Содержание

Введение

Инфокоммуникации являются новой отраслью экономики, развивающейся как единое целое информационных и телекоммуникационных технологий. В инфокоммуникациях технологии связи используются в качестве средства передачи различной информации на произвольные расстояния.

Еще недавно, развитие телекоммуникационных и информационных технологий шло отдельно и, по сути, независимо друг от друга. Предоставление телекоммуникационных услуг было неразрывно связано с операторами связи, которые являлись организациями, выстраивавшими свой бизнес на продаже голосового трафика. В свою очередь, развитие информационных технологий происходило самостоятельно, и было связанно с разработкой программного обеспечения.

Однако, постепенное развитие цифровых технологий способствовало тому, что компьютеры стали объединяться в небольшие локальные сети с целью более оперативного обмена информацией. В них стали возникать компьютеры-серверы, являющиеся специализированными мощными вычислительными машинами, ресурсы которых были доступны всем пользователям сети. Таким образом, стало происходить сегментирование компьютеров сети, расширялся круг решаемых задач, что, в свою очередь, подтолкнуло развитие сетевых технологий, поскольку увеличилась потребность в надежных высокоскоростных системах передачи.

Целью данного курсового проекта является реализация транспортной сети инфокоммуникаций между тремя офисами одной компании с использованием современных информационных технологий, с целью получения навыков построения транспортной сети инфокоммуникации.

Задачами данного проекта является:

Анализ принципов проектирования транспортных сетей инфокоммуникаций предприятий.

Проектирование компьютерной сети центрального офиса.

Проектирование филиала в г. Новгород.

Проектирование филиала, расположенного в сейсмоопасной зоне.

Объединение филиалов компании в единую сеть.

Курсовая работа состоит из постановки задачи, введения, шести глав, заключения и списка литературы, общий объем работы составляет 23 страницы.

1. Постановка задачи

Компания насчитывает три офиса:

Центральный офис, находящийся в Санкт-Петербурге состоит из 5 сотрудников, работающих с компьютерами, включая генерального директора и двух бухгалтеров, занимающихся всеми финансами. Основной задачей офиса является координирование деятельности, а также хранение и обработка данных поступающих с 2-ух удаленных офисов.

Первый удаленный офис располагается в Новгороде. Насчитывает 23 сотрудника, среди которых один руководитель филиала, 2 бухгалтера, и 20 сотрудников разной степени занятости.

Второй удаленный офис аналогичен первому, но офис находится в сейсмоопасной зоне.

Общие положения о ТСИ для компании:

Сеть должна учитывать уровни доступа к сетевым ресурсам компании.

ТСИ должно обеспечивать телефонную, интернет, факсимильную и конференц-связь между офисами. А так же локальную сеть обмена данными и локальную телефонную связь «внутри» офисов

Удаленные офисы должны иметь доступ к базе данных, расположенной на серверах центрального офиса. Доступ должен предоставляться с учетом уровней приоритетности;

При проектировании, ТСИ необходимо учитываться территориальные особенности, а также то, что второй удаленный офис находится в сейсмоопасной зоне.

На территории компании необходимо предусмотреть пять уровней доступа:

Уровень 1- предоставляется директору, директору по развитию, глав. бухгалтеру и главному инженеру. Позволяет получать данные из базы данных, информацию по бухгалтерии, FTP, файлового и почтового сервера каждого офиса компании, доступ в интернет.

Уровень 2 - предоставляется руководителям офисов инженеру проектировщику, инженерам офисов. Позволяет получать данные из БД , FTP, файлового и почтового сервера, доступ в интернет.

Уровень 3 - предоставляется бухгалтерам всех офисов. Каждый бухгалтер может получить доступ к бухгалтерии, базе данных, FTP, файловому серверу только своего офиса;

Уровень 4 - предоставляется только к сотрудникам компании. Данный уровень открывает доступ к базе данных, почтовому серверу, FTP и файловому-серверу только в пределах одного офиса.

Уровень 5 – предоставляется, начальнику отдела автоматизации, сотрудникам отдела автоматизации. Этот уровень позволяет получать доступ ко всем ресурсам сети для, отладки и оптимизации работы.

2. Принципы проектирования ТСИ для фирмы

С целью эффективного регулирования и управления хозяйственной и экономической политикой компании, получения исчерпывающей информации для принятия своевременных решений, контроля над производственными процессами и ходом выполнения работ, оперативным обменом документацией и сообщениями, компании необходимо иметь развитую инфокоммуникационную сеть.

