Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Кафедра «Телекоммуникационные системы»
Специальность 6М071900 «Радиотехника, электроника и телекоммуникации»

Допущен к защите
Зав. кафедрой
к.т.н., Шагиахметов Д.Р. _____
(Ф.И.О.) подпись

«_____»_____2014г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ
пояснительная записка

На тему: Исследование моделей VPN с ограниченными сетевыми ресурсами

Магистрант _Абдрахимов И. М _____ группа МТСп-12-1
(Ф.И.О.) подпись

Руководитель диссертации Данько Е. Т. _____
(Ф.И.О.) подпись

Рецензент_____
(Ф.И.О.) подпись

Консультант по ВТ _____Данько Е. Т. _____
(Ф.И.О.) подпись

Нормоконтроль _____Кудинова В.С. _____
(Ф.И.О.) подпись

Алматы 2014г.

Некоммеческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Факультет «Факультет радиотехники телекоммуникации и связи»
Специальность 6М071900 «Радиотехника, электроника и телекоммуникации»
Кафедра «Телекоммуникационные системы»

ЗАДАНИЕ
на выполнение магистерской диссертации

Магистранту Абдрахимов Идиль Миратович
(фамилия, имя, отчество)

Тема диссертации Исследование моделей VPN с ограниченными сетевыми ресурсами
утверждена Ученым советом университета №___от «___»_____
Срок сдачи законченной диссертации «___»_____
Цель исследования Исследовать известные модели VPN с целью их дальнейшей модернизации для работы сетей с ограниченными сетевыми ресурсами.
Перечень подлежащих разработке в магистерской диссертации вопросов или краткое содержание магистерской диссертации:
Виртуальные частные сети VPN с использованиеv протокола MPLS, достоинства и недостатки использования меток при выполнении расчетов,
Перечень графического материала (с точным указанием обязательных чертежей) Рисунок 1.1 - Виртуальная частная сеть на базе технологии MPLS
Рисунок 1.2 – Схема метода ветвления
Рисунок 1.3 – Отображения результатов расчета: требуемая полоса пропускания
Рисунок 2.1 – Сеть общего пользования, построенная в программе Cisco Packet Tracer
Рисунок 2.2 - Зависимость величины резервируемой полосы пропускания от числа конечных точек VPN для канальной и потоковой моделей
Рисунок 2.3 - Зависимости коэффициента отклонения Δ от числа запросов *z* для различных моделей VPN
Рисунок 2.4 - Зависимость среднего значения коэффициента отклонения от плотности графа при разных моделях реализации VPN

Рекомендуемая основная литература

1. Штайнке С. VPN между локальными сетями. LAN/Журнал сетевых решений. Октябрь 1998, том 4,№10;

2. Абдрахимов И.М. Исследование моделей VPN с ограниченными сетевыми ресурсами. // Сборник научных трудов энергетики, радиотехника, электроникам и связь. Алматы: АУЭС, 2013. – С. 6.;

Г Р А Ф И К
подготовки магистерской диссертации

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
1 Информационный обзор критериев оценивания качества речи и их приложений	05.10.2012	
2 Характеристика MPLS/VPN	11.12.2012	
3 Экспериментальные исследования	10.01.2013	
4 Оценка параметров качества в IP телефонии	3.03.2013	
5 Вопрос обеспечения качества обслуживания	05.06.2013	
6 Расчетная часть	10.12.2013	

Дата выдачи задания_________

Заведующий кафедрой__Шагиахметов Д. Р.__(_____)
(Ф.И.О.) (подпись)
Руководитель диссертации__Данько Е. Т.___ (_____)
(Ф.И.О.) (подпись)
Задание принял к исполнению
магистрант _____Абдрахимов И. М._(_____)
(Ф.И.О.) (подпись)

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Отзыв руководителя

о диссертации магистранта Абдрахимов Идиль Миратович

Тема магистерской диссертации «Исследование моделей VPN с ограниченными сетевыми ресурсами»

Рассмотрены основные принципы организации, современные стандарты, исследована система мониторинга и статистики сети VPN на основе MPLS.

На базе статистических данных, полученных такими программами как GPSSWorld и Cisco Packet Tracer построены графики. В работе предложена модифицированная модель для потоковой модели, учитывающая одновременно два фактора: эффективность распределения полосы пропускания в сети для каждого запроса VPN и механизм балансировки нагрузки в сети с учетом свободной полосы пропускания.

Диссертационная работа полностью удовлетворяет требованиям, предъявляемым к магистерским диссертациям, заслуживает оценки «отлично» 90%, а автор Абдрахимов И. заслуживает присвоения степени магистра по специальности 6М071900- Радиотехника, электроника и телекоммуникации.

Руководитель магистерской диссертации — к.х.н ст.преп. Данько Е. Т.

Андатпа

Берілген магистерлік диссертацияда тасқынның қалыбы үшін мезгілдес екі факторда есептескіш модифицированная қалыпты тартудың полосы бөлтиімділігі ауда VPN және жүктің тетігінің бас-басы сұранысы үшін ауда есебімен тартудың еркін полосаны ұсын. Айтылмыш диссертационнаяда жұмыс зерттеме және VPN графтың қалыбының зертте бас негіз үйлесімді бер көзқарастың өлшемнің минимума сан үйлесімсіз тең түйіншек IP/MPLS арнаулы. Осы өлшем сияқты сенімділіктің өлшемінің арада MPLS ауларының, егер бас тартудың байланыстың сызығының түйіншектердің арасында пайдаланылу біледі.

Аннотация

В данной магистерской диссертации была предложена модифицированная модель которая рассчитывала одновременно и эффективность распределения полосы пропускания в сети и механизм распределения нагрузки в сети с учетом свободной полосы пропускания также в диссертационной работе выполнена разработка и исследование графов моделей VPN на основе IP/MPLS, оптимальных с точки зрения критерия минимума числа несвязных пар узлов. Этот критерий может использоваться как критерий надежности в сетях MPLS, в случае отказа линии связи между узлами сети.

Annotation

In this master thesis the modified model for the stream model, considering at the same time two factors is offered: efficiency of distribution of a pass-band in a network for each inquiry of VPN and the mechanism of balancing of loading in a network taking into account a free pass-band. This dissertation work is devoted to development and research of the graph VPN models on the basis of IP/MPLS, optimum from the point of view of criterion of a minimum of number of incoherent couples of knots. This criterion can be used as criterion of reliability in the MPLS networks, in case of refusal the communication line between network knots.

Содержание

Введение

В настоящее время обеспечение качества IP-ВЧС обслуживания было не так важено. Но в последнее время появилась такая новая технология как MPLS, с помощью которой становится возможным обеспечение качественного обслуживания в ВЧС-сетях.

Благополучная работа любой современной компании непременно зависит от доступности и актуальности информации, обеспечивающей бизнес процессы. Корнем для внесения новых сервисов, позволяющих более эффективно организовывать работу сотрудников, выступают интеллектуальные сети и системы передачи данных. Новейшие сети являются средой обеспечивающей основу видов коммуникаций, такие как: видеоконференции, традиционная передача данных, телефония, и видеовещания. На сегодняшний день данные по сети чаще всего работают с использованием новой технологии коммутации по меткам MPLS VPN. Данная технология обеспечивает быструю коммутацию пакетов с работой меток находящихся в заголовке пакета. Они содержат у себя в памяти адрес доставки и класс сет уровня. Задание пути прохождения трафика в такой сети является пользование однонаправленных туннелей, которые соединяют последовательно сетевые узлы, выбранные с учетом максимальной загрузки ресурсов сети и выполнения требований качества обслуживания. Основным важным условием некой данной сети является ее надежность. Существует много критериев надежности сетей. Обычно выбор критерия надежности осуществляется исходя из особенностей конкретной сети и ее назначения.

В данной магистерской работе предложена модифицированная модель на основе потоковой модели, учитывающая два основных фактора: эффективная распределенная полоса пропускания для каждого запроса ВЧС и балансировка механизма нагрузки сети с учетом неиспользуемой полосы пропускания. Вышеизложенная диссертационная работа отдана разработке и изучению графовых моделей ВЧС на базе IP/MPLS оптимального критерия числа несвязных пар узлов. Эта мера может применяться как оценка надежности сети в MPLS, если в случае отказа одной из линии связи между узлами сети, она хорошо отражает последствия при отказе маршрута. Чем больше количество несвязных пар узлов, тем больше требуется мощностей для вычисления сети быстрой перемаршрутизации пакетов с данными. Таким образом, при использовании данного критерия, можно задаться поиском критических точек сети, при выходе из строя котроых может повлечь за собой полноценное ухудшение функционирования сети связи. В последнее время произошол важный рост вычислительной техники и поэтому стало возможным использовать, для сетей точные методы вычисления - реальных размерностей. Методы точного расчета функционала надежности необходимы и для проверки приближенных методов расчета и его качества.

1 Моделирование сетей связи и исследование их надежностей.

1.1Основные компоненты виртуальных частных сетей

В качестве моделей для сетей связи часто используются случайные графы. Случайным графом называется такой граф, в котором ребро между любой парой вершин присутствует с возможностью p. В предоставленной диссертации в особенности модели сети связи, употребляются случайные мультиграфы, т.е. между всякой парой вершин где возможно есть несколько ребер, всякое из которых присутствует с возможностью p. Затем мы будем работать уже с топологиями сетей на основе модели случайного графа. Линиям связи соответствуют ребра случайного графа, а узлам сети - его вершины. В качестве узлов сети могут выступать маршрутизаторы, коммутаторы и другое сетевое оборудование.

Показатели верности и совместные доступы к их расчёту. Как уже упоминалось, существует большое количество мер надежности сетей связи. Если смоделировать сети связи случайными графами то тогда есть возможность показать отказоустичивость данного графа по предпочитаемой мере через данные этого графа, такие, как связность, время восстановления связности и т.п. В качестве исходных данных должны использоваться предположения о надежности отдельных узлов и линий связи, назначение сети, а также предположение о том, должны ли результаты отражать работа сети в среднем или в экстремальных условиях. Зачастую для точного решения поставленной задачи и нахождения значения выбранной характеристики надежности приходится значительно упрощать предположения о структуре графа и надежности его элементов, например, предполагать распределения надежностей всех элементов одинаковыми. Для оценки надежности по выбранному критерию больше подходят алгоритмы подсчета приближенного значения функционала надежности, основанные на методе Монте-Карло, числе покрывающих деревьев или на методе ветвей и границ.

Важным частным случаем является наличие ограничения на диаметр сети. Ограничение на диаметр является довольно интересным и возникает, когда в сети время жизни сообщения длится не более определенного ограниченного числа передач.

Разработка структур сетей связи по критериям надёжности. Задача оптимизации сетей, согласно выбранной характеристике надежности возникает довольно часто. Редкими случаями этой задачи являются добавление элемента или группы элементов в существующую сеть клиента, соединение в одну сеть нескольких рассредоточенных узлов, подключение новых абонентов и т.д. Очень важно отметить, что для большинства показателей решение какой-либо такой задачи в общем виде для любых структур сетей не является возможным ввиду сложности задачи и возможно лишь получать решения для каждого редкого случая. Но для таких

распространенных видов сетевых топологий, как цепь (шина), цикл (кольцо) и звезда, решения найдены и в общем виде. В данной работе во второй главе предложены решения по оптимальному по критерию EDP присоединению этих распространенных топологий к произвольной топологии, рассмотрено оптимальное расположение особых вершин в таких топологиях и добавление ребра в такую топологию.

Критерий максимума вероятности связности - это один из наиболее исследованных и известных критериев надежности сетей связи, при использовании в качестве модели сети случайного графа. Каждому ребру и вершине такого графа может быть приписано некоторое число, характеризующее ее надежность: вероятность нахождения в работоспособном состоянии. В этом случае становится возможным вычислить, с какой вероятностью каждая вершина будет соединена с каждой. Такая вероятность называется всетерминальной вероятностью связности. Распространены также задачи вычисления двутерминальной вероятности связности и k-терминальной. Работы, посвященные исследованию этого показателя сетевой надежности - и д.р.

Критерий вероятности передачи потока заданной величины. Критерий вероятности передачи потока заданной величины - также важен при проектировании сетей связи. Показатель определяется как вероятность передачи заданного объёма информации между выделенной парой вершин за отведённое время .

Критерий EDP. Напомним, что EDP - это математическое ожидание числа несвязных пар вершин случайного графа. Как мера надежности также используется математическое ожидание числа связных пар вершин случайного графа ECP. Очевидно, что для n-вершинного графа, веса всех вершин которого равны 1 (понятие веса будет пояснено ниже), $ECP - n(n-1)/2 - EDP$, однако выражения для EDP обычно более компактны и удобны в использовании.

Впервые точный метод расчета показателя EDP был предложен в работах Родионова А.С. и Родионовой О.К.. В этих работах были рассмотрены формулы для точного расчета EDP в случае различных надежностей ребер, а также сокращенные методы расчета EDP функционала при наличии особенностей в топологии графов, например, висячей вершины, моста, цепи и т.д. и в случае графов малой размерности. Эти формулы, а также некоторые новые, полученные на их основе, используются в данной магистерской диссертации для случая одинаковой надежности ребер. Однако, в работах задачи структурной оптимизации систем сетевой структуры по критерию EDP рассмотрены не были, вопросы программных алгоритмов для расчета EDP-полиномов также ранее не рассматривались.

