Содержание

Введение

Сегодня информационные технологии ежедневно развиваются и получают широкое распространение. В частности, использование персональных компьютеров — это неотъемлемые условия для нормального функционирования любого предприятия. Как правило, на предприятиях компьютеры объединяют в общую сеть, что дает ряд преимуществ в отличии от локального использования. Отдельные места сотрудников перестают быть изолированными и становятся уже частью единой системы. Это предоставляет возможность разделять программные и аппаратные ресурсы, тем самым повышая эффективность работы.

Развитие бизнеса не может существовать без слаженных действий и быстрого своевременного обмена данными и оперативного контроля над всей деятельностью компании.

Для создания корпоративной сети, используют оборудование ведущих производителей. Плюсами предлагаемых сетевых решений являются: высокая экономическая эффективность, надежность и безопасность, возможность модернизации.

При использовании корпоративной сети, у организации появляется масса возможностей. Внедрив в организацию корпоративную сеть, появляется возможность четко отладить и организовать взаимодействие между разными офисами, объединив их в единую систему.

В список преимуществ корпоративной сети входят следующие пункты:

- функционал организации становится прозрачным для управляющих кадров и руководства;
- контроль работы всех структурных подразделений организации;
- доступ ко всем базам данных, документации и отчетности производится в режиме реального времени;
- локальная сеть влияет на экономию затрат на междугородние, международные звонки и курьерские услуги.

Множество программных и аппаратных средств, технологий и сервисов позволяют каждый день повышать удобство и скорость работы с данными. Сложно выбрать из имеющихся технологий действительно полезные и научиться использовать их с максимальной пользой.

На данный момент существует очень много предприятий с развитой корпоративной сетью и хорошим потенциалом на расширение и модернизацию. Один раз правильно построенная сеть, может существенно облегчить жизнь в дальнейшем при каких-либо инновациях в организации.

В данной выпускной квалификационной работе бакалавра будет разрабатываться корпоративная сеть с использованием технологии виртуализации. Данная технология имеет место быть, так как использование серверов в корпоративной сети — это неотъемлемая часть для совместного использования баз данных, для установки каких-либо требовательных сетевых программ, рассчитанных на работу сервер-клиент, для организации файловых хранилищ и т.д.

Выпускная квалификационная работа бакалавра состоит из введения, трех разделов, заключения и списка использованных источников.

В первом разделе будет рассмотрено определение понятия «виртуализация», что это такое, для чего это нужно, и кто на российском рынке готов предоставить данную технологию. Будет проанализирована востребованность поставщиков в данном сегменте.

Во втором разделе осуществляется проектирование сети связи. Будет осуществлена постановка задачи и цели разработки, произведен расчет активного сетевого и серверного оборудования, определена топология и архитектура сети, произведен расчет плана IP-адресации. Также будет осуществлено внедрение технологии виртуализации.

В третьем разделе будут проведены расчеты основных технических характеристик проектируемой сети.

1. Обзор средств виртуализации

1.1. Понятие виртуализации и ее типы

Виртуализация — это предоставление набора вычислительных ресурсов или их логического объединения, абстрагированное от аппаратной реализации, и обеспечивающее при этом логическую изоляцию друг от друга вычислительных процессов, выполняемых на одном физическом ресурсе [1].

Под виртуализацией понимается выделение вычислительной мощности оборудования для эмуляции некоторого количества гостевых операционных систем.

Когда компания производит покупку нового дорогого оборудования, то она планирует максимально использовать его ресурсы. Для этого возможно переносить в виртуализированную среду средненагруженные серверы, такие как веб-сервер, сервер базы данных, контроллер доменов. Так же виртуализацию можно использовать при тестировании нововведений. Тогда компании не надо покупать или заарендовывать оборудование для тестирования нового сервиса. Можно устанавливать различное ПО, которые конфликтуют друг с другом, или разные версии одинакового ПО.

С помощью виртуализации можно эмулировать работу различных физических устройств: ПК, стационарные телефоны, планшеты и смартфоны. Виртуализация может управлять характеристиками физических устройств для большего приближения к реальной ситуации.

Используя технологию виртуализации, происходит экономия на содержание и модернизацию сети. Например, приобретя одно мощное оборудование, можно разделить вычислительную мощность для выполнения нескольких функций. При необходимости возможно изменить выделенную мощность для более эффективной работы. При модернизации гостевые машины не заметят изменения физического сервера. Так же повышается отказоустойчивость, при отказе одного физического устройства виртуальная система практически мгновенно будет использовать другое. При работе

нескольких серверов, использующих технологию виртуализации, происходит распределение производительности. Например, если один сервер полностью нагружен, а другой простаивает, то происходит автоматическая балансировка нагрузки.

Разработка компании IBM конца 60-х и начала 70-х годов технологии виртуализации и гипервизоров использовалась в основном для тестирования новых операционных систем и новых концепций. Создание технологии виртуализации позволило развертывать системы и устранять неисправности, не подвергая риску основную систему. В средине 2000-х годов гипервизоры делаю большой шаг вперед, многие операционные системы, такие как Linux, Unix начинают использовать эту технологию. И уже в 2005 году разработчики начали добавлять аппаратную виртуализацию [2].

Из-за того, что виртуальные машины хоть и работают на одном физическом оборудовании, они логически отделены. При сбое на одной из виртуальных машин, это не распространится на остальные виртуальные машины.

Существует две технологии виртуализации: аппаратная и программная.

Программная виртуализация в свою очередь делится на динамическую трансляцию и паравиртуализацию.

Динамическая трансляция.

Так как ядро операционной системы не находится в привычном месте при передаче первой же команды порушилось вся структура вычислительной машины. Для предотвращения этой ошибки используется гипервизор, который делает команды менее привилегированными, тем самым результат команд подается так же, как если гостевая операционная система была самой привилегированной. Именно такой подход был реализован командой разработчиков в 1999 году в продукте VMware Workstation [3].

Паравиртуализация.

Концепция, которая предполагает, что гостевая операционная система знает о своем нахождении в виртуальной машине и знает, как обращаться к хостовой операционной системе за определенными системными функциями.

Аппаратная виртуализация.

Производители процессоров ввели дополнительные инструкции для предоставления доступа к ресурсам процессора из гостевых операционных систем. Такие процессоры могут работать в двух режимах root operation и non-root operation. В первом режиме есть специальное программное обеспечение, являющееся прослойкой между гостевыми операционными системами и оборудованием, оно называется гипервизор. Для перевода процессора в режим виртуализации, передается управление гипервизору, который запускает виртуальную гостевую систему [4].

Преимущества:

- Упрощение разработки платформ виртуализации за счет предоставления аппаратных интерфейсов управления и поддержки виртуальных гостевых систем.
- Возможность независимого запуска нескольких виртуальных платформ с возможностью переключения между ними на аппаратном уровне.
- Отвязывание гостевой системы от архитектуры хостовой платформы и реализации платформы виртуализации.
- Возможность увеличения быстродействия платформ виртуализации.

Из недостатков можно отметить, что из-за простоты написания платформ есть возможность создания вредоносного программного обеспечения, которая может осуществлять действия за пределами хостовой системы.

1.2. Основные типы гипервизоров и их назначение

Гипервизор – это процесс, который разделяет операционную систему компьютера от опорного физического оборудования. Под гипервизором обычно

понимают программное обеспечение, так же существуют встроенные гипервизоры [5].

Выделяют следующие основные типы гипервизоров:

- Тип 1 (bare-metal) не требует операционный системы общего назначения. Управляет распределением вычислительных ресурсов и операциями ввода вывода, контролирует все обращения виртуальных машин к устройствам
- Тип 2 (hosted) – это приложения, работающие поверх хостовой операционной системы. Все обращения виртуальных машин обрабатываются хостовой системой. Гипервизор второго типа ограничен по производительности, так как делит ресурсы с другими пользовательскими приложениями. Второй тип гипервизоров подходит для кроссплатформенной разработки и развертывания стендов на машинах разработчиков программного обеспечения.
- Тип 1+ (гибрид) изолирует базовую операционную систему в родительский раздел или родительский домен. За распределение ресурсов отвечает гипервизор, а родительский домен обрабатывает обращения к драйверам устройств и операциям ввода вывода. Родительский домен становится провайдерам между сущностями стека виртуализации. В гипервизор не надо добавлять драйвера устройств и вследствие чего увеличивается список поддерживаемого оборудования [6].

1.3. Анализ основных решений по виртуализации

По данным исследования аналитической компании Gartner, проведенного в первом квартале 2020 года компания VMware является одним из лидеров технологий виртуализации (рисунок 1.1). По сообщениям авторов исследования на это повлияло развитие решения VMware vSAN, которое дорабатывалось в

прошедшем году весьма активно, а также анонс архитектуры VMware Project Pacific.

Рисунок 1.1 – Магический квадрант Gartner о конвергентной инфраструктуре за сентябрь 2022 года

VMware vSAN это конвергентное решение, позволяющее создать инфраструктуру из типовых блоков, которые будут объединять сразу несколько функций. Управление становится проще, так как мы осуществляем контроль через единый интерфейс, а масштабируем путём добавления нового блока. Каждый блок — это отдельный сервер. На каждом сервере есть от 1 до 5 дисковых групп. В каждой группе – минимум один SSD-диск и от 1 до 7 HDD-дисков. SSD-диски в этих дисковых группах составляют общий пул

кэширования данных. VSAN в первую очередь читает данные в кэше; если данных в кэше нет, VSAN отправляется к HDD-дискам.

Многие пользователи хотят развёртывать инфраструктуру контейнеризованных приложений на физической инфраструктуре, и не надо следить за издержками на гипервизоре и лицензии. Такие приложения в контейнерах все равно взаимодействуют с корпоративными сервисами. Такое сочетание физической и виртуальной среды тяжело обслуживать. Платформа VMware Project Pacific позволяет администратору видеть и управлять инфраструктурой контейнеризованного приложения как единым блоком из нескольких виртуальных машин.

С помощью этих нововведений компания VMware на начало 2020 года по мнению аналитической компании Gartner стала основным гиперконвергентным коробочным решением VMware является платформа VMware Cloud Foundation (VCF) - комплексное программное решение, которое включает в себя компоненты VMware vRealize Suite, VMware vSphere Integrated Containers, VMware Integrated OpenStack, VMware Horizon, NSX и другие, работающие в онпремизной, облачной или гибридной инфраструктуре предприятия под управлением SDDC Manager.

У компании VMware есть продукт vSphere 7. Он создан для уменьшения числа используемых физических серверов, так же повышается степень консолидации серверов. Используя vSphere 7 возможно распределять ресурсы во время крупных рабочих нагрузок с помощью планировщика, который использует подход, ориентированный на рабочие нагрузки. Тем самым увеличивается отказоустойчивость корпоративной сети. Администраторы с данной технологией могут применять политику сразу для целевой группы виртуальных машин, кластеров Kubernetes и контейнеров. Упрощается управление жизненным циклом и предоставляются средства безопасности для гибридных облачных инфраструктур [7].

У одной из крупнейших компаний Microsoft есть своя технология виртуализации, встроенная в операционную систему Windows. Её название - Hyper-V, он позволяет запускать несколько операционных систем на одной физической машине. Данная технология встроена в операционную систему Windows, поэтому эффективнее и удобнее создавать виртуальные машины на данной операционной системе. При управлении памятью Hyper-V на сервере предполагается, что на нем запущены только виртуальные машины. В Hyper-V для Windows при управлении памятью учитывается тот факт, что кроме виртуальных машин на большинстве клиентских компьютеров работает локальное программное обеспечение [8].

В таблице 1.1 приведены основные поставщики и их продукты для виртуализации серверов. В столбце «вспомогательное ПО» указаны продукты для настройки и управления данной платформой виртуализации.

Таблица 1.1 – Основные поставщики и их продукты для виртуализации серверов

Поставщик	Программный продукт	Тип виртуализации	Вспомогательное ПО
VMWare	VMware ESXi Server	на «голое» железо	VMware vSphere Client
Parallels	Parallels Virtuozzo Containers	на уровне ОС	-
Microsoft	Windows Server 2012 Hyper-V	на уровне ОС	-
Citrix	XenServer	на «голое» железо	XenCenter
Red Hat	Red Hat Enterprise Virtualization Hypervisor	на уровне ОС	-

В ходе вышеупомянутого исследования компания Gartner привела данные о процентной доле рынка, которую занимают основные поставщики решений для виртуализации серверов. Данные представлены на рисунке 1.2.

