включает корпоративные или внутридомовые сети, а также каналы связи, обеспечивающие их подключение к узлу (узлам) распределения сети (Fast/Gigabit Ethernet, ISDN, xDSL, Wi-Fi, WiMAX).

Для управления MPLS требуется высокоуровневая интеллектуальная система. В сети одновременно передается множество разных видов трафика, причем для каждого из них требуется безусловное соблюдение одних параметров и допускаются более или менее серьезные уступки по другим, требуется использование специализированных средств, не допускающих перегрузки сети и нарушения требуемого качества. Сеть должна самостоятельно устранять перегрузки, автоматически решая, чем можно пожертвовать в разных случаях — полосой пропускания, временем доставки или, для отдельных потоков, целостностью информации.[2]

1.1.2 Что такое - мультисервисные сети MPLS?

Мультисервисная сеть представляет собой универсальную среду для передачи любого вида трафика (данные, голос, видео) и на сегодняшний день самой распространенной технологией для таких сетей является IP-MPLS. К мультисервисным сетям применяются повышенные требования с точки зрения надежности, гарантированности предоставления сервиса и минимальной стоимости передачи в расчете на единицу объема информации.

MPLS должны обеспечивать работу разнородных информационных и телекоммуникационных систем и приложений в единой транспортной среде. Кроме этого, мультисервисная сеть предоставляет сервис-провайдерам много возможностей по построению многообразных наложенных сервисов поверх универсальной транспортной среды – от передачи голоса по IP до интерактивного телевидения и веб-служб.

1.1.3 Сведения об использовании MPLS в мультисервисных сетях

На сегодняшний день многопротокольная коммутация информационных потоков в соответствии с метками (Multiprotocol Label Switching, MPLS) рассматривается как основная технология для конвергенции услуг и построения мультисервисных сетей следующего поколения (NGN), в которых возможна передача разнородного трафика через интегрированную телекоммуникационную инфраструктуру вместо нескольких различных сетей.

Также немаловажно, что использование единой транспортной среды позволяет снизить издержки на построение и эксплуатацию сети за счет унификации оборудования, стандартов, технологий и единой централизованной системы управления сетью. С другой стороны современные мультисервисные сети обладают широкими возможностями по поддержке заданного SLA (Service Level Agreement) - качество и уровень обслуживания гарантируются не только на уровне договорных соглашений с сервис-провайдером, но и на уровне технологий и сетей.

В основе MPLS лежит принцип обмена меток. Любой передаваемый пакет ассоциируется с тем или иным классом сетевого уровня (Forwarding Equivalence Class, FEC), каждый из которых идентифицируется определенной меткой. Значение метки уникально лишь для участка пути между соседними узлами сети MPLS, коммутирующими по меткам (Label Switching Router, LSR). Метка передается в составе любого пакета, причем способ ее привязки к пакету зависит от используемой технологии канального уровня.

Распределение меток между LSR приводит к установлению внутри домена MPLS путей с коммутацией по меткам (Label Switching Path, LSP). Каждый маршрутизатор LSR содержит таблицу, которая ставит в соответствие паре «входной интерфейс, входная метка» тройку «префикс адреса получателя, выходной интерфейс, выходная метка». Получая пакет, LSR по номеру интерфейса, на который пришел пакет, и по значению привязанной к пакету метки определяет для него выходной интерфейс. Старое значение метки заменяется новым, содержавшимся в поле «выходная метка» таблицы, и пакет отправляется к следующему устройству на пути LSP.

1.1.4 Управление трафиком

В настоящее время используется несколько методов управления трафиком.

Динамическая маршрутизация (RIP, OSPF, IGRP, BGP и т.д.). Здесь нет средства резервирования полосы, но предусмотрен механизм изменения маршрута при изменении значений метрики или из-за выхода из строя узла или обрыва канала. Некоторые из таких протоколов (OSPF, IGRP) могут строить отдельные таблицы маршрутизации для каждого уровня TOS/QO, но метрики для каждого уровня задаются сетевым администратором. Эти протоколы работают только в пределах одной автономной системы (AS). Протокол же BGP, используемый для прокладки путей между автономными системами, не способен в настоящее время как-либо учитывать уровень ToS/QoS (применяет алгоритм вектора расстояния, что связано с трудностью согласования значений метрик состояния канала администраторами разных AS). Новая версия многопротокольного расширения MPBGP специально создана для совместной работы с MPLS при формировании виртуальных сетей, но и он безразличен к TOS/QOS. [3]

Формирование виртуальных сетей на уровнях L2 и L3. Протоколы VLAN обеспечивают повышенный уровень безопасности, но, как правило, не способны резервировать полосу. К этому типу относится и протокол MPLS.

Резервирование полосы в имеющемся виртуальном канале (протокол RSVP). RSVP может работать с протоколами IPv4 и IPv6. Протокол достаточно сложен для параметризации, поэтому для решения этой задачи был разработан протокол COPS, который существенно облегчает параметризацию. Функция COPS сходна с задачей языка RPSL для маршрутизации.

Качество обслуживания QoS

QoS связана с возможностью сети предоставить клиенту необходимый ему уровень услуг в условиях работы поверх сетей с самыми разнообразными технологиями, включая Frame Relay, ATM, Ethernet, сети 802.1, SONET и маршрутизируемые IP-сети.

QoS представляет собой собрание технологий, которые позволяют приложениям запрашивать и получать предсказуемый уровень услуг с точки зрения пропускной способности, временного разброса задержки отклика, а также общей задержки доставки данных. В частности, QoS подразумевает улучшение параметров или достижение большей предсказуемости предоставляемых услуг.

1.2 VPN – виртуальные частные сети

Любая организация, будь она производственной, торговой, финансовой компании или государственным учреждением, обязательно сталкивается с вопросом передачи информации между своими филиалами, а также с вопросом защиты этой информации. Не каждая фирма может себе позволить иметь собственные физические каналы доступа, и здесь помогает технология VPN, на основе которой и соединяются все подразделения и филиалы, что обеспечивает достаточную гибкость и одновременно высокую безопасность сети, а также существенную экономию затрат.

1.2.1 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. Еще одной важной характеристикой VPN-решений является диапазон поддерживаемых протоколов аутентификации. Большинство популярных продуктов работают со стандартами, основанными на использовании открытого ключа, такими как X.509. Это означает, что, усилив свою виртуальную частную сеть соответствующим протоколом аутентификации, вы сможете гарантировать, что доступ к вашим защищенным туннелям получают только известные вам люди (рисунок 1.5).

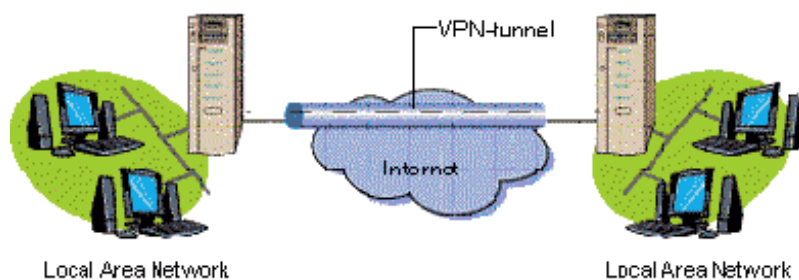


Рисунок 1.5 - Принцип работы технологии VPN

Сегодня технология завоевала всеобщее признание и любой администратор считает своим долгом организовать VPN-каналы для сотрудников, работающих вне офиса (рисунок 1.6).

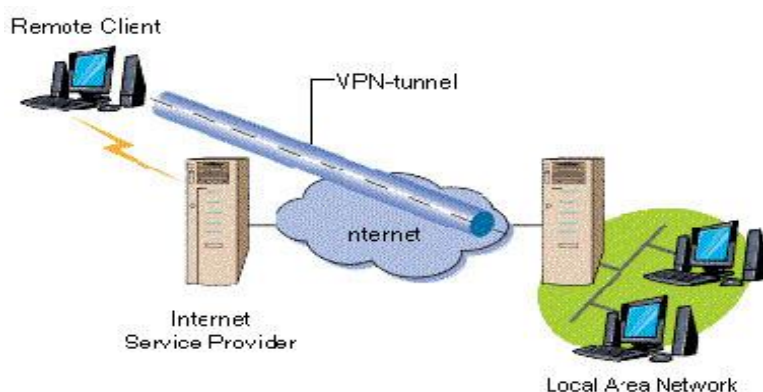


Рисунок 1.6 - VPN для удаленных пользователей

VPN (рисунок 1.7) 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.

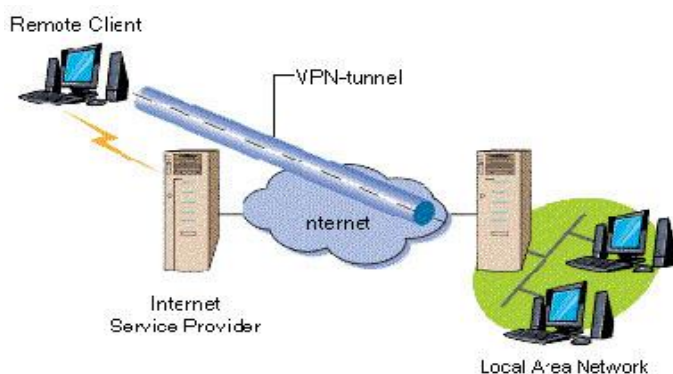


Рисунок 1.7 - VPN для двух офисных сетей

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.[4]

1.2.2 Достоинства VPN

Виртуальные частные сети имеют несколько преимуществ над традиционными частными сетями. Главные из них - экономичность, гибкость и удобство использования.

Экономичность. С помощью VPN-сетей предприятиям удастся хотя бы частично ограничить рост числа модемов, серверов доступа, коммутируемых линий и других технических средств, которые организации вынуждены внедрять, чтобы обеспечить удаленным пользователям доступ к своим корпоративным сетям. Кроме того, виртуальные частные сети дают возможность удаленным пользователям обращаться к сетевым ресурсам компании не по дорогим арендованным линиям, а через местную телефонную связь.

Особенно выгодны виртуальные частные сети в тех случаях, когда пользователи удалены на большие расстояния и поэтому арендованные линии обходятся очень дорого, а также когда таких пользователей много, в связи с чем и им требуется большое количество арендованных линий.

Исследовательская компания Forrester Research опубликовала следующие данные, характеризующие преимущество применения VPN поверх Internet (из расчета 1000 пользователей) по сравнению с созданием центра удаленного доступа (Remote Access Service).

Таблица 1.1 - Преимущество применения VPN поверх Internet

Статья затрат	Удаленный доступ (в млн. долл.)	VPN(в млн. долл.)
Оплата услуг провайдера связи	1,08	0,54
Расходы на эксплуатацию	0,3	0,3
Капиталовложения	0,1	0,02
Прочие расходы	0,02	0,03
Всего	1,5	0,89

Из таблицы можно видеть, что использование VPN позволяет снизить многие статьи затрат, включая закупку коммуникационного оборудования, оплату услуг Internet-провайдера и т.д. Эти, а также другие исследования,

позволили Международной Ассоциации Компьютерной Безопасности (International Computer Security Association, ICSA) причислить технологию VPN к десятке самых известных технологий, которые будут в первую очередь применяться многими компаниями.

1.3 Функции VPN по защите данных

Подключение любой корпоративной сети к публичной вызывает два типа угроз:

- несанкционированный доступ к ресурсам локальной сети, полученный в результате входа в эту сеть;
- несанкционированный доступ к данным при передаче трафика по публичной сети.

Для создания защищенного канала средства VPN используют процедуры шифрования, аутентификации и авторизации.

Шифрование. Методов шифрования довольно много, поэтому важно, чтобы на концах туннеля использовался один и тот же алгоритм шифрования. Кроме того, для успешного дешифрования данных источнику и получателю данных необходимо обменяться ключами шифрования. Следует отметить, что шифрование сообщений необходимо не всегда. Часто оно оказывается довольно дорогостоящей процедурой, требующей дополнительных приставок для маршрутизаторов, без которых они не могут одновременно с шифрованием обеспечивать приемлемый уровень быстродействия.

1.3.1 Технологии создания виртуальных частных сетей

Среди технологий построения VPN можно назвать такие технологии, как: IPSec VPN, MPLS VPN, VPN на основе технологий туннелирования PPTP и L2TP. Во всех перечисленных случаях трафик посылается в сеть провайдера по протоколу IP, что позволяет провайдеру оказывать не только услуги VPN, но и различные дополнительные сервисы (контроль за работой клиентской сети, хостинг Web и почтовых служб, хостинг специализированных приложений клиентов).

На рисунке 1.8 представлен общий вариант построения виртуальной частной сети на базе общедоступной сети провайдера. Сеть каждого клиента состоит из территориально распределенных офисов, которые связаны между туннелями, проложенными через сеть провайдера.

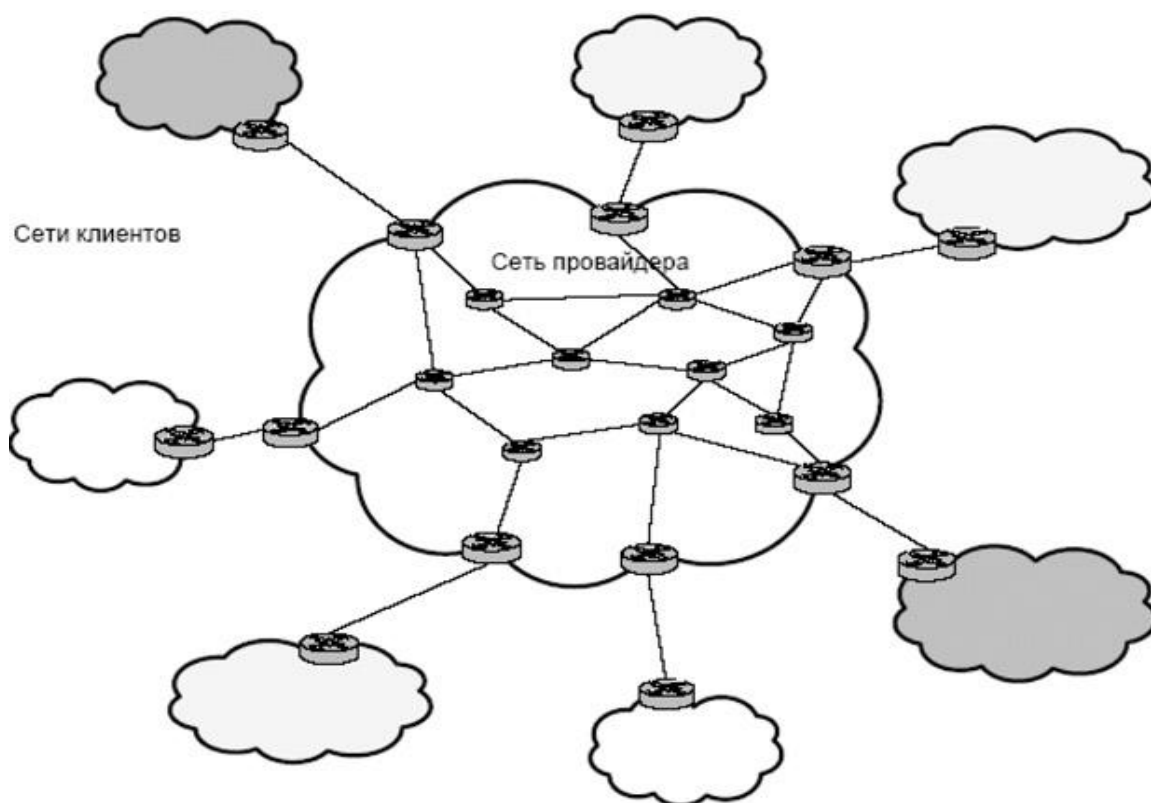


Рисунок 1.8 - Общий вариант построения виртуальной частной сети

1.3.2 Варианты построения

Можно выделить четыре основных варианта построения сети VPN, которые используются во всем мире. Данная классификация предлагается компанией Check Point Software Technologies, которая не без основания считается законодателем моды в области VPN. Так, например, по данным независимых консалтинговых и аналитических агентств компания Check Point захватила 52% мирового рынка VPN-решений (по данным Dataquest).

Вариант «Intranet VPN», который позволяет объединить в единую защищенную сеть несколько распределенных филиалов одной организации, взаимодействующих по открытым каналам связи. Именно этот вариант получил широкое распространение во всем мире, и именно его в первую очередь реализуют компании-разработчики.

Вариант «Remote Access VPN», который позволяет реализовать защищенное взаимодействие между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который

подключается к корпоративным ресурсам из дома (домашний пользователь) или через notebook (мобильный пользователь).

Вариант «Client/Server VPN», который обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и сервером.