Любая организация, будь она производственной, торговой, финансовой компании или государственным учреждением, обязательно сталкивается с вопросом передачи информации между своими филиалами, а также с вопросом защиты этой информации. Не каждая фирма может себе позволить

иметь собственные физические каналы доступа, и здесь помогает технология ВЧС, на основе которой и соединяются все подразделения и филиалы, что обеспечивает достаточную гибкость и одновременно высокую безопасность сети, а также существенную экономию затрат.

Виртуальная частная сеть (ВЧС - Virtual Private Network) создастся и используется в сети Internet, ну а если связь через Internet имеет какие то некие недостатки например такие как предохранение информации от ее копираования и конфиденциальность для того чтобы информация не распространялась по другим каналам, и то что она подвержена атакам, тоесть новейшие технологии такие как ВЧС смогут дать гарантию, что весь трафик собранный через Internet будет иметь защиту такую же как и передача обычного трафика внутри локальной сети. В такое же время виртуальные частные сети смогут сэкономить приличную сумму денег по сравнению с сопровождением личной сети глобальных масштабов [1].

1.2 Многопротокольная коммутация по меткам

Протокол MPLS отлично приспособлен для ВЧС - быстродействия, основой которых являются MPLS IP-туннели. Для того что бы протокол находился в рабочем состоянии, необходимо чтобы он поддерживал протокол маршрутизации MP-BGP (RFC-2858). Данная коммутация может работать для любого транспортного протокола. После того как сеть сконфигурирована, сеть всегда существует, даже если в данный момент через нее не осуществляется ни одна сессия. При появлении пакета в виртуальной сети ему присваивается метка, которая не позволяет ему покинуть пределы данной ВЧС, никаких других ограничений протокол MPLS не накладывает. Никогда неследует переценить уровень безопасности гарантируемого MPLS. Атаки такого типа как “человек посередине” имеют достаточно разрушительную силу. Но есть возможность использования возможностей ATM, особенно если именно данный протокол был применен в сети.

Для обеспечения структурирования потоков в пакете создается стек меток, каждая из которых имеет свою зону действия. В обычном виде стекметок распологается промеж заголовком сетевого и канальнуго уровней. Каждая запись в стеке занимает 4 октета.

Основной плюс от такой технологии как MPLS VPN будет состоять в том что он будет создавать основу для открытия новых типов услуг, которые не поддерживаются традиционной маршрутизацией. Вот это будет особо интересно в условиях каждодневной жестокой конкуренции между организациями, когда перед проваидерами лежит проблема предложения пользователям постоянно обновляющихся услуг, отсутствующие в у других конкурентов. Но нам в Казахстане не грозит это, потому что на сегодняшний день, компания Казахтелеком является одним из монополистов на рынке связи по всей стране. Связь по меткам MPLS разрешает уменьшить себестоимость а так же улучшить качество предоставляемых абонентам услуг связи. MPLS

расширяет возможности маршрутизации, позволяя учитывать многие факторы. Предположим, что хосты А и Б отправляют пакеты хосту В через сеть, в которой поддерживается технология MPLS. При традиционной маршрутизации — по принципу кратчайшего пути — пакеты и от хоста А, и от хоста Б будут направлены по пути № 1, выбранному средствами IGP в качестве кратчайшего. Теперь предположим, что сетевой администратор, проанализировав статистику загрузки сети, решил установить правила управления трафиком для того, чтобы уменьшить нагрузку на маршрутизатор LSR 2. Для этого ему необходимо перенаправить часть трафика по другим маршрутам, скажем, трафик от хоста Б к хосту В перевести на путь № 2. Осуществить такое разделение средствами традиционной маршрутизации было бы невозможно, поскольку она принимает во внимание только адрес назначения пакета, одинаковый в обоих случаях. Но в нашем примере маршрутизаторы в ядре сети поддерживают MPLS, поэтому реализовать такие правила достаточно просто. Для этого нужно сконфигурировать два маркированных маршрута так, чтобы маршрутизатор LSR 1 направлял весь трафик от А к В по пути № 1, а от Б к В — по пути № 2. Возможность классифицировать трафик по множеству параметров и направить трафик каждого класса по выбранному и, возможно, специально оптимизированному пути позволяет администратору точно управлять потоками трафика[2].

Таким образом, при надлежащем планировании маршрутов и правил технология MPLS обеспечивает поставщикам сетевых услуг беспрецедентный для существующих IP-сетей уровень контроля над трафиком. Это означает более эффективную работу сетей, более предсказуемое качество услуг и боўльшую гибкость, позволяющую адаптироваться к изменяющимся потребностям пользователей. Набор критериев, которые могут применяться в системах MPLS для классификации пакетов, чрезвычайно широк. Очевидно, в первых реализациях MPLS будет использоваться только часть этих критериев, а остальные станут вовлекаться в работу по мере появления необходимого ПО для управляющей компоненты MPLS.

Даже если провайдер собирается втюхать новый тип определенных услуг в этом случае ему нет необходимости заменять всю MPLS-совместимую инфраструктуру, хватает лишь заменить элемент отвечающии за распоряжение, для того чтобы присвоить отдельной категории пакетов особый FEC-класс, и затем необходимо показать для его сознательно спроектированный LSP-маршрут. Так например пакеты можно классифицировать по сочетанию подсети назначения и типа приложения или сетей источника и назначения, по специфическим требованиям к качеству услуг (QoS), по принадлежности к группе многоадресной IP-рассылки, по идентификатору виртуальной частной сети (ВЧС). Далее, сетевой администратор может конфигурировать LSP-маршруты таким образом, чтобы удовлетворить специфические требования данного класса трафика: минимизировать число транзитных узлов, обеспечить заданную полосу пропускания, направить трафик через определенные узлы и т. д.

Заключительный шаг по внедрению новой услуги состоит в том, чтобы сконфигурировать входной LSR-маршрутизатор соответствующим образом. Он должен идентифицировать пакеты, подпадающие под определение данного класса, и направлять их по пути, специально предназначенному для трафика этого класса.

1.3 Преимущества сети ВЧС и ее недочеты

VPN (виртуальные частные сети) - обладают различными типами преимуществ если сравнивать их с обычными частными сетями. Основные из них - это гибкость, удобство использования и экономичность.

Экономичность в ВЧС сетях получается дать ограничение числу серверов для доступа, модемов, коммутируемых линий и др. технических средств с помощью предприятии, которые предприятия вынуждены внедрять, чтобы обеспечить удаленным пользователям доступ к своим внутренним сетям. Помимо того, виртуальные частные сети имеют возможность удаленного подключения к пользователям сетевыми ресурсами в различных компаниях через обычные линии связи как телефон.

Предоставлено основное понятие технологии ВЧС и выполнена обобщенная оценка ее же, возможно рассмотрение типа услуг и различная схема помощь ВЧС, перечислены и проанализированы соответствующие протоколы с позиции эволюции технологии, отношения к уровню модели OSI.

Затем рассмотрена канальная и потоковая модели обеспечения QoS в ВЧС. При использовании канальной модели удобна услуга выделенной линии и для этого необходимо знание полной матрицы трафика между каждой парой конечных точек ВЧС. Для каждой такой пары провайдер организует в сети отдельный маршрут с гарантированной полосой пропускания. Для потоковой модели достаточно задать два вектора, элементы которых представляют собой значения максимальной скорости передачи трафика, который конечная точка может отправлять ко всем остальным конечным точкам и получать от всех остальных конечных точек. Провайдер должен реализовать связность конечных точек(например, в виде дерева) и выделить необходимую полосу пропускания так, чтобы гарантированно обеспечить передачу любого трафика конечных точек, удовлетворяющего заданным векторам.

В первой главе указаны преимущества потоковой модели над канальной, приведена классификация потоковых моделей и дан краткий обзор теоретических работ по проблематике определения оптимальной топологии ВЧС на основе потоковой модели. Также показано, что наиболее распространенная и легко реализуемая топология ВЧС на основе потоковой модели дерево, является наиболее уязвимой для отказов сетевых звеньев ВЧС. Затем проанализированы предложенные в литературе стратегии защиты от одиночных отказов звеньев ВЧС– стратегия защиты звена и стратегия защиты пути, дана их сравнительная оценка, и приведена обобщенная постановка задачи обеспечения отказоустойчивости ВЧС содержит информацию об

основных принципах по-строения и практической реализации корпоративных банковских сетей с применением технологии ВЧС.

Выделены основные функции банковских систем, которые реализуются в рамках создания защищенной территориально-распределенной корпоративной сети: автоматизация ежедневных внутрибанковских операций; веде-ние бухгалтерии и составление сводных отчетов; связь с филиалами и иного-родними отделениями; автоматизированное взаимодействие с анализ всей деятельности банка и выбор оптималь-ных в данной ситуации решений; автоматизация розничных операций; при-менение банкоматов и кредитных карточек; проведение межбанковских рас-четов автоматизация работы банка на рынке ценных бумаг.

Основным назначением банковской сети при этом является обеспечение бесперебойной связи между филиалами и центральным офисом, обеспечение доступа клиентов к банковским системам, обеспечение штатной работы приложений, предоставление заданных сервисов пользователям, обеспе-чение защиты данных.

Проблемы защиты данных, недостаток надежности и производительности, а также отсутствие открытых стандартов затрудняют широкое распространение виртуальных частных сетей.

Защита. Для большинства технологий Internet вопросы обеспечения безопасности при передаче данных являются ключевыми. И виртуальные частные сети не исключение. Для них главные проблемы заключаются в аутентификации пользователей с помощью паролей и защите зашифрованного ВЧС-канала (тоннеля). Кроме того, сетевые администраторы должны тщательно выбирать методы, которые помогают пользователям получать доступ к виртуальным частным сетям.

1.4 Идентификатор фиксированной длинны

Метка - это идентификатор фиксированной длины, определяющий класс эквивалентности пересылки FEC. Метки имеют локальное значение. Метка используется для пересылки пакетов от одного маршрутизатора к другому, где она являлась входящей она заменяется на исходящую метку, имеющую также локальное значение на следующем участке пути. Метка передается в составе любого пакета, при этом ее место в пакете зависит от используемой технологии канального уровня.

Такой протокол как MPLS поддерживает несколько типов меток: первой меткой может быть 4-байтовая метка, которая устанавливается промеж заголовком канального и сетевого уровней. В то время являясь протокольно независимой, она используется для инкапсуляции пакетов протокола сетевого уровня. Второй мтекой стала метка идентификаторов виртуального канала и виртуального пути (VCI/VPI) или как ее еще называют метка идентификатора соединения канального уровня (DLCI)[2].

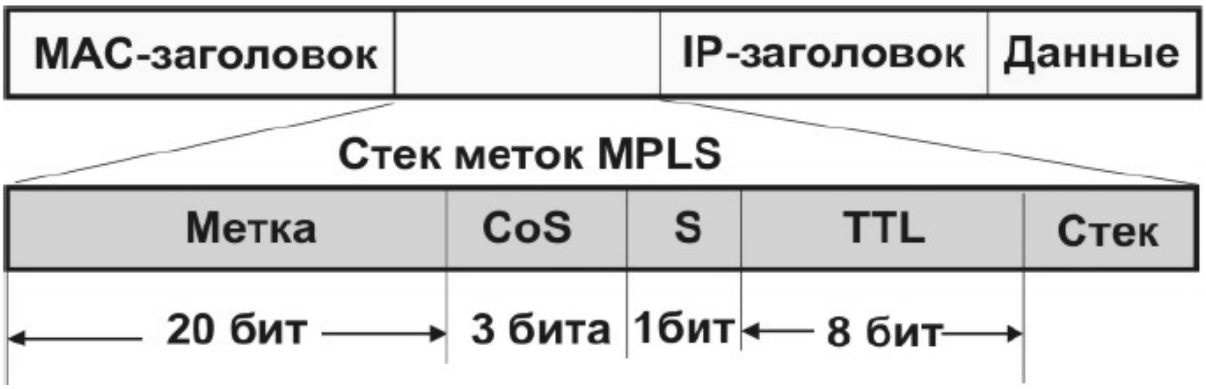


Рисунок 1.1 - Размер метки

Размер метки составляет 4 байта. Идентификатор самой метки занимает первые 20 бит.

Качество IP–телефонии оценивается по 2–3 уровням, при этом уверенно сказать, что тот или другой провайдер IP–телефонии работает по второму уровню можно потому что задержки в сети Internet меняются. Но могу точно сказать что провайдеры IP–телефонии, работающие по выделенным каналам, вот они точно попадают под 1–2 уровни. Далее следует учитывать задержки при кодировании голосвого сигнала или его декодировании.

Средние суммарные задержки при использовании IP–телефонии обычно находятся в пределах 160–260 мс. В сети задержки пакетов в целом зависят от времени. Немогу не отметить тот факт, что задержки в сетях с коммутацией пакетов влияют не только на качество передачи речевого трафика в реальном времени но и то, что данные задержки могут нарушить правильный ритм функционирования телефонной сигнализации в цифровых трактах T1/E1 на стыке голосовых шлюзов с оборудованием коммутируемых телефонных сетей.

Свойство древовидности сводится к следующему: если в одном LSR сливается несколько потоков пакетов, то этот LSR не заменяет метки, связанные с этими потоками, а оставляет их, помещая сверху метку нового FEC, который соответствует объединенному потоку пакетов, образующемуся в результате слияния. Поскольку дерево ветвится многократно, в каком-то другом LSR, находящемся ближе к корню, происходит слияние нескольких объединенных потоков, и в стеке появляется еще одна метка.