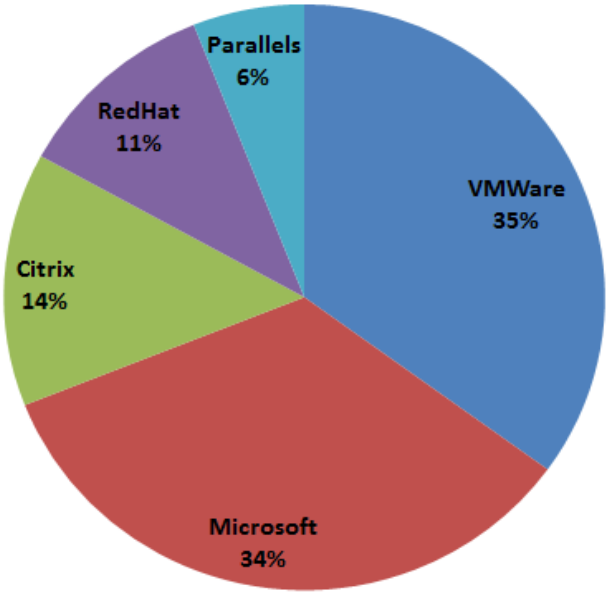

Рисунок 1.1 – Процентная доля основных поставщиков решений для виртуализации

1.4. Целесообразность внедрения технологии виртуализации

В случае если расценивать виртуализацию в общем значении, можно прийти к понятию виртуализации ресурсов, включающую в себе подходы к организации виртуальных сред.

Виртуализация ресурсов дает возможность сосредоточивать, абстрагировать и упрощать контроль группами ресурсов, таких как сети, хранилища информации и пространства имен.

Виртуализация ОС за последние 4 года неплохо подвинулась вперед, как в технологическом, так и в рекламном значении. Использовать продукты виртуализации стало гораздо легче, они сделались наиболее надежными и многофункциональными.

Ключевой ролью в дипломной работе будет затрагиваться лишь консолидация серверов.

Виртуализация серверов дает возможность на одном физическом сервере сформировать несколько виртуальных серверов и поместить на него ранее бывшие самостоятельными физические сервера, повысив нагрузку только одного сервера до 60-80 % и, повысив коэффициент применения техники. Это позволяет значительно сэкономить на технике, сопровождении и электроэнергии. Освобождая сервера, консолидировав их функции на другой не полностью загруженный сервер, мы экономим в деньгах, ведь уже не придется закупать дополнительное оборудование для каких-то новых функций и ПО. Наглядный пример развертки нескольких изолированных сред на одном сервере можно увидеть на рисунке 1.3.

Рисунок 1.3 – Развернутые изолированные среды на одном сервере

К достоинствам еще можно отнести возможности разработки и тестирования приложений. Продукты виртуализации дают возможность запускать изрядное количество ОС параллельно, предоставляя возможность разработчикам и тестерам программного обеспечения тестировать их приложения на всевозможных платформах и конфигурациях. Также имеются удобные средства по организации «снимков» протекающего состояния системы одним кликом мыши и такого же легкого восстановления из этого состояния, дают возможность организовывать тестовые среды для всевозможных конфигураций, что значительно увеличивает темп и качество разработки.

Применяя виртуализированные серверы, можно свободно организовывать резервные копии рабочих станций и серверов (попросту скопировав папку), возводить системы, обеспечивающие самое малое время возобновления после сбоев, и т.п. К предоставленной группе разновидностей применения относятся те бизнес-решения, которые применяют главные достоинства виртуальных машин.

Отличный существующий вид виртуализации – применение виртуальных рабочих станций. С приходом эпохи виртуальных машин станет нелепо сооружать себе рабочую станцию с ее привязкой к технике. Сегодня создав один раз виртуальную машину с собственной рабочей или домашней средой, появится возможность пользоваться ею на любом ином компьютере. Также позволяется пользоваться готовыми шаблонами виртуальных машин, которые решают конкретную задачу. Концепция подобного применения виртуальных рабочих станций имеет возможность быть выполненной на базе хост-серверов для запуска на них перемещаемых виртуальных рабочих станций пользователей. В будущем эти рабочие станции пользователь сможет захватить с собой, не синхронизируя данные с ноутбуком. Данная версия применения в свою очередь дает возможность организации защищенных пользовательских рабочих станций, которые смогут быть использованы, например, для демонстрации способностей программы клиенту. Можно сузить время применения виртуальной машины – и по истечении данного времени виртуальная машина не станет запускаться. В этом виде использования, заложены огромные возможности [3].

1.5. Выводы

В разделе был проведен анализ технологии виртуализации и рассмотрены основные поставщики решений по виртуализации. В данной выпускной квалификационной работе бакалавра будет использоваться продукт для виртуализации серверов от компании VMware. Выбор обуславливается тем, что

компания VMware по приведенным данным является лидером в сфере виртуализации, а предлагаемые ею решения показали себя как очень востребованные, гибкие и надежные.

2. Разработка территориально-распределенной информационной сети предприятия

2.1. Исходные данные

В данной главе будет произведена разработка сети организации, произведен выбор архитектуры и топологии сети, будут выбраны комплектующие и будет проведен анализ, как они будут взаимодействовать. Чтобы приступить к данным вопросам, необходимо привести исходные данные.

Для начального этапа необходимы сведения о составе организации, ее численности и о входящих в нее подразделениях.

В данной разработке будет рассматриваться банковская организация, которая будет иметь головной центральный офис и вспомогательные филиалы.

Такая сеть будет считаться распределенной сетью – то есть системой, для которой отношения местоположений элементов будут играть существенную роль с точки зрения функционирования системы.

Разобравшись со сферой организации, необходимо знать численность сотрудников, которые будут работать в сети.

В таблице 2.1.1 представлен численный состав подразделений организации.

Таблица 2.1.1. - Численный состав подразделений и его функционал в организации

Наименование подразделения	Функционал	Численность сотрудников
Кредитно-депозитное управление	Предоставление кредитов для частных и юридических лиц, размещение денежных средств: депозиты, банковские вклады, банковские гарантии.	33

Таблица 2.1.1. - Численный состав подразделений и его функционал в организации (продолжение)

Наименование подразделения	Функционал	Численность сотрудников
Отдел информационных технологий	Поддержка сотрудников в техническом плане, модернизация сети, обновление и внедрение новых сервисов, ПО, технических компонентов сети.	25
Юридический департамент	Правовое сопровождения деятельности банка, открытие счетов юридическим лицам и индивидуальным предпринимателям.	33
Отдел обеспечения	Организация административно-хозяйственной и материально-технической деятельности. Занимается содержанием транспортных средств, оргтехники и иного оборудования.	20
Отдел бухгалтерии	Осуществление оформления документов, начисление заработанной платы и т.д.	20
Департамент обеспечения безопасности	Контроль проходного пункта, охрана помещений, оборудования и иного имущества.	24

Общее количество человек в организации:	155

Количество человек в центральном офисе будет состоять из 135 сотрудников и по 10 сотрудников в филиалах.

В таблице 2.1.2 приведен численный состав подразделений, входящих в состав центрального офиса и двух филиалов организации.

Таблица 2.1.2. - Численный состав подразделений в центральном офисе и в филиалах

Наименование подразделения	ЦО «Павелецкий»	ДО «Лубянка»	ДО «Пражская»
Кредитно-депозитное управление	25	4	4
Отдел информационных технологий	25	-	-
Юридический департамент	25	4	4
Отдел обеспечения	20	-	-
Отдел бухгалтерии	20	-	-
Департамент обеспечения безопасности	20	2	2

Центральный офис будет представлять собой трехэтажное здание, которое будет иметь на каждом этаже серверную комнату. Серверная комната – это помещение со специально созданными условиями. В ней будет находиться все сетевое и серверное оборудование организации. В данных комнатах будет производиться коммутация розеток. Под коммутацией розеток имеется в виду, что в коммуникационную панель, будет подаваться сигнал от сетевого оборудования непосредственно на рабочие места сотрудников. Сигнал будет подаваться с помощью витой пары категории 5е.

2.2. Выбор топологии и архитектуры сети

При построении сети будет использоваться топология «дерева» - иерархическое соединение узлов, идущее из общего узла-корня. Между двумя любыми узлами в подобный сети есть лишь один маршрут. Иными словами, предоставленную топологию еще именуют «звезда».

Технологии физического и канального уровней, на которых будет выстраиваться наша сеть - Fast Ethernet и Gigabit Ethernet. Выбор технологии Fast Ethernet и Gigabit Ethernet даст возможность предоставить высокое быстродействие.

Стандарт Fast Ethernet осуществляет передачу информации на скорости 100 Мбит/сек и поддерживает два варианта передающей среды - витая пара и волоконно-оптический кабель. UTP - неэкранированная витая пара с 4 витыми парами, категории 5e. Отдаление между станциями ограничено и не должно превосходить 100 м. Наилучшею сетевой технологией станет 100Base-TX с методом доступа CSMA/CD, потому как она имеет обширное использование в наши дни, её легко модифицировать и у нее имеется большая отказоустойчивость.

CSMA/CD (Carrier-Sense MultIPle Access with Collision Detection) — это технология множественного доступа к единой передающей среде в местной компьютерной сети с контролем коллизий. CSMA/CD принадлежит к децентрализованным случайным методам. Он применяется как в обыкновенных сетях типа Ethernet, так и в скоростных сетях (Fast Ethernet, Gigabit Ethernet). Так же называют сетевой протокол, в котором используется схема CSMA/CD. Протокол CSMA/CD работает на канальном уровне в модели OSI. [5]

Любая организация определяет личные запросы к конфигурации сети. В предоставленном случае это 155 сотрудников, и соответственно 135 рабочих станций в центральном офисе и 10 сотрудников, соответственно 10 рабочих станций, которые будут находиться в филиалах. Иным фактором считается иерархия компании. Организация будет выстроена по принципу вертикальной

структуры, в которой точно понятно, какой работник и к какой информации обязан обладать доступом.

С программной точки зрения возможны две структуры: доменная структура и структура рабочих групп.

Для проектирования сети избрана доменная структура как более практичный вариант администрирования.

Предоставленная структура применяется в средних и больших сетях. Домен – административная единица, где учетная информация о пользователях сети держится на основном контроллере домена и копируется на резервных контроллерах. Запросы пользователей на регистрацию в сети проверяются на одном из контроллеров. К дополнительным возможностям можно отнести:

- поддержка динамических обновлений;
- безопасные соединения (DNSsec);
- поддержка всевозможных видов данных (SRV-записи).

2.3. Этапы разработки сети

Конструирование компьютерных сетей уместно изображать в виде трехуровневой иерархической модели, которая включает следующие уровни:

- уровень ядра;
- уровень распределения;
- уровень доступа.

Уровень ядра специализирован для скоростной передачи сетевого трафика и высокоскоростной коммутации пакетов, формирует ядро сети. На вершине иерархии данный уровень отвечает за скорую и надежную пересылку крупных объемов трафика между разными сегментами уровня распределения. На этом уровне обрабатываются немалые объемы трафика, поэтому не менее существенно принимать во внимание скорость и задержки. Традиционно при конструировании пытаются применять быстродействующие сети Multi-GigabitEthernet и GigabitEthernet. Чаще всего, в качестве оборудования, на

уровне ядра выступает маршрутизатор.

Уровень распределения применяется для суммирования маршрутов. Суммирование проводится для снижения сетевого трафика на верхних уровнях сети. Главными функциями уровня распределения считаются фильтрация, маршрутизация и доступ к сетям. Если нужно, то и определение правил доступа пакетов к уровню ядра. Коммутаторы уровня распределения связаны с маршрутизаторами уровня ядра.

На уровне доступа в основной массе вариантов применяется коммутатор второго уровня модели OSI. Данный уровень предназначается для подключения серверов и обычных рабочих станций к сети организации. Для осуществления этого уровня используют приемлемое по цене оборудование, не требующее каких-либо сложных конфигураций. Уровень доступа представляется переходным средством от рабочих станций и серверов к следующему уровню иерархической модели сети.

Данные уровни дают возможность создания сети, начиная с нуля, от рабочих станций и заканчивая маршрутизатором, открывающим возможность выхода в интернет и возможность связи с другими дополнительными офисами и их сетями. [6,8]

Составим иерархическую модель для проектируемой сети (рисунок 2.1).

На рисунке 2.1 можно увидеть, что все коммутаторы в головном офисе и филиалах будут находиться на уровне доступа. На уровне распределения в головном офисе будет находиться коммутатор 3 уровня модели OSI. А на уровне ядра будет находиться маршрутизатор, предоставляющий доступ к сети Интернет. Маршрутизаторы в филиалах будут выступать как оборудование, функционирующее, как на уровне распределения, так и на уровне ядра сети и предоставляющее доступ к сети Интернет.