Последний вариант «Extranet VPN» (рисунок 1.9) предназначен для тех сетей, к которым подключаются пользователи «со стороны» (партнеры, заказчики, клиенты и т.д.), уровень доверия к которым намного ниже, чем к своим сотрудникам. [5]

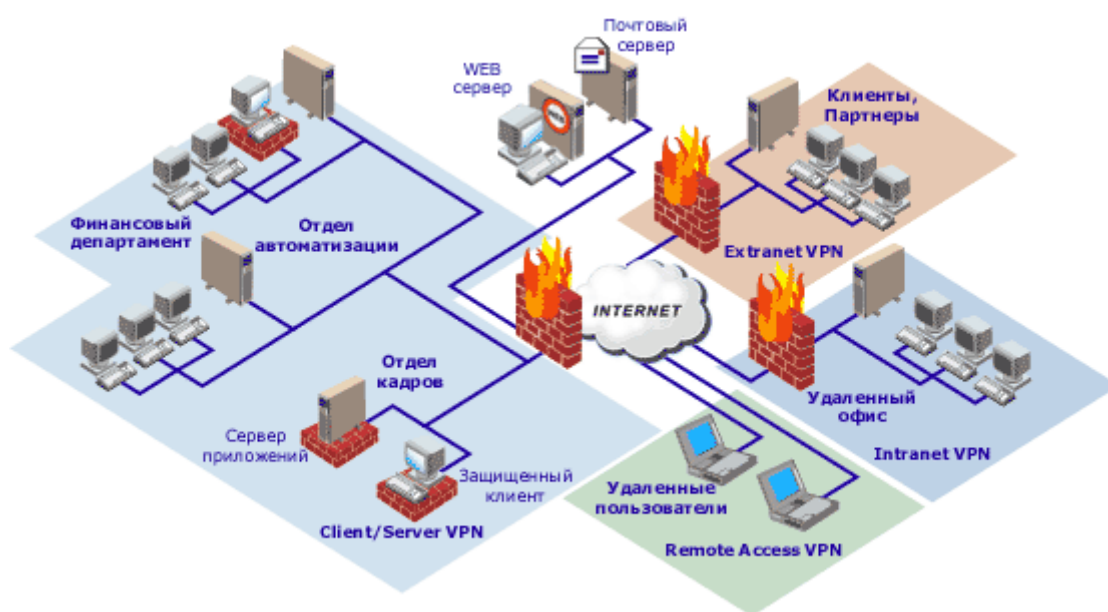


Рисунок 1.9 - Последний вариант «Extranet VPN»

1.4 MPLS VPN

Технология MPLS в настоящее время является одной из наиболее перспективных технологий создания VPN.

Использование MPLS для построения VPN позволяет сервис-провайдерам быстро и экономично создавать защищенные виртуальные частные сети любого размера в единой инфраструктуре.

Сеть MPLS VPN делится на две области: IP-сети клиентов и внутренняя (магистральная) сеть провайдера, которая служит для объединения клиентских сетей. В общем случае у каждого клиента может быть несколько территориально обособленных сетей IP, каждая из которых в свою очередь

может включать несколько подсетей, связанных маршрутизаторами. Такие территориально изолированные сетевые элементы корпоративной сети принято называть сайтами. Принадлежащие одному клиенту сайты обмениваются IP-пакетами через сеть провайдера MPLS и образуют виртуальную частную сеть этого клиента. Обмен маршрутной информацией в пределах сайта осуществляется по одному из внутренних протоколов маршрутизации IGP. Структура MPLS VPN предполагает наличие трех основных компонентов сети:

Customer Edge Router, CE – пограничный маршрутизатор клиента (Edge LSR в терминологии MPLS);

Provider Router, P – внутренний маршрутизатор магистральной сети провайдера (LSR в терминологии MPLS);

Provider Edge Router, PE – пограничный маршрутизатор сети провайдера. (рисунок 1.10).

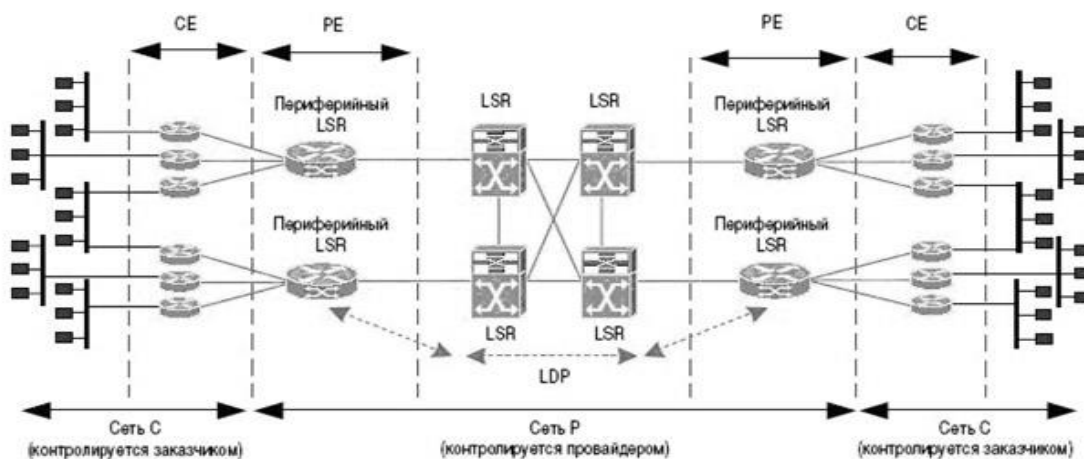


Рисунок 1.10 - MPLS VPN

Пограничные маршрутизаторы клиента служат для подключения сайта клиента к магистральной сети провайдера. Эти маршрутизаторы принадлежат сети клиента и ничего не знают о существовании VPN. CE-маршрутизаторы различных сайтов не обмениваются маршрутной информацией непосредственно и даже могут не знать друг о друге. Адресные пространства подсетей, входящих в состав VPN, могут перекрываться, т.е. уникальность адресов должна соблюдаться только в пределах конкретной подсети. Этого удалось добиться преобразованием IP-адреса в VPN-IP-адрес и использованием протокола MP-BGP для работы с этими адресами. Считается, что CE-маршрутизатор относится к одному сайту, но сайт может принадлежать к нескольким VPN.

Обмен маршрутной информацией между сайтами каждой отдельной VPN выполняется под управлением протокола MP-BGP (Multiprotocol BGP).

1.4.1 Применение туннелей для VPN

Протоколы защищенного канала, как правило, используют в своей работе механизм туннелирования. С помощью данной методики пакеты данных транслируются через общедоступную сеть как по обычному двухточечному соединению. Между каждой парой «отправитель – получатель данных» устанавливается своеобразный туннель – безопасное логическое соединение, позволяющее инкапсулировать данные одного протокола в пакеты другого. [6]

Технология туннелирования позволяет зашифровать исходный пакет целиком, вместе с заголовком, а не только его поле данных. Такой зашифрованный пакет помещается в другой пакет с открытым заголовком. Этот заголовок используют для транспортировки данных на участке общей сети. В граничной точке защищенного канала извлекается зашифрованный заголовок, который будет использоваться для дальнейшей передачи пакета. Как правило, туннель создается только на участке сети общего пользования, где существует угроза нарушения конфиденциальности и целостности данных. Помимо защиты передаваемой информации, механизм туннелирования используют для обеспечения целостности и аутентичности. При этом защита потока реализуется более полно.

Туннелирование применяется также и для согласования разных транспортных технологий, если данные одного протокола транспортного уровня необходимо передать через транзитную сеть с другим транспортным протоколом. Следует отметить, что процесс туннелирования не зависит от того, с какой целью он применяется. Сам по себе механизм туннелирования не защищает данные от несанкционированного доступа или от искажений, он лишь создает предпосылки для защиты всех полей исходного пакета. Для обеспечения секретности передаваемых данных пакеты на транспортном уровне шифруются и передаются по транзитной сети.

1.4.2 Сравнительный анализ туннелей MPLS и обычных туннелей

Туннели MPLS позволяют передавать данные любого протокола вышестоящего уровня (например IP, IPX, кадры Frame Relay, ячейки ATM),

так как содержимое пакетов вдоль всего пути следования пакета остается неизменным, меняются только метки. В отличие от них, туннели IPSec поддерживают передачу данных только протокола IP, а протоколы PPTP и L2TP позволяют обмениваться данными по протоколам IP, IPX или Net BEUI. Безопасность передачи данных в MPLS обеспечивается за счёт определённой сетевой политики, запрещающей принимать пакеты, снабжённые метками, и маршрутную информацию VPN-IP от непроверенных источников. Она может быть повышена использованием стандартных средств аутентификации и/или шифрования (например шифрование IPSec). Протокол L2TP поддерживает процедуры аутентификации и туннелирования информационного потока, а PPTP помимо данных функций снабжен и функциями шифрования. Применение меток MPLS позволяет реализовать ускоренное продвижение пакетов по сети провайдера. Транспорт MPLS не считывает заголовки транспортируемых пакетов, поэтому используемая в этих пакетах адресация может носить частный характер. Содержимое пакетов не считывается и при передаче IP-пакетов по протоколам IPSec, PPTP и L2TP. Однако, в отличие от MPLS, традиционные протоколы туннелирования для транспортировки IP-пакетов используют традиционную IP-маршрутизацию. При выборе пути следования пакета в MPLS учитываются различные параметры, оказывающие влияние на выбор маршрута.

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.

1.4.3 Компоненты MPLS VPN

Прежде всего, сеть MPLS VPN делится на две области: сети IP клиентов и внутренняя (магистральная) сеть MPLS провайдера, которая необходима для объединения сетей клиентов (см. Рисунок 1.11).

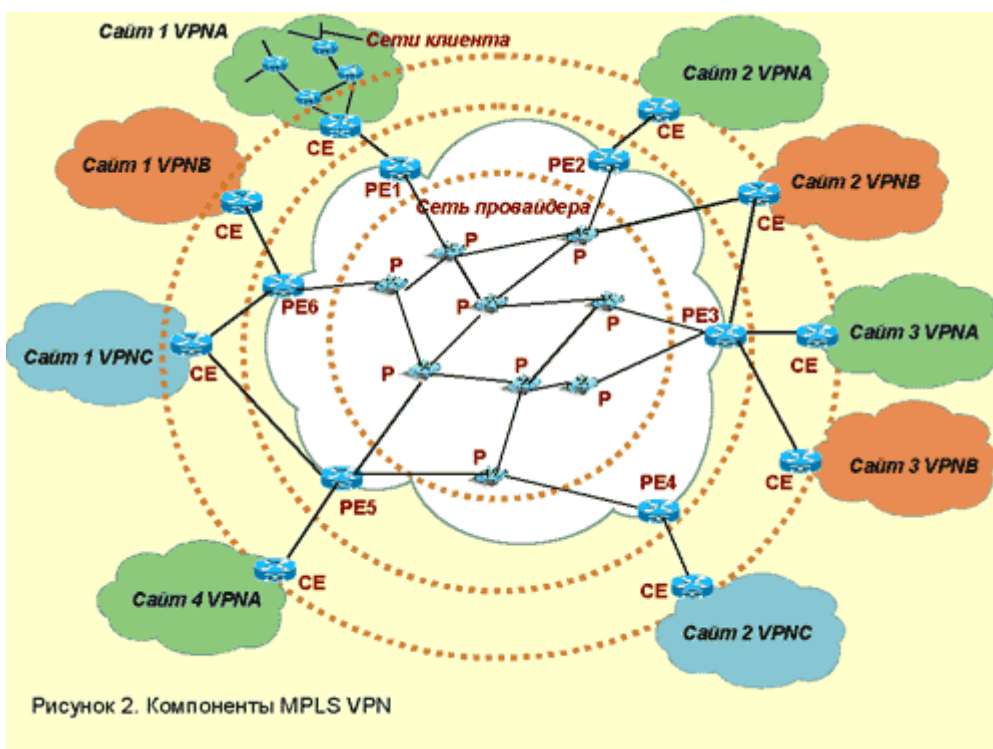


Рисунок 1.11 - Компоненты MPLS VPN

В общем случае у каждого клиента может быть несколько территориально обособленных сетей IP, каждая из которых в свою очередь может включать несколько подсетей, связанных маршрутизаторами. Такие территориально изолированные сетевые «островки» корпоративной сети принято называть сайтами. Принадлежащие одному клиенту сайты обмениваются пакетами IP через сеть провайдера и образуют виртуальную частную сеть этого клиента. Например, в корпоративной сети, в которой сеть центрального отделения связывается с тремя удаленными филиалами, можно сказать, что она состоит из четырех сайтов. Для обмена маршрутной информацией в пределах сайта узлы пользуются одним из внутренних протоколов маршрутизации (Interior Gateway Protocol, IGP), область действия которого ограничена автономной системой: RIP, OSPF или IS-IS.

Магистральная сеть провайдера является сетью MPLS, где пакеты IP продвигаются на основе не IP-адресов, а локальных меток (более подробно о технологиях этого типа можно прочитать в статье Н. Олифер «Пути-дороги через сеть» в данном номере). Сеть MPLS состоит из маршрутизаторов с коммутацией меток (Label Switch Router, LSR), которые направляют трафик по предварительно проложенным путям с коммутацией меток (Label Switching Path, LSP) в соответствии со значениями меток. Устройство LSR — это своеобразный гибрид маршрутизатора IP и коммутатора, при этом от маршрутизатора IP берется способность определять топологию сети с

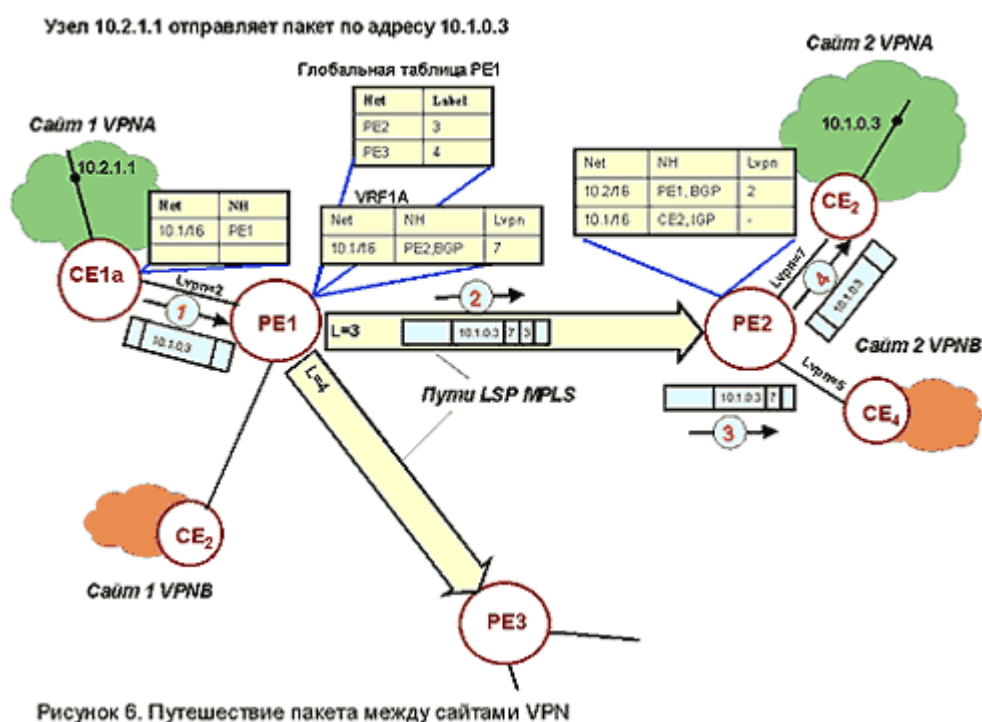
помощью протоколов маршрутизации и выбирать рациональные пути следования трафика, а от коммутатора — техника продвижения пакетов с использованием меток и локальных таблиц коммутации. Устройства LSR для краткости часто называют просто маршрутизаторами, и в этом есть свой резон — они с таким же успехом способны продвигать пакеты на основе IP-адреса, если поддержка MPLS отключена.

В магистральной сети провайдера только пограничные маршрутизаторы PE должны быть сконфигурированы для поддержки виртуальных частных сетей, поэтому только они «знают» о существующих VPN. Если рассматривать сеть с позиций VPN, то маршрутизаторы провайдера P непосредственно не взаимодействуют с маршрутизаторами заказчика CE, а просто располагаются вдоль туннеля между входным и выходным маршрутизаторами PE.[7]

1.4.4 Путешествие пакета по сети MPLS VPN

Теперь, когда мы обсудили схему распространения маршрутной информации по сети MPLS VPN, давайте посмотрим, 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 1.12).



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 Р, пакет будет снабжен двумя метками — внутренней $L_{vpn}=7$ и внешней $L=3$. Метка L_{vpn} 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 Р вдоль туннеля, метка L анализируется и заменяется новым значением. И только после достижения конечной точки туннеля маршрутизатора PE2 из стека извлекается метка L_{vpn} . В зависимости от ее значения пакет направляется на тот или иной выходной интерфейс маршрутизатора PE2.

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.

1.4.5 Безопасность в сетях MPLS-VPN

Функциональность MPLS-VPN поддерживает уровень безопасности, эквивалентный безопасности оверлейных виртуальных каналов в сетях Frame Relay и ATM. Безопасность в сетях MPLS-VPN поддерживается с помощью сочетания протокола BGP и системы разрешения IP-адресов.

BGP-протокол отвечает за распространение информации о маршрутах. Он определяет, кто и с кем может связываться с помощью многопротокольных расширений и атрибутов community. Членство в VPN

зависит от логических портов, которые объединяются в сеть VPN и которым BGP присваивает уникальный параметр Route Distinguisher (RD). Параметры RD неизвестны конечным пользователям, и поэтому они не могут получить доступ к этой сети через другой порт и перехватить чужой поток данных. В состав VPN входят только определенные назначенные порты. В сети VPN с функциями MPLS протокол BGP распространяет таблицы FIB (Forwarding Information Base) с информацией о VPN только участникам данной VPN, обеспечивая таким образом безопасность передачи данных с помощью логического разделения трафика. [8]

Именно провайдер, а не заказчик присваивает порты определенной VPN во время ее формирования. В сети провайдера каждый пакет ассоциирован с RD, и поэтому попытки перехвата пакета или потока трафика не могут привести к прорыву хакера в VPN. Пользователи могут работать в сети интранет или экстранет, только если они связаны с нужным физическим или логическим портом и имеют нужный параметр RD. Эта схема придает сетям Cisco MPLS-VPN очень высокий уровень защищенности.