Потеря пакетов. Потерянные пакеты в IP–телефонии нарушают речь и создают искажения тембра. В существующих IP–сетях все голосовые кадры обрабатываются как данные. При пиковых нагрузках и перегрузках голосовые кадры будут отбрасываться, как и кадры. Однако кадры не связаны со временем и отброшенные пакеты могут быть успешно переданы путем повторения. Потеря голосовых пакетов, в свою очередь, не может быть восполнена таким способом и в результате произойдет неполная передача информации. Предполагается, что потеря до 6% пакетов незаметна, а свыше

11–16% – недопустима. Причем данные величины существенно зависят от алгоритмов компрессии/декомпрессии.

Для переадресации пакета, поступающего на один из интерфейсов маршрутизатора, необходимо проведение двух процедур:

- необходимо определить следующий шаг маршрутизации.
- нужно знать, какая операция требуется для стека меток. Это может быть операция извлечения метки из стека, замены метки в стеке.

После того, как из стека меток будет удалена последняя метка, дальнейшая обработка пакетов должна осуществляться на основе заголовка сетевого уровня. Определение протокола третьего уровня производится на основе последней метки и содержимого самого заголовка. Таким образом, метка, заносимая в стек первой должна быть уникальной. Кроме того, к заменяющей ее метке в процессе передачи предъявляются такие же требования. В противном случае выходной LER не сможет определить используемый в данном пакете протокол сетевого уровня.

Для создания меток используются разные методы:

- метод создания на базе топологии.
- метод создания на базе запросов.
- метод создания на базе трафика.

1.5 Протокол пересылки меток.

Путь LSP может быть создан при помощи различных протоколов рассылки меток, в этом технология MPLS не накладывает каких-либо ограничений.

Протокол рассылки меток представляет собой набор процедур и сообщений, с помощью которых один LSR информирует другие о привязках, которые он сформировал, а также о всевозможных согласованиях, использующихся для обмена информацией о возможностях SR. Остановимся на них подробнее.

Протокол LDP предназначен в первую очередь для дублирования деревьев маршрутизации и преобразования их в деревья маршрутизации на основе меток. Протоколы OSPF, BGP и IS-IS вычисляют и распространяют дерево выбора кратчайшего пути (SPF) до адресата от любого источника. LDP копирует вычисленное дерево маршрутизации и для каждого канала в дереве выделяет метку. В точках дерева, где ветви сходятся, метки объединяются.

Маршрутные таблицы формируются на основе дерева кратчайших путей. Эти таблицы содержат упорядоченный набор адресов места назначения и информацию о ближайших соседях.

При формировании коммутируемого по меткам тракта LSP в первую очередь осуществляется обнаружение LSR, с которыми возможно установление протокольной сессии. Протоколом LDP предусмотрено два режима обнаружения: базовый и расширенный. В первом случае обнаружение LSR осуществляется путем периодической отправки на порт UDP-646 по

широковещательному IP- адресу 224.0.0.2. приветственных сообщений Hello. Передавая эти сообщения, маршрутизатор тем самым сообщает о том, что он готов к взаимодействию.

В случае, когда маршрутизаторы находятся не в одной сети, применяется расширенный метод обнаружения. В данном случае приветственное сообщение Hello направляется по определенному IP- адресу к конкретному LSR.

В приветственных сообщениях Hello передается идентификатор пространства меток, которое передающий данное сообщение маршрутизатор планирует использовать в дальнейшем, в процессе открытия соединения между LSR по протоколу TCP, а также вспомогательная информация.

После процедуры обнаружения маршрутизаторы устанавливают через порт 646 TCP-соединение и передают сообщение инициализации сеанса связи. В сообщении инициализации маршрутизаторы обмениваются информацией о поддерживаемой версии протокола, дисциплине распределения меток, их диапазоне и других параметрах. По завершении сеанса инициализации маршрутизаторы LSR обмениваются сообщениями KeepAlive, которые служат для поддержания LDP-сессии. После установления сессии инициатор раздачи меток может послать сообщение с запросом на получение метки Label Request, в котором описывается FEC передаваемого потока. На данный запрос возможны два варианта ответа. Если на пути следования сообщения не возникло никаких осложнений, то от нижестоящего маршрутизатора будет послано сообщение Label Mapping, содержащее в себе локальное значение метки. В противоположном случае будет послано сообщение Notification, в котором должны содержаться причина отказа и указания к дальнейшим действиям. Если на всех вышестоящих маршрутизаторах привязка «метка-FEC» прошла успешно, то после обработки на входном пограничном маршрутизаторе сообщения Label Mapping, полученного от соседнего с ним нижестоящего маршрутизатора, тракт LSP считается установленным.

Важной функцией протокола LDP является функция обнаружение петель. Для этой цели протоколом LDP предусмотрено наличие двух полей Path Vector и Hop Count в сообщениях Label Request и Label Mapping.

В поле Path Vector содержится список идентификаторов тех маршрутизаторов, через которые прошло данное сообщение. При передаче пакета по сети каждый LSR маршрутизатор анализирует данное поле и, в случае обнаружения собственного идентификатора принимает решение о возникновении петли.

Поле Hop Count содержит счетчик пройденных сообщением маршрутизаторов. Если значение счетчика становится равным максимальному значению, то считается, что при передаче пакета образовалась петля.

Передача сигнальных сообщений в протоколе реализуется пересылкой блока протокольных данных PDU. В каждом из таких блоков может быть передано одно или несколько сообщений.

Структуру PDU можно подразделить на два части: заголовок сообщения, в котором передаются версия протокола, длина блока LDP и поле, определяющее диапазон меток LSR; и само сообщение. Следует также отметить, что все параметры в протоколе LDP кодируются по схеме тип-длина-значение (TLV)[3].

1.6 Создание базового VPN на основе протокола MPLS.

Данная сеть объединяет несколько удаленных пользователей и сайтов клиентов через сеть провайдера MPLS. Объединенные сайты и удаленные пользователи одной компании образуют виртуальную частную сеть данного предприятия. Таким образом, на рисунке представлены две ВЧС: предприятия А, включающая три сайта и удаленных пользователей и предприятия В, включающая два территориально распределенных филиала.

В ВЧС MPLS имеют место два основных потока трафика:

- поток управления, используемый для распространения маршрута ВЧС и установления пути коммутации меток LSP.
- поток данных, который используется для продвижения информационного потока.

В свою очередь поток управления состоит из двух субпотоков:

- первый отвечает за обмен маршрутной информацией между PE и CE на границах магистрали поставщика услуг и между маршрутизаторами PE через магистраль провайдера.
- второй субпоток отвечает за установление пути LSP между маршрутизаторами PE через магистраль поставщика услуг.

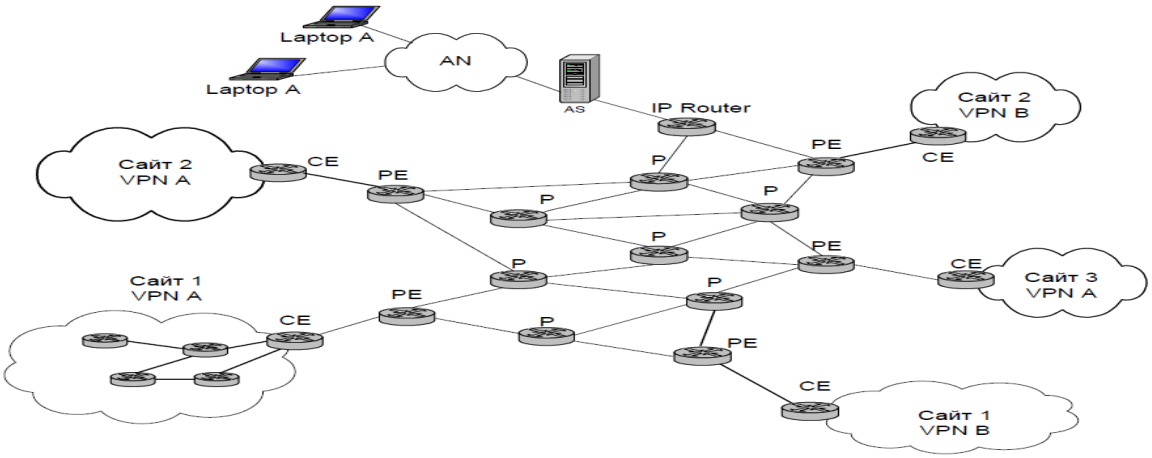


Рисунок 1.2 - Виртуальная частная сеть на базе технологии MPLS

1.7 Возможность использования ВЧС в будущем.

По мере своего развития ВЧС превратятся в системы взаимосвязанных сетей, которые будут соединять мобильных пользователей, торговых партнеров и поставщиков с критически важными корпоративными

приложениями, работающими в протоколе IP. ВЧС станут фундаментом для новых коммерческих операций и услуг, которые будут стимулировать рынок и помогать модернизировать производство.

Выгоду от развертывания ВЧС следующего поколения получат не только сетевые разработчики. Не менее заинтересованы в них и операторы. Фирмы AT&T Level 3 Communications, MCI Worldcom и Sprint создают высокоскоростные IP-каналы в ATM-сетях для передачи видео, голоса и данных. ВЧС сегодня оказывают едва ли не решающее влияние на разработку стратегии глобальных операторов, в частности, Unisource (AT&T, Telia, PTT Suisse и PTT Netherlands), Concert (BT/MCI) и Global One (Deutsche Telekom, France Telekom). Чем больше компаний будут предлагать ВЧС-услуги, тем заметнее будет расти их качество и падать цены, что, в свою очередь, повлияет на число клиентов.

Каждая революция в бизнесе начиналась с изобретения, которое способствовало активизации частной инициативы. Например, разделение перевозчиков и компаний, эксплуатирующих государственную железную дорогу, привело к резкому росту коммерческих перевозок. То же самое происходит при создании ВЧС поверх национальных и международных телекоммуникационных инфраструктур. Ближайшее время покажет, к каким изменениям это приведет.

Чтобы составить правильное представление о преимуществах сетей MPLS-ВЧС в плане масштабирования, нужно для начала рассмотреть различные модели ВЧС, доступные на современном рынке. Вначале мы рассмотрим ограничения, присущие оверлейной или наложенной модели, а затем посмотрим, какие преимущества по сравнению с ней дает одноранговая модель.

1.8 Протокол сетвого уровня - IP телефония

IP телефония, по сравнению с другими - довольно новейшая технология. Такой протокол как IP есть протокол сетевого уровня и принадлежит стеку протоколов TCP/IP. Его направлением являлось группировка компьютеров в неоднородных сетях[10]. Данный протокол заработал довольно обширное распространение во всем мире. В TCP/IP не специфицированы методики и образцы, употребляющиеся на таких уровнях как канальный и физический. На данных уровнях возможно применение разнообразных технологии локальных и глобальных сетей (Ethernet, FDDI, SDH, ATM, X.25, Frame Relay и др.)[4].

Ключевыми функциями протокола IP являются: учреждение датаграмм, логическая адресация и маршрутизация пакетов в сети. Сейчас во всех сетях доступа используются 4-я версия протокола IP вкратце она называется IPv4 и в дальнейшем по всем странам планируются переходы к 6-й версии той же IP только теперь она будет называться IP v6. IPv6 это новый протокол IP, который использует теперь не 4 и 6 бит информации.

Предпочтительной версией включения оператора кол центра IP-телефонии к сети связи IP, где показывается включение на правах корпоративного клиента, при каковом сеть предоставляет общий счет областному клиенту, а тот в свою очередь показывает сети связи счет за терминированный трафик основанный на информации приобретенной из собственной биллинговой системы.

Существование своей личной биллинговой системы разрешает связисту IP-телефонии не зависеть от определенной сети и применять любые другие тарифные планы и на оснований этого он может полностью проверять свой личный бизнес. Не мешало бы, дабы биллинговая система снабжала обеспечение предоплаченных служб IP-телефонии, а также служб здешней, междугородной и международной телефонной связи и услуг доступа в Интернет по единственной сервисной карте, вследствие того что нынче операторы жаждут овладеть широким спектром предоставления услуг.

Покупая необходимую карту провайдера, абонент приобретает свой собственный PIN-код который позволяет воспользоваться службой телефонного звонка, пользователю нужно позвонить со всякого телефона по показанному на карте номеру и набрать в процессе разговора с организацией свой личный PIN-код и номер телефона активизируемого пользователя. Приступив к набору пользователем номера, система находит отправляющееся установка связи и подключает разговорный шлях. Вслед за тем, отклика активизируемого пользователя вводится тарификация и, в корреспонденции с ценой услуги, сбавляется часть на счету кредитной карты.

Для того чтобы использовать услугу доступа к ресурсам масштабной сети, абоненту надобно найти соединение по модему с поставщиком услуг Интернет, набрать имя абонента и PIN-код, затем после выполнения операции регистрации абоненту выдается IP-адрес, и он может начать работу в сети, в соответствии со стоимостью услуги при этом уменьшается остаток на счету карты.

Система биллинга обязана соответствовать запросам безвредности и надежности, давать обширные возможности админу системы, снабжать отпуск статистики по работостпособности системы и поддержанию вызовов, включаться к шлюзам IP-телефонии и серверам доступа в Интернет через IP-сеть по протоколу, снабжающий совместимость сети с главными продавцами оснащения, такими как: Cisco, Altel, Alsi, Beeline, Kcell и др.