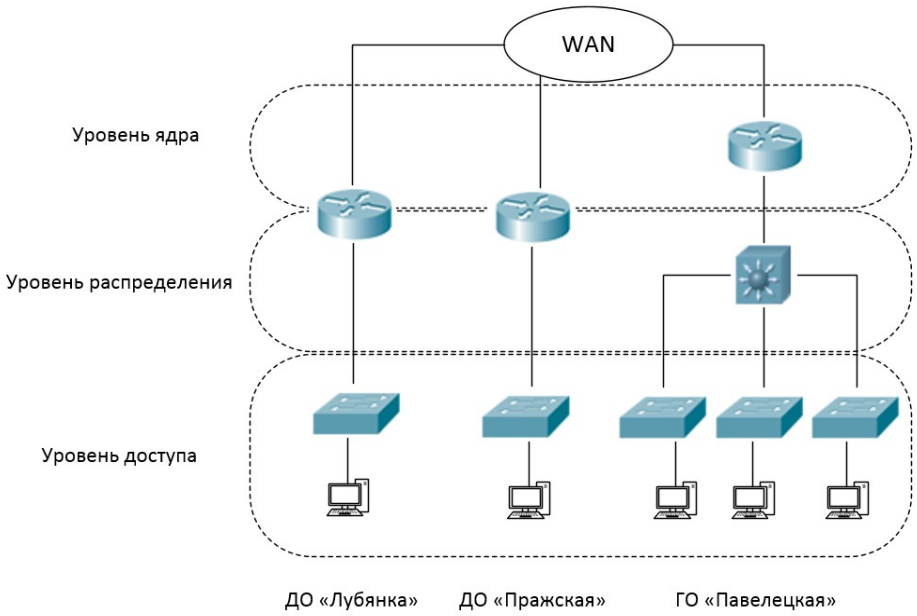

Рисунок 2.1 – Иерархические уровни проектируемой сети

В следующем параграфе будет произведен выбор оборудования, начиная с оборудования, которое будет находиться на уровне доступа и заканчивая оборудованием на уровне ядра.

2.4. Выбор оборудования для центрального офиса

В качестве активного сетевого оборудования предлагается использовать оборудование фирмы Cisco, которое является одним из наиболее качественных продуктов на мировом рынке. Данная фирма зарекомендовала себя на рынке, как поставщик качественной и надежной продукции.

Для начала подберем оборудование для нашего центрального офиса.

В качестве коммутаторов будут использоваться коммутаторы Cisco Catalyst WS-C2960X-48LPS-L. Данные коммутаторы с точки зрения иерархии сети будут выступать как оборудование уровня доступа.

Выбранный коммутатор легок в конфигурировании и обслуживании, а также крайне надежен. Может управляться централизованно с помощью программного обеспечения Cisco Network Assistant. Применяя данное ПО можно наладить централизованное управление коммутаторами,

маршрутизаторами и устройствами беспроводного доступа производства Cisco. Эта бесплатная программа содержит простые настройки оборудования Cisco, которые позволяют обнаруживать неполадки в работе устройства. [7]

Ряд существенных преимуществ данного коммутатора:

- разнообразие вариантов подключения;
- гибкость и скорость передачи данных;
- множество конфигураций коммутаторов;
- сниженное энергопотребление устройств;
- безопасность передачи данных;
- улучшенная отказоустойчивость сети;
- возможности резервного питания;
- отличное качество обслуживания;
- 4 порта 1000Base-X(SFP);
- организация контроля сети и оптимизация ширины канала с использованием QoS;
- поддержка USB накопителей, для быстрой резервной копии, дистрибуции и упрощения управления.

В коммутаторах Cisco Catalyst 2960X увеличена эффективность полосы пропускания за счет использования расширенных возможностей управления качеством обслуживания (QoS). Например, доступна настройка по IP-адресу отправителя/получателя, MAC-адресу отправителя/получателя, по данным в заголовках QoS. Имеется строгая очередь приоритетов (Strict priority queuing), гарантированная полоса пропускания виртуального канала до 1 Мбит/с. Улучшена отказоустойчивость сети. Для более легкой координации асинхронных потоков в коммутаторах Cisco Catalyst 2960X использованы средства входящего контроля и ограничения трафика.

В устройстве Cisco Catalyst 2960X поддерживаются списки прав доступа ACL и широковещательные службы. ACL могут быть созданы по портам.

Отбор осуществляется по MAC-адресам - доступ к сети получают устройства, адреса которых указаны в списках.

Cisco Catalyst 2960X работают с протоколом IEEE 802.1w Rapid Spanning Tree Protocol 02.1x и позволяют назначать виртуальную сеть на пользователя (VLAN).

Поддерживаются протоколы удаленного контроля, передачи файлов SSHv2 и протокол управления связью SNMP в третьей версии.

При создании нашей сети будут задействованы коммутаторы с 48 портами. Так как для текущего количества человек в нашей организации одного такого коммутатора будет мало, нам потребуются три таких коммутатора, по одному на этаж.

Для маршрутизации трафика между ними выбран коммутатор 3 уровня модели OSI Cisco Catalyst WS-C3650-24TD. Данный коммутатор поддерживает IP маршрутизацию, то есть он может не только разбить сеть на виртуальные сегменты, но и маршрутизировать трафик между этими сегментами. Использоваться он будет как коммутатор, находящийся на уровне распределения, и будет предназначаться для агрегирования коммутаторов уровня доступа.

Его необходимость в проектируемой сети актуальна из-за большого количества коммутаторов. Главная цель — это избежать соединения коммутатор-коммутатор и иметь возможность расширять сеть в будущем без осложнений.

Для выхода в глобальную сеть и для маршрутизации трафика с филиалами организации будет задействован маршрутизатор Cisco 4451, который будет находиться на уровне ядра сети.

Маршрутизатор Cisco 4451 – является одним из лучших интегрированных решений для малого бизнеса или организации работы удаленных офисов. Так как в организации не больше 200 человек, его мощности вполне хватит для функционирования проектируемой сети.

Данный маршрутизатор функционирует на 3 уровне модели OSI и будет использоваться для выхода в сеть Интернет.

Главные его достоинства это:

- функция IP маршрутизации;
- NAT (подмена локального IP адреса на внешний IP адрес, который виден в интернете);
- VPN (для объединения центрального офиса и филиалов в одну сеть);
- межсетевой экран для организации безопасности.

2.5. Выбор оборудования для филиалов

Подобрав оборудование для центрального офиса, приступим к филиалам. Так как филиалы по численности сотрудников будут намного меньше, требования к оборудованию тоже снизятся.

В качестве коммутаторов уровня доступа в филиалах будут выступать коммутаторы фирмы Cisco Catalyst C1000-16P-2G-L, с ограниченным количеством портов до 16 штук. Данного количества портов вполне хватит на маленький опер-зал и охрану в филиалах. Ведь основная функция дополнительных офисов – это выполнение денежных операций, направленных исключительно на обслуживание клиентов.

На уровне распределения будет находиться маршрутизатор Cisco 1841. Он же будет считаться оборудованием уровня ядра.

Подводя итоги, сведём все выбранное сетевое оборудования в одну таблицу 2.5.1

Таблица 2.5.1. - Необходимое сетевое оборудование для проектирования сети.

Наименование оборудования	Модель оборудования	Необходимое количество
Центральный офис «Павелецкий»		
Коммутатор	Cisco Catalyst WS-C2960X-48LPS-L	3

Коммутатор (L3)	Cisco Catalyst WS-C3650-24TD	1
Маршрутизатор	Cisco 4451	1
Наименование оборудования	Модель оборудования	Необходимое количество
Дополнительный офис «Лубянка»		
Коммутатор	Cisco C1000-16P-2G-L	1
Маршрутизатор	Cisco 1841	1
Дополнительный офис «Пражская»		
Коммутатор	Cisco C1000-16P-2G-L	1
Маршрутизатор	Cisco 1841	1

В исходных данных в параграфе 2.1, предполагалось, что на каждом этаже головного офиса и каждом филиале будет находиться серверная комната, выделенная для сетевого оборудования и коммутации розеток. Приведем схему подключения оборудования в серверных комнатах (рисунок 2.2).

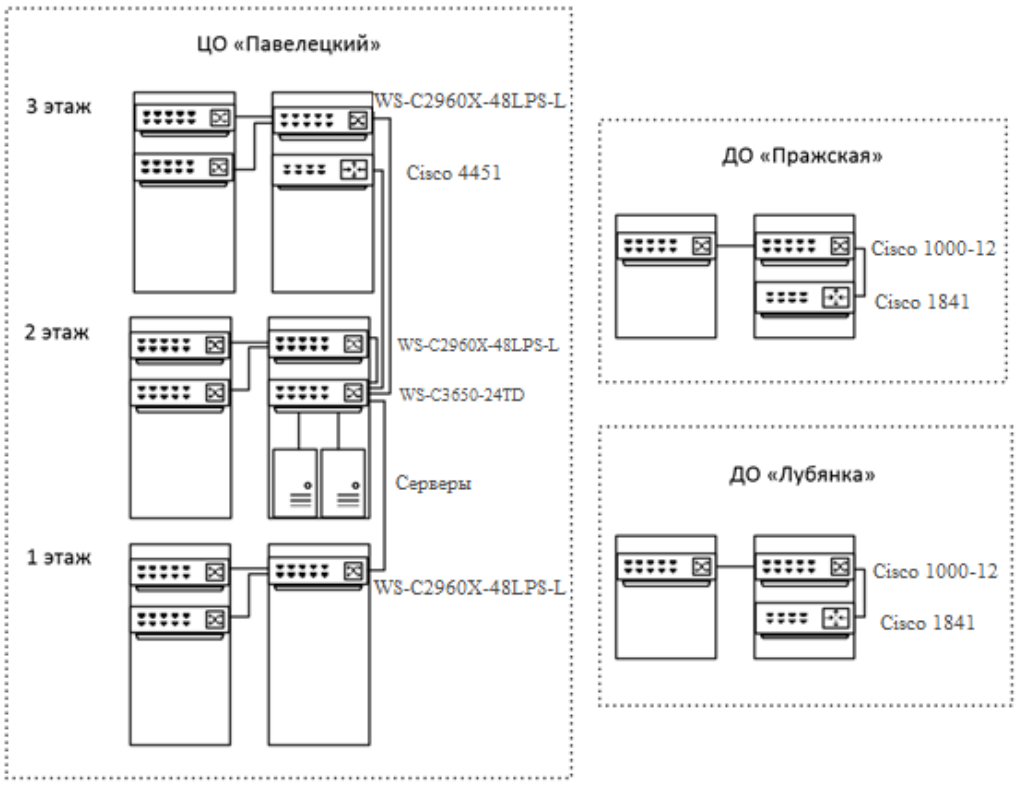

Рисунок 2.2 – Схема оборудования в серверных комнатах.

На рисунке 2.2 левая часть подключения — это коммутационные патч-панели, ведущие к рабочим местам сотрудников, справа – установленное сетевое оборудование. Серверы будут установлены также в серверной комнате, для упрощения подключения и обслуживания.

2.6. Разработка физической схемы сети

Все физические подключения и количество человек в каждой сети изображено на рисунке 2.3. На рисунке можно увидеть, что все подключения «коммутатор – рабочие станции» реализованы технологией Fast Ethernet. Ее вполне хватит для комфортной работы в сети. Для соединения между коммутаторами уровня доступа и распределения, а также между коммутатором уровня распределения и маршрутизатором уровня ядра используется технология Gigabit Ethernet, так как данные сегменты должны иметь большую пропускную способность.

В филиалах реализована только технология Fast Ethernet. Это обуславливается небольшим количеством человек в них.

Пунктиром на рисунке обведены виртуальные локальные сети и главные сегменты сети. К главным сегментам относятся головной офис «Павелецкий» и его филиалы «Пражская» и «Лубянка».