На текущее время, компьютерная сеть является важнейшей составляющей, которая необходима для эффективного управления предприятием с целью повышения прибыли. Поэтому отсутствие связи даже в течение часа может способствовать появлению больших финансовых потерь.

В самом общем смысле, корпоративная сеть является сложным аппаратно - программным комплексом взаимосвязанных и согласованно функционирующих компонентов, обеспечивающих информационный обмен между различными удаленными приложениями и системами, используемыми на предприятии.

Наличие нескольких центров обработки данных, позволяет отнести корпоративные сети к распределенным (или децентрализованным) вычислительным системам, которые необходимо рассматривать в различных аспектах, а именно:

-структурном;

-системнотехническом;

-функциональном.

В структурном аспекте, корпоративная сеть является сетью смешанной топологии, объединяющей несколько локальных вычислительных сетей. Корпоративная сеть связывает филиалы предприятия, создавая тем самым, единое информационное корпоративное пространство. Корпоративная сеть

является собственностью предприятия и отражает его структуру. В зависимости от масштабов предприятия различают [11]:

-сети отделов;

-сети зданий и кампусов;

-сети масштаба предприятий.

В функциональном аспекте, корпоративная сеть является эффективной средой передачи данных, необходимых для организации производственного процесса и решения задач предприятия.

С системнотехнической точки зрения корпоративная сеть рассматривается как целостная структура, которая состоит из нескольких уровней, взаимосвязанных и взаимодействующих между собой.

Таким образом, в системнотехническом аспекте, корпоративная сеть является системой, обеспечивающей доступ пользователям и программам к набору полезных услуг (сервисов), общесистемных и специализированных приложений. Такая система содержит в себе службы, гарантирующие нормальное функционирование корпоративной сети [11].

Для обеспечения всех потребностей предприятия, в офисах целесообразно развернуть локальные сети, и связать их между собой с помощью региональной сети.

Локальная сеть (ЛВС, локальная сеть; англ. Local Area Network, LAN) — это компьютерная сеть, развернутая обычно на относительно небольшой территории и объединяющая, как правило, несколько зданий.

Офисы, особенно центральные, являются центрами обработки и хранения информации. В них стекает вся информация из других филиалов. Это накладывает на ТСИ для данной структуры определенные требования по отказоустойчивости, ТСИ должна гарантировать работу в 99,98% случаев. Также сеть должна быть масштабируемой, что предусматривается на случай расширения предприятия.

Для обеспечения стабильной работы локальной сети, следует первоначально спроектировать сети, приобрести необходимое оборудование

и произвести высококвалифицированный монтаж коммуникаций локальной сети в офисе. Как правило, проектирование и монтажные работы осуществляется компанией подрядчиком.

Для обеспечения бесперебойной работы сети и сетевых терминалов, необходимо исключить риски при таких непредвиденных обстоятельствах как отключение электропитания. Это влечет за собой необходимость приобретения источников бесперебойного питания (ИБП). Эта мера, так же положительно влияет и на срок службы электроприборов, так как ИБП исключает возможность выхода SIN за допустимые отклонения (220В ±10%) и выравнивает напряжение, что способствует увеличению срок службы приборов на 20-30%, а также экономии на предприятии.

Как правило, архитектура офисных локальных сетей имеет иерархическое построение. В таких сетях выделяется один или несколько специальных компьютеров – серверов. Серверами обычно являются высокопроизводительные ПК, на которых установлена серверная операционная система. Серверы оснащаются отказоустойчивыми дисковыми массивами и системой защиты от сбоев. Обычно, на компьютерах - серверах локальные пользователи не работают, поэтому принято говорить о выделенном сервере. Серверы осуществляют управление сетью и хранение информации, которую совместно используют остальные компьютеры сети.

С точки зрения системного администрирования, сеть с выделенным сервером наиболее управляемая и контролируемая, хотя и более сложная в создании и обслуживании.

Преимущества иерархической архитектуры:

-выход из строя рабочих станций, не отражается на работоспособности сети в целом;

-простота организации локальных сетей с большим количеством рабочих станций;

-администрирование сети осуществляется централизованно — с сервера;

-обеспечивается высокий уровень безопасности данных.