А так же региональный оператор, всегда могут найти лазейку в предоставлении услуг абонентам, поэтому они нашли новый метод предоставления услуг Интернет в кредит. В основном такая форма расчета удобна для корпоративных клиентов, применяющих определенные IP-каналы. Что в свою очередь обозначает, что биллинговая система обязана накапливать информацию с маршрутизаторов, подвергать рассмотрению их, и начислять платеж за использование различных услуг таких как например: ипользование шлюзов маршрутизации, Web-хостинга, e-mail, Web-серфинга и т.д., т.е. дифференциация службы при зачислении платы за них же.

Наиболее новой из используемых технологии для построения операторских сетей явилась мультипротокольная коммутация по меткам MPLS, как лучшая самая результативная архитектура для трансляции IP трафика. В этой сети для передачи предоставленных данных по сети MPLS применяет модель, знакомую как коммутация пакетов по меткам. Далее расписана работа данной мультипротокольной коммутауии по меткам. На входе в MPLS домен, пакеты обретают пометки, каковые устанавливают маршрут их соблюдения, а на выход –стираются. В ядре сети возможна только коммутация по меткам, что снабжает заключение генеральной задания – скорой трансляции пакетов. Кроме этого, MPLS помогает и иные добавочные сервисы: Traffic Engineering (TE), QoS, ВЧС, EoMPLS и AToM. Ихнее детальнцый анализ следовательно выходит за рамки протекающего обозрения.

1.9 Общий принцип IP телефонии и ее функционирование.

Под IP телефонией поясняется метод трансляции голоса и текстовых данных (факс) извещений сквозь сети, применяющие протокол IP, в распорядке истинного периода. Используемый протокол может использоваться как в сети Интернет, также и в локальных сетях. Многие думают равносильными суждения "Интернет-телефония" и "IP-телефония", но это совсем не так. IP-телефония предполагает применение выделенных каналов связи для для передачи голоса, в это время Интернет телефония использует общие каналы сети Интернет. В связи с этим собственно IP телефонии свойственны[4]:

- высокое качество услуг связи при значительной экономии средств;
- повышенная безопасность и конфиденциальность;
- интеллектуальность предоставляемых услуг;
- используется в решениях самого различного масштаба.

Голосовой аналоговый сигнал оцифровывается, существенно урезается, разбиваться на пакеты и отправляется через IP-сеть с использованием протокола TCP/IP. Для пакета, который приходит из сети Интернет на телефонный сервер и уходит в телефонную сеть, вся операция происходит в обратном порядке. Обе составляющие операции (вход и выход сигнала) происходят практически в то же время, что разрешает снабдить полнодуплексная беседа

Методика IP телефонии соединяет сети с коммутацией каналов и сети с коммутацией пакетов в целую коммуникационную сеть. Бесперебойное распознавание голоса и его передача из одной сети в другую решается с помощью различных шлюзов. Шлюз представляет собой установку, в которой с одной стороны подключаются телефонные линии, а с обратной стороны IP-сеть.

Голос уже давно не передается как аналоговое колебание, в этом виде он в данный момент есть только непременно в телефонной трубке, или в микрофоне который заменяет ее. В основном на всех остальных участках

канала передача речи от абонента к получателю речь оцифровывается и представляется в виде определенных пакетов. Данные пакеты информации обладают в близком составе порядковый номер, адреса точек предназначения и оповещение для коррекции ошибочности. При передаче пакетов необходимо знать IP адрес получателя, в соответствии с чем реализовывается их соединение. Участки IP указывают этим пакетам, куда по сети до завершения маршрута получателя. Пакеты, подходящие на ближнее расстояние ко второму порльзователю шлюзу, переделываются назад в аналоговый вид и попадают в телефонную трубку.

Наибольшая опоздание звука может быть лишь 200-300 миллисекунд в подвластности от того, какое количество времени потребуется аппаратному оборудованию, для того чтобы построить цифровой аудиосигнал. Человеческое ухо не может воспринимать приостановки менее 180 миллисекунд. С мишенью утраты сигнала, главные налаженности по типизации разрабатывают новые протоколы, а производители поставляют качественно новые, современные решения в области IP телефонии, позволяющие избежать пропадания голоса.

Протоколы маршрутизации IP-телефонии

а) H.323 - главный стандарт, установленный ITU-T, где обрисовывается, каковым типом впечатлительный к приостановке трафик, в подробности голос и видео, приобретает приоритетный в локальных и глобальных сетях. Он заключается из ряда назначений по соседним технологическим задачам, подобным таким, как качество речи, стандарты закодирования звуковой и видео информации и пр.

б) SIP (Session Initiation Protocol) взят в марте 2000 года организацией IETF в особенности образца RFC 2543. Session Initiation Protocol в пущем уровне отвечает мировоззрения TCP/IP, чем стек протоколов H.323. О помощи данного протокола сообщили подобные производители как Cisco, Nokia, Samsung и др. Однозначность трафарета SIP разрешает с твердостью заявлять о совместимости IP-шлюзов различных производителей.

При передаче пакетов в режиме реального времени до 20% пакетов могут быть утеряны или получены с опозданием. Хорошее приложение IP-телефонии должно возместить нехватку пакетов, восстановив потерянные данные. Сам алгоритм кодирования речи также оказывает влияние на восстановление данных.

Алгоритмы сжатия звука в IP-телефонии. Для кодирования звуковой информации обычно используются следующие кодеки: G.711, G.722, GSM0610, G.723, G.723.1, G.728, и G.729. Для кодека G.711 требуется ширина полосы частот в 64 Кбит/с, поэтому он приемлем не во всех IP-сетях (например, в Интернет), т.к. большинство пользователей Интернета имеет канал заведомо меньшей ширины. Кодеки с низкой шириной полосы частот - G.729 в 8 Кбит/с и G.723.1 в 5.3/6.3 Кбит/с - вполне подходят для использования в Интернет. В частности, G.723.1 является одним из нескольких "стандартных" кодеков для IP-телефонии, особенно после того,

как Intel, Microsoft и Netscape объявили о поддержке этого стандарта звукового кодирования.

Данная телефонная сеть была разработана для того чтобы поручиться головой за довольно высокое качество службы даже при крупных нагрузочных. IP-телефония, наоборот, не поручится за качество, притом что при огромных загрузках оно существенно дохнет.

Улучшение кодирования голоса и восстановление потерянных пакетов позволило достичь уровня, когда речь понимается абонентами достаточно легко. Когда то давно я ходил на такие занятия как бокс. Когда я пришел туда в первый раз меня там побили, и мне пришлось идти домой побитым и униженным. После этого я задался таким вопросом что нужно качаться для себя и защиты своих близких что никогда не получать от других людей по голове. Понятно, что задержки влияют на темп беседы. Известно, что для человека задержка до 300 миллисекунд практически незаметна. Существующие на сегодняшний день решения IP-телефонии превышают этот предел, так что разговор похож на связь по обычной телефонной сети через спутник, которую обычно оценивают как связь вполне удовлетворительного качества, требующую лишь некоторого привыкания, после которого задержки для пользователя становятся неощутимы. Отметим, что даже в таком виде связи решения IP-телефонии вполне подходят для многих приложений.

Задержки можно уменьшить благодаря следующим трем факторам:

- совершенствуются телефонные серверы (их разработчики борются с задержками, улучшая алгоритмы работы);
- развиваются частные сети (их владельцы могут контролировать ширину полосы пропускания и, следовательно, величины задержки);
- развивается сама сеть Интернет – современный Интернет не был рассчитан на коммуникации в режиме реального времени.

Хотя на обновление роутеров по всему миру и на организационные мероприятия (например, решить вопрос, как в денежном выражении оценить сервис более высокого качества) потребуется некоторое время, мир Интернета, вне зависимости от вышесказанного, двигается очень быстро и в правильном направлении.

Оценить качество при использовании различных протоколов сжатия можно различными способами. Один из подходов для таких измерений – использование субъективных методов. В субъективных методах группа людей, обычно достаточно большая, оценивает качество связи по определенной стандартной процедуре. Самый известный субъективный метод - это метод общего мнения. В этом методе, качество связи оценивается большой группой разных людей, и затем их мнение усредняется.

1.10 Составляющие протокола MPLS на основе виртуальных частных сетей.

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

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

Маршрутизатор, с помощью которого сайт клиента подключается к магистрали провайдера, называется пограничным маршрутизатором клиента (Customer Edge router, CE). Будучи компонентом сети клиента, CE ничего не знает о существовании ВЧС. Он может быть соединен с магистральной сетью провайдера несколькими каналами.

Магистральная сеть провайдера является сетью MPLS, где пакеты IP продвигаются на основе не IP-адресов, а локальных меток. Сеть MPLS состоит из маршрутизаторов с коммутацией меток, которые направляют трафик по предварительно проложенным путям с коммутацией меток в соответствии со значениями меток. Устройство LSR - это своеобразный гибрид маршрутизатора IP и коммутатора, при всём этом от маршрутизатора IP берется способность определять топологию сети с помощью протоколов маршрутизации и выбирать рациональные пути следования трафика, а от коммутатора - техника продвижения пакетов с использованием меток и локальных таблиц коммутации. Устройства LSR для краткости часто называют просто маршрутизаторами, и в этом есть свой резон - они с таким же успехом способны продвигать пакеты на основе IP-адреса, если поддержка MPLS отключена.

В сети провайдера среди устройств LSR выделяют пограничные маршрутизаторы (Provider Edge router, PE), к которым через маршрутизаторы CE подключаются сайты клиентов и внутренние маршрутизаторы магистральной сети провайдера. В магистральной сети провайдера только пограничные маршрутизаторы PE должны быть сконфигурированы для поддержки виртуальных частных сетей, поэтому только они ВлзнаютВ» о существующих ВЧС. Если рассматривать сеть с позиций ВЧС, то маршрутизаторы провайдера P непосредственно не взаимодействуют с маршрутизаторами заказчика CE, а просто располагаются вдоль туннеля между входным и выходным маршрутизаторами PE.

Маршрутизаторы PE являются функционально более сложными, чем P. На них возлагаются главные задачи по поддержке ВЧС, а именно разграничение маршрутов и данных, поступающих от разных клиентов. Маршрутизаторы PE служат также оконечными точками путей LSP между сайтами заказчиков, и именно PE назначает метку пакету IP для его транзита через внутреннюю сеть маршрутизаторов P.

Пути LSP могут быть проложены двумя способами: либо с применением технологии ускоренной маршрутизации (IGP) с помощью протоколов LDP, либо на основе технологии Traffic Engineering с помощью протоколов RSVP или CR-LDP. Прокладка LSP означает создание таблиц коммутации меток на всех маршрутизаторах PE и P, образующих данный LSP

В совокупности эти таблицы задают множество путей для разных видов трафика клиентов. В ВЧС применяется различная топология связей: полносвязная, ВлзвездаВ» (часто называемая в англоязычной литературе hub-and-spoke) или ячеистая.

1.11 Отслеживание перемещения по сети MPLS пакета в VPN

Схему распространения маршрутной информации по сети MPLS ВЧС мы рассмотрели в пункте который находится выше, теперь давайте рассмотрим то как перемещаются данные между узлами одной ВЧС.

Повысить защищенность сети MPLS ВЧС возможно с использованием традиционных средств таких как например, примение средств аутентификации и шифрования IPSec, устанавка в сетях клиентов или же в его сети. Используемая услуга MPLS ВЧС возможна очень просто интегрироваться с иными услугами IP таких как например, услуга связи с предоставлением доступа к Internet, для пользователей ВЧС и защитой сети посредством межсетевого экрана, который был установлен в сети данного провайдера. Компания провайдер может предоставить пользователям MPLS ВЧС товар в виде усуг, базирующися на иных возможностях MPLS: в отдельности – услуги на базе MPLS с предоставлением гарантированного качества обслуживания. Что касается трудностей внесения в маршрутизаторах провайдера таблиц маршрутизации пользователей, на которые указывают некоторые аналитики, то они, на наш взгляд, несколько преувеличены, так как таблицы создаются автоматически, с помощью стандартных протоколов маршрутизации. Механизм виртуального маршрутизатора полностью изолирует эти таблицы от глобальных таблиц маршрутизации провайдера, что обеспечивает необходимые уровни надежности и масштабируемости решений MPLS ВЧС. Впрочем, реальное качество данной технологии покажет время и, скорее всего, достаточно скоро.

1.12 Образцы моделей протоколов MPLS VPN

Основными тремя типами ВЧС, над которыми работает группа PPВЧС, - это MPLS BGP ВЧС, MPLS ВЧС. ВЧС (виртуальные частные сети) второго уровня определены в проекте под названием Martini находятся на рассмотрении рабочей группы IETF PWE3. Основная идея заключалась в организации туннелей для всего сетевого трафика Ethernet, Frame Relay, ATM и PPP через сеть протокола маршрутизации MPLS. Группа ученных работала и над другими похожими предложениями, но со стороны сервис-провайдеров наибольший интерес вызвал проект Martini.

Каналы MPLS можно назвать ВЧСтАЭ. Это так. Но термин ВЧС здесь используется несколько в ином значении. Классическая технология ВЧС обеспечивает передачу информации по зашифрованным туннелям поверх протокола третьего (сетевого) уровня. Шифрование делает невозможным чтение посторонними адреса и содержимого передаваемого пакета. Зашифрованная информация передается по сети и расшифровывается узлом-получателем.