В опорной сети информация о маршрутах передается с помощью стандартного протокола Interior Gateway Protocol (IGP), такого как OSPF или IS-IS. Пограничные устройства PE в сети провайдера устанавливают между собой связи-пути, используя LDP для назначения меток. Атрибут Community BGP ограничивает рамки информации о доступности сетей и позволяет поддерживать очень крупные сети, не перегружая их информацией об изменениях маршрутной информации. BGP не обновляет информацию на всех периферийных устройствах PE, находящихся в провайдерской сети, а приводит в соответствие таблицы RIB только тех PE, которые принадлежат к конкретной VPN. [9]

В сетях MPLS-VPN пакет, поступающий в магистраль, в первую очередь ассоциируется с конкретной сетью VPN на основании того, по какому интерфейсу (подин-терфейсу) пакет поступил на PE-маршрутизатор. Затем IP-адрес пакета сверяется с таблицей передачи (forwarding table) данной VPN. Указанные в таблице маршруты относятся только к VPN принятого пакета. Таким образом, входящий интерфейс определяет набор возможных исходящих интерфейсов. Эта процедура также предотвращает как попадание несанкционированного трафика в сеть VPN, так и передачу несанкционированного трафика из нее.

2 РАЗРАБОТКА СЕТИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ MPLS-VPN ДЛЯ НК «КТЖ» ШЧ 19

2.1 Место реализации проекта

Организация: Национальная Компания «Казахстан Теміржолы».

ШЧ-19 - Карагандинская дистанция сигнализации и связи, на участке которой более 20 станции (рисунок 2.1).



Рисунок 2.1 – показательный рисунок НК «КТЖ»

Филиал обеспечивает безопасность движения поездов. Автоматизирует управление дежурным маневрами при сортировке поездов на станциях, и блокирует возможные не правильные действия дежурного по станции. На участках между станциями (перегонах) осуществляет интервальное движение поездов с контролем их местоположения.

Так же с помощью микропроцессорной диспетчерской централизацией вся информация сводится к поездным диспетчерам, которые управляют движением поездов из единого центра в Караганде, давая команды дежурным находящимся на станциях. В конце вся эта информация передается в город Астана.

Основная деятельность Национальной компании «Казахстан Темиржолы» это пассажирские перевозки, грузовые перевозки и транзитные перевозки. Сотрудники компании обязаны обеспечить безопасность пассажиров и своевременную доставку грузов. Но вся эта работа невозможна без качественной, производительной, быстродействующей и безопасной работы внутренней компьютерно-коммуникационной сети компании.

Один из методов повышения качества работы компьютерной – коммуникационной сети компании рассматривается в данном проекте – разработка сети с использованием технологии MPLS.[10]

2.1.1 Разработка структурной схемы организации сети

MPLS наиболее привлекательная технология для операторов связи. Данное решение применяется при строительстве распределенных сетей, которые ориентированы на предоставление услуг по передаче данных, голоса и видео по протоколу IP. MPLS является базой для реализации целого ряда услуг, таких как:

- организация каналов точка-точка (P2P) VPWS - Virtual Private Wire Service или AoMPLS Any transport over MPLS;
- организация прозрачных соединений (на втором уровне OSI: 802.1q, Frame Relay, ATM...) типа точка-точка через MPLS;
- организация многоточечных каналов (P2M) VPLS - Virtual Private LAN Service;
- эмуляция распределенных ЛВС.
- Виртуальные выделенные каналы с возможностью восстановления за 50 мс.

Преимущества MPLS технологии:

- быстрая передача данных (по сравнению с маршрутизацией использующей ip адреса);
- приоритезация данных и гарантированное качество обслуживания (QoS, Traffic Engineering);
- перераспределение потоков (возможность явно задать один или несколько маршрутов передачи данных, позволяет оптимизировано использовать полосы пропускания);
- создание частных виртуальных сетей L3 VPN.

2.2 Описание и характеристики выбранного оборудования

2.2.1 Set-top Box ADB3800 компании ADB

Гибридный (IPTV с поддержкой DVB-T) HD Set-top Box ADB3800 компании ADB это полнофункциональный цифровой приемник на базе новейшего микропроцессора STb7100, оптимизированный под телекоммуникационные сети, основанные на IP, и дополнительно работает в эфирных сетях стандарта DVB-T.



Рисунок 2.3 – Цифровой приемник Set-top Box ADB3800

Основные особенности гибридного HD ресивера ADB3800:

- микропроцессор STb7100;
- совместимость с DVB-T;
- поддержка стандартов MPEG-2 и MPEG-4;
- видео стандартной (SD) и высокой четкости (HD);
- поддержка звука MPEG-1 (Layer 1, 2), HE AAC;
- поддержка всех основных систем условного доступа;
- высокоскоростной порт USB 2.0;
- 2 выхода SCART и 1 выход RCA;
- SPDIF цифровой выход звука;
- HDMI выход.

Технические характеристики гибридного HD ресивера ADB3800 компании ADB:

Видео:

- MPEG-2 SD; MP@ML;

- MPEG-2 HD; MP@HL;
- H.264 (MPEG-4 part 10) MP и HP level 4.1;
- разрешение: 1080i, 720p, 576i, 576p;
- формат экрана: 4:3, 16:9.

Звук:

- MPEG-1 Layer I/II (Musicam);
- Mono, Dual Mono, Stereo, Joint Stereo;
- AAC, HE AAC.

Программное обеспечение:

- графический интерфейс пользователя;
- базовый пакет приложений;
- электронный программный гид;
- условный доступ: Поддержка всех основных систем условного доступа.
- HDMI;
- RJ-45 Ethernet порт;
- RS-232 последовательный порт (опция);
- ВЧ выход;
- USB 2,0 высокоскоростной порт.

2.2.2 DIB-120 Цифровая телевизионная приставка высокого разрешения

Описание:

Поток Live Internet

Цифровая телевизионная IP-приставка высокого разрешения DIB-120 позволяет просматривать цифровой контент поверх любой широкополосной IP-сети. Интерактивное навигационное меню позволяет пользователям получать доступ к постоянно растущему каталогу развлечений online, спортивным событиям и новостям. С помощью широкополосного доступа каждый может дома в комфортных условиях смотреть видео в режиме HDTV в удобное для себя время.

Услуга видео по запросу

DIB-120 поддерживает видео высокого разрешения и соответствующие кодеки (MPEG2 MP@HL / H.264 MPEG-4 part10 MP@L4). Это позволяет пользователям просматривать on-line медиа-контент с сервера Video on demand (VOD) в режиме высокого разрешения (HDTV) или стандартного разрешения (SDTV). Сервер VOD обеспечивает высокое качество

изображения и позволяет легко осуществлять поиск в режиме on-line. При этом заказчик получает простоту и удобство управления.

Передаче видео с высоким разрешением

Цифровая телевизионная приставка DIB-120 позволяет пользователю наслаждаться с друзьями и семьей цифровым видео на большом экране телевизора с поддержкой HDTV. DIB-120 обеспечивает высочайшее качество передачи видео. Достаточно просто подключить телевизионную приставку к IP-сети и домашнему кинотеатру, и весь функционал IPTV доступен для использования.



Рисунок 2.4 - Цифровая телевизионная IP-приставка высокого разрешения DIB-120

Характеристики:

- Стандарты LAN Ethernet/IEEE 802.3;
- UDP/IP;
- DHCP Client;
- TCP/IP v4.0;
- IGMPv3;
- RTSP, RTP, SDP.

Встроенный ТВ-браузер

- «Горячие» клавиши для HOME, Back, Forward, Stop, Refresh;
- Окно ввода URL;
- HTTP 1.0/1.1 (http, https);
- Шрифт True type;
- HTML 4.0, поддержка каскадного размещения окон;
- Java(ECMA) script;
- CSS 2 и некоторый функционал CSS 3;
- XML;
- GIF, JPEG, BMP, animated GIF, PNG, IPTV;
- Встроенная ОС Linux.

Язык/символы/шрифт

- Английский;
- Кириллица (ISO-8859-5);
- True Type.

Дополнительные функции

- IME (Input Method editor) для Remote controller;
- Удаленная клавиатура IrDA5;
- USB Smart Card reader (Smart card CA)5.

Формат видео на выходе

- PAL / NTSC;
- 4:3 / 16:9.
- Температура хранения: -25~55°C;
- Влажность: 5 ~ 95% без образования конденсата.[9]

2.2.3 DES-3526 Коммутатор управляемый 24x10XMbps, 2 SFP

Управляемый коммутатор 2 уровня с 24 портами 10/100Base-TX + 2 комбо-портами 1000Base-T/Mini GBIC (SFP) Коммутаторы серии 10/100 Мбит/с D-Link DES-3500 являются взаимно стекируемыми коммутаторами уровня доступа, поддерживающими технологию Single IP Management (SIM, управление через единый IP-адрес). Эти коммутаторы, имеющие 24 или 48 10/100BASE-TX портов и 2 комбо-порта 1000BASE-T/SFP Gigabit Ethernet в стандартном корпусе для установки в стойку, разработаны для гибкого и безопасного сетевого подключения. Коммутаторы серии DES-3500 могут легко объединяться в стек и настраиваться вместе с любыми другими коммутаторами с поддержкой D-Link Single IP Management, включая коммутаторы 3-го уровня ядра сети, для построения части многоуровневой сети, структурированной с магистралью и централизованными быстродействующими серверами



Рисунок 2.5 – DES-3526 Коммутатор управляемый 24x10XMbps, 2 SFP

Экономичный виртуальный стек. В основном, коммутаторы серии DES-3500 формируют стек сети уровня подразделения, предоставляя порты 10/100 Мбит/с и возможность организации гигабитного подключения к магистрالي. Трафик, передаваемый между устройствами стека, проходит через интерфейсы Gigabit Ethernet с поддержкой полного дуплекса и обычные провода сети, позволяя избежать использования дорогостоящих и громоздких кабелей для стекирования.

Управление через единый IP-адрес (Single IP Management) Коммутаторы серии DES-3500 упрощают и ускоряют задачу управления, т.к. множество коммутаторов могут настраиваться, контролироваться и обслуживаться через уникальный IP-адрес с любой рабочей станции, имеющей Web-браузер. Стек управляется как единый объект, и все устройства стека определяются по единственному IP-адресу. [11]

Для повышения производительности и безопасности сети коммутаторы серии DES-3500 обеспечивает расширенную поддержку VLAN, включая GARP/GVRP, 802.1Q и асимметричные VLAN. Управление полосой пропускания позволяет установить лимит трафика для каждого порта, что дает возможность управлять объемом трафика на границе сети. Коммутатор поддерживает установку резервного источника питания. Другие характеристики включают поддержку 802.3ad Link Aggregation, 802.1d Spanning Tree, 802.1w Rapid Spanning Tree и 802.1s Multiple Spanning Tree для повышения надежности и доступности виртуального стека.

Многоуровневое качество обслуживания (QoS). Серия DES-3500 имеет широкий набор многоуровневых (L2, L3, L4) QoS/CoS функций, для гарантии того, что критически важные сетевые сервисы, подобные VoIP, ERP, Intranet или видеоконференции будут обслуживаться. [12]

Дополнительные мини GBIC SFP трансиверы:

- DEM-310GT - SFP трансивер для 1000BASE-LX, одномодовый кабель, макс. расстояние 10 км, 3.3В;
- DEM-311GT - SFP трансивер для 1000BASE-SX, многомодовый кабель, макс. расстояние 550 м, 3.3В;
- DEM-314GT - SFP трансивер для 1000BASE-LHX, одномодовый кабель, макс. расстояние 50 км, 3.3В;
- DEM-315GT - SFP трансивер для 1000BASE-ZX, одномодовый кабель, макс. расстояние 80 км, 3.3В.

Дополнительные резервные источники питания

- DPS-200 - резервный источник питания 60 Ватт.

Таблица 2.1 - Общие характеристики коммутатора DES-3526

Аппаратура	
Количество портов	24 порта 10/100BASE-TX, 2 комбо-порта 1000BASE-T/MiniGBIC (SFP)
Стандарты и функции	IEEE 802.3 10BASE-T/802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T/802.3z 1000BASE-SX/LX ANSI/IEEE 802.3 NWay автосогласование IEEE 802.3x управление потоком Автоматическое определение полярности MDI/MDIX Зеркалирование портов
Поддержка SFP	IEEE 802.3z 1000BASE-LX (DEM-310GT трансивер) IEEE 802.3z 1000BASE-SX (DEM-311GT трансивер) IEEE 802.3z 1000BASE-LH (DEM-314GT трансивер) IEEE 802.3z 1000BASE-ZX (DEM-315GT трансивер)
Топология	Поддержка топологий «кольцо» и «звезда»
Программное обеспечение	
VLAN	IEEE 802.1Q Tagged VLAN VLAN на базе портов GARP/GVRP Максимальное количество VLAN на устройство: 255 VLAN (суммарно статических и динамических)
Очереди приоритетов (CoS)	Стандарт: IEEE 802.1p Количество очередей: 4

2.2.4 Коммутаторы EX-серии

Современным предприятиям необходим новый подход, стратегическое и инновационное решение, которое позволит расходовать меньше средств на сетевую инфраструктуру и активнее финансировать развитие технологий, которые будут приносить предприятиям прибыль и увеличивать их продуктивность, благодаря чему бизнес приобретет конкурентное преимущество.

Компания Juniper Networks предлагает именно такое решение. Это новый класс Ethernet-коммутаторов масштаба предприятия, разработанных специально для того, чтобы отвечать требованиям современного высокопроизводительного бизнеса. Предлагаемые компанией Juniper коммутаторы серий EX меняют правила игры, предоставляя современным сетям новое поколение технологий коммутации. [13]



Рисунок 2.6 - Коммутаторы Ethernet серий EX 3200, EX 4200 и EX 8200

С EX-серией, бизнес организации приобретают Высокую Доступность, единые коммуникации, встроенную безопасность и операционную эффективность которые требуются им сегодня, и в тоже время приобретают защиту инвестиций, за счет поддержки требований которые будут завтра.

Высокая надежность

Ничто так не воодушевляет, как успех. Вот почему в производстве коммутаторов серий EX используется большинство технологий компании Juniper, которые уже зарекомендовали себя в отрасли. Включая высокопроизводительные специализированные процессоры (ASIC); проверенная модульная архитектура и операционная система JUNOS™, которая обеспечивает успешную работу сетей крупнейших в мире поставщиков услуг. В результате получилось надежное, высокопроизводительное решение для построения локальных сетей.

Виртуализация сети

В новых коммутаторах серий EX представлена технология Виртуального Шасси (Virtual Chassis™), разработанная компанией Juniper. Она позволяет объединять до десяти коммутаторов серии EX 4200 и управлять ими как единой системой. В действии эта технология

демонстрирует идентичные показатели надежности по сравнению с системами на базе независимых шасси, но в гораздо более рентабельном и компактном формате. Таким образом, новые устройства вбирают в себя лучшие качества традиционного оборудования, добавляя к ним современные технологии.

Преимущества программного обеспечения JUNOS

На коммутаторах серий EX установлено то же модульное программное обеспечение JUNOS™, что и на маршрутизаторах компании Juniper, что обеспечивает согласование реализации функций органов управления на всю инфраструктуру устройств Juniper. Используя единую операционную систему для управления всеми своими продуктами, компания Juniper помогает своим клиентам значительно сократить затраты на обучение персонала, поддержку системы и управление ею, уменьшая общую стоимость владения. [14]

Строгий и элегантный подход к разработке операционной системы JUNOS базируется на трёх базовых принципах единства: единый исходный код, единая цепь выхода версий и единая модульная архитектура. Единый репозиторий исходного кода гарантирует, что JUNOS останется единой, связанной операционной средой на всём протяжении разработки продукта, независимо от конкретного типа оборудования, работающего под ее управлением. Единая цепь версий обозначает, что набор функций каждой новой версии ОС JUNOS является надмножеством всех предыдущих. Другими словами, любая новая функция всегда реализуется в новой версии, а не при помощи разнообразных «заплаток», для того, чтобы гарантировать стабильность и доступность функций из предыдущей версии в новой. Наконец, модульная архитектура операционной системы JUNOS обеспечивает более чёткий контроль над процессом разработки, чем при использовании монолитного ядра. [15]

Спецификация

Коммутаторы серии EX 3200

Автономные коммутаторы на 24 и 48 портов, стандарта Gigabit Ethernet. 10 GbE модули с оптическими интерфейсами могут обеспечить достаточную емкость портов, поддерживают полную или частичную поддержку питания по сети (PoE), лучшее решение для 10/100/1000BaseT коммуникаций сегодняшних конвергентных сетей.

Коммутаторы серии EX 4200

EX 4200 серия коммутаторов с технологией Виртуального Шасси (Virtual Chassis™), которая позволяет увеличивать плотность портов по мере

необходимости. Эта инновационная технология позволяет объединять до 10 коммутаторов серии EX 4200 с использованием общей шины производительностью 128-гбит/с, в результате чего будет создано единое логическое устройство.

Коммутаторы серии EX 8200

Модульные терабитные коммутаторы Ethernet серии EX 8200 обеспечат высокопроизводительное высоко масштабируемое решение для 10 Гигабит Ethernet ядра корпоративной сети с высокой плотностью портов и агрегации. Совмещая в себе распределенную модель обработки пакетов на каждом линейном модуле и технологию аппаратных специализированных процессоров разработанных компанией Juniper, устройства серии EX 8200 приносят в мир Ethernet-коммутации высочайшую производительность и надежность операторского класса.[16]

2.3 Этапы настройки

В данном разделе приведены решения для реализации L3 VPN на базе сети MPLS использующей в качестве внутреннего протокола маршрутизации (IGP) EIGRP. В филиале Национальной Компании «Казахстан Темиржолы», ШЧ 19 - Карагандинской дистанции сигнализации и связи использовалось оборудование Cisco Systems 26xxXM, 36xx с программным обеспечением IOS 12.3.10.