К недостаткам данной архитектуры можно отнести:

- выход из строя или сбой единственного сервера может парализовать всю сеть. Поэтому необходимо всегда предусмотреть резервные каналы;

-наличие выделенных серверов повышает общую стоимость сети;

-IT-персонал должен иметь необходимые знания и навыки администрирования домена.

Для организации связи между удаленными локальными сетями целесообразно использовать выделенные гарантированные VPN каналы, пропускная способность которых гарантирована и не зависит от дня недели или времени суток. Также постоянным гарантированным и высоким будет качество IP-телефонии, предоставляемой по корпоративным каналам связи.

VPN соединение представляет собой подключения типа «точка-точка» в частной или публичной сети, например в Интернете. Для виртуального обращения на виртуальный порт VPN-сервера используются специальные туннельные протоколы, на основе TCP/IP. При обычной реализации VPN клиент инициирует по Интернету виртуальное подключение типа «точка-точка» к серверу удаленного доступа. Сервер удаленного доступа принимает вызов, выполняет проверку подлинности вызывающей стороны и формирует ответ в виде данных, которые затем передаются между VPN-клиентом и частной сетью организации.

При организации канала типа «точка-точка» к данным добавляется заголовок, содержащий сведения маршрутизации, обеспечивающие прохождение данных по общей или публичной сети до конечного пункта. Добавление заголовка у данным называется инкапсуляцией. При организации частного канала, в целях обеспечения конфиденциальности, данные шифруются перед процессом передачи. В случае перехвата пакетов в общей или публичной сети, их невозможно расшифровать без ключей шифрования. Такой канал, по которому частные данные передаются в

инкапсулированном и зашифрованном виде, и называется VPN-подключением.

3. Проектирование компьютерной сети центрального офиса

Центральный офис компании является самым главным центром приема, передачи и обработки данных со всех офисов. Схема физической топологии центрального офиса показана на рисунке 1.