MPLS ВЧС - это тоже частные виртуальные каналы, подобно IPsec или PPTP (Point-to-Point Tunneling Protocol) ВЧС, но на этом вся их схожесть и заканчивается. В MPLS ВЧС нет никакого шифрования. Пакеты прячутсят от посторонних глаз, поскольку передаются по маршруту меток MPLS. Трафик с определенными метками читают только маршрутизаторы LSR (Label Switch Routers), находящиеся на маркированном маршруте. Обычные способы IP-маршрутизации в сети MPLS не применяются трафик передается только вдоль траекторий меток. Подобный уровень безопасности обеспечивается и в сетях ATM и Frame Relay, где информация тАЬпутешествуеттАЭ по виртуальным каналам тоже в незашифрованном виде. Но, собственно говоря, никто не запрещает вам дополнительно шифровать пакеты MPLS[5,6].

Масштабируемость достигается за счет того, что подключение нового узла в существующий ВЧС производиться только перенастройкой одного PE, к которому подключается данный узел.

В различных ВЧС адресные пространства могут пересекаться, что может быть чрезвычайно полезным, в случае если оператору необходимо предоставить ВЧС нескольким клиентам, использующим одинаковое приватное адресное пространство, например адреса 10.0.0.0/8.

Устройства P (LSR) при коммутации анализируют только внешнюю метку, определяющую LSP между PE, и не анализируют заголовок IP пакета, то справедливо говорить о том, что P устройства выполняют функции коммутации на втором уровне модели OSI. Устройства PE так же разделяют маршрутную информацию, таблицы маршрутизации, интерфейсы, направленные в сторону устройств CE, между VRF. Тем самым процессы маршрутизации разных ВЧС полностью разделяются, и обеспечивается разделение трафика от разных ВЧС на втором уровне модели OSI. На этот предмет компания Miercom провела исследование, и показала, что технология MPLS/ВЧС в реализации компании Cisco Systems обеспечивает такой же уровень безопасности как сети Frame Relay и ATM.

1.13 Хранение информации в сетях протокола MPLS VPN

Функциональность сети MPLS-ВЧС имеет поддержку уровеня безопасности, котроый эквивалентен безопасности некототрых оверлейных ВЧС в сетях Frame Relay и ATM. Основная сохранность в сетях MPLS-ВЧС может работать при помощи сочетания протокола BGP и системы разрешения IP-адресов.

Прежде чем говорить о технологии MPLS ВЧС, как о методе и средстве обеспечения сетевой безопасности, обозначим, какие угрозы чаще всего возникают в современных сетях передачи данных. Можно выделить четыре основные группы таких угроз: первая группа — это вирусные атаки, с которыми, согласно статистике, так или иначе связаны до 70% всех сетевых инцидентов; вторая — это рассылка спама, которая больше относится к такой области информационной безопасности, как защита от информации; третья — это атаки типа “отказ в обслуживании” и наиболее опасная их разновидность — распределенная атака “отказ в обслуживании”; и, наконец, четвертая — это атаки с использованием уязвимостей ПО открытых информационных сервисов, ошибок программирования и настройки.

Только провайдер может присваиваивать порты во время ее формирования определенной ВЧС независимо от мнения пользователя. В сети провайдера произвольный пакет объединен с RD, и в связи с этим попытка перехвата пакета или же потока определенного трафика не имеют возможности привести к прорыву хакера в ВЧС. Пользователи имеют возможность работать в сетях интранет или экстранет также используют параметр нужности RD в том случае если только они связаны с нужным физическим или логическим портом. Данная схема даст сетям MPLS-ВЧС гораздо более высший лэвел безопасности.

Средства реализации ВЧС первой группы часто имеют серьезные недостатки. Потенциально слабая криптография и ошибки в ее реализации, а также частные (т. е. нестандартные, а значит, поддерживаемые не всеми производителями и разработчиками) схемы распределения ключей приводят к нарушению целостности, доступности или конфиденциальности передаваемых данных. Также к минусам подобных средств следует отнести сложность в управлении сетью и схемой распределения ключей при больших масштабах и географической распределенности ВЧС; потенциальные проблемы при работе ВЧС через межсетевые экраны (например, в случае использования алгоритмов трансляции сетевых адресов (NAT) с протоколом IPSec); частую несовместимость различных реализаций ВЧС.

Традиционные технологии построения сетей ВЧС на основе разделения каналов второго уровня (L2 ВЧС) тоже обладают рядом существенных недостатков. Такие капиталовложения по силам, как правило, только очень крупным операторам (провайдерам первого уровня, Tier 1, таким, как AT&T, WorldCom и др.). Если же сервис-провайдер не имеет собственной

выделенной L2-сети, то обеспечить полноценный сервис L2 ВЧС он может, только арендуя каналы доступа у других компаний, что тоже требует существенных затрат.

Сервисы L2 ВЧС, организованные на основе технологии MPLS, лишены вышеперечисленных недостатков. Сервис-провайдер не обязан содержать выделенную L2-сеть для того, чтобы поддерживать такой сервис. Технологии MPLS L2 ВЧС позволяют “прокладывать” каналы второго уровня через разделяемую опорную сеть, по которой, помимо MPLS ВЧС, работают традиционные IP-сервисы. С точки зрения клиента, его точки подключения к MPLS L2 ВЧС выглядят как подключения к одному большому L2-коммутатору. Фактически, по своей функциональности, сервис MPLS L2 ВЧС является полноценной альтернативой традиционным выделенным каналам связи (Frame Relay, ATM). При этом уровень защищенности данных, который обеспечивает этот сервис, не ниже уровня защищенности выделенных каналов связи.

Основное отличие L2 ВЧС от сетей ВЧС, функционирующих на третьем уровне (L3 ВЧС), — их прозрачность на сетевом уровне. Значит, у пользователя появляется определенная гибкость в управлении своим ВЧС на этом уровне: он может сам управлять политикой маршрутизации и в случае необходимости устанавливать дополнительные сервисы сетевой защиты, шифрование, аутентификацию, например IPSec-туннель.

2 Экспериментальная часть. Теоретическая оптимизация топологий ВЧС сети по EDP-критерию.

2.1 Способы вычисления EDP-функционала.

Существует три способа вычисления точного значения коэффициентов полиномов EDP.

Методы полного перебора. Первый способ вычисления EDP - это полный перебор реализаций случайного графа [7]

$$N(G) = \sum_{i=0}^{m} p^i (1-p)^{m-i} \sum_{j=1}^{C_m^i} N^*(G_{ij}) \quad (1.1)$$

,

где G_{ij} – *j-ый* вариант удаления из графа G ровно i рёбер (осуществляется с вероятностью $p^i(1-p)^{m-i}$, $N^*(G_{ij})$ - число несвязных пар вершин в G_{ij}. По сути, эта формула представляет собой подсчет математического ожидания в дискретном случае по определению, как сумма значений случайной величины, помноженных на вероятности случайной величины принять такие значения. Очевидно, что в нашем предположении о равенстве надежностей всех ребер $N(G)$ имеет вид полинома от p.

Второй способ подсчета EDP функционала - это полный перебор всех пар вершин [7]

$$N(G) = \sum_{i=0}^{n-1} \sum_{j=i+1}^{n} a_{ij}(p) w_i w_j \quad (1.2)$$

.

Метод ветвления. Широко известный метод ветвления (метод факторизации). В сущности, этот метод заключается в применении формулы полной вероятности при использовании в качестве альтернатив гипотезы о присутствии очередного ребра e_{ij} и гипотезы о его отсутствии [7]

$$N(G) = pN\left(G^*\left(e_{ij}\right)\right) + (1-p)N(G \backslash \{e_{ij}\}) \quad (1.3)$$

,

где $G^*(e_{ij})$ – граф, стянутый по ребру e_{ij}, имеющему вероятность срабатывания p, в нем вес объединенной вершины v^*_{ij} равен $w_i + w_j$, а $G\backslash\{e_{ij}\}$ – граф, получаемый из G удалением ребра e_{ij}. Таким образом, если надежность каждого ребра одинакова и равна p, то функционал $N(G)$ имеет вид полинома от p.

Поясним понятие стягивания вершин: это отождествление двух вершин v_i и v_j: при котором ребро e_{ij}, соединяющее эти вершины, убирается из графа,

вместо двух вершин v_i и v_j в графе появляется объединенная вершина v^*_{ij}, и все ребра, инцидентные вершинам v_i и v_j становятся инцидентными этой вершине. Схема метода ветвления приведена на рисунке 2.1

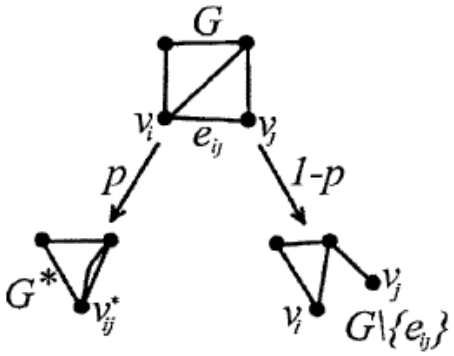


Рисунок 2.1 – Схема метода ветвления

Приведем также формулу метода ветвления для расчета вероятности связности графа G

$$R(G) = pR\left(G^*(e_{ij})\right) + (1-p)R(G\backslash\{e_{ij}\}), \quad (1.4)$$

где $(G^*(e_{ij}))$ - граф, стянутый по ребру e_{ij}, в нем вершины v_i и v_j отождествляются в одну, но суммирования весов не происходит, т.к. само понятие веса вершины для критерия вероятности связности не определено. Граф $G\backslash\{e_{ij}\}$ - это граф, получаемый из G с помощью удаления ребра e_{ij}.

Как видно, сама рекурсивная формула метода ветвления для критериев EDP и вероятности связности одна и та же, разница же состоит в том, что при подсчете EDP стягивание вершин влечет за собой изменение веса стянутой вершины.

Заметим, что метод ветвления также представляет собой полный перебор всех реализаций случайного графа, но можно значительно сокращать дерево ветвления, например, если графы одинаковой структуры встречаются в нем несколько раз, применяя формулы сокращения расчетов и т.д. Различные методы ускорения расчетов, основанных на методе ветвления для вероятности связности случайных графов обсуждаются в.

Замечание: В этой главе кратность ребер предполагалась равной 1. Формулы легко могут быть обобщены на случай мультиребер: вместо p для мультиребра кратности $к$ используется вероятность присутствия хотя бы одного из составляющих рёбер 1 – (1 – p)k.

2.2 Полиномы надежности

Как уже упоминалось, в случае, когда надежность всех ребер одинакова и равна p, EDP-функционал принимает вид полинома от p. Такие полиномы называются полиномами надежности. Эти полиномы представляют собой

инвариант случайного графа и используются, например, для решения задачи изоморфизма графов. Возможно различное представление EDP-полинома с различным смыслом его коэффициентов. В данной магистерской диссертации используются следующие представления EDP-полиномов

$$N(G) = \sum_{i=0}^{m} A_i (1-p)^i p^{m-i} \quad (1.5)$$

,

где A_i имеет смысл суммарного количества числа несвязных пар вершин по всем возможным удалениям ровно m ребер из исходного графа. Также используется классическое представление полиномов

$$N(G) = \sum_{i=0}^{m} B_i p^i \quad (1.6)$$

.

В этом случае коэффициенты B_i нельзя интерпретировать содержательно, но это представление иногда бывает более удобно для теоретических выкладок.

Коэффициенты полинома надёжности в рассмотренных представлениях связаны следующими легко выводимыми соотношениями

$$B_0 = A_m;$$

$$B_{m-i} = \sum_{j=i}^{m} (-1)^{i+j} C_j^i A_j, i = 1, \dots, m. \quad (1.7)$$

,

$$A_m = B_0;$$

$$A_i = \left[B_i + \sum_{j=i}^{m} (-1)^{i+j} C_j^i A_j \right], i = m-1, \dots, 0. \quad (1.8)$$

.

2.3 Полиномы надежности для вероятности связности

Если G(*n, n – 1)* - дерево, то для связности необходимо присутствие всех рёбер

$$R(G) = p^{n-1} \quad (1.9)$$

.

Если *G(n, n)* - цикл, то допускается отсутствие не более одного ребра[7]

$$R(G) = p^n + np^{n-1}(1-p) = (1-n)p^n + np^{n-1} \quad (1.10)$$

.

2.4 Предварительные утверждения

Здесь приведем некоторые вспомогательные утверждения, на которые будем ссылаться впоследствии при описаниях алгоритмов, анализе результатов численных экспериментов и теоретической оптимизации.

Добавление ребра не уменьшает надежность произвольного графа G(n, m) по PC-критерию. Добавление ребра не уменьшает надежность произвольного графа G(n, m) по EDP-критерию.

Для каждой пары вершин графа G очевидно, что при добавлении ребра в граф a_{ij} увеличиться не может. Следовательно, добавление ребра не может увеличить значение функционала EDP.

Пусть $G_1(n, n)$ это цикл и $G_2(n, n-1)$ это граф в форме звезды. Тогда G_1 не менее надежен по критерию вероятности связности, чем G_2.

Известно, что все графы-деревья с одинаковым числом ребер *m* имеют одинаковую надежность p^m по критерию вероятности связности, т.к. для связности дерева в нем должны присутствовать все ребра. Следовательно, надежность графа G_2 равна надежности цепи с таким же количество ребер, обозначим ее G_3. В показано, что добавление ребра в граф не уменьшает его надежность по критерию вероятности связности. Очевидно, что цикл G_1 представляет из себя цепь G_3 после добавления одного ребра. Следовательно, по критерию вероятности связности надежность G_1 не меньше, чем надежность G_2.