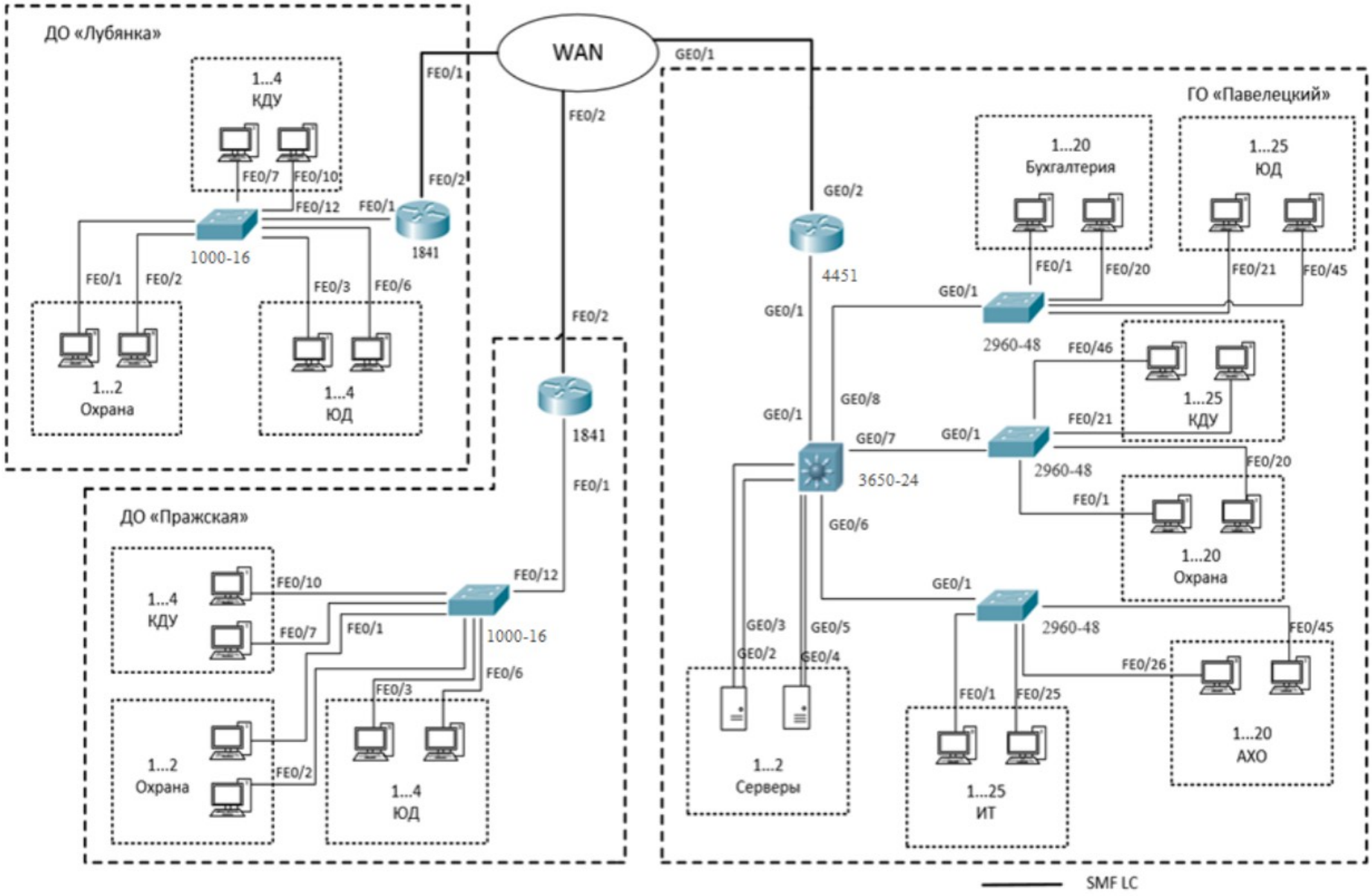

Рисунок 2.3 – Структурная схема сети

2.7. Расчет плана IP-адресации и использование VLAN

Как одна из многих важных вещей в проектировании сети связи выступают виртуальные локальные сети (VLAN - Virtual Local Area Network). Собой они представляют группу устройств, которые имеют возможность взаимодействовать друг с другом напрямую на канальном уровне, не учитывая то, что физически могу быть подключены к разным коммутаторам. Если же устройства будут находиться в разных VLAN, они будут невидимы друг для друга на канальном уровне, даже если подключены к одному коммутатору и связь между ними возможна только на сетевом и более высоких уровнях. Используются VLAN в основном для построения логических топологий сети и уменьшения широковещательного трафика. Другими словами, VLAN увеличивает возможность управляемости сети, это упрощение применений разных политик и правил безопасности. В этом случае их можно будет применить к целой сети, а не к каждому устройству отдельно. Для организации VLAN используется открытый стандарт IEEE 802.1Q.

Так как в организации имеются разные подразделения, рационально было бы поместить каждый отдел в свой VLAN. Серверы тоже должны быть определены в отдельный VLAN.

Все созданные подсети можно увидеть в таблице 2.7.1.

Таблица 2.7.1 – Разбиение сети на отдельные VLAN для каждого подразделения

Наименование подразделения	Диапазон IP адресов	Маска подсети	Номер VLAN
Отдел бухгалтерии (Бухгалтерия)	192.168.1.0 – 192.168.1.63	255.255.255.192	2
Департамент обеспечения безопасности (Охрана)	192.168.1.64 - 192.168.1.127	255.255.255.192	3
Кредитно-депозитное управление (КДУ)	192.168.1.128 - 192.168.1.255	255.255.255.128	4

Таблица 2.7.1 – Разбиение сети на отдельные VLAN для каждого подразделения (продолжение)

Наименование подразделения	Диапазон IP адресов	Маска подсети	Номер VLAN
Отдел информационных технологий (ИТ)	192.168.2.0 - 192.168.2.127	255.255.255.128	5
Юридический департамент (ЮД)	192.168.2.128 - 192.168.2.255	255.255.255.128	6
Отдел обеспечения (АХО)	192.168.3.0 - 192.168.3.63	255.255.255.192	7
Серверы	192.168.3.64 – 192.168.3.95	255.255.255.224	8

2.8. Разработка логической схемы сети

Разбив все подразделения на VLAN, построим логическую схему сети (рисунок 2.4). На данной схеме можно увидеть, как элементы сети взаимодействуют между собой, какой путь преодолевает передаваемая информация.

На рисунке 2.4 показано, что каждое подразделение находиться в своем VLAN, в своей отдельной сети.

Маршрутизаторы Cisco 1821 и Cisco 4451 будут использоваться как каналообразующее оборудование для связи головного офиса и прилегающих филиалов с применением технологии VPN.

VPN (виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети, например Интернет.

Технология VPN будет использоваться для объединения сегментов корпоративной сети.

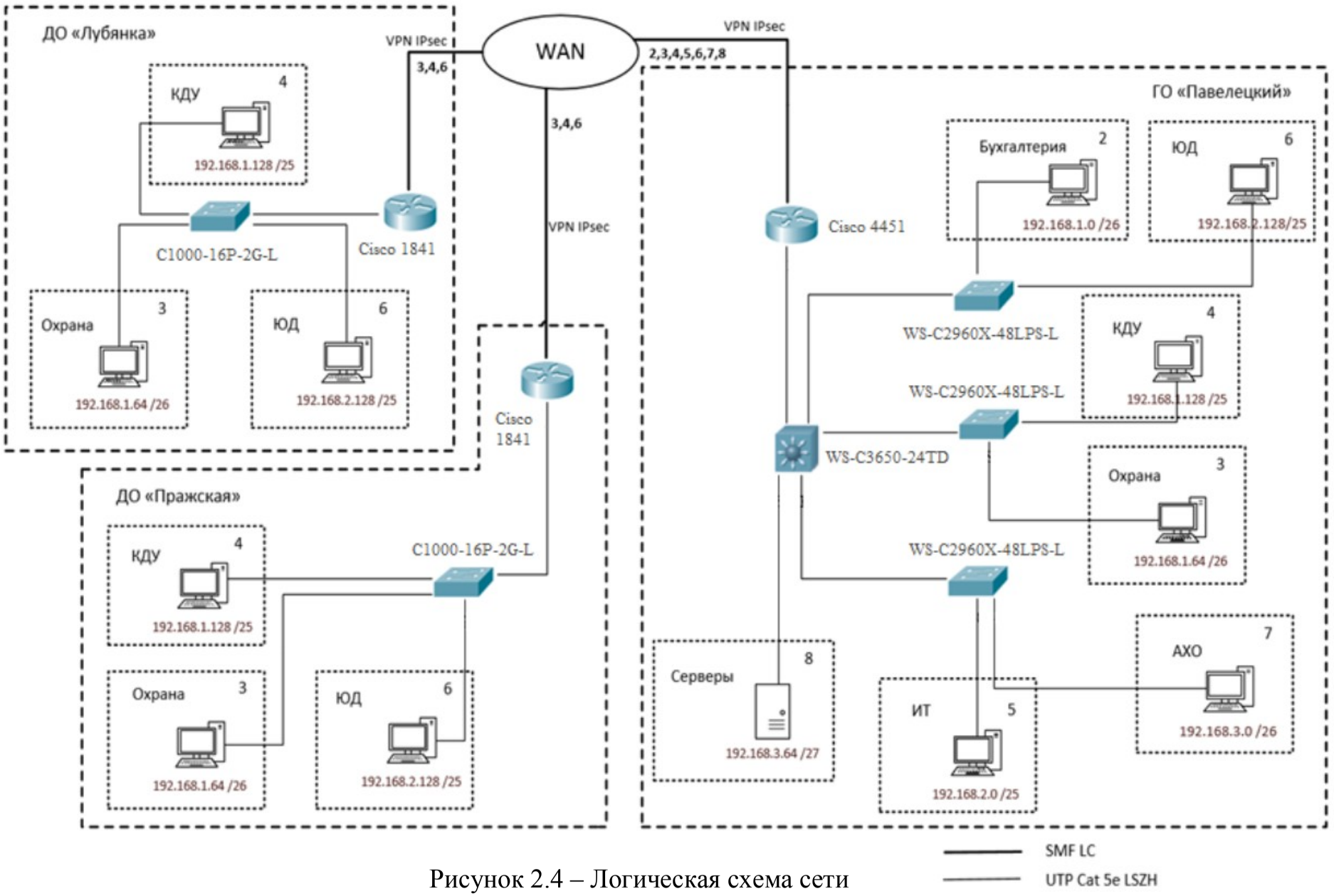

Рисунок 2.4 – Логическая схема сети

Технология VPN реализована на основе протокола IPsec для создания общей локальной сети между центральным офисом и филиалами.

IPsec (IP Security) – набор протоколов для организации защиты данных, передаваемых по межсетевому протоколу IP. Данные наборы протоколов позволяют осуществить аутентификацию (подлинность), проверку целостности и шифрование IP пакетов. Также в состав IPsec входят протоколы для обмена ключами в глобальной сети Интернет. Главная применение – организация VPN-соединений. В настоящее время используются стандарты RFC 2401- RFC 2412.

Устанавливается соединение между двумя сторонами, которое называется Security Association (SA). Соединение SA является однонаправленным. При этом стоит отметить, что стандарты IPsec дают возможность конечным точкам защищенного канала использовать как одно соединение (SA), так и произвольное их число, что будет увеличивать степень детализации защиты. Установка соединения начинается с взаимной аутентификации обеих сторон. Далее происходит выбор параметров (шифрование, проверка целостности данных) и необходимые протоколы передачи данных AH или ESP.

Отличия структуры пакетов при использовании идентификаторов протокола безопасности можно посмотреть на рисунке 2.5.

Рисунок 2.5 – Протоколы защиты данных (AH и ESP)

2.9. Организация маршрутизации в разрабатываемой сети

Маршрутизация – это процесс определения пути следования информации в сетях связи. Маршрутизация в проектируемой сети будет выполняться специальными программно-аппаратными средствами – маршрутизаторами.

В рамках настоящей работы будет использоваться протокол маршрутизации EIGRP. Данный протокол разработан компанией Cisco для маршрутизации в сетях с использованием сетевого оборудования Cisco. К преимуществам данного протокола можно отнести применяемый в его составе алгоритм Route Poisoning, который способен предотвращать возникновение маршрутных петель.

Таблицы маршрутизации всех маршрутизаторов со списком распространяемых ими сетей показаны на рисунке 2.6.