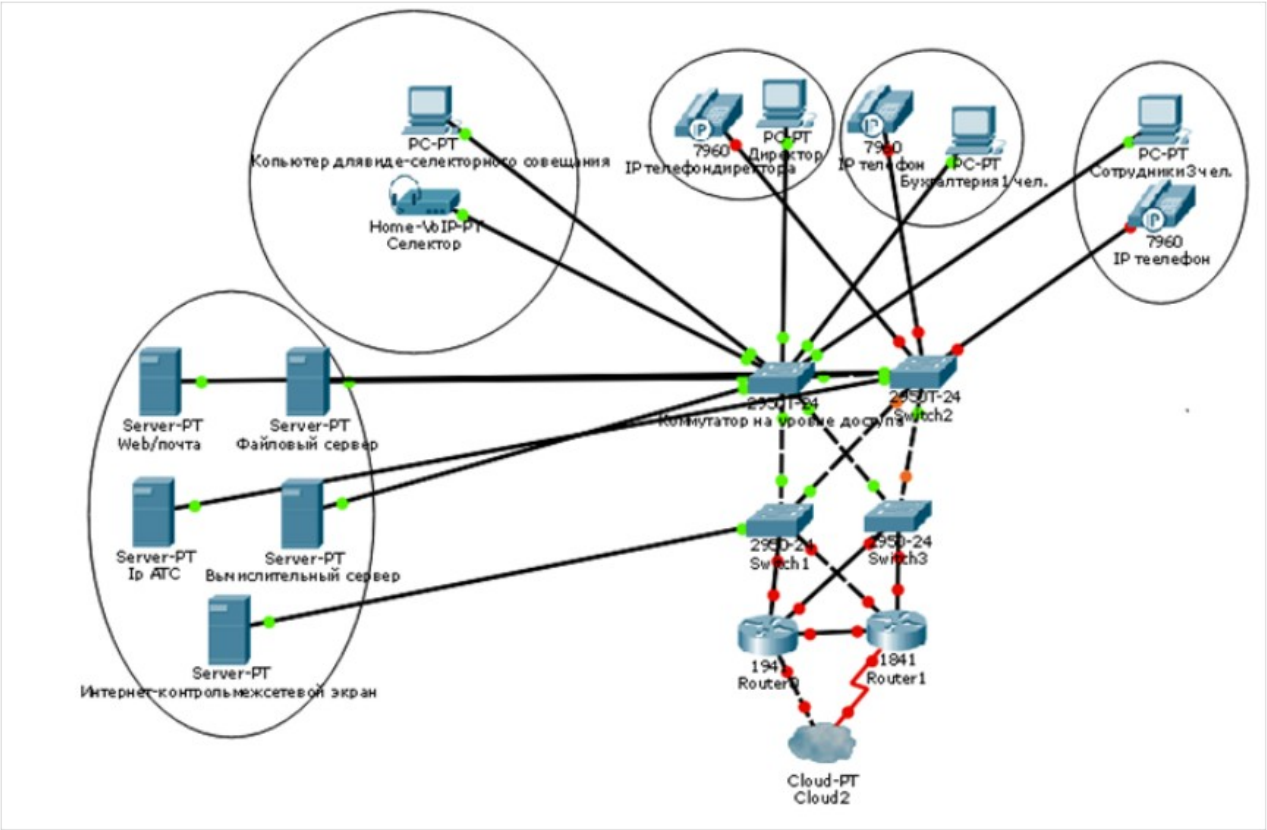


Рисунок 1 - Схема физической топологии центрального офиса

В центральном офисе развернута локальная сеть, типичная для небольшого офиса. На всей территории офиса располагается 10 розеток локальной сети (ЛВС): 5 используются для постоянного подключения компьютеров сотрудников, остальные 5 розеток, смонтированы на случай появления новых сотрудников или могут использоваться в качестве резервных при непредвиденных обстоятельствах. На каждом рабочем столе сотрудника устанавливается IP-телефон. Каждый из компьютеров и

телефонов в офисе подключен к одному из портов коммутатора ЛВС, расположенного в специально выделенном помещении. Данное помещение, является коммутационным узлом и серверной, где располагаются также 5 серверов (сервер электронной почты, сервер учета трафика, веб сервер, сервер IP АТС, вычислительный сервер и файловый сервер, 1С:Бухгалтерия), обслуживающих офис. Сюда же заведены оптоволоконные линии связи оператора.

В северном помещении имеется также селектор видео-совещаний. Такой тип групповой видео конференции позволяется принимать участие в совещании до 80 пользователям, при одновременном показе не более трёх участников (ведущий, докладчик и выступающий). Пользователи подключаются к совещанию посредством ввода логина и пароля, либо по приглашению ведущего.

Всех участников совещания можно разделить на две группы:

- вещающие. от них доступен для всех остальных участников. Обычно это докладчик, ведущий и выступающий;

- зрители, которыми выступают все остальные. Видео от зрителей не показывается никому, однако, в ходе совещания они имеют возможность посылать аудио сообщения всем участникам, используя специальные функции клиентского приложения;

Администратор назначает ведущего, который определяет роли тем или иным участникам совещания. Эти роли не постоянны, а могут переназначаться в процессе общения. Единственное исключение – функции ведущего не могут быть переданы никому другому.

У ведущего есть следующие возможности:

- приглашение участников совещания;

- передача роли докладчика другому участнику совещания;

- передача роли выступающего другому участнику совещания, как правило, по запросу последнего.

Для обеспечения стабильной работы селекторного совещания необходимо иметь интернет соединение с минимальными скоростями: исходящая - 128 кбит/с, входящая - 384 кбит/с.

Топология сети центрального офиса обладает большой избыточность, так как она должна функционировать постоянно и выдерживать больше нагрузки.

Для обеспечения работы сети центрального офиса используются такие компоненты как маршрутизатор и коммутатор.

Маршрутизатор представляет собой специализированный сетевой компьютер, имеющий как минимум один сетевой интерфейс и обеспечивающий пересылку пакетов данных между различными сегментами сети. Посредством маршрутизатора связываются разнородные сети различных архитектур, он также принимает решения о пересылке на основании информации о сетевой топологии и определенных правил, заданных администратором.

Сетевой коммутатор представляет собой устройство, обеспечивающее соединение нескольких узлов компьютерной сети в пределах одного или нескольких сетевых сегментов.

Так как центральный офис имеет не большое количество сотрудников, то достаточно будет установить 2 коммутатора с поддержкой VLAN на 24 порта - один основной, другой резервный.

VLAN (Virtual Local Area Network) — логическая локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. Поддержка VLAN необходима для того, чтобы разделить сотрудников на группы.

Для реализации разных уровней доступа используются прокси-сервер, в некоторых случаях можно использоваться списки контроля доступа (ACL).