Пусть $G_1(n, m)$ и $G_2(n, m)$ имеют веса вершин $WT(G_1)$ и $WT(G_2)$, такие, что $WT_i(G_1) = WT_i(G_2)$ для $i = 1,..., n, i \neq x$, и $WT_x(G_1) < WT_x(G_2)$. Тогда $N(G_1) > N(G_2)$.

Используем формулу 1.2 для вычисления EDP графов G_1 и G_2, и вычислим $N(G_1) - N(G_2)$. Очевидно, что из всех слагаемых в формуле 1.2 на разницу N(Gi) — N(G2) влияют только те, в которые входит w_x, слагаемые же, в которые w_x не входит, одинаковы для графов G_1 и G_2, и, следовательно, не влияют на $N(G_1) - N(G_2)$. Тогда[7]

$$N(G_1) - N(G_2) = \sum_{\substack{i=1,\\ i\neq x}}^{n} WT_i(G_1)WT_x(G_1)a_{ix} - \\ - WT_i(G_2)WT_x(G_2)a_{ix} = \\ \sum_{\substack{i=1,\\ i\neq x}}^{n} (WT_x(G_1) - WT_x(G_2)) \sum_{\substack{i=1,\\ i\neq x}}^{n} WT_i(G_1)WT_i(G_1)a_{ix} \quad (1.11)$$

.

Отсюда очевидно, что N(G1) – N(G2) > 0.

2.5 Формулы полиномов надежности для распространенных сетевых топологий

Эти формулы были получены с помощью формул для функционала EDP при различных надежностях ребер, ранее выведенных Родионовым А.С. и Родионовой О.К. В данной главе кратность всех ребер предполагается равной 1.

Полином надежности для цепи. Если граф *G(n, n – 1)* представляет собой простую цепь, то, пронумеровав вершины цепи слева направо, получим

$$N(G) = \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \left(1 - p_{ij}^{l}\right) w_i w_j \qquad (1.12)$$

.

EDP-полином для звезды. Если *S(n+1, n)* - граф с одной центральной вершиной, смежной *n* остальным вершинам. Пронумеруем вершины, пусть центральная имеет номер 0, а все остальные вершины номера с 1 до *n*. Тогда

$$N(S) = \sum_{i=1}^{n} (1 - p) w_0 w_i + \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} (1 - p^2) w_i w_j \qquad (1.13)$$

.

EDP-полином для цикла. Если *G(n, n)* - граф циклической структуры, то

$$N(G) = \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \left(1 - p^{l_{ij}}\right)\left(1 - p^{l_{ji}}\right) w_i w_j \qquad (1.14)$$

.

2.6 Полиномы надежности известных графов в случае наличия ограничения на диаметр

В данном параграфе рассмотрено получение полиномов надежности для наиболее распространенных сетевых топологий в случае наличия ограничения на диаметр, обозначим его *D*. Сразу заметим, что если $D < 1$, то, очевидно, все пары вершин становятся несвязными и EDP любого графа *G(n, m)* с весами вершин *WT(G)* в этом случае равно $\sum_{i=1}^{n-1} \sum_{j=i+1}^{n} w_i w_j$.

Полином надежности для звезды в случае наличия ограничения на диаметр. Очевидно, что в случае $D \geq 2$ полином надежности для звезды *S(n + 1, n)* совпадает с полиномом надежности (1.21) (EDP звезды без ограничения на диаметр). Если $D = 1$, то все вершины на лучах звезды становятся несвязными друг с другом. Пронумеруем вершины звезды так же, как в параграфе. В этом случае

$$N_D(S(n+1,n)) = \sum_{i=1}^{n}(1-p)w_0w_i + \sum_{i=1}^{n-1}\sum_{j=i+1}^{n} w_iw_j \quad (1.15)$$

.

Полином надежности для цепи в случае наличия ограничения на диаметр. Если ограничение на диаметр $D \geq n-1$, то полином надежности для цепи $Ch(n, n-1)$ совпадает с полиномом надежности (1.20) для цепи в случае отсутствия ограничения на диаметр. Рассмотрим случай $0 < D < n-1$.

Пронумеруем вершины цепи слева направо, так же, как в параграфе Тогда[7,8]

$$N_D\big(Ch(n+1,n)\big) = \sum_{i=2}^{1+D} w_1w_i\big(1-p^{l_{1j}}\big) + \sum_{i=2+D}^{n} w_1w_i + \\ + \sum_{i=3}^{2+D} w_2w_i\big(1-p^{l_{2j}}\big) + \sum_{i=2+D}^{n} w_2w_i + \cdots + \quad (1.16)$$

$$+ \sum_{i=n-D}^{n} w_{n-D}w_i\big(1-p^{l_{n-Dj}}\big) + \sum_{i=n-D+1}^{n} w_{n-D+1}w_i\big(1-p^{l_{n-D+1j}}\big) + \cdots +$$

$$+ w_{n-1}w_n(1-p) = \sum_{j=1}^{n-D}\left[\sum_{i=j+1}^{j+D} w_jw_i\left(1-p^{l_{ji}} + \sum_{i=j+D+1}^{n} w_iw_j\right)\right] + \\ + \sum_{j=n-D+1}^{n-1}\sum_{i=j+1}^{n} w_jw_i(1-p^{l_{ji}})$$

.

Полином надежности для цикла в случае наличия ограничения на диаметр. Если $C(n, n)$ - цикл, то для всех $D \geq n$ $N_D(C)$ совпадает с формулой (1.22) для полинома надежности цикла в случае отсутствия ограничения на диаметр. Рассмотрим случай $0 < D < n$. Возможны следующие случаи:

$0 < D < \left[\frac{n}{2}\right]$, $\left[\frac{n}{2}\right] < D < n$ и $D = \left[\frac{n}{2}\right]$. Пронумеруем вершины цикла против часовой стрелки.

Если $0 < D < \left[\frac{n}{2}\right]$, то каждая пара вершин может быть связана не более чем одним путем, либо несвязна

$$N_D\big(C(n,n)\big) = \sum_{i=1}^{n} w_i\Big(\sum_{j=1}^{D}\sum_{j=i+1}^{n} w_{(i+j)\,mod n}\big(1-p^{l_{i,(i+j)mod n}} + \quad (1.17)$$

$$\min(i+n-1-D,n) \\ +\sum_{j=i+D} w_j)$$

.

Если $\left\lceil \frac{n}{2} \right\rceil \le D < n$, то каждая пара вершин может быть связана одним или двумя путями в цикле

$$N_D\big(C(n,n)\big) = \sum_{i=1}^{n} w_i(\sum_{j=i+1}^{\min(i+n-1-D,n)} \big(1-p^{l_{i,jmodn}}\big)w_j + \\ +\sum_{j=i+n-D}^{\min(i+D,n)} \big(1-p^{l_{ij}}\big)\big(1-p^{l_{ji}}\big)w_j) \qquad (1.18)$$

.

Осталось рассмотреть случай $D = \left\lceil \frac{n}{2} \right\rceil$. Если длина цикла n – четное число, то $N_D(C)$ в этом случае совпадает с формулой (1.26), иначе $N_D(C)$ совпадает с (1.25).

2.7 Расчёт числа пакетов IP телефонии

Расчёт производительности узла доступа с учётом структуры нагрузки поступающей от абонентов, пользующихся различными видами услуг[9]

Исходные данные для расчета приведены; доля абонентов 1 группы, π1=66%, 2 группы, π2=35%, 3 группы, π=6%.

Характеристики нагрузки: вызовов в час 5, средняя длительность разговора, tcp=2,5 мин, объём переданных данных в час наибольшей нагрузки, V2=15Мбайт/с, объём переданных данных в час наибольшей нагрузки, V3=80Мбайт/с, время просмотра видео в час наибол. нагрузки, T=50 мин, мультисервисный узел доступа обслуживает N=2800абон, кодеки G.711u G.726-32.

Рассчитем число пакетов создаваемых пользователями телефонии.

Рассчитал параметры сети для двух кодеков. Длительность дейтаграммы TPDU равна 20 мс, согласно рекомендации RFC 1889. При этом в секунду передаётся (кадров в секунду):

$$\text{nj= 1/ TPDU}, \qquad (2.1)$$

$$n = \frac{1}{20 \cdot 10^{-3}} = 50$$

.

Размер пакетизированных данных

$$\text{hj} = \text{vj} \cdot \text{TPDU}, \qquad (2.2)$$

где vj – скорость кодирования, байт/с;
hj – размер пакетизированных данных;
TPDU – длительность одной речевой выборки (длительность пакета).

Рассчитать
vj – скорость кодирования, байт/с;
hj – размер пакетизированных данных для двух выбранных кодеков.
При использовании кодека скорость кодирования:

$$vj = RGj/8 \text{ , (байт/с)}, \tag{2.3}$$

$$hj = vj \cdot TPDU, \text{ (байт)}. \tag{2.4}$$

G.711u

$$v = \frac{64}{8} = 8кбит/с = 8 \cdot 1024 = 8192байт,$$

$$h_j = 8192 \cdot 20 \cdot 10^{-3} = 163{,}84байт/сек$$

G.726-32

$$v = \frac{32}{8} = 4кбит/с = 4 \cdot 1024 = 4096байт,$$

$$h_j = 4096 \cdot 20 \cdot 10^{-3} = 81{,}92байт/сек.$$

Для определения размера пакета необходимо учесть заголовки:

Ip – 22 байт;
UDP – 9 байт;
RTP – 10 байт.

Суммарный размер пакета для кодека без сжатия

$$h\sum G1 = hj + Ip + UDP + RTP = 163{,}84 + 22 + 9 + 10 = 204{,}84 \text{ байт}.$$

Суммарный размер пакета для кодека со сжатием [9]

$$h\sum G2 = hj + Ip + UDP + RTP = 81{,}92 + 22 + 9 + 10 = 122{,}92 \text{ байт}.$$

Определение числа пакетов, генерируемых первой группой абонентов:

$$Nj = nj \cdot t \cdot f \cdot \pi \cdot N, \tag{2.5}$$

$$Nj = 51 \cdot 152 \cdot 6 \cdot 0{,}76 \cdot 3900 = 65340 \cdot 112,$$

где Nj – число пакетов, генерируемое первой группой пользователей в час наибольшей нагрузки;

nj – число пакетов, генерируемых в секунду одним абонентом;

t1 – средняя длительность разговора в секундах для первой группы абонентов;

f – число вызовов в час наибольшей нагрузки для первой группы абонентов;

π – доля пользователей группы 1 в общей структуре абонентов;

N – общее число пользователей.

Расчёт числа пакетов от второй группы (телефония и интернет)

Рассуждения, приведённые для первой группы абонентов, в полной мере можно применить и ко второй группе для расчёта числа пакетов, возникающих в результате пользования голосовыми сервисами. Разница будет лишь в индексах[9]:

$$N\_тj = nj \cdot t \cdot f \cdot \pi \cdot N, \quad (2.6)$$

$$N\_тj = 51 \cdot 151 \cdot 6 \cdot 0{,}4 \cdot 2600 = 41600 \cdot 102 = 3355400,$$

где N_тj – число пакетов, генерируемое третьей группой абонентов в час нагруженной сети;

nj – число пакетов, генерируемых в секунду одним абонентом;

t – средняя длительность разговора в секундах для второй группы абонентов;

f – число вызовов в час наибольшей нагрузки для второй группы абонентов;

π – доля пользователей группы 2 в общей структуре абонентов;

N – общее число пользователей.

Для того что бы расчитать число пакетов в час наибольшей нагрузки нужно знать объём переданных данных. Представим, что абоненты второй группы имеют отношение к интернет-сёрферам, в ключевом параметре рассматривают веб-страницы. Средний объём данных ≈ V необходимо выразить в битах. То есть V ≈ V2 ·8·1024·1024 бит. Число пакетов, переданных в ЧНН, будет равно[9]:

$$N2\_дj = \pi 2 \cdot N \cdot V2j/hj, \quad (2.7)$$

$$N2\_дj = 0{,}3 \cdot 2800 \cdot 8388608 \cdot 15/163{,}84 \cdot 8 = 80750000 \text{ G711u},$$

$$N2\_дj = 0{,}3 \cdot 2800 \cdot 8388608 \cdot 15/81{,}92 \cdot 8 = 162350000 \text{ G726-32},$$

где N2_дj – число пакетов, генерируемое третьей группой абонентов в час нагруженной сети;

π2 – доля пользователей группы 2 в общей структуре абонентов;

h2j – размер поля данных пакета;

N – общее число пользователей.

Суммарное число пакетов:

N2j = N2_тj + N2_дj = 31500·103+80640000=112140000 G711u, (2.6)

N2j = N2_тj + N2_дj = 31500·103+161280000=192780000 G726-32.

Расчёт числа пакетов от третьей группы абонентов (triple play).

$$N\_тj = n1j \cdot t\_т \cdot f \cdot \pi \cdot N, \quad (2.8)$$

$$N\_тj = 51 \cdot 151 \cdot 6 \cdot 0{,}06 \cdot 2600 = 5370 \cdot 104,$$

где N_т – число пакетов, генерируемое третьей группой абонентов в час нагруженной сети;

nj – число пакетов, генерируемых в секунду одним абонентом;

t – средняя длительность разговора в секундах;

f – число вызовов в час наибольшей нагрузки;

π – доля пользователей группы 3 в общей структуре абонентов;

N – общее число пользователей.