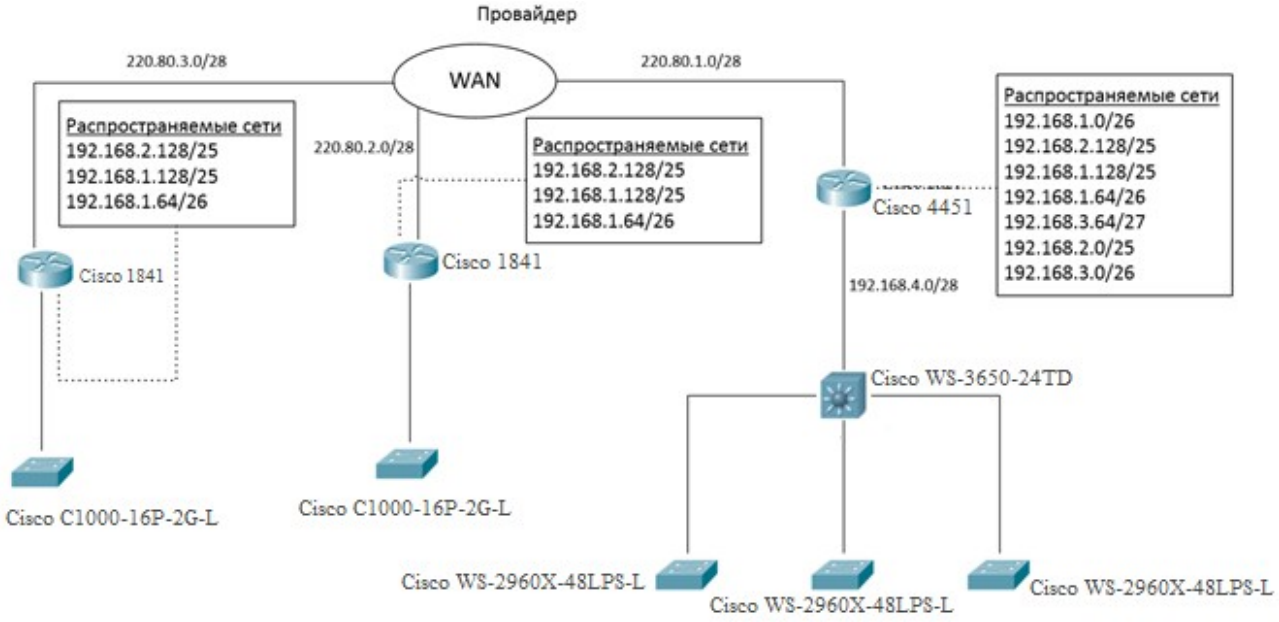

Рисунок 2.6 - Таблицы маршрутизации. Распространяемые сети

2.10. Виртуализация серверной подсистемы

Перед тем как переходить к вопросу виртуализации серверной подсистемы, необходимо понять, какие функции будут ей выполняться в сети.

В организации должно быть реализовано следующее:

- Принт-сервер – сервер, с установленной на нем операционной системой, содержащей подключения ко всем имеющимся в организации принтерам, которые находятся в открытом, общем доступе для всех пользователей внутри корпоративной сети. Данный сервер необходим для упрощения подключения и обслуживания принтеров.
- Файловый сервер – сервер, который имеет большой объем памяти для хранения данных, которые также должны быть общедоступны для пользователей, находящихся внутри сети организации.
- Сервер баз данных – сервер, с установленной на нем операционной системой и СУБД, на базе которой развернута та или иная база данных. Например, база данных 1С. Данный сервер выполняет обслуживание и управление базой данных и отвечает за целостность и сохранность данных, а также обеспечивает операции ввода-вывода при доступе клиента к информации.
- Почтовый сервер – сервер, на котором развернут программный продукт Microsoft Exchange Server 2019 для обмена сообщениями и совместной работы.
- Контролер домена. Сервер, контролирующий область компьютерной сети (домен). Запускает службы Active Directory. Контроллеры домена хранят данные каталога и управляют взаимодействиями пользователя и домена, включая процессы входа пользователя в систему, проверку подлинности и поиски в каталоге.

В обычном случае, для каждого из перечисленных серверов потребовался бы отдельный программно-аппаратный комплекс. Технология виртуализации позволяет минимизировать затраты на аппаратные и программные компоненты, электроэнергию, охлаждение и их обслуживание, таким образом позволяя снизить капитальные и эксплуатационные затраты на информационную сеть.

В данном случае осуществляется виртуализация серверной подсистемы для достижения более рационального использования ресурсов серверов.

Организация будет иметь 2 сервера со схожими характеристиками. Характеристики этих двух серверов приведены в таблице 2.10.1.

Таблица 2.10.1. - Характеристики серверов виртуализации

Процессор	INTEL® Xeon® CPU E5-2680 v2 @2.80GHz 2.80 GHz (2 processors)
Оперативная память	32,0 GB памяти DDR3 ECC Reg (512GBMAX)
Жесткий диск	6 дисков 450ГБ SAS 10 тыс. об/мин
Сетевое оборудование	2-портовый контроллер GbE Intel I350T2

Имея серверы, также было бы рационально использовать внешнее сетевое хранилище данных (СХД). Разница внешнего СХД и обычными внутренними дисками в первую очередь заключается в надежности, объеме и скорости.

Для серверов будет использоваться система хранения данных HP StoreVirtual 4130, представляющая собой архитектурное решение для подключения устройств хранения данных, таких как ленточные библиотеки, дисковые массивы, оптические приводы таким образом, чтобы операционная система, подключенная к данной СХД, распознавала подключенные ресурсы как локальные. Такую СХД сеть хранения данных называют SAN (Storage Area Network). Данный СХД будет подключаться к коммутатору 3 уровня Cisco WS-C3650-24TD.

Существует несколько типов систем хранения данных: SAN, NAS, DAS.

DAS – внешняя память, которая напрямую подсоединена к компьютеру и используется только им.

NAS – говоря простым языком, это выделенный файловый сервер с подключенной к нему дисковой подсистемой. В состав ее иногда может входить оптическая или ленточная библиотека. Данные сервер напрямую подключается в сеть и представляет хостам доступ к файлам на своей интегрированной подсистеме внешней памяти. Использует такие протоколы как: NFS, FTP, SFTP, HTTP и др.

Выбранный тип СХД - SAN. Данное оборудование будет работать по протоколу ISCI через TCP\IP.

Технические характеристики внешнего СХД HP StoreVirtual 4130 G2 приведены в таблице 2.10.2.

Таблица 2.10.2. - Технические характеристики СХД HP Store Virtual 4130

Емкость	от 2,4 ТБ максимум 76,8 ТБ
Описание накопителя	4 диска SAS малого типоразмера
Интерфейс массива	4 порта 1 GbE iSCSI
Функции обеспечения доступности	- резервные блоки питания с возможностью горячей замены - резервные вентиляторы - резервные жесткие диски с возможностью горячей замены, встроенный контроллер хранения данных с автономным кэш-буфером на флэш-памяти диск RAID 5 - сверхизбыточная кластеризованная система хранения - сетевой RAID уровней 0, 5, 6, 10, 10+1 и 10+2 (для каждого тома) с возможностью создания до четырех копий данных
Совместимые операционные системы	Apple OS X. Citrix Xen Server, HP-UX, IBM AIX, Microsoft Windows Server 2008, Microsoft Windows Server 2012, Novell NetWare, Oracle Enterprise Linux, Red Hat Linux, Oracle Solaris, SUSE Linux, VMware

Виртуализация серверов будет организована с помощью программных продуктов: VMware ESXi и VMware vSphere. VMware ESXi – это лучший в отрасли специализированный аппаратный гипервизор.

Гипервизор – программный продукт или аппаратная схема, обеспечивающая или позволяющая синхронную, параллельную реализацию нескольких операционных систем на одном и том же хост-компьютере. Гипервизор также гарантирует изоляцию ОС друг от друга, защиту и надежность, распределение ресурсов между разными запущенными ОС и регулирование ресурсами. Гипервизор непосредственно в определенном роде сам считается минимальной операционной системой. Он дает запущенным под его управлением операционным системам сервис виртуальной машины, виртуализируя или эмулируя действительное (физическое) аппаратное обеспечение конкретной машины, и распоряжается этими виртуальными машинами, выделением и освобождением ресурсов для них. Гипервизор дает возможность независимого «включения», перезагрузки, «выключения» любой виртуальной машины. При этом операционная система, функционирующая в виртуальной машине под управлением гипервизора, имеет возможность, но не обязана «знать», что она выполняется в виртуальной машине, а не на настоящем аппаратном обеспечении.

Гипервизоры бывают двух видов.

Гипервизоры, устанавливаемые на аппаратную часть (рисунок 2.7).

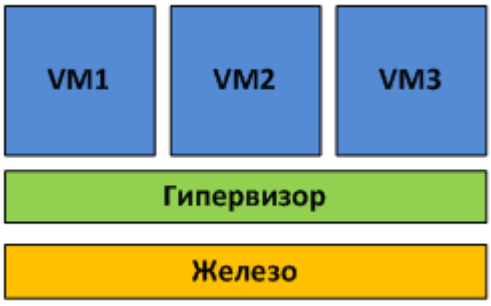

Рисунок 2.7 – Гипервизор, устанавливаемый на аппаратную часть.

Работа гипервизоров непосредственно с оборудованием позволяет достичь большей производительности, надежности и безопасности.

К примеру, такие гипервизоры используются во многих решениях Enterprise-класса: Microsoft Hyper-V, VMware ESXi Server, Citrix Xen Server

И второй вид – это программные гипервизоры, встроенные в ОС (рисунок 2.8).

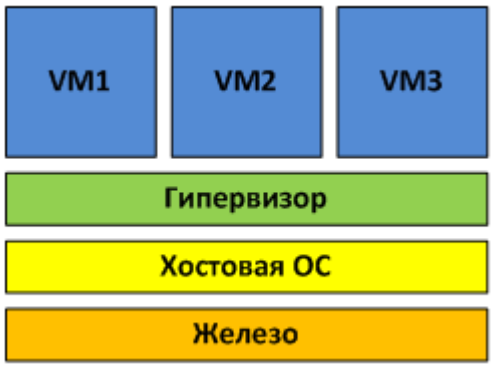

Рисунок 2.8 – Гипервизор, встроенный в ОС

Виртуальные машины при этом запускаются в пользовательском пространстве хостовой ОС, что не самым лучшим образом сказывается на производительности.

Примерами программных гипервизоров служат MS Virtual Server и VMware Server, а также продукты виртуализации рабочих станций – MS Virtual PC и VMware Workstation.

По архитектуре гипервизоры можно разделить на 2 типа: монолитная и микроядерная.

Гипервизоры монолитной архитектуры включают драйверы аппаратных устройств в свой код (рисунок 2.9).

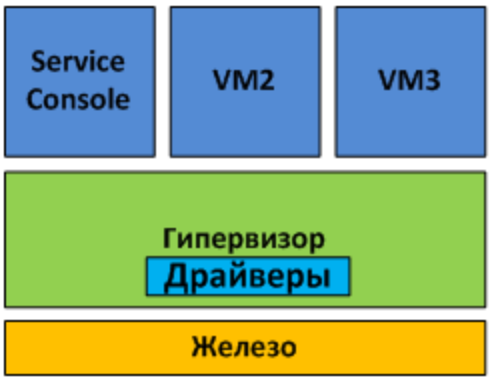

Рисунок 2.9 - Монолитная архитектур.

Монолитная архитектура обладает своими плюсами и минусами. Среди плюсов можно выделить:

- более высокую продуктивность из-за определения драйверов в пространстве гипервизора;
- более высокую надежность, так как перебои в работе правящей ОС (в определениях VMware – «Service Console») не повергнет к сбою все запущенные виртуальные машины.

Минусы монолитной архитектуры:

- имеет поддержу лишь то оборудование, драйверы на которое присутствуют в гипервизоре. Из-за этого поставщик гипервизора обязан плотно кооперироваться с поставщиками оборудования, для того чтобы драйвера для работы всего новейшего оборудования с гипервизором своевременно писались и добавлялись в код гипервизора. По тому же фактору при переходе на новенькую аппаратную платформу может потребоваться переход на другую версию гипервизора, и напротив – при переходе на новенькую версию гипервизора может потребоваться замена аппаратной платформы, так как прошлое оборудование уже не сопровождается поддержкой.
- вероятна невысокая безопасность – из-за подключения в гипервизор стороннего кода в облике драйверов устройств. Так как код драйверов исполняется в пространстве гипервизора, есть абстрактная вероятность пользоваться уязвимостью в коде и заполучить контроль как над хостовой ОС, так и над абсолютно всеми гостевыми.

Наиболее часто встречаемым образцом монолитной архитектуры является VMware ESXi.

При микроядерной архитектуре драйверы устройств функционируют внутри хостовой ОС (рисунок 2.10). Хостовая ОС в данном случае запускается в таком же виртуальном окружении, как и все ВМ, и называется «родительской партицией». Все другие окружения называются «дочерние». Единственная разница между родительской и дочерними партициями заключается в том, что лишь родительская партиция имеет конкретный доступ к оборудованию

сервера. Выделением памяти же и планировкой процессорного времени занят сам гипервизор.

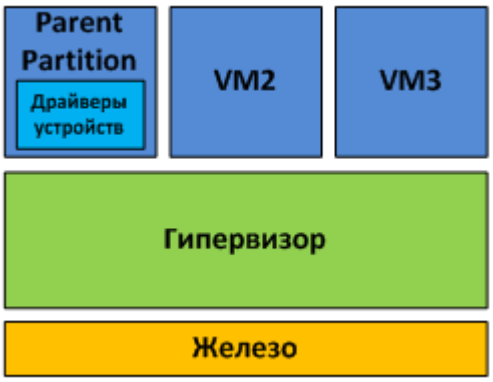

Рисунок 2.10 - Микроядерная архитектура.