Для проекта в качестве внутреннего протокола маршрутизации MPLS домена был выбран протокол EIGRP. Данный протокол маршрутизации является гибридным протоколом маршрутизации. Создание EIGRP есть попытка соединить в одном протоколе достоинства «дистанционно-векторных» (distance-vector) протоколов маршрутизации и протоколов «состояния канала» (link-state) без недостатков присущих этим протоколам. EIGRP комбинирует простоту и надежность «дистанционно-векторных» протоколов, а также быструю сходимость протоколов «состояния канала. EIGRP поддерживает маршрутизацию протоколов IP, IPX, AppleTalk. С версии IOS 12.3 поддерживает VPN/MPLS с использованием EIGRP (разумеется в train релизах 12.2 эта возможность появилась раньше). В качестве протокола распространения меток был выбран протокол TDP.

Этапы настройки

- настройка EIGRP и CEF;
- настройка TDP;

- настройка VRF;
- настройка MP - BGP;

Настройка маршрутизации между устройствами PE-CE с использованием протоколов:

- EIGRP;
- OSPF;
- RIP.

Этапы настройки приведены в приложении

2.4 Организация VPN на базе MPLS

Данный раздел описывает принципы организации и функционирования VPN на базе MPLS:

- общие понятия;
- функционирование PE;
- отличие понятий VPN и VRF;
- механизм коммутации пакетов;
- обмен маршрутной информацией между PE;
- организация VPN;
- преимущества организации VPN на базе MPLS;
- сравнение механизмов организации VPN на базе MPLS и туннелей (IPSec и GRE);
- документация.

Общие понятия

VPN - это принцип объединения узлов клиента, находящихся под единым административным подчинением, через публичную сеть оператора(ов).

Определим следующие понятия:

CE - маршрутизатор со стороны узла клиента, который непосредственно подключается к маршрутизатору оператора.

PE - граничный маршрутизатор со стороны оператора (MPLS домена), к которому подключаются устройства CE. PE устройства выполняют функции E-LSR-ов.

P - маршрутизатор внутри сети Оператора (MPLS домена). P устройства выполняют функции LSR.[17]

Пусть сеть оператора использует технологию MPLS/VPN. Маршрутизаторы сети Оператора образуют MPLS домен. Список узлов клиентов представлен в табл. N1, схема их подключения на рисунке 2.9

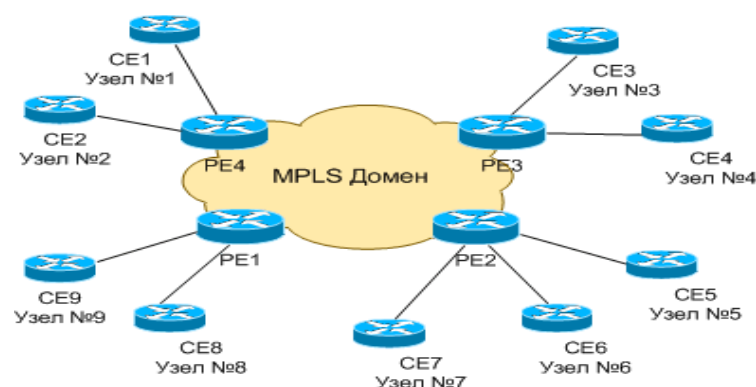


Рисунок 2.9 - Схема MPLS домена и подключенных узлов клиентов

Таблица 2.2 - Схема объединения узлов в VPN

Клиент	VPNs	Узлы
Станция N1	A	1, 6
Станция N2	B	3, 4, 5
Станция N3	C	2, 8
Станция N4	D	7, 9

Каждый клиент в рамках своей VPN может свободно обмениваться IP трафиком.

VPN могут объединяться в группы так:

Узлы 3, 4, 5, 7, 9 - образуют закрытую абонентскую группу (Closed User Group - CUG).

VPN 1, 2, 6, 7, 8, 9 - hub-and-spoke, где узлы 1 и 6 - центральные, 2, 7, 8 и 9 - периферийные VPN (spokes).

В этом случае, допускается пересечения адресных пространств у узлов 3, 4, 5 с 1, 6 и 3, 4, 5 с 2, 8.

Функционирование PE

Для обслуживания клиентов разных VPN на устройстве PE (к которому эти клиенты присоединены) создается несколько виртуальных объектов (по одной на каждый VPN). Называются такие объекты - VPN Routing and Forwarding (VRF). VRF образуются:

- отдельной таблицей IP-маршрутизации, использующейся для маршрутизации пакетов VPN (далее VRF-таблица);

- множеством интерфейсов устройства PE, по которым подключены устройства CE, принадлежащие одной VPN. То есть, интерфейс на устройстве PE, к которому подключен узел, входящий в VPN X, принадлежит VRF X.

Между устройствами CE и PE необходима настройка статической маршрутизации или протокола динамической маршрутизации. В качестве протокола динамической маршрутизации может быть использован RIP, OSPF или BGP. Маршрутная информация, полученная от устройства CE устанавливается в соответствующую VRF-таблицу. Рассмотрим пример на рис. N2. К устройству PE1 подключено три узла CE1, CE2, CE3. CE1 и CE2 принадлежат VPN-у A, а CE3 VPN-у B.

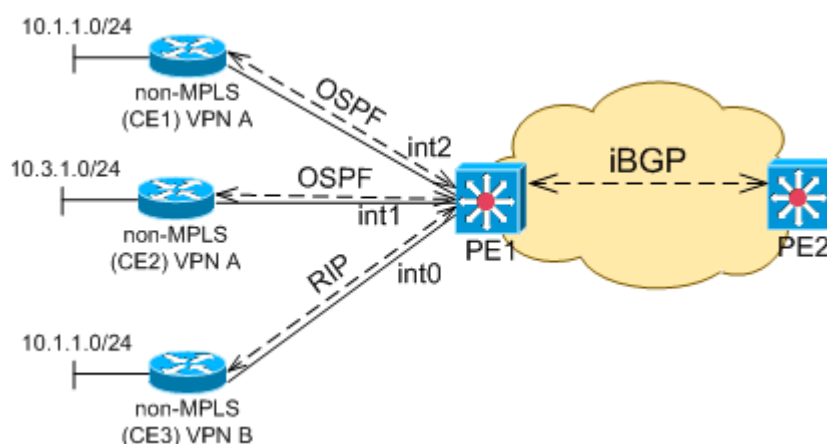


Рисунок 2.10 - Подключение узлов маршрутизаторов CE к PE.

Таблица 2.3 - Разбиение интерфейсов по VRF

Интерфейс	Сосед	VP N	VRF
int0	CE3	B	B
int1	CE2	A	A
int2	CE1	A	A

Таблица маршрутизации на устройстве PE1 представлена в таблице 2.4

Таблица 2.4 - Таблица маршрутизации на устройстве PE1

	Протокол	VRF	Подсеть	Next-Hop
	OSPF	A	10.1.1.0/24	CE1
	OSPF	A	10.3.1.0/24	CE2
	RIP	B	10.1.1.0/24	CE3

Описание полей таблицы:

Протокол - название протокола маршрутизации, по которому была получена маршрутная информация о префиксе. VRF - название VRF-таблицы, которой принадлежит префикс. Подсеть, Next-hop - уже знакомые нам поля.

Отличие понятий VPN и VRF

VPN - это принцип объединения узлов клиента, находящихся под единым административным подчинением, через публичную сеть оператора(ов). Описывается VPN множеством узлов, которые он объединяет и технологией использующейся для организации VPN.

Механизм коммутации пакетов

Определим следующие понятия:

- входной PE - первое устройство PE на пути следования IP пакета от одного устройства CE до другого через MPLS домен;
- выходной PE - последнее устройство PE на пути следования IP пакета от одного устройства CE до другого через MPLS домен.

Понятия входной/выходной PE определяются для конкретного направления трафика. Например, если пакет следует от CE1 до CE2 (см. рис. N3), то устройство PE1 будет входным PE, а PE2 выходным. Если же пакет следует в обратную сторону, то наоборот, устройство PE2 будет входным, а PE1 выходным.

Для коммутации пакетов VPN между устройствами PE используется две метки, образующие стек. Это означает, что IP пакету, полученному от CE, входной PE назначает стек из двух меток. Одна («внешняя») используется непосредственно для коммутации пакета устройствами LSR (или P). «Внешняя» метка определяет LSP от одного PE до другого. Вторая метка - «внутренняя» идентифицирует VRF на выходном PE, которому принадлежит пакет.[18]

Рассмотрим MPLS домен, к которому подключены два VPN A и B (рисунок 2.10). VPN A образован узлами CE1 и CE2, VPN B - узлами CE3 и

CE4. Как видно из рисунка IP адресация внутри VPN A и B пересекается. Таблица маршрутизации (включая VRF-таблицы) представлена в таблице 2.5.

Таблица 2.5 - Таблица маршрутизации на PE1.

N	Протокол	VRF	Подсеть	Next-Hop	Метка	Комментарий
1	OSPF	A	10.1.1.0/24	CE1	---	
2	iBGP	A	10.2.1.0/24	PE2	1000/345	О назначении меток будет сказано далее
3	RIP	B	10.1.1.0/24	CE3	---	
4	iBGP	B	10.2.1.0/24	PE2	1020/345	О назначении меток будет сказано далее
5	OSPF/LDP	---	PE2	P1	345	О назначении меток будет сказано далее

3 Программное обеспечение

В данном разделе приведены решения для реализации L3 VPN на базе сети MPLS использующей в качестве внутреннего протокола маршрутизации (IGP) EIGRP. В филиале Национальной Компании «Казахстан Темиржолы», ШЧ 19 - Карагандинской дистанции сигнализации и связи использовалось оборудование Cisco Systems 26xxXM, 36xx с программным обеспечением IOS 12.3.10.

Cisco Systems, Inc. - американская транснациональная компания, разрабатывающая и продающая сетевое оборудование. Стремится представить полный спектр сетевого оборудования, и таким образом предоставить возможность клиенту закупить абсолютно всё необходимое сетевое оборудование исключительно у Cisco Systems.[19]

Одна из крупнейших в мире компаний, специализирующихся в области высоких технологий. Изначально занималась только корпоративными маршрутизаторами. Cisco называет себя «мировым лидером в области сетевых технологий, предназначенных для сети Интернет».

В рамках технологии MPLS/VPN принято использование следующих терминов: CE (Customer Edge) - маршрутизатор со стороны узла клиента, который непосредственно подключается к маршрутизатору оператора. PE (Provider Edge) - граничный маршрутизатор со стороны оператора (MPLS домена), к которому подключаются устройства CE. PE устройства выполняют функции E-LSR-ов. На нашем полигоне эту роль выполняют маршрутизаторы Router_A, Router_B, Router_C, Router_I, Router_F. P (Provider) - маршрутизатор внутри сети Оператора (MPLS домена). P устройства выполняют функции LSR. На нашем полигоне роль маршрутизатора P возложена на маршрутизатор Router_G. [20]

3.1 Код программы

Для начало необходимо запустить на всех маршрутизаторах водящих в MPLS домен протокол маршрутизации и включить на этих маршрутизаторах коммутации Cisco Express Forwarding(CEF)

```
router eigrp 1
network 10.0.0.0
no auto-summary
ip cef
```

```
Current configuration : 1122 bytes
!
```

```

version 12.3
!
hostname Router_B
!
ip cef
no tag-switching ip
!
interface Loopback0
ip address 10.108.254.45 255.255.255.255
!
interface FastEthernet0/0
ip address 10.18.1.1 255.255.255.0
!
interface Serial0/0:0
description Router_C
ip address 10.108.253.190 255.255.255.252
!
interface Serial0/1:0
description Router_A
ip address 10.108.253.201 255.255.255.252
!
router eigrp 1
network 10.0.0.0
no auto-summary
!
end
Router_B#show debug
MPLS:
  MPLS events debugging is on
  LFIB data structure changes debugging is on
  LFIB enable/disable state debugging is on
  MPLS adjacency debugging is on
MPLS ldp:
  LDP Label Information Base (LIB) changes debugging is on
  LDP received messages, excluding periodic Keep Alive debugging is on
  LDP sent PDUs, excluding periodic Keep Alive debugging is on
  LDP transport events debugging is on
  LDP transport connection events debugging is on
  LDP session state machine (low level) debugging is on
Router_B(config)#interface Serial0/0:0
Router_B(config-if)#tag-switching ip

01:32:07: mpls: Add mpls app; Serial0/0:0
01:32:07: mpls: Add mpls app; Serial0/0:0
01:32:07: mpls: Add mpls app; i/f status change; Serial0/0:0
01:32:07: ldp: enabling ldp on Serial0/0:0
01:32:07: LFIB: enable entered, table does not exist, enabler type=0x1
01:32:07: LFIB: enable, TFIB allocated, size 6032 bytes, maxtag = 500
01:32:07: tib: find route tags: 10.18.1.0/24, Fa0/0, nh 0.0.0.0, res nh 0.0.0.0
01:32:07: tagcon: tibent(10.18.1.0/24): created; find route tags request
01:32:07: tagcon: tibent(10.18.1.0/24): label 1 (#2) assigned
01:32:07: tagcon: announce labels for: 10.18.1.0/24; nh 0.0.0.0, Fa0/0, inlabel imp-null,
outlabel unknown (from 0.0.0.0:0), find route tags

```

```

01:32:07: tib: find route tags: 10.108.253.188/30, Se0/0:0, nh 0.0.0.0, res nh 0.0.0.0
01:32:07: tagcon: tibent(10.108.253.188/30): created; find route tags request
01:32:07: tagcon: tibent(10.108.253.188/30): label 1 (#4) assigned
01:32:07: tagcon: announce labels for: 10.108.253.188/30; nh 0.0.0.0, Se0/0:0, inlabel imp-null
        outlabel unknown (from 0.0.0.0:0), find route tags
01:32:09: ldp: ptcl_adj:10.108.253.189(0x82EA0A60): Non-existent -> Opening Xport
01:32:09: ldp: create ptcl_adj: tp = 0x82EA0A60, ipaddr = 10.108.253.189
01:32:09: ldp: ptcl_adj:10.108.253.189(0x82EA0A60): Event: Xport opened;
        Opening Xport -> Init sent
01:32:09: ldp: tdp conn is up; adj 0x82EA0510, 10.108.254.45:11000 <-> 10.108.254.40:711
01:32:09: ldp: Sent open PIE to 10.108.254.40 (pp 0x0)
01:32:09: ldp: Rcvd open PIE from 10.108.254.40 (pp 0x0)
01:32:09: ldp: ptcl_adj:10.108.253.189(0x82EA0A60): Event: Rcv Init;
        Init sent -> Init rcvd activ
01:32:09: ldp: Rcvd keep_alive PIE from 10.108.254.40:0 (pp 0x0)
01:32:09: ldp: ptcl_adj:10.108.253.189(0x82EA0A60): Event: Rcv KA;
        Init rcvd activ -> Oper
01:32:09: tagcon: Assign peer id; 10.108.254.40:0: id 0
01:32:09: %LDP-5-NBRCHG: TDP Neighbor 10.108.254.40:0 is UP
01:32:09: ldp: Sent address PIE to 10.108.254.40:0 (pp 0x82EA0C10)
01:32:09: ldp: Sent bind PIE to 10.108.254.40:0 (pp 0x82EA0C10)
01:32:09: ldp: Rcvd address PIE from 10.108.254.40:0 (pp 0x82EA0C10)
01:32:09: tagcon: 10.108.254.40:0: 10.108.254.40 added to addr<->ldp ident map
01:32:09: tagcon: 10.108.254.40:0: 10.108.253.189 added to addr<->ldp ident map
01:32:09: ldp: Rcvd bind PIE from 10.108.254.40:0 (pp 0x82EA0C10)
01:32:09: tagcon: tibent(10.108.253.188/30): label imp-null from 10.108.254.40:0 added
01:32:09: tib: Not OK to announce label; nh 0.0.0.0 not bound to 10.108.254.40:0
01:32:09: tagcon: omit announce labels for: 10.108.253.188/30; nh 0.0.0.0, Se0/0:0,
        from 10.108.254.40:0: add rem binding: connected route
01:32:09: tagcon: tibent(10.108.254.40/32): label imp-null from 10.108.254.40:0 added
01:32:09: tagcon: announce labels for: 10.108.254.40/32; nh 10.108.253.189, Se0/0:0,
        inlabel 16, outlabel imp-null (from 10.108.254.40:0), add rem binding
01:32:09: LFIB: set loadinfo,tag=16,no old loadinfo,no new loadinfo
01:32:09: LFIB: delete tag rew, incoming tag 16
01:32:09: LFIB: create tag rewrite: inc 16,outg Imp_null
-----
01:32:09: tagcon: tibent(10.108.254.39/32): label 19 from 10.108.254.40:0 added
01:32:09: tib: Not OK to announce label; nh 10.108.253.202 not bound to 10.108.254.40:0
01:32:09: tagcon: omit announce labels for: 10.108.254.39/32; nh 10.108.253.202, Se0/1:0,
        from 10.108.254.40:0: add rem binding: next hop = 10.108.253.202
01:32:11: ldp: Send tdp hello; Serial0/0:0, src/dst 10.108.253.190/255.255.255.255, inst_id 0
01:32:13: ldp: Rcvd tdp hello; Serial0/0:0, from 10.108.253.189 (10.108.254.40:0), intf_id 0, opt 0x4
01:32:15: ldp: Send tdp hello; Serial0/0:0, src/dst 10.108.253.190/255.255.255.255, inst_id 0
01:32:17: ldp: Rcvd tdp hello; Serial0/0:0, from 10.108.253.189 (10.108.254.40:0), intf_id 0, opt 0x4g
Router_B#show mpls ip binding
  10.108.254.39/32
    in label: 17
    out label: imp-null lsr: 10.108.254.39:0 inuse
  10.108.254.40/32
    in label: 16
    out label: imp-null lsr: 10.108.254.40:0 inuse
  10.108.254.254/32 (no route)
    in label: 20