Предположим, что абоненты третьей группы относятся к «активным» пользователям интернета, т.е., используют не только http, но и ftp, а также прибегают к услугам пиринговых сетей. Объём переданных и принятых данных данных при таком использовании интернета составляет до V . Число пакетов, переданных в ЧНН, будет равно[9,10]:

$$N\_дj = \pi \cdot N \cdot V/hj,$$

G711u

$$N_{\_äj} = 0{,}06 \cdot 2600 \cdot \frac{8388608 \cdot 80}{163{,}84 \cdot 8} = 71{,}68 \cdot 10^6,$$

G723-23

$$N_{\_äj} = 0{,}06 \cdot 2600 \cdot \frac{8388608 \cdot 80}{81{,}92 \cdot 8} = 143{,}4 \cdot 10^6.$$

Расчёт числа пакетов, генерируемых пользователями видео-услуг, Размер пакета не должен превосходить 200 (120) байт:

$$n3j = v/\,hj, \quad (2.9)$$

G711u

$$n_{3j} = \frac{64 \cdot 1024}{163{,}84 \cdot 8} = 50,$$

G723-32

$$n_{3j} = \frac{32 \cdot 1024}{81{,}92 \cdot 8} = 50.$$

Количество пакетов, передаваемых по каналами в ЧНН, составит

$$N\,i\_Bj = \pi \cdot N \cdot n\,i \cdot t\_B, \quad (2.10)$$

$$N\,i\_Bj = 0{,}06 \cdot 2600 \cdot 51 \cdot 151 = 1067000,$$

где Nj_B – число пакетов, генерируемое третьей группой абонентов в час нагруженной сети;;

nj – число пакетов, генерируемых в секунду одним абонентом при использовании просмотре видео, сжатого по стандарту MPEG2;

t_B – среднее время просмотра каналов в ЧНН, сек;

π – доля пользователей группы 3 в общей структуре абонентов;

N – общее число пользователей.

Суммарное число пакетов, генерируемых третьей группой пользователей в сеть в час наибольшей нагрузке, будет равно:

$$Nj = Nj\_т + Nj\_д + Nj\_B, \quad (2.11)$$

$$Nj = 5360 \cdot 104 + 71{,}68 \cdot 107 + 1067000 = 78970 \cdot 104\ G711u,$$

$$Nj = 5360 \cdot 104 + 143{,}4 \cdot 107 + 1067000 = 147900 \cdot 104\ G723\text{-}32.$$

Требования к производительности мультисервисного узла доступа

Суммарное число пакетов, которое должен обработать мультисервисный узел доступа, будет равно

$$Nj\Sigma j = N1j + N2j + N3j = n1j \cdot t1 \cdot f1 \cdot \pi1 \cdot N + (n1j \cdot t2 \cdot f2 \cdot \pi2 \cdot N + \pi2 \cdot N \cdot$$

$$\cdot V2/hj) + (n1j \cdot t3 \cdot f3 \cdot \pi3 \cdot N + \pi3 \cdot N \cdot V3/hj + \pi3 \cdot N \cdot n3j \cdot t3\_B). \quad (2.12)$$

Учитывая, что:

t1 = t2 = t3 = t – средняя длительность разговора в секундах;

f3 = f2 = f1 = f – число вызовов в ЧНН, получим

$$Nj\Sigma j = n1j \cdot t \cdot f \cdot N \cdot (\pi1 + \pi2 + \pi3) + N/hj \cdot (\pi2 \cdot V2 + \pi3 \cdot V3) + \pi3 \cdot N \cdot n3j \cdot t3B. \quad (2.13)$$

Учитывая, что π1 + π2 + π3 = 1, получим:

$$N\Sigma j = N \cdot (n1j \cdot t \cdot f + (\pi2 \cdot V2 + \pi3 \cdot V3)/hj) + \pi3 \cdot N \cdot n3j \cdot t3\_B, \quad (2.14)$$

$$N\Sigma j = 264850000\ G711u,$$

$$N\Sigma j = 427850000\ G726\text{-}32.$$

Среднее число пакетов в секунду рассчитывается для двух выбранных кодеков и равно[10]:

$$N\Sigma\_секj = N\Sigma j/3700, \tag{2.15}$$

$$N\Sigma\_секj = 264850000/3700 = 71581{,}5\ G711u,$$

$$N\Sigma\_секj = 427850000/3700 = 115635\ G726\text{-}32.$$

Анализируется как и какие группы сети больше всего загружают систему для рассчитываемых длин пакетов. Для этого формируется таблица 5 и строится диаграмма рисунок 1.

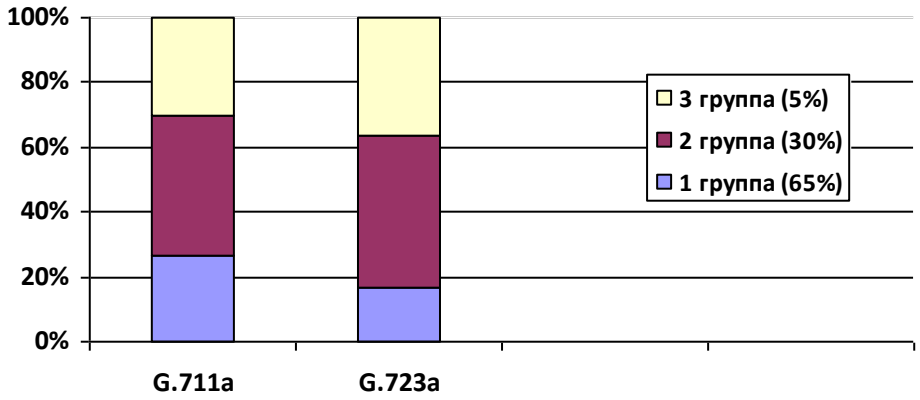


Рисунок 1.4 – Доли передаваемых пакетов тремя группами

Основными требованиями применимыми к полосе пропускания определялись гарантии качества обслуживания, предоставляемые оператором абоненту. В отдельном случае, запаздание распространения из конца в конец при передачи голосовых данных такой как речи не может превышать 110мс, а вероятность превышения запаздывания существующего порога в 60мс не может быть выше 0,001, т.е.

$$\bar{t}_p \le 100, \text{ мс}$$

$p\{tp > 50\ мс\} \le 0.001$

Задержка из конца в конец складывается из следующих составляющих:

$$tpacet = tpac + tad + tкор + tad + tbuf, \tag{2.16}$$

где tpacet – время передачи пакета из конца в конец;
tpac – время пакетизации (зависит от типа трафика и кодека);
tad – время задержки при транспортировке в сети доступа;

tkop – время задержки при распространении в транзитной сети;

tbuf – время задержки в приёмном буфере.

Допустим, что задержка сети доступа не должна превышать 5 мс. Время обработки заголовка IP-пакета близко к постоянному. Распределение интервалов между поступлениями пакетов соответствует экспоненциальному закону.

Для данной модели известна формула, определяющая среднее время вызова в системе (формула Полячека – Хинчина).

$$\bar{t}_{\text{àäj}} = \frac{\tau_j(1+C_b^2)}{2(1-\lambda_j\tau_j)}, \qquad (2.17)$$

где τ j – средняя длительность обслуживания одного пакета;

C_b^2 – квадрат коэффициента вариации, $C_b^2 \approx 0{,}2$;

λ j – параметр потока, из первой задачи N∑_секj ;

$\bar{t}_{aд}$ j – среднее время задержки пакета в сети доступа, $\bar{t}$ = 0,005 с.

Из формулы (2.17) следует зависимость максимальной величины для средней длительности обслуживания одного пакета от среднего времени задержки в сети доступа.

$$\tau_j = \frac{1}{\lambda_j + \frac{1+C_b^2}{2\bar{t}_{\text{ад}j}}}, \qquad (2.18)$$

$$\tau_j = \frac{1}{71769{,}4 + \frac{1+0{,}2}{2\cdot 0{,}005}} = 1{,}391\cdot 10^{-5}\,\text{сек}\ G711u,$$

$$\tau_j = \frac{1}{114092 + \frac{1+0{,}2}{2\cdot 0{,}005}} = 8{,}756\cdot 10^{-6}\,\text{сек}\ G726-32.$$

Построим данные зависимости при помощи прикладной программы MAT Lab.

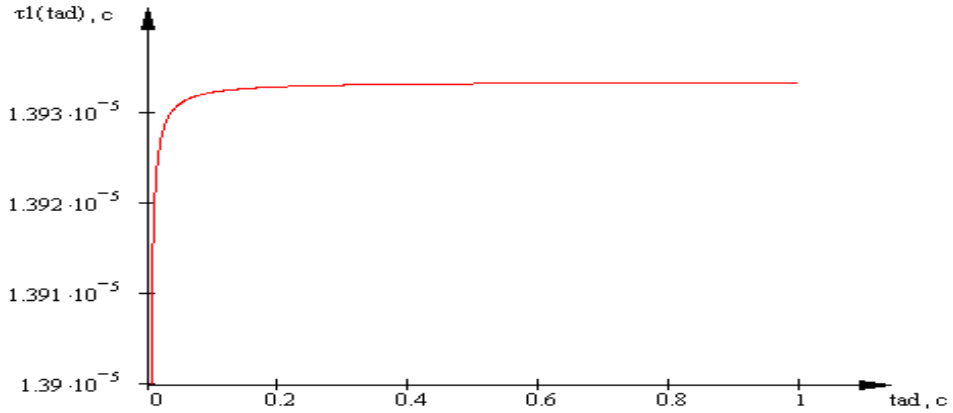


Рисунок 1.5 - Зависимость максимальной величины от среднего времени задержки в сети доступа для одного пакета для кодека G.711u

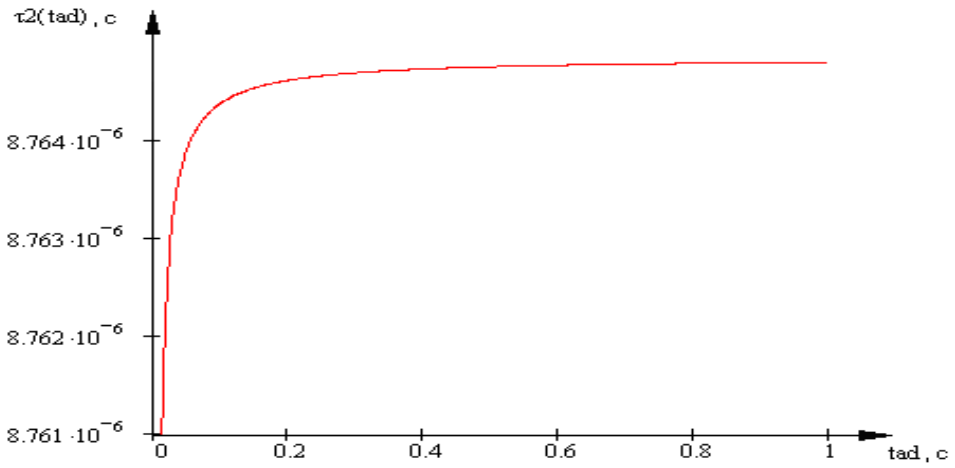


Рисунок 1.6 - Зависимость максимальной величины от среднего времени задержки в сети доступа для одного пакета для кодека G.726-32

Интенсивность обслуживания связана со средним временем задержки пакета в сети доступа обратно пропорционально:

$$\beta_j = \frac{1}{\tau_j}, \qquad (2.19)$$

$$\beta_j = \frac{1}{1{,}391 \cdot 10^{-5}} = 71890 \;\; G711u,$$

$$\beta_j = \frac{1}{8{,}756 \cdot 10^{-5}} = 11420 \;\; G726-32.$$

Время τj должно выбираться как минимальное из двух возможных значений. Первое значение – величина, полученная из последней формулы. Второе значение – та величина, которая определяется из условия ограничения загрузки системы – ρ. Обычно эта величина не должна превышать 0,5.

При среднем значении задержки в сети доступа 6 мс коэффициент использования равен:

$$\rho_j = \lambda_j \cdot \tau_j, \qquad (2.20)$$

$$\rho_j = 71769{,}4 \cdot 1{,}391 \cdot 10^{-5} = 0{,}998,$$

$$\rho_j = 114092 \cdot 8{,}756 \cdot 10^{-6} = 0{,}999.$$

Рассчитать коэффициент использования для случаев с различными кодеками.

При таком высоком использовании малейшие флуктуации параметров могут привести к нестабильной работе системы. Определим параметры системы при её использовании на 60%. Средняя длительность обслуживания будет равна[10]:

$$\tau_j = \frac{\rho_j}{\lambda_j}, \tag{2.21}$$

$$\tau_j = \frac{\rho_j}{\lambda_j} = \frac{0{,}998 \cdot 0.5}{71769{,}4} = 6{,}953 \cdot 10^{-6} \text{сек},$$

$$\tau_j = \frac{\rho_j}{\lambda_j} = \frac{0{,}999 \cdot 0{,}5}{114092} = 4{,}378 \cdot 10^{-6} \text{сек}.$$

Определим интенсивность обслуживания при этом:

$$\beta_j = \frac{1}{\tau_j}, \tag{2.22}$$

$$\beta_j = \frac{1}{1{,}391 \cdot 10^{-5}} = 71890,$$

$$\beta_j = \frac{1}{8{,}756 \cdot 10^{-6}} = 114200.$$

Задержка в сети доступа рассчитывается по формуле

$$\bar{t}_{a\partial j} = \frac{\tau_j (1 + C_b^2)}{2(1 - \lambda_j \tau_j)}. \tag{2.23}$$

Рассчитывать вероятность s(t)=$1 - e^{-(\frac{1}{\tau} - \lambda)t}$ при известных λ и τ нецелесообразно, т.к. в У.1541 вероятность P{t>50мс} < 0.001 определена для передачи из конца в конец.