Плюсы у данной архитектуры следующие:

- Нет необходимости в драйверах, «заточенных» под гипервизор. Гипервизор микроядерной архитектуры совместим с любым оборудованием, располагающим драйверами для ОС.
- Так как драйвера исполняются внутри родительской партиции – у гипервизора остается преимущественно много времени на наиболее необходимые задачи – контроль памяти и работу планировщика.
- Наиболее высокая безопасность. Гипервизор не включает постороннего кода, поэтому и перспектив для атаки на него остается меньше.

Наиболее колоритным образцом микроядерной архитектуры считается, собственно, продукт Microsoft Hyper-V.

ESXi оборудован интегрированными драйверами, не находится в зависимости от операционной системы. Устанавливается на физический сервер (аппаратную часть) и делит его на некоторое количество логических серверов. Клиенты имеют все шансы применять продукт ESXi бесплатно совместно с ПО vSphere Hypervisor или приобрести его в составе коммерческой редакции vSphere.

Виртуальные машины, функционирующие на базе vSphere ESXi, дают следующие возможности:

- поддержка до 128 виртуальных ЦП на виртуальной машине;

- поддержка до 4 Тбайт ОЗУ;
- поддержка устройств USB 3.0 новейшим контроллером xHCI;
- поддержка до 120 устройств на виртуальную машину вследствие нового интерфейса Advanced Host Controller Interface (AHCI);
- максимальный объем VMDK-диска - 62 Тбайт;
- возврат дискового пространства в пул ресурсов при освобождении хранилища гостевой ОС;
- усовершенствованная технология виртуализации ЦП предполагает передачу виртуальной машине наиболее детальных данных об архитектуре ЦП узла. Это дает наиболее обширные возможности для отладки, регулировки и ликвидации неисправностей операционных систем и приложений на данной виртуальной машине.

Узлы vSphere ESXi можно подсоединить к домену Active Directory. В следствии этого Active Directory будет способен приводить проверку подлинности пользователей и ликвидирует надобность в создании локальных пользовательских учетных записей на каждом узле. Сам гипервизор от VMware является бесплатным при регистрации на сайте и активации с помощью ключа, указанного там же. Без активации данная программа работает только 60 дней. Минусом бесплатного гипервизора VMware ESXi является то, что он не предполагает технической поддержки, так что, если будет необходима техническая поддержка, придется все-таки приобретать платную версию. Для установки будет взята версия VMware ESXi 6.5.

После установки данного ПО, производится его настройка: задается пароль для корневых пользователей root, назначаются сетевые настройки сервера и возможность настройки его по сети.

На данном этапе основные настройки гипервизора считаются законченными. Для конфигурирования и уже создания виртуальных машин на этом сервере, используется программа VMware vSphere Client 6.5, которую можно поставить на любой другой ПК в той же сети что и сервер и иметь

удаленный доступ по настройке данного сервера и создания в нем виртуальных машин.

После подключения к хосту ESXi с помощью программы VMware vSphere Client 6.5 получаем следующие основные возможности:

- создать виртуальную машину (New Virual Machine);
- создать Resource Pool (возможность настройки использования ресурсов физического сервера виртуальными машинами);
- подключение к СХД (системе хранения данных).

После установки всех необходимых программ, с помощью программы VMware vSphere Client 6.5, на серверах появится возможность развернуть все необходимые виртуальные машины для ранее перечисленных функций: принт-сервер, файл-сервер и т.д. Тем самым будем иметь ограниченное количество машин для обслуживания.

Так как в организации не очень большое количество людей, ресурсов двух серверов, характеристики которых предоставлены в таблице 2.10.1, вполне хватит.

Выделение ресурсов под основные задачи отображены в таблице 2.10.3.

Таблица 2.10.3. - Выделение ресурсов для каждой изолированной среды

Наименование сервера	Кол-во ядер	Частота процессора (МГц)	Оперативная память (ОЗУ Gb)	Физическая память (Гб)
Принт-сервер	3	2800	4	300
Файловый сервер	3	2800	16	6000
Сервер баз данных	5	2800	20	1000
Почтовый сервер	5	2800	12	6000
Контролер домена	4	2800	8	200

2.11. Пример установки программного обеспечения для виртуализации

серверной подсистемы

Для развертывания технологии виртуализации и дальнейшего управления ею необходимо два программных продукта: VMware ESXi 6.5 и VMware vSphere Client 6.5.

Первым шагом нужно установить VMware ESXi 6.5. Для этого образ установщика «.ISO» записывается на диск или флеш-носитель. Сам образ можно взять с официального сайта VMware. Дальше с помощью записанного образа, выбрав нужный носитель, начинаем локально устанавливать ПО на будущий наш сервер. Начнется установка (рисунок 2.11 и рисунок 2.12).

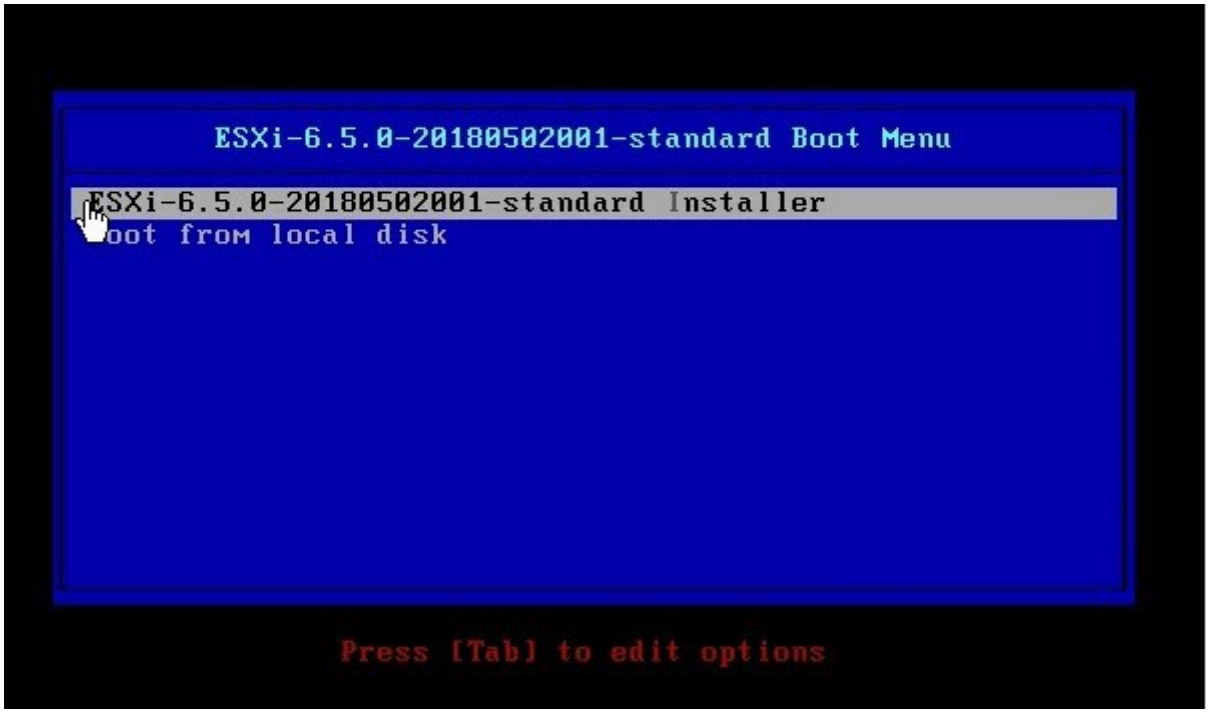

Рисунок 2.11 – Загрузка установщика WMware ESXi 6.5

Рисунок 2.12 – Загрузка установщика WMware ESXi 6.5

После этапа, изображенного на рисунках 2.11 и 2.12 установщик будет проверять технические характеристики сервера. Минимальные технические характеристики для сервера при установке VMware ESXi – это количество процессоров больше одного и 4 ГБ оперативной памяти. Также процессор сервера должен поддерживать аппаратную виртуализацию (Intel Virtualization Technology или AMD Virtualization).

Далее программа установщик выводит приветственное сообщение и по нажатии начинает проверку совместимости оборудования. Если и бывают ошибки при установке, то, как правило только на этапе проверки совместимости. Самый распространённые проблемы – это проблемы, связанные с сетевыми драйверами. Поэтому, перед тем как ставить данный продукт, необходимо сверять драйверы сетевых адаптеров с поддерживаемыми версиями.

Далее происходит выбор постоянного запоминающего устройства (ПЗУ) (рисунок 2.13) и выбор локализации (рисунок 2.14).

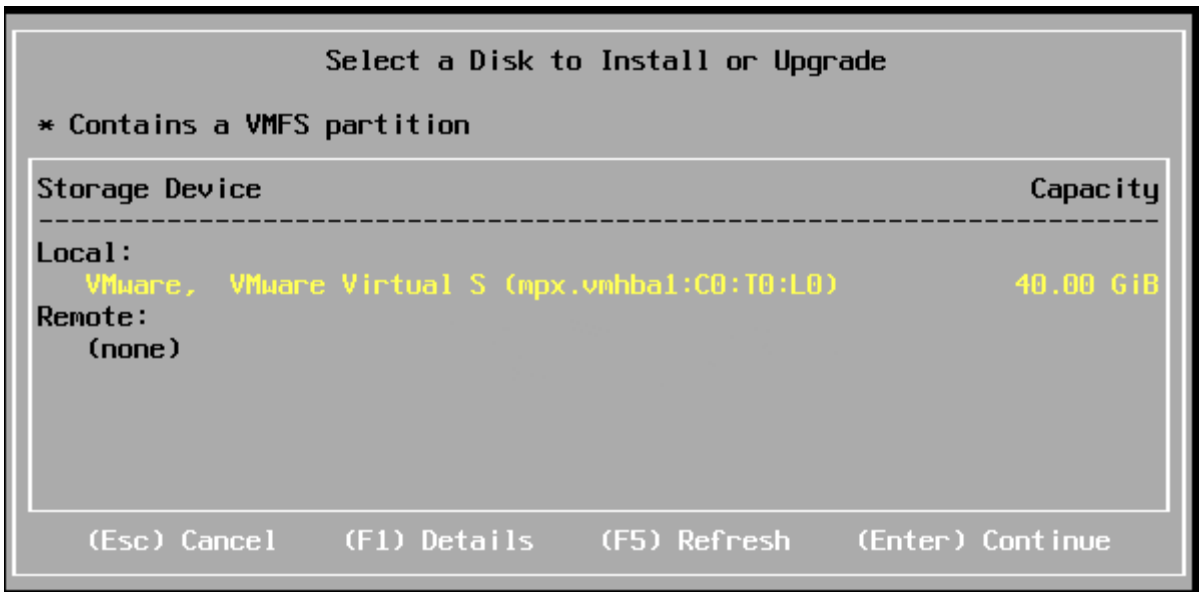

Рисунок 2.13 – выбор ПЗУ для установки

Рисунок 2.14 – Выбор локализации

После этапа выбора локализации необходимо ввести пароль администратора, он будет необходим для подключения с помощью программы VMware vSphere Client 6.5 к уже настроенному серверу (рисунок 2.15).

После подтверждения установки, начнется установка гипервизора ESXi (рисунок 2.16).

Рисунок 2.15 – Ввод пароля администратора

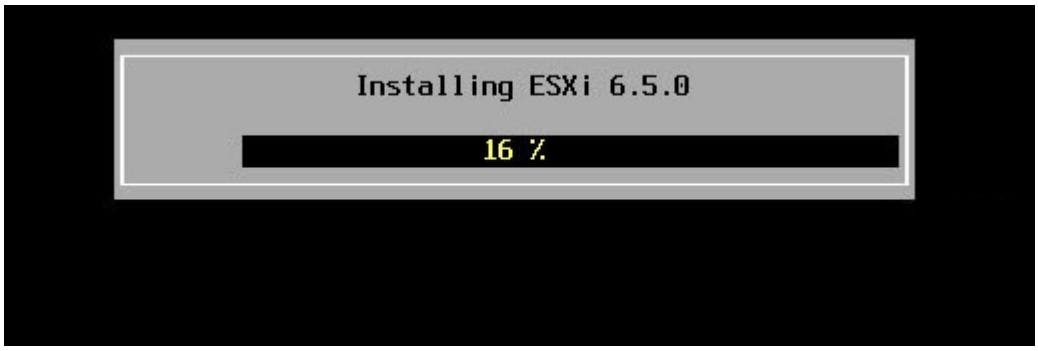

Рисунок 2.16 – Процесс установки

На этом установка завершена, о чем будет говорить соответствующее сообщение.