```



```

    out label: 17    lsr: 10.108.254.39:0
    out label: 17    lsr: 10.108.254.40:0
Router_B#
Router_B#show mpls ldp bindings
  tib entry: 10.108.254.39/32, rev 12
    local binding: tag: 17
    remote binding: tsr: 10.108.254.40:0, tag: 19
    remote binding: tsr: 10.108.254.39:0, tag: imp-null
  tib entry: 10.108.254.40/32, rev 8
    local binding: tag: 16
    remote binding: tsr: 10.108.254.40:0, tag: imp-null
    remote binding: tsr: 10.108.254.39:0, tag: 19
Router_B#
Router_B#show mpls ldp bindings
  tib entry: 10.108.254.39/32, rev 12
    local binding: tag: 17
    remote binding: tsr: 10.108.254.40:0, tag: 19
    remote binding: tsr: 10.108.254.39:0, tag: exp-null
  tib entry: 10.108.254.40/32, rev 8
    local binding: tag: 16
    remote binding: tsr: 10.108.254.40:0, tag: exp-null
    remote binding: tsr: 10.108.254.39:0, tag: 19
Router_B#
Router_C#show mpls forwarding-table
Local Outgoing Prefix      Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id  switched interface
16 Pop tag 10.108.253.200/30 0      Se0/1:0 point2point
17 Pop tag 10.108.254.45/32 0      Se0/1:0 point2point
18 Pop tag 10.18.1.0/24    0      Se0/1:0 point2point
19 17      10.108.254.39/32 0      Se0/1:0 point2point
Router_C#

Router_A#show mpls forwarding-table
Local Outgoing Prefix      Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id  switched interface
16 Pop tag 10.108.253.188/30 0      Se0/0:0 point2point
17 Pop tag 10.108.254.45/32 0      Se0/0:0 point2point
18 Pop tag 10.18.1.0/24    0      Se0/0:0 point2point
19 16      10.108.254.40/32 0      Se0/0:0 point2point
Router_A#
Router_B#show mpls ldp neighbor
  Peer TDP Ident: 10.108.254.40:0; Local TDP Ident 10.108.254.45:0
  TCP connection: 10.108.254.40.711 - 10.108.254.45.11004
  State: Oper; PIs sent/rcvd: 8/8; Downstream
  Up time: 00:03:25
  TDP discovery sources:
    Serial0/0:0, Src IP addr: 10.108.253.189
  Addresses bound to peer TDP Ident:
    10.108.254.40 10.108.253.189
Router_B#show mpls ldp parameters
Protocol version: 1
Downstream label generic region: min label: 16; max label: 100000

```

Session hold time: 180 sec; keep alive interval: 60 sec
Discovery hello: holdtime: 15 sec; interval: 5 sec
Discovery targeted hello: holdtime: 90 sec; interval: 10 sec
Downstream on Demand max hop count: 255
TDP for targeted sessions
LDP initial/maximum backoff: 15/120 sec
LDP loop detection: off
Router_B#

Router_A# show ip route vrf vpn_1

Routing Table: vpn_1

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 9 subnets, 4 masks

C 10.112.12.0/24 is directly connected, FastEthernet0/1

Router_A#

Router_C#show running-config

Настройка VRF и MP-BGP

ip vrf vpn_1

rd 1:1

route-target export 1:1

route-target import 1:1

!

ip cef

!

interface Loopback0

ip address 10.108.254.40 255.255.255.255

!

interface FastEthernet0/0

ip vrf forwarding vpn_1

ip address 10.17.1.1 255.255.255.0

!

interface Serial0/0:0

description Router_G

ip address 10.108.253.185 255.255.255.252

tag-switching ip

!

!

interface Serial0/1:0

description Router_B

ip address 10.108.253.189 255.255.255.252

tag-switching ip

```

!
router eigrp 1
 network 10.0.0.0
 no auto-summary
!
 address-family ipv4 vrf vpn_1
 redistribute bgp 1 metric 1000 1000 1 255 1500
 network 10.0.0.0
 no auto-summary
 autonomous-system 3
 exit-address-family
!
!
router bgp 1
 bgp router-id 10.108.254.40
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 10.108.254.39 remote-as 1
 neighbor 10.108.254.39 update-source Loopback0
!
 address-family vpnv4
 neighbor 10.108.254.39 activate
 neighbor 10.108.254.39 send-community extended
 exit-address-family
!
 address-family ipv4 vrf vpn_1
 redistribute eigrp 3
 no auto-summary
 no synchronization
 exit-address-family
!
!
ip vrf vpn_3
 rd 1003:1003
 route-target export 1003:1003
 route-target import 1003:1003
!
!
ip vrf vpn_1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
ip cef
!
interface Loopback0
 ip address 10.108.254.45 255.255.255.255
!
interface FastEthernet0/0
 ip vrf forwarding vpn_1
 ip address 10.18.1.1 255.255.255.0

```

```

!
interface Serial0/0:0
 ip address 10.108.253.190 255.255.255.252
 tag-switching ip
!
interface Serial0/1:0
 ip address 10.108.253.201 255.255.255.252
 tag-switching ip
!
interface Serial0/2
 description Router_D
 ip vrf forwarding vpn_3
 ip address 10.108.253.205 255.255.255.252
!
router eigrp 1
 network 10.0.0.0
 no auto-summary
!
 address-family ipv4 vrf vpn_1
 redistribute bgp 1 metric 1000 1000 1 255 1500
 network 10.0.0.0
 no auto-summary
 autonomous-system 3
 exit-address-family
!
 address-family ipv4 vrf vpn_3
 redistribute bgp 1 metric 1000 1000 1 255 1500
 network 10.0.0.0
 no auto-summary
 autonomous-system 2
 exit-address-family
!
router bgp 1
 bgp router-id 10.108.254.45
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 10.108.254.40 remote-as 1
 neighbor 10.108.254.40 update-source Loopback0
!
 address-family vpnv4
 neighbor 10.108.254.40 activate
 neighbor 10.108.254.40 send-community extended
 exit-address-family
!
 address-family ipv4 vrf vpn_1
 redistribute eigrp 3
 no auto-summary
 no synchronization
 exit-address-family

```

```

!
address-family ipv4 vrf vpn_3
redistribute eigrp 2
no auto-summary
no synchronization
exit-address-family
!
end
Router_C#show running-config
!
ip vrf vpn_3
rd 1003:1003
route-target export 1003:1003
route-target import 1003:1003
!
ip vrf vpn_1
rd 1:1
route-target export 1:1
route-target import 1:1
!
ip cef
!
interface Loopback0
ip address 10.108.254.40 255.255.255.255
!
interface FastEthernet0/0
ip vrf forwarding vpn_1
ip address 10.17.1.1 255.255.255.0
!
interface Serial0/0:0
description Router_G
ip address 10.108.253.185 255.255.255.252
tag-switching ip
!
!
interface Serial0/1:0
description Router_B
ip address 10.108.253.189 255.255.255.252
tag-switching ip
!
interface Serial0/2
description Router_K
ip vrf forwarding vpn_3
ip address 10.108.253.193 255.255.255.252
!
router eigrp 1
network 10.0.0.0
no auto-summary
!

```

```

address-family ipv4 vrf vpn_1
redistribute bgp 1 metric 1000 1000 1 255 1500
network 10.0.0.0
no auto-summary
autonomous-system 3
exit-address-family
!
address-family ipv4 vrf vpn_3
redistribute bgp 1 metric 1000 1000 1 255 1500
network 10.0.0.0
no auto-summary
autonomous-system 2
exit-address-family
!
router bgp 1
bgp router-id 10.108.254.40
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 10.108.254.39 remote-as 1
neighbor 10.108.254.39 update-source Loopback0
!
address-family vpnv4
neighbor 10.108.254.39 activate
neighbor 10.108.254.39 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn_1
redistribute eigrp 3
no auto-summary
no synchronization
exit-address-family
!
!
address-family ipv4 vrf vpn_3
redistribute eigrp 2
no auto-summary
no synchronization
exit-address-family
!
end
Router_I#show running-config
hostname Router_I
!
ip vrf vpn_2
rd 100:100
route-target export 100:100
route-target import 100:100
route-target import 1:1
end.

```

4 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

4.1 Анализ условий труда обслуживающего персонала при эксплуатации технического оборудования

Анализ условий труда в дипломном проекте «Разработка MPLS сети для филиала Национальной Компании «Казахстан Темиржолы» - ШЧ 19» позволит определить оптимальные и комфортные условия труда и основные потенциально опасные источники угроз жизнедеятельности.

4.1.1 Вид и характеристики используемого оборудования

Персональный компьютер (6 шт).

Технические характеристики устройства:

- персональный компьютер Intel Core2Duo E6420 2,13 GHz/Intel BroadwaterDQ965GF(SIS651+SB)/1Gb DDRII/160 Gb Seagate 7200 SATAII /Intel GMA 3000 128 Mb/Intel 82566DM Gigabit Network Connection/D-Link Air Plus Xtreme G DWL-6520/FDD/k/m/p/SP/Lite-On DVD-RW LH-18A1P;
- монитор 17” Samsung SyncMaster 740N×0,26 dpi;
- габариты: 1200×750×1150 (Д×Г×Ш, мм) (персональный компьютер + стол);
- электропитание: переменное напряжение 220-250 В, частотой 50 Гц. Мощность 450 Вт;

- Точка доступа Cisco Aironet 1200 Series: AIR-AP1231G-E-K9 (2 шт).

Технические характеристики устройства:

- 802.11g IOS AP w/Avail CBus Slot, ETSI Config;
- электропитание: переменное напряжение 220-250 В, частотой 50 Гц;
- габариты 171×40×181 (Д×Г×Ш, мм).

Точка доступа Cisco Aironet 1300: AIR-AP1310G-E-K9-P (2 шт).

Технические характеристики устройства:

- Aironet 1310 Outdoor AP/BR w/RP-TNC Connectors, ETSI Config;
- электропитание: переменное напряжение 220-250 В, частотой 50 Гц;
- габариты 203×78,7×205,7 (Д×Г×Ш, мм).

Точка доступа LinkSys WRT-350N (2 шт).

Технические характеристики устройства:

- Wireless-N Gigabit Router with USB Storage Link;
- электропитание: переменное напряжение 220-250 В, частотой 50 Гц;

- габариты 188×40×176 (Д×Г×Ш, мм).

Антенна AIR-ANT4941 (8 шт).

Технические характеристики устройства:

- тип – всенаправленная;
- диаграмма направленности – 3600×600;
- коэффициент усиления 2.2 дБи.

Осветительное оборудование: лампы ЛБ40-4 (12 штук)

- электропитание: переменное напряжение 220-250 В, частотой 50 Гц, мощность каждого светильника 160 Вт.

Все электротехническое оборудование является потенциальным источником возникновения пожарной опасности. Оборудование малошумящее – вредность в качестве повышенного шума отсутствует. Рабочее помещение, расположенное в здании филиала ШЧ 19- Карагандинская дистанция сигнализации и связи, не находится в непосредственной близости от железнодорожной магистрали или нагруженной автомагистрали, аэропорта и так далее, поэтому внешних источников шума, влияющих на процесс работы – нет. Повышенный уровень электромагнитных излучений отсутствует (применены мониторы типа LCD, а также беспроводное оборудование, соответствующее международным санитарным нормативам по мощности излучения для внутриофисных сетей).

При эксплуатации электрооборудования существует опасность поражения электрическим током. Поражение электрическим током может произойти при коротком замыкании, при не правильном обращении с компьютером, при случайном попадании воды на токоведущие части. В целях предотвращения поражения электрическим током в системе питания электрооборудования предусмотрено защитное зануление (все вилки и розетки имеют контакты зануления).

4.1.2 Рабочее место, виды работ

Выполняемая работа относится к категории легких работ (категория Ia), выполняемых в сидячем положении (ГОСТ 12.2.032-78);

Высота рабочей поверхности: 725 мм, высота сиденья: 420 мм (ГОСТ 12.2.032-78), данные ГОСТа указаны в таблице 4.1;

Таблица 4.1 – Виды работ (ГОСТ 12.2.032-78)

Наименование работ	Класс работ	Пол работника	Высота рабочей поверхности при организации рабочего места	Высота сиденья
Легкие работы (конторская работа)	Класс Ia (работа, выполняемая в сидячем положении)	Мужской, женский	725 мм	420 мм

размер различаемых в процессе работы объектов: 1 мм, расстояние от объекта до глаз работника: 500 мм – разряд зрительной работы: IV (СНиП РК 2.04.-0.5-2002), данные СНиП а указаны в таблице 4.2.

Таблица 4.2 – Разряд зрительной работы (СНиП РК 2.04.-0.5-2002)

Размер минимального различаемого объекта, мм	Расстояние от объекта до глаз работника, мм	Разряд зрительной работы
0,5-1	500	IV

4.1.3 Здание и помещение

Характеристики здания и помещения:

- здание: филиала Национальной компании «Казахстан Темиржолы» ШЧ 19, расположено в городе Караганда (черта города). Здание четырехэтажное;

- рабочее помещение находится на третьем этаже здания, в кабинете тдля технической поддержки;

- размеры рабочего помещения: длина l=5,5 м, ширина s=5,7 м высота h=3,2 м

- остекление помещения – двойное (два окна размером 2000x1800 мм) без стального переплетения;

- внутренняя отделка стен – светлая;

- искусственное освещение – светильники: люминесцентные лампы ЛБ40-4 (12 штук);

План помещения представлен на рисунке 4.1.

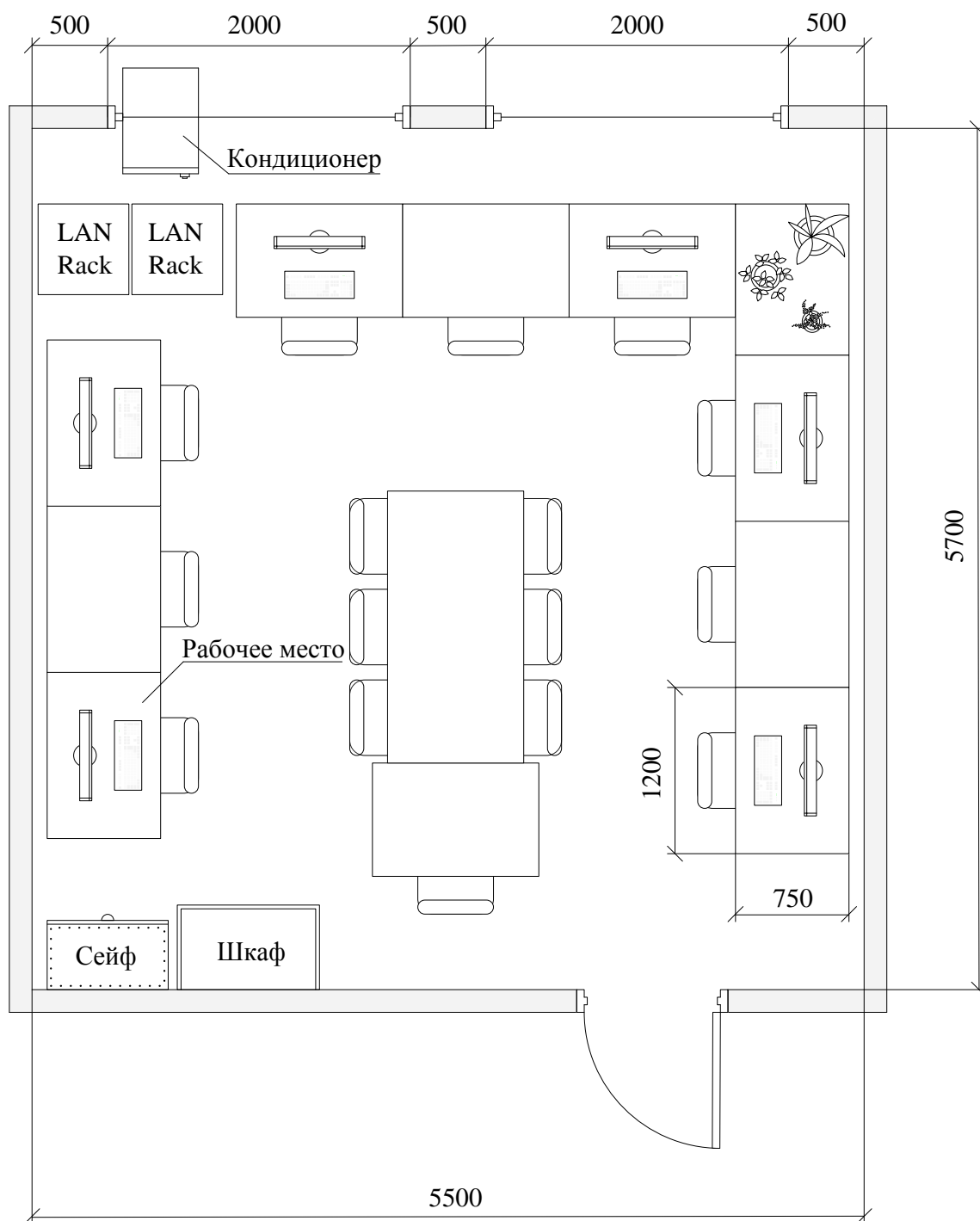


Рисунок 4.1 – План рабочего помещения

Режим работы (продолжительность рабочего дня) 800 – 1700.