Прокси-сервер представляет собой службу (пакет программ) в компьютерных сетях, которая дает возможность клиентам выполнять косвенные запросы к другим сетевым службам. Первоначально клиент подключается к прокси-серверу и посылает запрос на доступ к какому-либо ресурсу (например, e-mail), расположенному на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кеша (в случаях, если прокси имеет свой кеш). В некоторых случаях запрос клиента или ответ сервера может быть изменён прокси-сервером в определённых целях. Прокси-сервер позволяет защищать компьютер клиента от некоторых сетевых атак и помогает сохранять анонимность клиента.

Прокси-сервер можно использовать для доступа из филиалов к базе данных или 1С:Бухгалтерии, т.е. для доступа из удаленных филиалов.

Для поддержки приоритетности внутри офиса используются ACL.

Все компьютеры в локальной сети имеют статический IP-адрес, что позволяет ограничить доступ пользователям разных групп по определенным критериям отбора.

Так информация о всей деятельности компании доступна будет только директору, главному бухгалтеру, и директорам филиалов.

Чем выше уровень, тем меньше привилегий у пользователя.

В качестве резервного канала связи используются USB-модемы Yota.

4. Проектирование филиала в г. Новгород

Второй офис компании находится г. Новгород. Схема физической топологии второго офиса показана на рисунке 2.