После перезагрузки, с помощью пароля администратора необходимо зайти в настройки (рисунок 2.17). Здесь необходимо выставить статический IP-адрес. Для этого будет необходимо зайти в пункт «Configure Management

Network» и выставить статический IP-адрес.

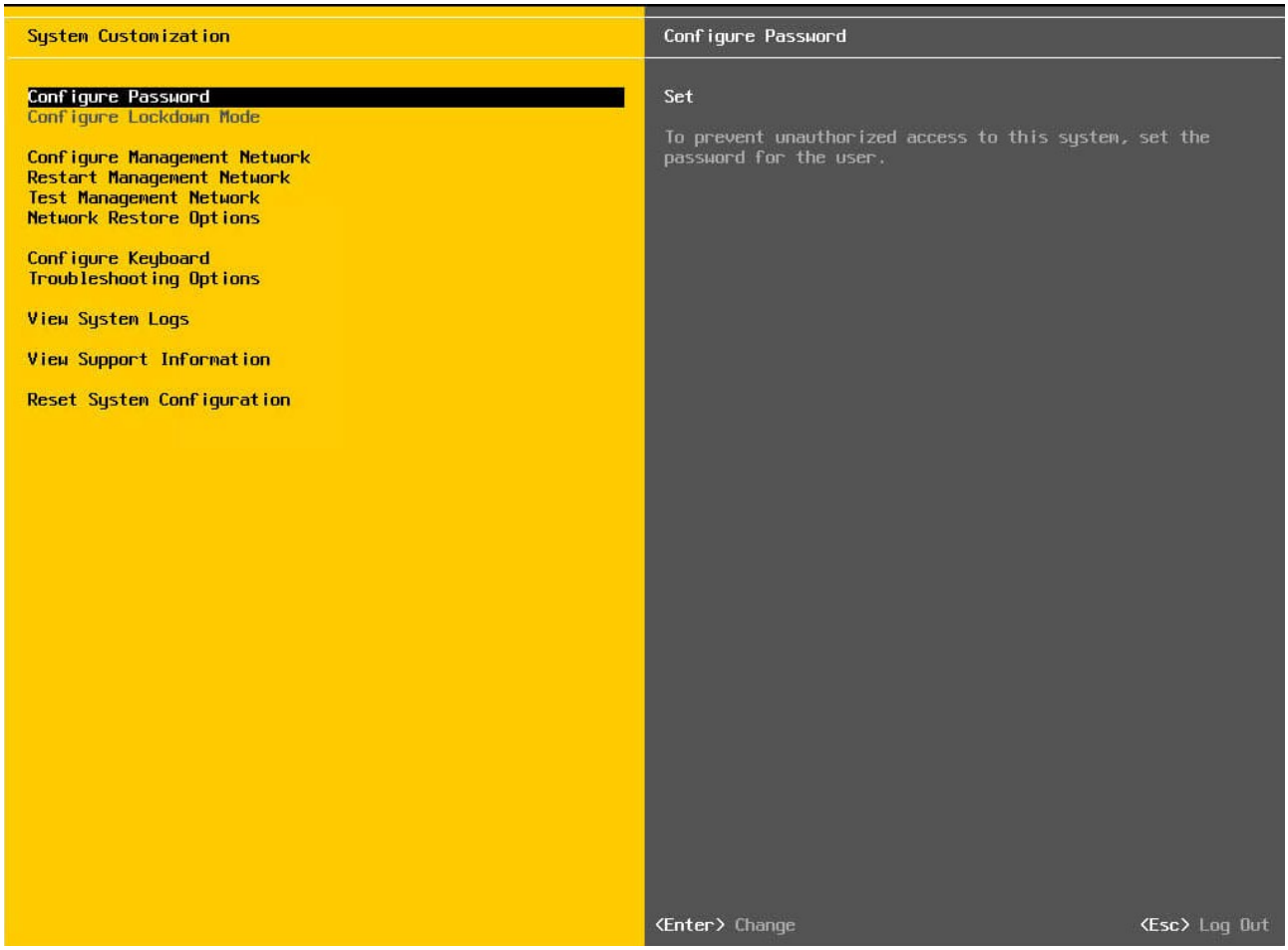

Рисунок 2.18 – Пункты настроек сервера

После произведенных настроек все манипуляции на сервере прекращаются. Последующее управление производится через программу VMware vSphere Client 6.5 с любого компьютера в той же сети, что и сервер. Для подключения понадобится IP-адрес или имя сервера и пароль администратора, который вводили при установке сервера. Интерфейс управления представлен на рисунке 2.19.

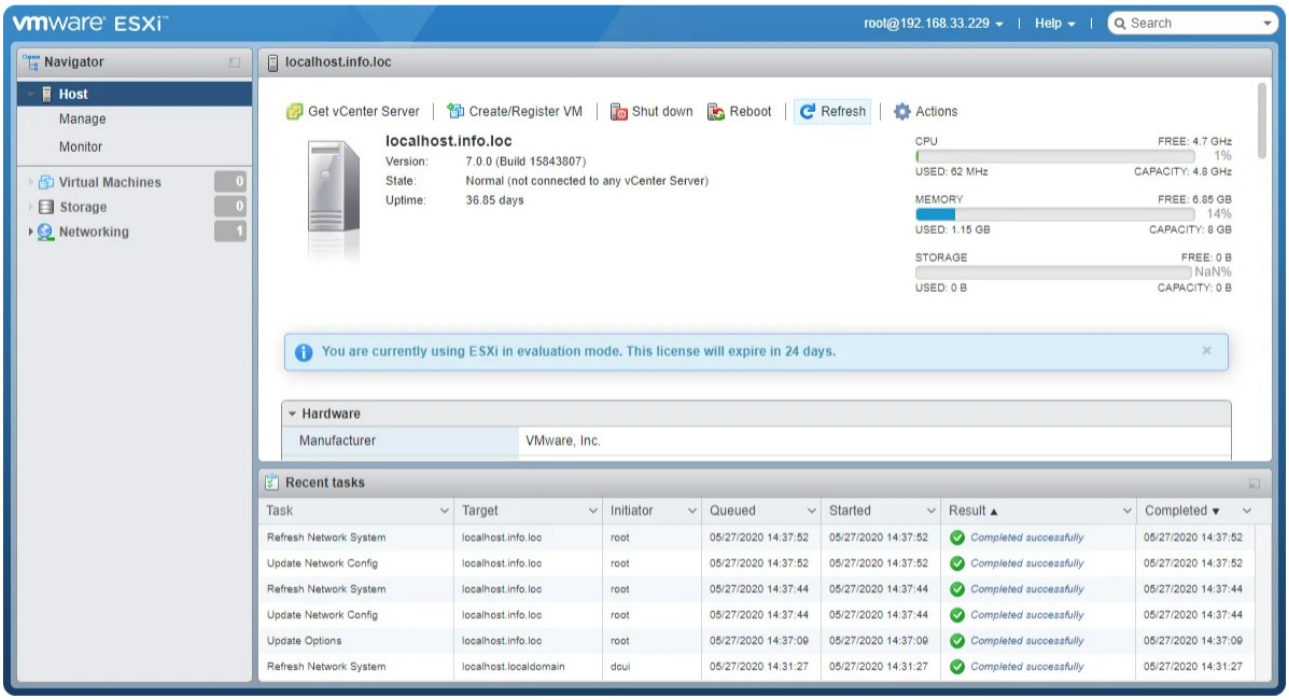

Рисунок 2.19 – Интерфейс управления

2.12. Выводы

Во втором разделе было рассмотрено создание сети связи. Были определены исходные данные для создаваемой сети, такие как сфера деятельности организации, ее численность, входящие в нее подразделения и наличие у нее отдаленных филиалов. Для проектируемой сети была выбрана топология «звезда» и определена архитектура сети. Произведен подбор сетевого оборудования согласно иерархической модели сети с указанием его технических характеристик для центрального офиса и филиалов.

Как наглядная демонстрация была приведена структурная схема сети с изображением на ней всего выбранного оборудования и методом его подключения. Для представления пути прохождения данных по сети была построена логическая схема и схема маршрутизации с распространяемыми ими сетями.

Внедрение и адаптация для проектируемой сети технологии виртуализации показало, что ее внедрение зачастую не представляет сильных проблем, но в итоге решает значительные проблемы с рациональным распределением мощностей на серверах. На примере внедрения виртуализации

в проектируемую сеть был произведен выбор поставщика технологии виртуализации, описаны виды виртуализации и основные понятия. Также приведен пример установки платформы на сервер и дальнейшее взаимодействие с ним.

3. Расчет основных технических характеристик сети

3.1. Расчет необходимой пропускной способности канала связи, требуемой для передачи данных

Для расчета пропускной способности в проектируемой сети, приведем исходные данные с численностью организации (таблица 3.1.1).

Таблица 3.1.1. - Общая численность терминалов сети

Наименование офиса	Число терминалов сети передачи данных
Павелецкая	135
Лубянка	10
Пражская	10
Итого:	155

В соответствии с исходными данными (таблица 3.1.1), общее количество абонентов, использующих сеть передачи данных, составляет 155 сотрудников.

Нагрузка от абонентов имеет следующие характеристики:

- скорость, требуемая для работы с ресурсами офиса из расчета на одного пользователя, составляет 256 Кбит/с;
- процент одновременно использующих ресурсы офиса сотрудников составляет 50%.

Таким образом, среднее число работников, одновременно использующих ресурсы офиса, составляет:

$135 \cdot 0,5 \approx 68$ человек в центральном офисе.

$10 \cdot 0,5 \approx 5$ человек в каждом филиале.

Требуемая полоса пропускания для передачи данных при одновременном использовании сотрудниками ресурсов составляет:

$68 \cdot 256$ Кбит/с = 17408 Кбит/с для центрального офиса.

$5 \cdot 256$ Кбит/с = 1280 Кбит/с для каждого филиала.

Также рассмотрим необходимую пропускную способность для поддержания видеоконференций в центральном офисе. В филиалах такой

необходимости нет.

При использовании устройств видеоконференцсвязи с поддержкой современных алгоритмов сжатия видеосигнала, таких как H.264, обычно достаточно полосы пропускания канала 256 Кбит/с. Однако, для передачи заголовков IP-пакетов и возможной дополнительной отсылки утерянных данных необходимо резервировать полосу пропускания на 20% больше номинальной скорости видеокодека.

Для организации сеансов видеоконференцсвязи между терминалами, находящимися в удаленных офисах, используется кодек с номинальной скоростью кодирования равной 384 Кбит/с. [11]

Наибольшие требования к каналу связи предъявляются при организации сеанса видеоконференцсвязи с участием, 5 абонентских терминалов видеоконференцсвязи. Для обеспечения возможности организации связи в данном режиме необходимо обеспечить гарантированную пропускную способность в размере:

$$5 \cdot (384 \cdot 1,2) = 2304 \text{ Кбит/с}$$

В соответствии с полученными результатами, минимальная пропускная способность канала связи должна составлять:

17408 Кбит/с + 2304 Кбит/с = 19712 Кбит/с ≈ 19,7 Мбит/с для центрального офиса.

1280 Кбит/с ≈ 1,3 Мбит/с для каждого филиала.

3.2. Определение основных параметров для расчета пропускной способности

Входные параметры рассматриваемой системы включают в себя число абонентов (S), среднее количество запросов на передачу файлов в расчете на одного абонента в пиковый период времени – час (M), пропускную способность (A), средний размер файла (F), средний размер пакета (P), качество обслуживания (вероятность перегрузки) (α).

Пусть информацией, передаваемой по каналам передачи данных, будет трафик веб-страниц, который получают пользователи сети Интернет. Возьмем среднее значение файлов, скачиваемых и отправляемых пользователем сети. Эта информация служит для определения среднего количества запросов на передачу файлов в пиковый период времени M. Средний размер файла F определяется в байтах. Качество обслуживания α выражается через процент времени.

Используя входные данные, необходимо выявить пропускную способность граничного маршрутизатора, то есть количество переданных пакетов в секунду (PPS).

Средняя скорость входящих запросов на передачу файлов (λ) рассчитывается путем умножения количества абонентов (S) на среднее число запросов на передачу файлов на одного абонента в пиковый период времени (M). Среднее время передачи файлов T рассчитывается путем деления среднего размера файла (F) на скорость доступа к линии (A).