Здание относится к I степени огнестойкости (СНиП РК 2.02-05-2002), данные СНиПа указаны в таблице 4.3.

Таблица 4.3 – Конструктивная характеристика зданий в зависимости от их степени огнестойкости (СНиП РК 2.02-05-2002)

Степень огнестойкости	Конструктивные характеристики
I	Здания с несущими и ограждающими конструкциями из естественных или искусственных материалов, бетона или железобетона с применением листовых и плитных негорючих материалов

Общая площадь помещения 31,4 м². Площадь, занимаемая оборудованием и мебелью 12,4 м².

4.1.4 Микроклимат рабочего помещения

Для вентиляции рабочего помещения используются каналы естественной вентиляции, прокладываемые при строительстве здания, открытые окна (в теплый период), а также система кондиционирования. Такая вентиляция позволяет поддерживать климатические параметры рабочего помещения в пределах нормы (таблица 4.4) в условиях климата города Караганда (в том числе – и в теплый период года).

Таблица 4.4 - Оптимальные нормы температуры, относительной влажности и скорости движения воздуха в обслуживаемой зоне жилых, общественных и административно-бытовых помещений (СНиП 2.04.05-91)

Период года	Температура воздуха, 0С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с.
Теплый	20-22	60-30	0,2, не более
	23-25	60-30	0,3, не более
Холодный и переходные условия	20-22	45-30	0,2, не более

4.1.5 Освещенность рабочего места

Рабочее помещение имеет естественное освещение в виде двух окон размером 2000х1800 мм. Также используется система общего освещения (искусственное освещение): люминесцентные лампы ЛБ40-4 (12 штук).

Существующая площадь окон соответствует нормативам естественного освещения (расчет приведен в следующей главе).

4.1.6 Пожарная безопасность

Рабочее помещение по вопросам пожарной безопасности относится к классу «Д».

Рабочее помещение (кабинет технического отдела) оборудовано химическим огнетушителем ОП в количестве 1 шт.

Все работники каждый год сдают экзамен по технике безопасности, также принимаются дополнительные меры безопасности: плакаты с напоминанием о необходимости осторожного обращения с огнем, выделенные места для курения и т.д.

Для тушения пожаров и возгораний необходимо установить автоматическую систему пожаротушения на основе спринклерной установки. Расчет данной системы приведен в следующей главе.

При возникновении пожара в производственных помещениях, помимо принятия мер по его ликвидации, необходимо также осуществить эвакуацию из опасной зоны работающего персонала. Эвакуация людей осуществляется по эвакуационным путям, обеспечивающим эвакуацию людей, находящихся в помещениях зданий и сооружений, через эвакуационные выходы в течение необходимого времени эвакуации.

4.2 Технические решения вопросов охраны труда и окружающей среды

4.2.1 Расчет зануления

В электроустановках напряжением до 1 кВт с заземленной нейтралью для надежной защиты людей от поражения электрическим током применяется зануление, обеспечивающее автоматическое отключение участка сети, на котором произошел пробой на корпус. Зануление называется преднамеренное электрическое соединение с нулевым защитным проводником металлических не токоведущих частей, которые могут оказаться под напряжением. Защитный эффект от зануления заключается в уменьшении длительности замыкания на

корпус, а следовательно, в сокращении времени воздействия электрического тока на человека.

В сетях однофазного тока электрооборудование включается между фазным и нулевым рабочим проводниками. В этом случае зануление осуществляется отдельным проводником, который одновременно не может служить проводником для рабочего тока, так как при обрыве рабочего нулевого проводника (перегорании предохранителя) все присоединенные к нему корпуса окажутся под фазным напряжением.

Расчет зануления сводится к определению условий, при которых обеспечиваются быстрое срабатывание максимально-токовой защиты и отключение поврежденной установки от сети.

Для расчета зануления и выбора автоматического выключателя необходимо знать потребляемую мощность и ток каждым электротехническим оборудованием:

- потребляемая мощность компьютера 450Вт. Переменное напряжение питания 220-250 В. Следовательно, потребляемый ток компьютером составит $I_K = 450/220 = 2 \text{ A}$;

- потребляемая мощность точек доступа 41,3Вт. Переменное напряжение питания 220-250 В. Следовательно, потребляемый ток точками доступа составит $I_T = 41,3/220 = 0,2 \text{ A}$.

В помещении работают 6 компьютер и 6 точек доступа. Следовательно, общая потребляемая мощность составит:

$$P_{\text{ит}} = 6 \cdot 450 + 6 \cdot 41,3 = 2947,8 \text{ Вт} \approx 3 \text{ кВт} = 4,3 \text{ кВт} \cdot \text{А}.$$

Напряжение питания $U = 220 \text{ В}$.

Расстояние от щитка до самого удаленного потребителя равно $L = 16,9 \text{ м}$.

Для электропитания оборудования применен кабель марки ВВГ 3×2,5 (с медными жилами). В кабеле электропитания предусмотрен провод зануления.

Основные технические параметры фазного и нулевого проводов:

- диаметр $d = 1,8 \text{ мм}$;
- сечение $S = 2,5 \text{ мм}^2$.

Расстояние между двумя проводниками (фазный и нулевой провод) соизмеримо с их размерами.

Для надежного отключения аварийного участка необходимо, чтобы ток в короткозамкнутой цепи ($I_{кзн}$) значительно превосходил ток уставки (I_H) автомата защиты, т.е. должно выполняться неравенство:

$$I_{кзн} \geq kI_H \quad (4.1)$$

где k – коэффициент, при защите автоматическими выключателями с номинальными токами до 100 А, $k=1,4$.

Номинальный ток определяется из формулы:

$$I_H = \frac{P_{\Pi}}{U} = \frac{4,3 \cdot 10^3}{220} = 19,5 \text{ А} \quad (4.2)$$

Тогда ожидаемый ток короткого замыкания из выражения (6.1) равен:

$$I_{кзн} \geq 1,4 \cdot 19,5 = 27,3 \text{ А}$$

Сопротивление фазного R_{Φ} и нулевого R_H проводов определяется по следующей формуле:

$$R = \rho \frac{L}{S}, \quad (4.3)$$

где ρ – удельное сопротивление, равное 0,018 Ом·м для меди;

L – длина провода, м;

S – сечение провода, мм².

Тогда сопротивление фазного провода равно:

$$R_{\Phi} = \rho \frac{L}{S_{\Phi}} = 0,018 \frac{16,9}{2,5} = 0,17 \text{ Ом.}$$

Нулевой провод имеет аналогичное исполнение, поэтому его сопротивление совпадает с сопротивлением фазного:

$$R_H = R_{\Phi} = 0,17 \text{ Ом.}$$

Внутренние индуктивные сопротивления фазного X_{Φ} и нулевого X_H проводов из меди малы и ими можно пренебречь.

Полное сопротивление цепи «фаза-нуль» определяется следующим образом [7]:

$$Z_{кз} = Z_{\Phi} + Z_H + jX_{\Pi} = (R_{\Phi} + R_H) + j(X_{\Phi} + X_H + X_B), \quad (4.4)$$

где X_{Π} – полное индуктивное сопротивление цепи «фаза-нуль»;

X_B – внешнее индуктивное сопротивление цепи «фаза-нуль».

Когда фазный и нулевой проводники расположены в непосредственной близости один от другого, сопротивление X_B мало и им можно пренебречь.

Тогда полное сопротивление Z_{K3} равно:

$$Z_{K3} = R_{\Phi} + R_H = 0,17 + 0,17 = 0,34 \text{ Ом.}$$

Ток однофазного короткого замыкания фазы на зануленный корпус определяется как [7]:

$$I_{K3} = \frac{U_{\Phi}}{\frac{Z_T}{3} + Z_{K3}} \quad (4.5)$$

где Z_T – полное сопротивление обмоток трехфазных трансформаторов при обмотках низшего напряжения 400/230В. Схема соединения обмоток трансформатора $\Delta/Y0$, мощность трансформатора равна 25кВ·А), $Z_T = 0,906$ Ом.

Тогда ток короткого замыкания составит:

$$I_{K3} = \frac{220}{\frac{0,906}{3} + 0,34} = 343,8 \text{ А.}$$

Выражение (6.1) выполняется для тока короткого замыкания, который значительно превышает номинальный ток ($343,8 \geq 27,3$). Таким образом, автоматический выключатель гарантированно сработает и отключит аварийный участок.

Автоматический выключатель выбирается на номинальный ток, полученный из выражения (4.2): $I_H = 19,5 \text{ А.}$

Выбирается двухполюсный автоматический выключатель S192 компании АВВ.

Технические характеристики:

- номинальный ток $I_H = 25 \text{ А;}$

- отключающая способность 6 кА;

- номинальное напряжение 230/240В;
- характеристика срабатывания С ($I_m=5...10I_n$), В ($I_m=3...5I_n$).
- напряжения прикосновения $U_{пр} = 50 \text{ В}$

4.2.2 Расчет естественного освещения

Необходимо рассчитать площадь боковых световых проемов помещения кабинета технического отдела для создания нормируемой освещенности на рабочем месте.

Помещение имеет размеры: длина $l = 5,5\text{м}$, ширина $s = 5,7\text{м}$, высота $h = 3\text{м}$. Высота рабочей поверхности над уровнем пола – 0,8 м, окно начинается с высоты 0,9 м, высота окна 1,8 м. Рабочее помещение находится в IV часовом поясе - город Караганда. Со всех сторон здания филиала ШЧ 19 затеняющих зданий нет.

Рабочие места расположены по периметру помещения (вдоль стен), а также в центре. Минимальная освещенность будет в точке, отстоящей на расстояние 5,5 м от оконного проема.

Общую площадь окон S_0 , м^2 определим по формуле:

$$100 \cdot \frac{S_0}{S_n} = \frac{e_n \cdot \eta_0}{\tau_0 \cdot r_1} \cdot k_{зд} \cdot k_3, \quad (4.6)$$

$$S_0 = \frac{S_n \cdot e_n \cdot \eta_0 \cdot k_{зд} \cdot k_3}{100 \cdot \tau_0 \cdot r_1}, \quad (4.7)$$

где S_n – площадь помещения, м^2 , равная произведению длины на ширину помещения: $S_n = l \cdot s = 5,5 \cdot 5,7 = 31,4 \text{ м}^2$;

e_n – нормированное значение КЕО, вычисляемое по формуле

$$e_n^{IV} = e_n \cdot m \cdot c, \quad (4.8)$$

где $m=0,9$, $c=0,75$ – для IV часового пояса;

$e_n=1,2$ для работ средней точности IV подряда,

$$e_n^{IV} = 1,2 \cdot 0,9 \cdot 0,75 = 0,81;$$

k_3 – коэффициент запаса, равный $k_3=1,2$;

τ_0 – общий коэффициент светопропускания равный:

$$\tau_0 = \tau_1 \cdot \tau_2 \cdot \tau_3 \cdot \tau_4, \quad (4.9)$$

где $\tau_1 = 0,8$, $\tau_2 = 0,6$, $\tau_3 = 0,8$, $\tau_4 = 1$,

$$\tau_0 = 0,8 \cdot 0,6 \cdot 0,8 \cdot 1 = 0,38.$$

n_0 – световая характеристика окон. Отношение длины комнаты к глубине наиболее удаленной точки от окна равно. $\frac{5,5}{5,7} = 0,97$ Отношение

ширины помещения к высоте от уровня рабочей поверхности до верха окна равно $\frac{5,7}{1,9} = 3$. Отсюда $n_0=18$ [5, таблица 1.3];

r_1 – коэффициент, учитывающий повышение КЕО при боковом освещении благодаря свету, отраженному от поверхностей помещения и подстилающего слоя, прилегающего к зданию. Отношение длины комнаты к глубине наиболее удаленной точки от окна равно 0,97, средний коэффициент отражения в помещении $\rho_{ср} = 0,5$, принимается одностороннее боковое освещение. Тогда $r_1 = 5,4$ [5, таблица 1.6];

$k_{зд}$ – коэффициент, учитывающий затенение окон противостоящими зданиями. Поскольку затеняющих зданий поблизости нет, то $k_{зд} = 1$ [5, таблица 1.9].

Тогда общая площадь окон из выражения (4.7) равна:

$$S_0 = \frac{31,4 \cdot 0,81 \cdot 18 \cdot 1 \cdot 1,2}{100 \cdot 0,38 \cdot 5,4} = 2,68 м^2;$$

Площадь имеющихся окон составляет $2 \cdot 2 \cdot 1,8 = 7,2 м^2$. Таким

образом, наглядно видно, что предусмотренные оконные проемы соответствуют нормативам естественного освещения.

4.2.3 Расчет системы автоматического пожаротушения

Рассматриваемое помещение является кабинетом технического отдела, где располагается электрооборудование: компьютеры, точки доступа и др. Для обеспечения пожарной безопасности в помещении необходимо установить автоматические установки пожаротушения. Данное помещение по степени опасности развития пожара относится к 1 группе.

Автоматические установки пожаротушения, предназначены для тушения пожаров распыленной водой, делятся на спринклерные и дренчерные.

Спринклерные установки служат для тушения пожаров и возгораний, охлаждения строительных конструкций и подачи сигнала о пожаре. Дренчерные установки предназначены для тушения пожаров по всей площади, создание водяных завес и сигнализации о пожаре.

Для помещений, относящихся к 1 группе, предусмотрены автоматические водяные спринклерные установки. Основные параметры и характеристики водяных спринклерных установок для 1 группы помещения представлены в таблице 4.5.

Таблица 4.5 – Основные параметры водяных спринклерных установок

Группа помещения	Интенсивность орошения, л/(с·м ²), не менее	Максимальная площадь, контролируемая одним оросителем, м ²	Площадь для расчета расхода воды, м ²	Продолжительность работы установки, мин	Максимальное расстояние между оросителями, м
1	0,08	12	120	30	4

На рисунке 4.2 представлена расчетная схема спринклерной установки водяного пожаротушения.

Каждый ороситель (рисунок 4.2) контролирует площадь в 7,84м².

Расход воды из первого оросителя (л/с) вычисляется по формуле [13]:

$$Q_1 = I \cdot f, \quad (4.10)$$

где I – интенсивность орошения, л/(с·м²);

f – площадь, защищаемая оросителем, м².

Тогда расход воды из первого оросителя равен:

$$Q_1 = 0,08 \cdot 7,84 = 0,627 \text{ л/с.}$$

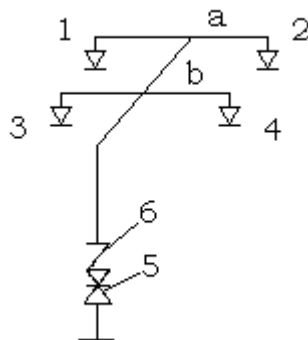


Рисунок 4.2 – Расчетная схема установки водяного пожаротушения
1, 2, 3, 4 – оросители; а, b – узловые точки;
5 – компрессор; 6 – клапан группового действия

Напор у первого оросителя (м) определяется [13]:

$$H_1 = Q_1^2 / K^2 \geq H_{\min}, \quad (4.11)$$

где K – коэффициент производительности оросителя, равный 0,2 для оросителя с диаметром выходного отверстия 8мм;

H_{\min} – минимальный свободный напор, равный 5м.

$$H_1 = 0,627^2 / 0,2^2 = 9,83 \text{ м} \geq 5 \text{ м.}$$

Потери напора на участке 1-а находятся по формуле:

$$h_{1-a} = l_{1-a} \cdot Q_1^2 / k_1, \quad (4.12)$$

где l_{1-a} – длина участка 1-а, равная 1,4 м;

k_1 – удельная характеристика трубопровода, $k_1 = 0,75$.

Напор в точке а равен:

$$H_a = H_1 + h_{1-a}, \quad (4.13)$$

$$H_a = 10,6 \text{ м.}$$

Правая ветвь с оросителем 2 симметрична левой (ороситель 1), поэтому расход для этой ветви будет равен $Q_1 = 0,627$ л/с, следовательно напор в точке а будет равен $H_a = 10,6$ м.

В итоге для первого ряда (оросители 1 и 2) напор равен $H_a = 10,6$ м и расход воды $Q_{P1} = 2Q_1 = 2 \cdot 0,627 = 1,25$ л/с.

Потери напора на участке а-б находятся по формуле:

$$h_{a-b} = l_{a-b} \frac{Q_{P1}^2}{k_1}, \quad (4.14)$$

где l_{a-b} – длина участка а-б, равная 2,85 м.

$$h_{a-b} = 2,85 \cdot \frac{1,25^2}{0,75} = 5,98 \text{ м.}$$

Напор в точке b равен:

$$\begin{aligned} H_b &= H_a + h_{a-b}, \\ H_b &= 10,56 + 5,98 = 16,54 \text{ м.} \end{aligned} \quad (4.15)$$

Второй ряд (оросители 3, 4) рассчитывается по его характеристике. Так как характеристики рядов, выполненных конструктивно одинаково, равны, характеристика второго ряда определяется по параметрам первого ряда.