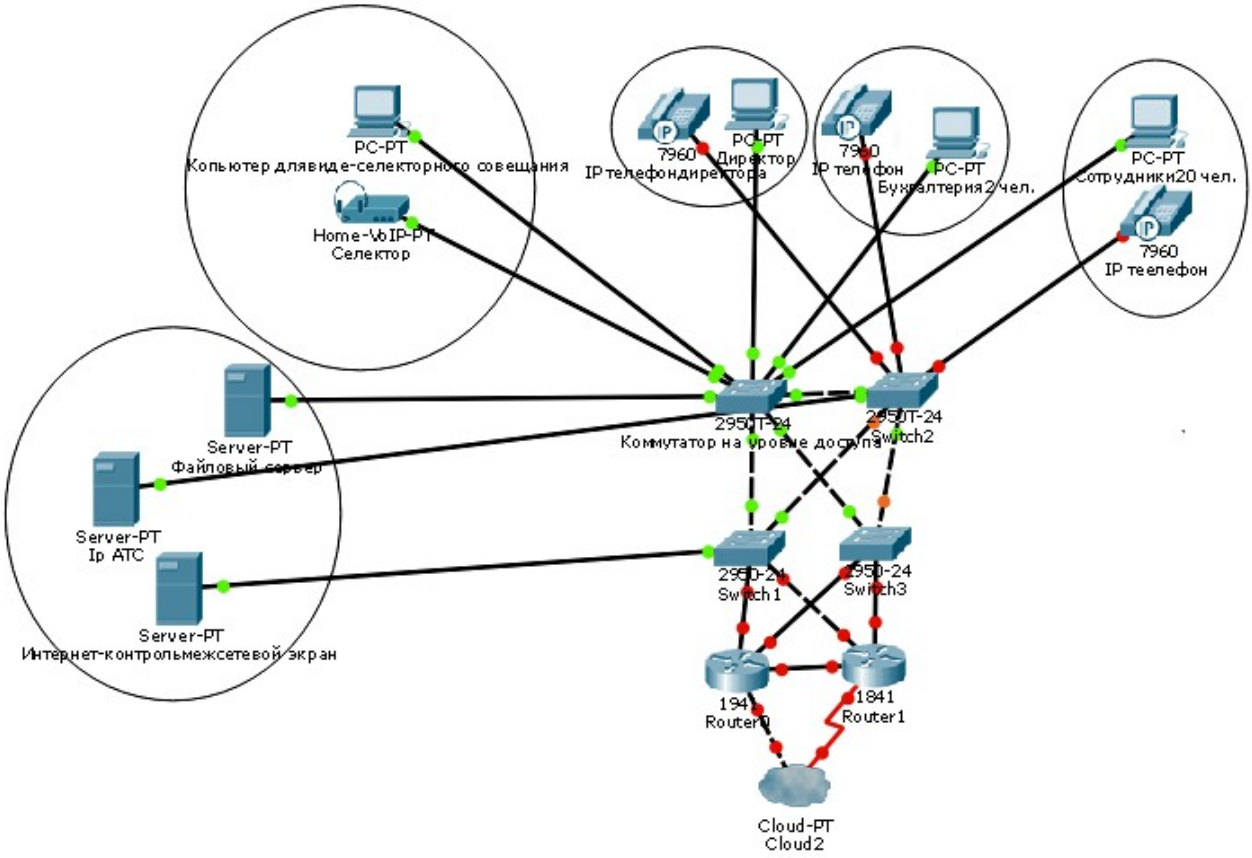


Рисунок 2- Схема физической топологии офиса в г. Новгород

Офис в г. Новгород также имеет иерархическую структуру построения, и обеспечен практически аналогично центральному офису. Офис имеет такую же реализацию приоритетов, за тем исключением, что понадобится использование мощных коммутаторов, так как количество сотрудников превышает головной офис практически в 4,5 раза.

Проведение селекторных совещаний проходит по одинаковому принципу, что и в главном офисе - выбирается ведущий и ведет разговор с собеседником.

Так как офис в г. Новгород является филиалом, то нет необходимости использовать большие вычислительные серверы с базами данных, бухгалтерией. Нагрузка распределена между серверами, поэтому офис в г. Новгород будет использовать только серверы для IP-телефонии, межсетевой экран и внешний и внутренний файловый сервер. Вся обработка информации осуществляется на серверах центрального офиса, будь то почта, расчеты, операции с базами данных. Описанный подход дает возможность сосредоточить всю документацию в одном месте, иметь постоянный доступ к информации.

Резервный канал связи также, как и в центральном офисе, является USB-модем от Beeline.

5. Проектирование филиала в сейсмоопасной зоне

Третий филиал компании располагается в сейсмоопасной зоне и имеет аналогичную структуру, что и офис в г. Новгород. Схема физической топологии офиса показана на рисунке 3.