Средняя скорость передачи пакетов или веб-страницы вычисляется делением скорости доступа к линии (A) на средний размер пакета (C), а мощность граничного маршрутизатора – умножением наибольшего количества одновременно передаваемых файлов или веб-страниц на среднюю скорость передачи файлов. [12]

Расчет оптимальной пропускной способности будет производиться по сегментам проектируемой сети: центральный офис, дополнительный офис «Лубянка», дополнительный офис «Пражская».

3.3. Расчет оптимальной пропускной способности центрального офиса в разрабатываемой сети

Максимальная пропускная способность коммутатора Cisco Catalyst WS-C2960S-48LPS-L равна 77400000 Mpps (Миллиона пакетов в секунду).

Входные параметры коммутаторов Cisco Catalyst WS-C2960S-48LPS-L

приведены в таблице 3.3.1.

Таблица 3.3.1 - Входные параметры коммутатора Cisco Catalyst WS-C2960S-48LPS-L

Число абонентов	S=45
Ср. кол-во запросов на передачу файлов от одного абонента в час	M=10
Пропускная способность, Мбит/с	A=100
Средний размер файла, байт	F=120000
Средний размер пакета, байт	P=250
Вероятность перегрузки маршрутизатора, %	α =5

Вычислим количество запросов к коммутатору в секунду по формуле 3.3.1:

$$\lambda = \frac{S * M}{3600} \quad (3.3.1)$$

где 3600 = 1час.

$$\lambda = \frac{45 * 10}{3600} = 0{,}125$$

Вычислим время прохождения пакета для заданной пропускной способности сети по формуле 3.3.2:

$$T = \frac{F * 8}{(A * 1048576)} \quad (3.3.2)$$

$$T = \frac{120000 * 8}{104857600} = 0{,}009$$

где 100 Мбит = 100*1024*1024 = 104857600

Получаем количество пакетов, передаваемых маршрутизатору в секунду(PPS) по формуле 3.3.3:

$$PPS = \frac{A/8}{P} \quad (3.3.3)$$

$$PPS = \frac{A/8}{P} = \frac{\frac{100 * 1048576}{8}}{250} = 52428,8 \approx 52429$$

Таким образом, при заданных входных параметрах используемая пропускная способность коммутатора Cisco Catalyst WS-C2960S-48LPS-L равна 52429 пакетов в секунду.

Так как в организации в центральном офисе имеются 3 таких коммутатора с одинаковым количеством подключенных рабочих мест, данный ответ будет уместен для остальных коммутаторов тоже.

Cisco Catalyst WS-C3560E-24TD-S

Максимальная пропускная способность коммутатора Cisco Catalyst WS-C3560E-24TD-S равна 77400000 Mpps (Миллиона пакетов в секунду).

Входные параметры коммутаторов Cisco Catalyst WS-C3560E-24TD-S приведены в таблице 3.3.2.

Таблица 3.3.2. - Входные параметры коммутатора Cisco Catalyst WS-C3560E-24TD-S

Число абонентов	S=8
Ср. кол-во запросов на передачу файлов от одного абонента в час	M=25
Пропускная способность, Мбит/с	A=1000
Средний размер файла, байт	F=120000
Средний размер пакета, байт	P=250
Вероятность перегрузки маршрутизатора, %	α =5

Вычислим количество запросов к коммутатору в секунду по формуле 3.3.1:

$$\lambda = \frac{8 * 25}{3600} = 0,055$$

Вычислим время прохождения пакета для заданной пропускной способности сети по формуле 3.3.2:

$$T = \frac{120000 * 8}{1048576000} = 0{,}0009$$

100 Мбит = 100*1024*1024 = 1048576000

Получаем количество пакетов, передаваемых маршрутизатору в секунду(PPS) по формуле 3.3.3:

$$PPS = \frac{A/8}{P} = \frac{\frac{1000 * 1048576}{8}}{250} = 524288$$

Таким образом, при заданных входных параметрах используемая пропускная способность коммутатора Cisco Catalyst WS-C3560E-24TD-S равна 52429 пакетов в секунду.

3.4. Расчет оптимальной пропускной способности для филиалов в разрабатываемой сети

Максимальная пропускная способность коммутатора Cisco 2950-12 равна 6600000 Mpps (Миллиона пакетов в секунду).

Входные параметры коммутаторов Cisco 2950-12 приведены в таблице 3.4.1.

Таблица 3.4.1. - Входные параметры коммутатора Cisco 2950-12

Число абонентов	S=10
Ср. кол-во запросов на передачу файлов от одного абонента в час	M=10
Пропускная способность, Мбит/с	A=100
Средний размер файла, байт	F=120000
Средний размер пакета, байт	P=250
Вероятность перегрузки маршрутизатора, %	α =5

Вычислим количество запросов к коммутатору в секунду по формуле 3.3.1:

$$\lambda = \frac{10 * 10}{3600} = 0{,}125$$

Вычислим время прохождения пакета для заданной пропускной способности

сети по формуле 3.3.2:

$$T = \frac{120000 * 8}{104857600} = 0{,}028$$

100 Мбит = 100*1024*1024 = 104857600

Получаем количество пакетов, передаваемых маршрутизатору в секунду(PPS) по формуле 3.3.3:

$$PPS = \frac{A/8}{P} = \frac{\frac{100 * 1048576}{8}}{250} = 52428{,}8 \approx 52429$$

Таким образом, при заданных входных параметрах используемая пропускная способность коммутатора Cisco 2950-12 равна 52429 пакетов в секунду.

Так как в организации имеется 2 филиала по 1 коммутатору в каждом, данный ответ будет уместен для обоих коммутаторов.

3.5. Выводы

В данном разделе была подсчитана необходимая пропускная способность для центрального офиса и филиалов для передачи данных и организации видеоконференций: 19,7 Мбит/с для центрального офиса и 1,3 Мбит/с для каждого филиала.

Также были произведены расчеты пропускной способности канала связи для передачи данных. Были определены основные параметры для расчетов. Представлены формулы для вычисления: количества запросов к оборудованию в секунду, время прохождения пакета для заданной пропускной способности и расчет количества пакетов, передаваемых маршрутизатору в секунду (PPS).

Заключение

В данной выпускной квалификационной работе бакалавра основной

целью работы стояла разработка распределенной сети связи с использованием технологии виртуализации.

Для достижения указанной цели перед работой был поставлен ряд задач. В первом разделе был произведен анализ поставщиков технологии виртуализации представленных на российском рынке. Были рассмотрены всевозможные программные продукты и их функционал, процентная доля принадлежащего рынка для каждой рассматриваемой компании.

При анализе, как поставщик технологии виртуализации была выбрана компания WMware.

Во втором разделе перед началом проектирования сети были определены исходные данные. Для разработки сети связи была взята банковская структура, имеющая один центральный офис и 2 филиала, находящиеся в отдаленных частях города. Была определена численность для каждого сегмента организации, это 135 человек в центральном офисе и по 10 человек на каждый филиал. Рассмотрены входящие в организацию подразделения и их функционал.

Как основная топология была выбрана топология «звезда». Разработка сети связи происходила согласно трехуровневой иерархической модели сети. Сетевое оборудование было подобрано исходя из численности человек, преследуя цель обеспечения комфортной работы и хорошей пропускной способности для всей сети. Для связи центрального офиса с филиалами была задействована технология VPN, использующая протокол IPsec.

Была разработана структурная и логическая схема сети связи. Представлена схема маршрутизаторов с распространяемыми ими сетями (VLAN).

Подходя к внедрению виртуализации, были приведены таблицы технических характеристик серверов и сетевой системы хранилища данных. Главной платформой виртуализацией был выбран продукт компании VMware ESXi 6.5. В конце второй главы была приведена пошаговая установка данной

платформы на сервер и пример взаимодействия с ней с помощью программы VMware vSphere Client 6.5

В заключительном третьем разделе были произведены: определение основных параметров для расчета пропускной способности и расчет ее для передачи данных. По итогам была подсчитана необходимая пропускная способность для центрального офиса и 2 филиалов для передачи данных и организации видеоконференций: 19,7 Мбит/с для центрального офиса и 1,3 Мбит/с для каждого филиала.

Таким образом, все задачи данной дипломной работы были решены, цель достигнута – была разработана распределённая сеть связи для банковской структуры с использованием технологии виртуализации.

Список использованных источников

1. Уорнер М. Виртуальные организации/ М.: Добрая книга, 2005. 296 с.
2. Величко В.В., Субботин Е.А., Шувалов В.П., Кокорева Е.В., Телекоммуникационные системы и сети/ Т. 3:Мультисервисные сети.. учебное пособие 2017г., 540 с.
3. Маликова Е.Е., Пшеничников А.П., Проектирование мультисервисной корпоративной сети/ учебное пособие 2018г., 73 с.
4. Олейник, П.П. Корпоративные информационные системы: Учебник для вузов. Стандарт третьего поколения / П.П. Олейник. - СПб.: Питер, 2012. - 176 с.
5. Федорова, Г.Н. Информационные системы / Г.Н. Федорова. - М.: Academia, 2018. - 544 с.
6. Новожилов, Е.О. Компьютерные сети: Учебное пособие / Е.О. Новожилов. - М.: Академия, 2018. - 176 с.
7. Vmware vsphere [Электронный ресурс] / https://www.vmware.com/ru/products/vsphere.html (дата обращения 18.12.2020).
8. Работа с Hyper-V и Windows PowerShell [Электронный ресурс] / https://docs.microsoft.com/ru-ru/virtualization/hyper-v-on-windows/ quick-start/try-hyper-v-powershell (дата обращения 20.12.2020).
9. Введение в виртуализацию [Электронный ресурс] // Team Computers. URL: http://www.team.ru/virt_intro.php;
10. Гультяев А.К. Виртуальные машины: несколько компьютеров в одном СПб.: Питер, 2016. — 224 с
11. «Gartner's Magic Quadrant for x86 Server Virtualization Infrastructure is a head scratcher», july 2017 [Электронный ресурс] // Gartner
    URL: http://www.zdnet.com/article/gartners-magic-quadrant-for-x86-server-virtualization-infrastructure-is-a-head-scratcher/
    Ручкин В.Н., Фулин В.А. Архитектура компьютерных сетей - М.: Диалог-МИФИ, 2012. - 240 с

12. Gartner Retires the Magic Quadrant for x86 Server Virtualization Infrastructure [Электронный ресурс] // Gartner.
URL: https://www.gartner.com/doc/3642418/gartner-retires-magic-quadrant-x;
13. VMware and Microsoft are the top virtualization leaders, according to Gartner [Электронный ресурс] // TechRepublic.
URL: https://www.techrepublic.com/article/vmware-and-microsoft-are-the-top-virtualization-leaders-according-to-gartner/;
14. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. – СПб.: Питер, 2016. – 992 с.
15. «Сетевое оборудование Cisco» [Электронный ресурс] // Cisco.
URL: http://www.Cisco.com/web/RU/
16. Майкл Палмер, Роберт Брюс Синклер, Проектирование и внедрение компьютерных сетей – СПБ: БХВ-Петербург, 2011. - 740 с
17. Вячеслав Корячко, Дмитрий Перепелкин, Анализ и проектирование маршрутов передачи данных в корпоративных сетях – М: Горячая Линия - Телеком, 2012 г. – 236 с
18. Михаил Михеев, Администрирование VMware vSphere – М: ДМК Пресс, 2010 г. - 408 с
19. Орлов А.И. Математика случая: учеб. пособие. М.: МЗ-Пресс, 2004.-110 с
20. Современные телекоммуникационные технологии / СПбГУТ; Сост.: М.А. Сиверс, П.Ю. Виноградов; Коллектив авторов. СПб, 2010. – 385с.,ил. ISBN 5-98595-004-2.
21. Портнов Э.Л. Оптические кабели связи и пассивные компоненты волоконно-оптических линий связи: Учебное пособие для вузов. – М: Горячая линия-Телеком, 2010. -464 с: ил. ISBN 5-93517-247-X.
22. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 3. – Мультисервисные сети / В.В. Величко, Е.А. Субботин, В.П. Шувалов, А.Ф. Ярославцев; под ред. профессора В.П. Шувалова. – М.:

Горячая линия-Телеком, 2010. – 592 с.: ил. ISBN 5-93517-257-7

23. Деарт В.Ю. Мультисервисные сети связи. Транспортные сети и сети доступа. – М.: Инсвязьиздат, 2007. – 166 с., 93 илл. ISBN 978-5-94874-028-7
24. Беленькая М.Н., Малиновский С.Т., Яковенко Н.В. Администрирование в информационных системах. Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2014. – 400с.,ил. ISBN 978-5-9912-0164-3.
25. ГОСТ 2.105-95 Единая система конструкторской документации. Общие требования к тестовым документам;
26. ГОСТ Р 53801-2010. Связь федеральная. Термины и определения.