Характеристика для первого ряда (B_{P1}) рассчитывается как:

$$\begin{aligned} B_{P1} &= Q_{P1}^2 / H_a, \\ B_{P1} &= 1,25^2 / 10,56 = 0,15 \text{ л}^2 / (\text{с}^2 \cdot \text{м}) \end{aligned} \quad (4.16)$$

Тогда расход воды для второго ряда (Q_{P2}) определяется по формуле:

$$\begin{aligned} Q_{P2} &= \sqrt{B_{P1} \cdot H_b}, \\ Q_{P2} &= \sqrt{0,15 \cdot 16,54} = 1,58 \text{ л/с.} \end{aligned} \quad (4.17)$$

Напор у водопитателя находится по формуле и не должен превышать 100 м [13]:

$$H = H_1 + 1,2h + h_{\text{КСК}} + z, \quad (4.18)$$

где h – суммарные потери напора, равные:

$$h = h_{1-a} + h_{a-b} = 0,73 + 5,98 = 6,71 \text{ м;}$$

$h_{\text{КСК}}$ – потери напора в узле управления, равная $3,02 \cdot 10^{-3}$ м;

z – высота подъема воды, 3 м.

$$H = 9,83 + 1,2 \cdot 6,71 + 3,02 \cdot 10^{-3} + 3 = 20,01_{\text{м}};$$

Выбираются 4 спринклерных оросителя водяного пожаротушения модели MX5(3)-SU DN10 компании Minimax.

Технические характеристики:

колба: 3 – 5 мм.;

отделка: латунь, хром;

номинальное давление: 12,5 бар;

температурный диапазон: 57°C 68°C, 79°C, 93°C, 141°C;

диаметр резьбы: 3/8», 1/2», 3/4»;

коэффициент K: 57, 80, 115.

5 ЭКОНОМИЧЕСКАЯ ЧАСТЬ

5.1 Резюме

Главной целью данного проекта является разработка MPLS сети для филиала Национальной Компании «Казахстан Темиржолы» - ШЧ 19

Основой экономической эффективности мультисервисных сетей является универсальная среда для передачи любого вида трафика (данные, голос, видео) и на сегодняшний день, данная технология является самой распространенной технологией. К мультисервисным сетям применяются повышенные требования с точки зрения надежности, гарантированности предоставления сервиса и минимальной стоимости передачи в расчете на единицу объема информации.

5.2 Компания и отрасль

Организация: Национальная Компания «Казахстан Темиржолы».

ШЧ-19 - Карагандинская дистанция сигнализации и связи, на участке которой более 20 станции.

Филиал обеспечивает безопасность движения поездов. Автоматизирует управление дежурным маневрами при сортировке поездов на станциях, и блокирует возможные не правильные действия дежурного по станции. На участках между станциями (перегонах) осуществляет интервальное движение поездов с контролем их местоположения.

Так же с помощью микропроцессорной диспетчерской централизацией вся информация сводится к поездным диспетчерам, которые управляют движением поездов из единого центра в Караганде, давая команды дежурным находящимся на станциях. В конце вся эта информация передается в город Астана.

Основная деятельность Национальной компании «Казахстан Темиржолы» это пассажирские перевозки, грузовые перевозки и транзитные перевозки. Сотрудники компании обязаны обеспечить безопасность пассажиров и своевременную доставку грузов. Но вся эта работа невозможна без качественной, производительной, быстродействующей и безопасной работы внутренней компьютерно-коммуникационной сети компании.

Один из методов повышения качества работы компьютерной – коммуникационной сети компании рассматривается в данном проекте – разработка сети с использованием технологии MPLS.

5.3 Описание продукции (услуги)

MPLS должны обеспечивать работу разнородных информационных и телекоммуникационных систем и приложений в единой транспортной среде. Кроме этого, мультисервисная сеть предоставляет сервис-провайдерам много возможностей по построению многообразных наложенных сервисов поверх универсальной транспортной среды – от передачи голоса по IP до интерактивного телевидения и веб-служб. Также немаловажно, что использование единой транспортной среды позволяет снизить издержки на построение и эксплуатацию сети за счет унификации оборудования, стандартов, технологий и единой централизованной системы управления. С другой стороны современные мультисервисные сети обладают широкими возможностями по поддержке заданного SLA (Service Level Agreement) - качество и уровень обслуживания гарантируются не только на уровне договорных соглашений с сервис-провайдером, но и на уровне технологий.

Основные особенности современных мультисервисных сетей

- универсальный характер обслуживания разных приложений;
- независимость от технологий услуг связи и гибкость получения набора, объема и качества услуг;
- полная прозрачность взаимоотношений между поставщиком услуг и пользователями;
- возможность передачи большому количеству пользователей в реальном времени очень больших объемов информации с необходимой синхронизацией и с использованием сложных конфигураций соединений;
- интеллектуальность (управление услугой, вызовом и соединением со стороны пользователя или поставщика сервиса, отдельная тарификация и управление условным доступом);
- инвариантность доступа (организация доступа к услугам независимо от используемой технологии);
- комплексность услуги (возможность участия нескольких провайдеров в предоставлении услуги и разделение их ответственности и дохода сообразно с видом деятельности каждого).

5.4 Анализ рынка сбыта. Изучение рынка услуг

Внедрение проекта позволит повысить качество, производительность, быстродействие и безопасность компьютерно-коммуникационной сети компании. Все это осуществимо с внедрением новой технологии MPLS-VPN. Внедрение сети с технологией MPLS позволит реализовать следующий ряд услуг:

- Организация каналов точка-точка (P2P) VPWS - Virtual Private Wire Service или AoMPLS Any transport over MPLS;
- Организация прозрачных соединений (на втором уровне OSI: 802.1q, Frame Relay, ATM...) типа точка-точка через;
- Организация многоточечных каналов (P2M) VPLS - Virtual Private LAN Service;
- Эмуляция распределенных ЛВС;
- Виртуальные выделенные каналы с возможностью восстановления за 50 мс.

Внедрение проекта даст следующие преимущества:

- Быстрая передача данных (по сравнению с маршрутизацией использующей ip адреса);
- Приоритезация данных и гарантированное качество обслуживания (QoS, Traffic Engineering);
- Перераспределение потоков (возможность явно задать один или несколько маршрутов передачи данных, позволяет оптимизировано использовать полосы пропускания);
- Создание частных виртуальных сетей L3 VPN;
- Динамическая перестройка маршрутов в обход отказавшего узла;
- Простое наращивание узлов в сетях VPN и подключение к ядру MPLS абонентов, применяющих разные технологии доступа;
- Объединение разнородных сетей (IP, ATM и Frame Relay) с сокращением операционных расходов.

5.5 Финансовый план

Этот раздел бизнес-плана является расчётным. Финансовый план включает: расчет величины, определение источника инвестиций, прогноз

объема реализации, доходы от продажи товаров или услуг, издержки, прибыль.

5.5.1 Расчет капитальных вложений

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

$$\sum K_v = K_{об} + K_m + K_{пр} + T \quad (5.1)$$

Где K_m – капитальное вложение на монтаж

$K_{пр}$ – капитальное вложение на проектирование сети

$K_{об}$ – капитальное вложение на приобретение оборудования

T – капитальные вложения на транспортные расходы

Транспортные расходы включены в стоимость оборудования.

На осуществление данного проекта необходимо задействовать 52 наименования оборудования и комплектующих, общей стоимостью 8 925 793 тенге без НДС.

Стоимость устанавливаемого оборудования и комплектующих сети отражены в таблице 5.1.

Таблица 5.1 - Затраты на оборудование комплектующие

Наименование оборудования и комплектующих	Кол-во	Цена тенге	Сумма тенге
Кабель UTP cat 5	19650	90,00	1768500,00
Коммутационная панель 24 порт. Cat 5E	11	12290,00	135190,00
Кабельный организатор 19"	12	3200,00	38400,00
Панель ввода электропитания 8 портов	2	6685,00	13370,00
Шкаф телекоммуникационный напольный со стеклянной дверцей 42U, 19", 600x600mm	2	176900,00	353800,00
Вентиляторная полка с термостатом производительность 300m3/в час	2	24500,00	49000,00
Выдвижная патч-панель на 50 портов cat. 3	3	15900,00	47700,00
Полка оптическая 19" 24 порта SC с кассетой для укладки	1	149040,00	149040,00
Pigtail F.O. 62,5/125	8	750,00	6000,00

Резервированный источник питания 1500Вт, Gamatronik (8battery+Rack)	1	41390,00	41390,00
Коммутационные шнур RJ45-RJ45 3м cat 5	131	310,00	40610,00
Коммутационные шнур RJ45-RJ45 0,5м cat 5	3	225,00	675,00
Коммутационные шнур RJ45-RJ45 2м cat 5	201	280,00	56280,00
Коммутационные шнур RJ45-RJ45 1м cat 5	61	240,00	14640,00
Труба винипластовая 25мм	150	300,00	45000,00
Труба гофрированная	810	400,00	324000,00
Труба ПВХ 50мм	200	200,00	40000,00
Fibre Optics Patch cord multimode bifibre SC/SC 2m	2	1275,00	2550,00
Fibre Optics Use Dielectric 8 Fibres outdoor 62,5/125 мкм	500	3294,00	1647000,00
L2 Stackable Manager Swith 24x10/100TX+2 10/100/1000T or 2x GBIC slots	5	26000,00	130000,00
Набор кр. М6 (упаковка 50 шт)	3	65,00	195,00
Cajun P333T, Stackable Switch 24ports 10/100+ Exp. Slot	1	340000,00	340000,00
Коробка для сух.штукатурки или гипсокартона 3 места, 116*187*50мм + суппорт и рамка	85	2500,00	212500,00
Рамка 2-х модулей RJ45, для 1012E	129	825,00	106425,00
3 модульная напольная коробка, глубина 93мм	46	8618,00	396428,00
Крышка к трёхмодульной напольной коробке	46	660,00	30360,00
UTP RJ45 Keystone jack (8 pin)	262	425,00	111350,00
Рамка 50*50	2	450,00	900,00
Module 50*25 для 1 коннектора с пылезащитной шторкой	2	370,00	740,00
Заглушка 50*25	2	1060,00	2120,00
Крепежный и расходный материал, комп.	94	2600,00	244400,00
Плата 16 цифровых абонентов 16DLI	1	34086,00	34086,00
Плата 16 аналоговых телефонов 16SLI	5	63180,00	315900,00
Мультиплексор RAD G703/SC	1	332640,00	332640,00
Плата центрального процессора MCP	1	24100,00	24100,00
Модуль интерфейсов IOM	1	7347,00	7347,00
Плата MISC	1	13455,00	13455,00

	Модуль 12 DTMF приемников	1	12206,00	12206,00
	Плата питания	2	29269,00	58538,00
	Плата 30 каналов ИКМ T1/E1 PRI	1	89990,00	89990,00
	Кабинет	1	77760,00	77760,00
	Кросс-кабель	6	4 600,00	27600,00
	Карта памяти (16М) SMART MEDIA вариант L	1	17040,00	17040,00
	Цифровой телефон, 24 программируемых кнопки, ЖК индикатор	1	29950,00	29950,00
	Цифровой телефон, 12 программируемые кнопки, ЖК индикатор	7	20667,00	144669,00
	Цифровая консоль, 48 программируемые кнопки	2	14580,00	29160,00
	ИТР-5012L, Large LCD, 12B, IP phone	10	75810,00	758100,00
	Базовый блок VoIP	1	180000,00	180000,00
	Блок расширения VoIP	1	133719,00	133719,00
	Плата расширения VoIP	1	90970,00	90970,00
	Аккумуляторная батарея 12В 38А.ч	4	15000,00	60000,00
	Программа тарификации (до 350 абонентов) шнур+ лицензия	1	140000,00	140000,00
	Итого			8925793,00

5.5.2 Расчет стоимости монтажа

Для подключения оборудования необходимо провести монтажные работы. Данные работы будет производить сторонняя организация. Общая стоимость монтажных работ составляет 1984900 тенге. Виды проведенных работ и их стоимость отражены в таблице 5.2

Таблица 5.2 – Данные по стоимости монтажа

№ п.п.	Наименование оборудования и работ, ед. изм.	Кол-во	Цена тенге	Сумма тенге
1	Монтаж волоконно-оптического кабеля, метр	500	500,00	250000,00
2	Измерение параметров сети, р.место	131	900,00	117900,00

3	Программирование телефонной системы, шт.	1	300000	300000,00
4	Установка программы тарификации, шт.	1	240000,0	240000,00
5	Монтаж кабельной системы передачи данных, р.место	131	7000,00	917000,00
6	Измерение параметров волоконного кабеля, фибер	8	20000,00	160000,00
Итого за работы				1984900,0

5.5.3 Расчет затрат на проектирование сети

В состав затрат на проектирование сети входят следующие статьи затрат:

- заарботная плата разработчиков;
- социальный налог;
- электроэнергия;
- амортизационные отчисления;
- накладные расходы.

Расходы на проектирование рассчитываются по формуле:

$$K_{IP} = \Phi OT + O_C + A + \mathcal{E} + H + M, \quad (5.2)$$

где ΦOT – фонд оплаты труда;

O_C – отчисления на социальные нужды;

A – амортизационные отчисления;

\mathcal{E} – электроэнергия на производственные нужды;

H – накладные расходы;

M – расходы на материалы.

5.5.4 Расчет затрат на материалы для проектирования сети

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

Бумага
Картридж принтера
CD диски

Для осуществления разработки данного проекта необходимо использовать все необходимые материалы. Общая стоимость материалов составляет 29600 тенге. Виды материалов и их стоимость отражены в таблице 5.3

Таблица 5.3 – Затраты на материалы

Наименование материала	Марка	Единица измерения	Кол-во	Цена за единицу, тенге	Сумма, тенге
Бумага (Ватман)	A1	шт.	50	300	15000
Бумага писчая	«Белоснежка» A4 95% 80 г/м	пачка	10	600	6000
CD диски	CD-R Verbatim	шт.	15	40	600
Картридж принтера	Cartridge for HP 1015	шт.	2	4000	8000
Итого					29600

5.5.5 Расходы по оплате труда

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

$$\text{ФОТ} = \text{ЗОСН} + \text{ЗДОП} \quad (5.3)$$

Основная заработная плата определяется как сумма оплаты труда всех исполнителей:

$$Z_{\text{осн}} = \sum_{i=1}^n Z_i \cdot T_i, \quad (5.4)$$

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

T_i – затраты времени i -го работника, дней.

Дополнительная заработная плата составляет 10% от основной заработной платы:

$$\text{ЗДОП} = 0,1 \cdot \text{ЗОСН} \quad (5.5)$$

Труд разработчиков оплачивается согласно штатному расписанию. Количество исполнителей и размер месячной заработной платы представлены в таблице 5.4.

Таблица 5.4 – Количество исполнителей и их заработная плата

Исполнитель	Количество, человек	Заработная плата за месяц, тенге
Инженер	2	120000
Руководитель проекта	1	150000
Итого		390000

Стоимость человека–дня вычисляется по формуле:

$$D = \frac{ЗП_m}{D_p}; \quad (5.6)$$

где: ЗП_м – заработная плата за месяц, тенге;

Д_р – среднемесячное количество рабочих дней.

среднемесячное количество рабочих дней – 24.

Для инженера: $T = \frac{120000}{24} = 5000$ (тенге),

Для руководителя проекта: $T = \frac{150000}{24} = 6250$ (тенге),

На основе данных стоимости одного человека дня и продолжительности выполнения каждого этапа рассчитываем затраты на оплату труда (таблица 5.5).

Таблица 5.5 – Трудозатраты

Исполнитель	Дневная зарплата, тенге	Количество дней	Сумма, тенге
Инженер	5000	65	325000
Руководитель проекта	6250	65	406250

Основная заработная плата определяется как сумма оплаты труда всех разработчиков:

$$З_{осн} = \sum_{i=1}^n (З_i \cdot T_i) = 325000 + 325000 + 406250 = 1056250 \quad (\text{тенге}) \quad (5.7)$$

Дополнительная заработная плата составляет 10 % от основной заработной платы:

$$З_{доп} = 0,1 \cdot З_{осн} = 0,1 \cdot 1056250 = 105625 \text{ (тенге)} \quad (5.8)$$

Суммарный фонд оплаты труда (ФОТ) составит:

$$ФОТ = ЗОСН + ЗДОП = 1056250 + 105625 = 1161875 \text{ (тенге)}$$

5.5.6 Расчет социальных отчислений

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

$$Ос = 0,11 \cdot (ФОТ - ПО) \quad (5.9)$$

где ПО – отчисления в пенсионный фонд.

ФОТ – фонд оплаты труда

0,11 – ставка на социальные нужды

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

$$ПО = 0,1 \cdot ФОТ \quad (5.10)$$

$$ПО = 0,1 \cdot 1161875 = 116187,50 \text{ тенге}$$

Тогда социальный налог будет равен

$$Ос = 0,11 \cdot (1161875 - 116188) = 115026 \text{ тенге}$$

5.5.7 Расчет затрат на электроэнергию

Затраты на электроэнергию, включают в себя расходы электроэнергии на разработку данного проекта и дополнительные нужды. Ввиду необходимости круглосуточной работы оборудования суммарная мощность будет вычисляться по следующей формуле:

$$\mathcal{E} = \mathcal{E}_{эл.эн.} + \mathcal{E}_{доп.нуж.}, \quad (5.11)$$

где $\mathcal{E}_{эл.эн.}$ – затраты на электроэнергии на разработку данного проекта;

$\mathcal{E}_{доп.нуж.}$ – затраты на дополнительные нужды (5% от затрат на электроэнергию на разработку данного проекта).