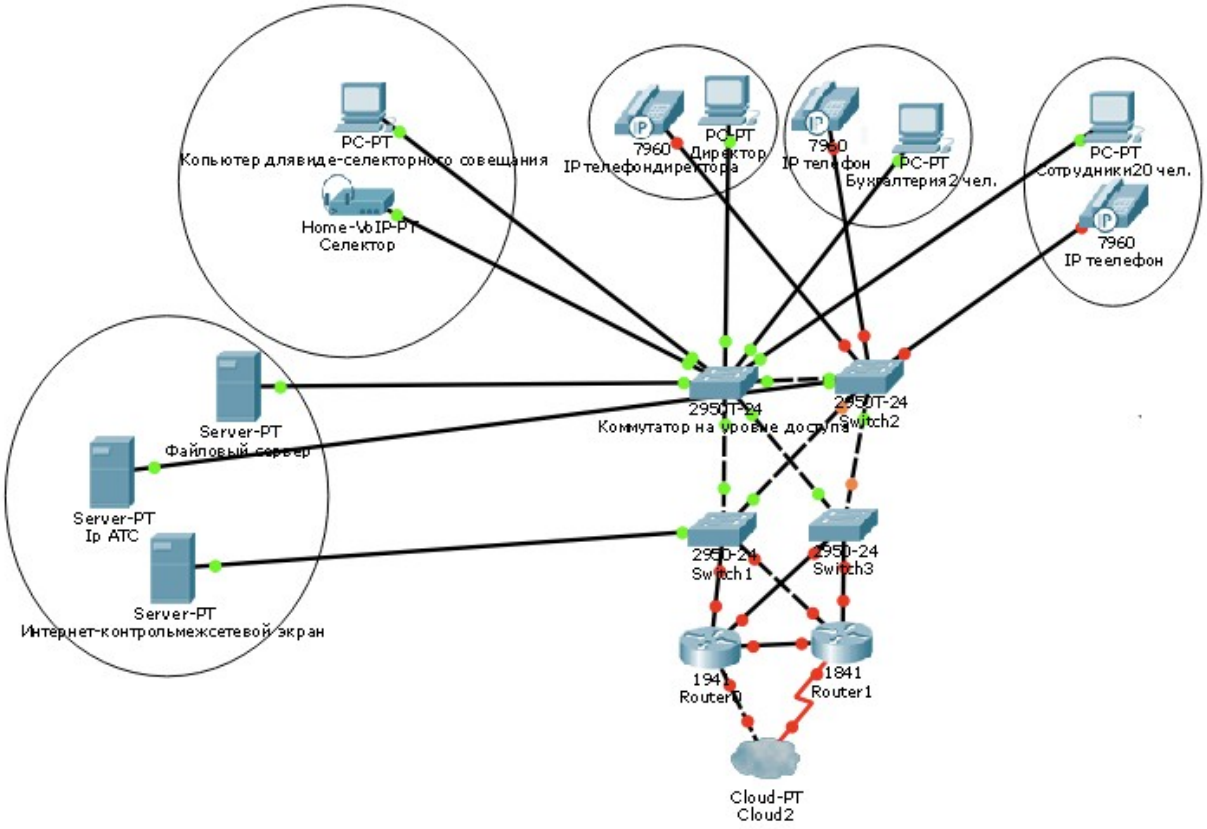


Рисунок 3 - Схема физической топологии офиса, расположенного в сейсмоопасной зоне.

Сетевая структура аналогична офису в г. Новгород. Но учитывая то, что данный филиал находится в сейсмоопасной зоне, то необходимо обеспечить устойчивость оборудования к возможным замлятресениям, оползням и прочим природным катаклизмам.

По статистическим данным среднемесячных и среднесуточных значений федерального прогностического параметра в сейсмоопасных

зонах Российской Федерации преобладают землетрясения незначительной силы, на уровне общей фоновой сейсмичности. Предположим, что данный офис находится в г. Сочи.

Поэтому прежде чем развертывать сеть, необходимо взять в аренду или построить здание, которое имеет специальную эластичную прослойку, позволяющую плавно сдвигать дом по горизонтали при подземных толчках. Это достигается посредством добавления в прослойку, резиновых элементов совместно со стальными конструкциями. Таким образом, в случае землетрясении здание имеет возможность спокойно двигатся по горизонтальной линии. Такой «разгон» может достигать 50 см. Это обеспечит наименьшую тряску оборудования.

Вся необходимая информация компании хранится на серверах, поэтому необходимо учитывать наибольшую безопасность этого оборудования.

Обязательным будет использование емких источников бесперебойного питания, для обеспечения бесперебойной работы в условиях отсутствия сетевого напряжения. Так как последствия стихии могут долгое время обесточить населенный пункт, лучше всегда иметь несколько дополнительных ИБП с полным зарядом.

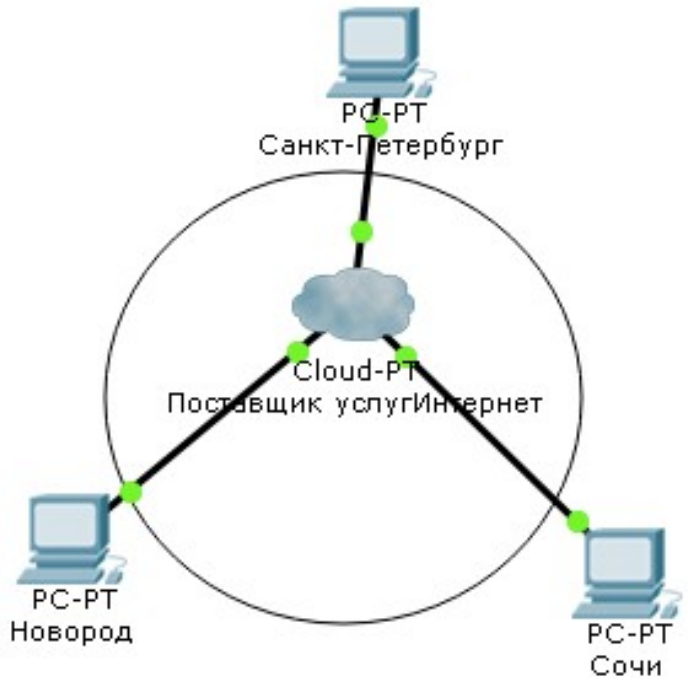
Серверные шкафы необходимо устанавливать на пружинах, с целью снижения вибрации от толчков. Такая технология используется при проектировании домов, ЛЭП, электрогенераторов или роторов в больших компаниях, таких как «Газпром» или «Роснефть».

Оборудование внутри шкафов стоит закрепить ремнями, но при этом необходимо учитывать амплитуду раскачивания для проводов, шкафа, в случае толчков или звукового удара.