Расходы электроэнергии рассчитывается по формуле

$$\mathcal{E}_{эл.эн.} = W \times T \times S, \quad (5.12)$$

где W – потребляемая мощность, 2 кВт;

T – время работы, T=520 ч;

S – тариф, 1 кВтч=17 тенге

$$З_{эл.эн.} = 2 \times 520 \times 17 = 17680 \text{ тенге}$$

Расходы на дополнительные нужды определяются по формуле

$$З_{доп.нуж.} = 0,05 \times З_{эл.эн.} \quad (5.13)$$

И составят:

$$З_{доп.нуж.} = 0,05 \times 17680 = 884 \text{ тенге}$$

Расходы на электроэнергию в соответствии с формулой 5.11 составят:

$$\mathcal{E} = 17680 + 884 = 18564 \text{ тенге}$$

5.5.8 Расчет амортизационных отчислений

В настоящее время норма амортизации (H_A) на компьютерное оборудование составляет 40% от стоимости всего оборудования и рассчитываются по формуле:

$$A_0 = \frac{H_A \cdot \sum K \cdot N}{100\% \cdot 12 \cdot n}, \quad (5.14)$$

где: $\sum K$ – сумма затрат на покупку оборудования;

N – количество дней на выполнение работы;

n – количество рабочих дней в месяце.

Так как нашей задачей является создание проекта разработки MPLS сети для филиала НК «КТЖ» ШЧ 19, то нам для осуществления данной цели необходимо два компьютера один принтер. Общая стоимость оборудования составляет 185 000 тенге.

$$A_0 = \frac{H_A \cdot \sum K \cdot N}{100\% \cdot 12 \cdot n} = \frac{40 \cdot 185000 \cdot 65}{100 \cdot 12 \cdot 24} = 16701 \text{ тенге}$$

5.5.9 Расчет накладных расходов

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

$$H = 0,25 \times (\Phi OT + З_{матер} + A_0 + \mathcal{E} + O_c + M) \quad (5.15)$$

И составляют:

$$H = 0,25 \times (1161875 + 29600 + 16701 + 115026 + 18564) = 335441,5$$

тенге

Результаты расчетов затрат по проектированию сети представлены в таблице 5.6.

Таблица 5.6 –Расходы по проектированию сети

Показатель	Сумма, тенге
ФОТ, тенге	1161875
Отчисления на социальные нужды, тенге	115026
Амортизационные отчисления, тенге	16701
Затраты на электроэнергию, тенге	18564
Затраты на материалы, тенге	29600
Накладные расходы, тенге	335441,5
Итого	1677207,5

Суммарные затраты на разработку и в соответствии с приведенной формулой (7.2) и расчетами составляют:

$$K_{\text{пр}} = \text{ФОТ} + H + A_0 + \text{Э} + O_c + M = 1677207,5 \text{ тенге}$$

Общая сумма капитальных затрат в соответствии с произведенными расчетами и согласно формуле (7.1) составит:

$$\sum K_{\text{в}} = K_{\text{об}} + K_{\text{м}} + K_{\text{пр}} = 8925793 + 1984900 + 1677207,5 = 12587900,5 \text{ тенге}$$

5.6 Эксплуатационные издержки.

Текущие затраты на эксплуатацию определяются по формуле:

$$\text{Э}_p = \text{ФОТ} + O_c + A_0 + \text{Э} + H \quad (5.16)$$

где ФОТ – фонд оплаты труда;

O_c – отчисления на соц. нужды;

A_0 – амортизационные отчисления;

Э – электроэнергия для производственных нужд;

Н – накладные затраты;

Стоимость поддержки устройства защиты состоит из следующих составляющих:

1) Заработная плата администратора;

Поддерживать устройства защиты будет системный администратор. Вычислим его годовую зарплату:

$$Зр_A = 12 \cdot 60000 = 720000 \text{ тенге,}$$

2) Социальные отчисления:

Согласно формуле (7.10) пенсионные отчисления будут равны:

$$ПО = 720000 \cdot \frac{10\%}{100\%} = 72000 \text{ тенге;}$$

Согласно формуле (7.9) социальный налог составит:

$$Ос = (720000 - 72000) \cdot 0,11 = 71280 \text{ тенге;}$$

3) Затраты на электроэнергию

W – потребляемая мощность, составляет 1,06 кВт;

S – стоимость киловатт-часа электроэнергии составляет 17 тенге.

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

$$T = 24 \cdot 365 = 8760 \text{ часов;}$$

В соответствии с формулой (5.11) расходы на электроэнергию составят:

$$\mathcal{E} = 1,06 \cdot 8760 \cdot 17 = 157855,2 \text{ тенге;}$$

4) Годовая амортизация оборудования:

Годовая амортизация на устройства коммутаторов Ethernet серий EX 3200, EX 4200 и EX 8200 будет равна:

$$A = \frac{15 \cdot 12587900,5}{100} = 1888185,08 \text{ тенге;}$$

Накладные расходы составляют 25 % от всех затрат и рассчитываются по формуле:

$$H = 0,25 \cdot (\Phi OT + O_c + A_o + \mathcal{E}) \quad (5.17)$$

Тогда накладные затраты составят:

$$H = 0,25 \cdot (720000 + 71280 + 1888185,08 + 157855,2) = 709330,07 \text{ тенге}$$

Таким образом эксплуатационные издержки составят:

$$\mathcal{E} = 720000 + 71280 + 1888185,08 + 157855,2 + 709330,07 = 35466500,35 \text{ тенге}$$

Таблица 5.7 – Годовые эксплуатационные расходы

Показатель	Сумма, тенге
ФОТ	720000
Отчисления на социальные нужды (Ос)	71280
Амортизационные отчисления (А ₀)	1888185,08
Затраты на электроэнергию (Э)	157855,2
Накладные расходы (Н)	709330,07
ИТОГО	3546650,35

5.7 Экономический эффект от внедрения технологии MPLS

Оценка экономической эффективности проекта производится на основе коэффициента абсолютной экономической эффективности и срока окупаемости.

Коэффициент экономической эффективности проекта рассчитывается по формуле:

$$E_p = \frac{ЧД}{Кв}; \quad (5.18)$$

где: ЧД – чистый доход;

Кв – капитальные вложения.

Рассчитаем условный доход, полученный от внедрения новой технологии.

Условный доход получим путем сокращения обслуживающего технического персонала на четыре штатные единицы.

Заработная плата инженера в месяц 120 000 тенге (согласно таблице 5.4). Тогда условный доход за год получим 5 760 000 тенге.

$$Д = (5760000 + 570240) = 6330240 \text{ тенге}$$

Условную прибыль найдем как разность годового дохода и эксплуатационных затрат на поддержку оборудования за первый год:

где: Д – условный годовой доход

Э – эксплуатационные издержки. (5.19)

$$П = Д - Э,$$

Рассчитаем по формуле:

$$П = 6330240 - 3546650.35 = 2783589.65 \text{ тенге;}$$

Таким образом коэффициент экономической эффективности составил:

$$E_p = \frac{2783589.65}{12636464} = 0,22$$

Срок окупаемости рассчитаем по формуле

$$T = \frac{1}{E}, \quad (5.22)$$

$$T = 1/0,22 = 4,5.$$

Проект окупается за 4,5 года, в последующие годы внедрение данной технологии с новым современным оборудованием принесет только прибыль.

Таким образом, коэффициент экономической эффективности от реализации проекта составил 0,22 при нормативном значении 0.2, а срок окупаемости проекта составил 4,5 года при нормативном значении 5 лет, то есть выполняется неравенства $T_p < T_n$ и $E_p > E_n$, что свидетельствует о целесообразности внедрения проекта.[21]

Вывод по разделу «Бизнес план»

В данной части дипломного проекта был представлен бизнес-план, в котором рассматривается вопрос о разработке MPLS сети для филиала Национальной Компании «Казахстан Темиржолы» - ШЧ 19.

Внедрение данной технологии дает следующие преимущества в работе сети:

- универсальный характер обслуживания разных приложений;
- независимость от технологий услуг связи и гибкость получения набора, объема и качества услуг;
- полная прозрачность взаимоотношений между поставщиком услуг и пользователями;
- возможность передачи большому количеству пользователей в реальном времени очень больших объемов информации с необходимой синхронизацией и с использованием сложных конфигураций соединений;
- интеллектуальность (управление услугой, вызовом и соединением со стороны пользователя или поставщика сервиса, раздельная тарификация и управление условным доступом);
- инвариантность доступа (организация доступа к услугам независимо от используемой технологии);
- комплексность услуги (возможность участия нескольких провайдеров в предоставлении услуги и разделение их ответственности и дохода согласно с видом деятельности каждого).

Коэффициент экономической эффективности от реализации проекта составил 0,22 при нормативном значении 0.2, а срок окупаемости проекта составил 4,5 года при нормативном значении 5 лет, то есть выполняется неравенства $T_p < T_n$ и $E_p > E_n$, что свидетельствует о целесообразности внедрения проекта.

ЗАКЛЮЧЕНИЕ

В проекте приводится описание разработки сети на основе технологии MPLS-VPN для филиала Национальной Компании «Казахстан Темиржолы», ШЧ 19 - Карагандинской дистанции сигнализации и связи, на участке которой находится более 20 станций.

В проекте рассмотрены мультипротокольная коммутация по меткам MPLS, VPN – виртуальные частные сети, обзор технологии VPN, технология MPLS – VPN. Приведена разработка сети с использованием технологии MPLS-VPN для НК «КТЖ» ШЧ 19;

В графической части работы показаны: структурная схема сети с технологией MPLS на ШЧ 19, схема сети филиала ШЧ 19, логическая схема сети филиала ШЧ 19, схема MPLS домена и подключенных узлов клиентов, подключение узлов маршрутизаторов, схема прохождения пакета VPN через MPLS домен, схема подключения маршрутизаторов

В технико-экономическом расчёте определены затраты на реализацию проекта и дана оценка экономической эффективности проекта.

В проекте также рассмотрены вопросы охраны труда и вопросы техники безопасности при работе с ПЭВМ. Представлены Нормы освещения, Нормы электрической безопасности по работе с ПЭВМ.

Внедрение данной технологии дает следующие преимущества в работе сети:

- универсальный характер обслуживания разных приложений;
- независимость от технологий услуг связи и гибкость получения набора, объема и качества услуг;
- полная прозрачность взаимоотношений между поставщиком услуг и пользователями;
- возможность передачи большому количеству пользователей в реальном времени очень больших объемов информации с необходимой синхронизацией и с использованием сложных конфигураций соединений;
- интеллектуальность (управление услугой, вызовом и соединением со стороны пользователя или поставщика сервиса, отдельная тарификация и управление условным доступом);
- инвариантность доступа (организация доступа к услугам независимо от используемой технологии);
- комплексность услуги (возможность участия нескольких провайдеров в предоставлении услуги и разделение их ответственности и дохода соответственно с видом деятельности каждого).

СПИСОК ЛИТЕРАТУРЫ

1. Гольдштейн А.Б., Гольдштейн Б.С. Технология и протоколы MPLS. — СПб.: БХВ – Санкт-Петербург, 2005.
2. Вивек Олвейн. Структура и реализация современной технологии MPLS. Руководство Cisco = Advanced MPLS Design and Implementation. — М.: Вильямс, 2004. — 480 с.
3. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. — СПб.: Издательство «Питер», 2008.
4. www.abn.ru
5. www.intuit.ru
6. www.osp.ru
7. <http://broadcasting.ru>
8. www.telecor.ru
9. www.microtest.ru
10. IBM 8245 10/100 Stackable Ethernet Hub//
<http://www.raccess.ru/redirect.asp?mode=1559>
11. Как работают локальные сети.//
<http://www.raccess.ru/ethernet/>.
12. Fast Ethernet как развитие классического Ethernet//
http://www.citforum.ru/nets/lvs/glava_2.shtml/.
13. Обзор стандарта кабельных систем ANSI/TIA/EIA-568-A //
http://www.madex.ru/html/view_ps_05.phtml/.
14. Локальная сеть для офиса //
<http://www.compdoc.ru/network/local/nonsdec/>.
15. <http://www.evrokom.com/>.
16. <http://www.sly.ru>
17. <http://www.sonet.ru/>
18. Базылов К.Б., Алибаева С.А., Бабич А.А. Методические указания для студентов всех форм обучения специальности 050719 – Радиотехника, электроника и телекоммуникации. — Алматы: АИЭС, - 2008. - 20 с.
19. Голубицкая Е.А., Жигуляская Г.М. Экономика связи. — М.: Радио и связь, 1999.
20. Юркова Т.И., Юрков С.В.. Учебное пособие (электронный учебник). Москва – 2006 г.
21. Тришкина Н.А.. Учебный курс (учебно-методический комплекс) «Экономика организации (предприятия)». Москва – 2010 г.

ГЛОССАРИЙ

CE (Customer Edge) - маршрутизатор со стороны узла клиента, который непосредственно подключается к маршрутизатору оператора.

PE (Provider Edge) - граничный маршрутизатор со стороны оператора (MPLS домена), к которому подключаются устройства CE. PE устройства выполняют функции E-LSR-ов. На нашем полигоне эту роль выполняют маршрутизаторы Router_A, Router_B, Router_C, Router_I, Router_F.

P (Provider) - маршрутизатор внутри сети Оператора (MPLS домена). Р устройства выполняют функции LSR. На нашем полигоне роль маршрутизатора Р возложена на маршрутизатор Router_G.

(FEC) forwarding equivalence class

Группа IP-пакетов, которые переадресуются каким-то образом (например, по тому же маршруту, с той же маршрутной обработкой)

Label merging — объединение меток

Замещение множественных приходящих меток для определенного FEC одной выходной меткой

Label swap — инверсия меток

Базовая операция переадресации, состоящая из просмотра входной метки с целью определения выходной метки, инкапсуляции, порта и другой информации, сопряженной с обработкой поступающих данных

Label swapping

Парадигма переадресации, позволяющая осуществлять переадресацию данных путем использования меток для идентификации классов информационных пакетов, которые обрабатываются при переадресации неразличимым образом

Label switched hop

Шаг между двумя узлами MPLS, на которые осуществляется переадресация с привлечением меток

Label switched path — путь с коммутацией меток

Путь через один или более LSR на одном уровне иерархии для пакетов с определенным FEC

Label switching router

Узел MPLS, который способен переадресовывать пакеты L3 согласно их меткам

Loop detection — детектирование петель

Метод, при котором разрешено формирование петлевых маршрутов; такие структуры позднее выявляются

Loop prevention — предотвращение петель

Метод, при котором данные никогда не передаются по петлевым маршрутам

Merge point

Узел, в котором произведено объединение меток

MPLS domain — домен MPLS

Непрерывный набор узлов, реализующих MPLS-маршрутизацию и находящихся в одном маршрутном и административном домене

MPLS edge node — пограничный узел MPLS

Узел MPLS, который соединяет MPLS-домен с узлом, находящимся вне домена, потому что он не поддерживает MPLS, и/или из-за того, что он размещен в другом домене. Заметим, что если LSR имеет соседнюю ЭВМ, которая не работает с MPLS, то этот LSR является пограничным узлом MPLS

MPLS egress node — выходной узел MPLS

Пограничный узел MPLS, если через него трафик выходит из домена MPLS

MPLS ingress node — входной узел MPLS

Пограничный узел MPLS, если через него трафик входит в домен MPLS

MPLS label — метка MPLS

Метка, которая содержится в заголовке пакета и которая представляет FEC пакета

MPLS node — узел MPLS

Узел, поддерживающий протокол MPLS. Узел MPLS распознает протоколы управления MPLS, реализует один или более протоколов маршрутизации L3 и способен переадресовывать пакеты на основе меток. Узел MPLS может опционно переадресовывать L3 пакеты в традиционном режиме

VC merge — объединение VC

Объединение меток, когда метка MPLS переносится в поле ATM VCI (или в комбинации полей VPI/VCI), чтобы позволить объединение нескольких VC в один VC

VP merge — объединение VP

Объединение меток, когда метка MPLS переносится в поле ATM VPI, чтобы позволить объединение нескольких VP в один. В этом случае две ячейки будут иметь одно и то же значение VCI, только если отправлены из одного узла. Это позволяет различать ячейки разных отправителей с помощью VCI

VPI/VC

Метка, используемая в сетях АТМ для идентификации виртуального канала

Акронимы и аббревиатуры

DLCI — Data Link Circuit Identifier — идентификатор канала передачи данных

FEC — Forwarding Equivalence Class — класс переадресации

FTN — FEC to NHLFE Map — соответствие FEC и NHLFE

IGP — Interior Gateway Protocol — внутренний протокол маршрутизации

ILM — Incoming Label Map — таблица соответствия входящих меток

LDP — Label Distribution Protocol — протокол пересылки меток

LSP — Label Switched Path — путь с коммутацией меток

LSR — Label Switching Router — маршрутизатор с коммутацией меток

NHLFE — Next Hop Label Forwarding Entry — запись, содержащая адрес следующего шага при коммутации меток

SVC — Switched Virtual Circuit — переключаемая виртуальная схема

SVP — Switched Virtual Path — переключаемый виртуальный путь

VC — Virtual Circuit — виртуальная схема

VC — Virtual Circuit Identifier — идентификатор виртуальной схемы

VP — Virtual Path — виртуальный путь

VPI — Virtual Path Identifier — идентификатор виртуального пути.

ПРИЛОЖЕНИЕ А

ПРИЛОЖЕНИЕ Б

ПРИЛОЖЕНИЕ В

ПРИЛОЖЕНИЕ Г

ПРИЛОЖЕНИЕ Д