6. Организация связи между филиалами

Компания имеет три филиала, расположенных в трех разных регионах России. Схема объединения офисов по средствам показана на рисунке 4.
Для любой компании развертывать собственную сеть на значительной территории – тяжелая задача с финансовой точки зрения. Поэтому с целью снижения материальных затрат связующим звеном между офисами компании будет являться поставщик услуг интернет (ISP).

Рисунок 4 - Общая структура корпоративной сети



Так как данные компании являются ее собственностью, то с целью обеспечения безопасности передачи информации будет использоваться зашифрованный VPN канал.

Организация VPN-канала между офисами дает компании следующие возможности:

-использовать сеть интернет для объединения своих офисов и филиалов;

-обеспечить защиту передаваемой информации посредством надежного шифрования VPN-каналов;

-обеспечить единую точку доступа в интернет через VPN-соединение;

Для организации VPN-канала может быть использована любая доступная физическая среда передачи данных: DSL, ADSL, WiFi и другие. Также для подключения VPN-канала пригодны скоростные сотовые сети передачи данных 3 или 4G от Мегафона, Билайн, МТС или других сотовых операторов.

Для защиты VPN-соединения используются различные виды шифрования, поэтому виртуальная частная сеть является надежным способом передачи конфиденциальной информации через интернет. VPN-канал дает возможность обеспечить безопасный удаленный доступ сотрудников к ресурсам корпоративных сетей, проводить селекторные совещания, исключая при этом, риск несанкционированного подключения к вашей сессии. Также появляется возможность найма удаленных сотрудников или работа из дома по выделенной линии.

Организация объединения офисов с помощью VPN-канала потребует финансовых затрат, но они значительно ниже тех, которые пришлось бы затратить на прокладку собственной сети, протяженностью порядка 4000 км.

Заключение

В данном курсовом проекте была спроектирована транспортная сеть инфокоммуникаций между тремя офисами - Санкт-Петербургом, Новгород и офисом, находящимся в сейсмоопасной зоне (выбран г. Сочи).

При проектировании учитывались все требования задания. Был организован необходимый приоритет доступа пользователей к данным, организована связь каждого офиса друг другом, разработана внутренняя структура сети, обеспечено проведение селекторных видео-совещаний, IP-телефония, коммутационный отсек. В проекте были так же учтены требования при развертывании локальной сети в сейсмоопасной зоне.

В центральном офисе сосредоточены все основные серверы компании - база данных, бухгалтерия и тд. Все филиалы компании имеют доступ к данным с помощью организованного защищенного VPN канала. Для обеспечения оперативной работы с документами сотрудников разных филиалов, используется локальное файловое хранилище для передачи файлов. Проведение совещаний обеспечивается посредством использования селектора или видео-конференции. Связь между сотрудниками филиалов компании обеспечивается при помощи IP -телефонии или электронной почты.

Список литературы

1. Гургенидзе А.Т., Кореш В.И. Мультисервисные сети и улуги широкополосного доступа. Наука и техника, 2013. – 400с.

2. Величко М.В. Технологии строительства сетей доступа– М.: Горячая линия-Телеком, 2015. –313 с.

3. Величко В.В.Телекоммуникационные системы и сети: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2014. – 592с.

4. Крухмалев В.В.,. Гордиенко В.Н, Моченов А.Д. Основы построения телекоммуникационных систем и сетей: Учебник для вузов, 2-е изд., испр. – М.: Горячая линия – Телеком, 2012.- 424 с.

5. Крук Б.И., Попантонопуло В.К., Шувалов В.П Телекоммуникационные системы и сети: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2013.- 648с.

6. Катунин Г.П Телекоммуникационные системы и сети: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2014.- 672с.

7. Ломовицкий В.В. Основы построения систем и сетей передачи информации: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2012. – 382 с.

8. Новиков Ю.В., Кондратенко С.В. Основы локальных сетей, Курс лекций. Учебное пособие - М.: Интернет — Ун-т Информ. Технологий, 2005. . – 383 с.

9. Олифер В. Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 3-е изд. – С-Пб.: Питер, 2006. – 985 с.

10.Столингс В. Современные компьютерные сети. – С-Пб.: Питер, 2013. – 783 с.

11. Финогеев А.Г., Бождай А.С. Сетевые технологии, Учебное пособие 3 часть. Углубленный уровень подготовки - Пенза 2013. – 412с.