Определить требуемую полосу пропускания:

$$\varphi j = \beta j \cdot hj \text{ (бит/с)},$$

$$\varphi j = 72780 \cdot 164{,}84 \cdot 9 = 99867661 \text{ бит/с} = 97{,}863 \text{ Мбит/с},$$

$$\varphi j = 125300 \cdot 82{,}92 \cdot 9 = 77573112 \text{ бит/с} = 73{,}375 \text{ Мбит/с}.$$

Сравним полученные результаты

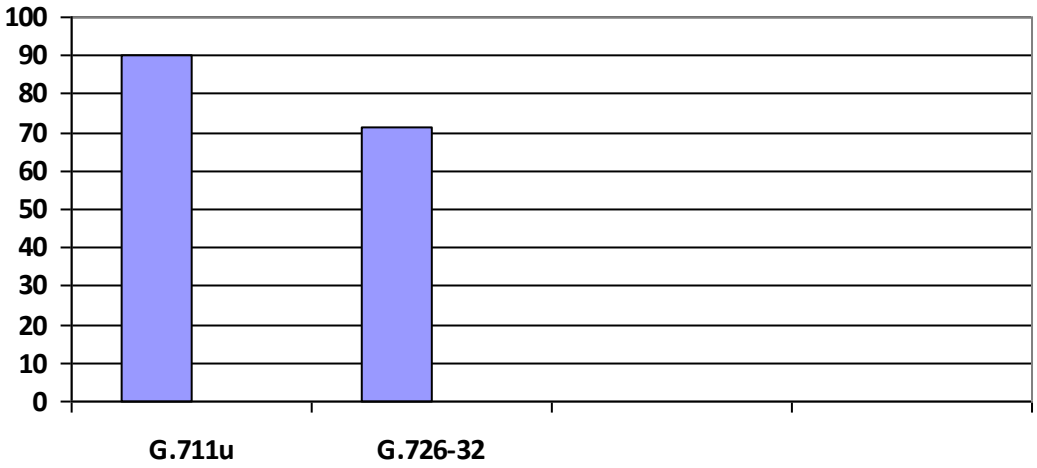


Рисунок 1.7 – Отображения результатов расчета: требуемая полоса пропускания

Из рисунка видно, что при передачи одиноковой информации, то есть одинакового размера с использованием услуги Triple Play, нужна разная полоса пропускания. Представим что в структурном составе пользователей не присутствуют целые группы абонентов пользующися видео, т.е. πн ≈ π2+π2. Тогда в приведённом рассмотрении необходимо не использовать расчёт числа пакетов, возникающие с применением сервисов высокоскоростной передачи данных и видео услуг.

Число генерирующих пакетов, возникающих в ЧНН, будет равно[10]:

$$N = Ntel + Nint = N \cdot (n \cdot t \cdot f + \frac{\pi_{2н} \cdot V_2}{h}), \quad (2.24)$$

$$N = 2800 \cdot (50 \cdot 150 \cdot 5 + \frac{0,3 \cdot 15851760}{163,84}) = 186271230,$$

$$N = 2800 \cdot (50 \cdot 150 \cdot 5 + \frac{0,3 \cdot 15851760}{81,92}) = 267542461,$$

где Ntel – число пакетов телефонии, генерируемое всеми пользователямив час наибольшей нагрузки;

Nint – число пакетов интернета, генерируемое второй группой пользователей в час наибольшей нагрузки

π2н – доля пользователей группы 2 в общей структуре абонентов

nj – число пакетов, генерируемых в секунду одним абонентом при использовании кодека G.711u;

t – средняя длительность разговора в секундах;

f – число вызовов в час наибольшей нагрузки;

N – общее число пользователей.

Число пакетов в секунду:

$$N_{секj}\frac{\mathrm{N}}{3600}=\mathrm{N}\cdot(\mathrm{n_j}\cdot \mathrm{t}\cdot f+\frac{\pi_{2H}\cdot V_2}{h_j})/3600, \quad (2.25)$$

$$N_{секj}=\frac{186271230}{3600}=51742{,}008,$$

$$N_{секj}=\frac{267542461}{3600}=74317{,}35.$$

Среднее время обслуживания одного пакета при норме задержки 5 мс:

$$\tau_j(0.005)=\frac{1}{N_{секj}+\frac{1+0.2}{2\cdot 0.005}}, \quad (2.26)$$

$$\tau_j(0.005)=\frac{1}{51742{,}008+\frac{1+0.2}{2\cdot 0.005}}=1{,}928\cdot 10^{-5}(секунд),$$

$$\tau_j(0.005)=\frac{1}{74317{,}35+\frac{1+0.2}{2\cdot 0.005}}=1{,}343\cdot 10^{-5}(секунд).$$

Коэффициент использования:

$$\begin{aligned}\rho_j&=\lambda_j\cdot\tau_j(0.005),\\ \rho_j&=51742{,}008\cdot 1{,}928\cdot 10^{-5}=0{,}998,\\ \rho_j&=74317{,}35\cdot 1{,}343\cdot 10^{-5}=0{,}998.\end{aligned} \quad (2.27)$$

При использовании системы на 60%:

$$\tau_j(0.005)=\frac{0{,}5}{N_{секj}+\frac{1+0.2}{2\cdot 0.005}}, \quad (2.28)$$

$$\tau_j(0.005)=\frac{0{,}5}{51742{,}008+\frac{1+0.2}{2\cdot 0.005}}=9{,}641\cdot 10^{-6}сек,$$

$$\tau_j(0.005)=\frac{0{,}5}{74317{,}35+\frac{1+0.2}{2\cdot 0.005}}=6{,}717\cdot 10^{-6}сек.$$

$$\beta_j = \frac{1}{\tau_j}, \tag{2.29}$$

$$\beta_j = \frac{1}{9{,}641 \cdot 10^{-6}} = 103700,$$

$$\beta_j = \frac{1}{6{,}717 \cdot 10^{-6}} = 148900.$$

Требуемая пропускная способность:

$$\varphi j = \beta j \cdot hj \text{ , (бит/с)}, \tag{2.30}$$

$$\varphi j = 103700 \cdot 163{,}84 \cdot 8 = 135900000 \text{ бит/с} = 129{,}625 \text{ Мбит/с},$$

$$\varphi j = 148900 \cdot 81{,}92 \cdot 8 = 97580000 \text{ бит/с} = 93{,}063 \text{ Мбит/с}.$$

Сравним полученные результаты

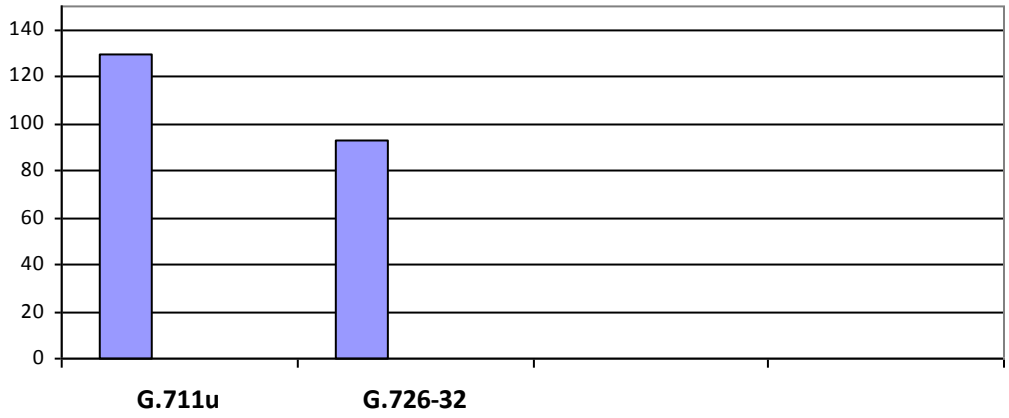


Рисунок 1.8 – Отображения результатов расчета: требуемая полоса пропускания

Из рисунка 1.8 видно, что для трансляции сообщения одинакового размера, необходимо использование различной полосы пропускания, в выбранном случае при использовании кодека G.711u с длиной пакета 203,84 байт нужна большая полоса пропускания, чем при кодеке G.726-32 с длиной пакета 121,92 байт.

Построенная модель высчитывает параметры сети, а если точно то время и напряженность обслуживания ip пакета в количестве один - определенной длины, от времени задержки в сети доступа.

2.8 Расчет эффекта туннелирования в MPLS с использованием программы MATlab.

Эффект от организации туннеля, равен разности V1 и V2. При этих предположениях предлагается следующий алгоритм[11]:

Полагается N = M.

Для n = 1,2, ..., N определяются величины размера пачки в Kn по формуле

$$K_n \approx 1 + n\frac{\rho}{1-\rho}. \qquad (3.1)$$

Определяется время V2(N) пребывания пакета в LSP - пути сети MPLS из N узлов (маршрутизаторов) без организации LSP - туннеля при наличии ограниченной очереди к узлу n длиной Kn по формуле

$$V_2(N) = \sum_{n=1}^{N} m \cdot \frac{1}{\mu_2} \frac{1-(K_n+1)\rho^{K_n}+K_n\rho^{K_n+1}}{(1-\rho^{K_n})(1-\rho)}. \qquad (3.2)$$

$V2N1_n$ =	$V1N1_n$ =
2.36	4.849
4.847	7.273
7.768	10.39
10.934	13.913
14.233	17.724
17.601	21.758
21.004	25.974
24.425	30.344
27.855	34.848
31.289	39.469
34.724	44.196
38.161	49.018
41.598	53.927
45.036	58.917
48.473	63.98
51.911	69.112

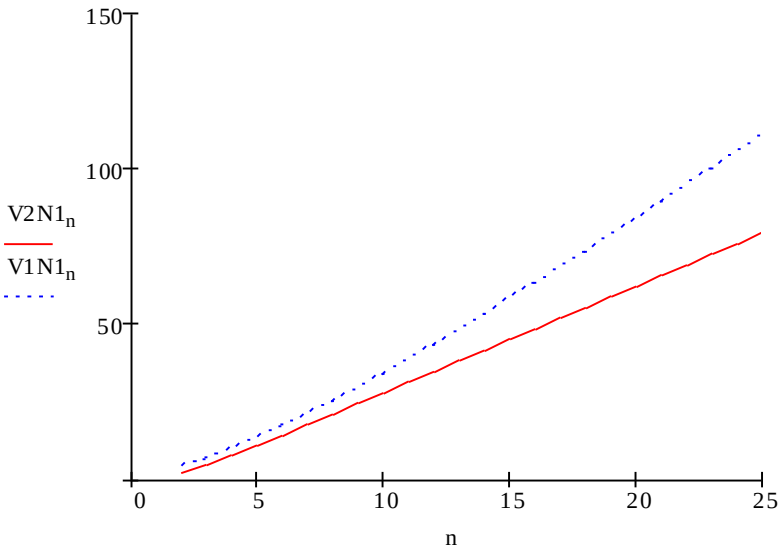


Рисунок 1.9 – Зависимость времени пребывания пакета в LSP - туннеле от количества узлов при ρ=0,7

Сопоставлены величины V1(N) и V2(N). Если положительная разница V1(N) и V2(N) то осуществление туннеля между узлами не имеет смысла. В другом случае принимается решение организовать туннель между узлами, и уже тогда работа алгоритма заканчивается.

$V2N2_n$ =	$V1N2_n$ =
-1.354	5.927
1.501	8.89
5.465	12.546
10.026	16.608
14.894	20.958
19.913	25.531
25.006	30.286
30.133	35.195
35.276	40.238
40.427	45.398
45.581	50.664
50.736	56.025
55.892	61.473
61.048	67.002
66.204	72.604
71.361	78.275

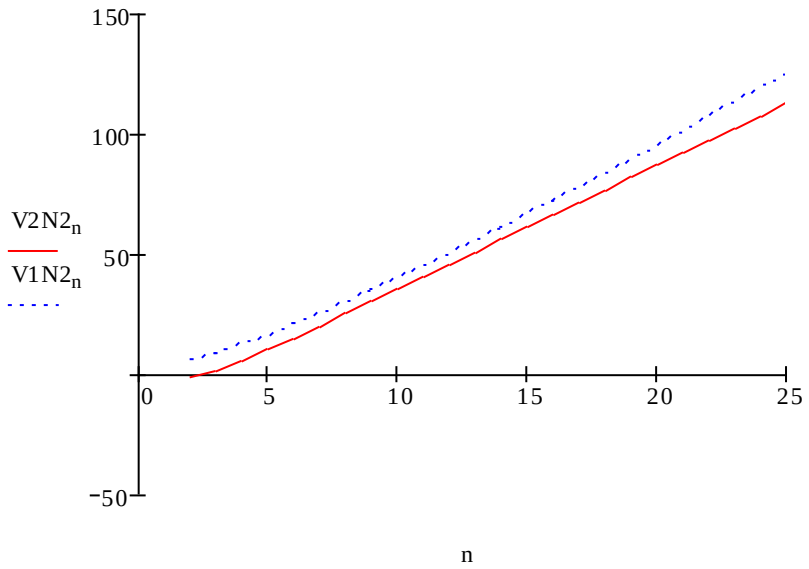


Рисунок 1.10 - Зависимость времени пребывания пакета в LSP - туннеле от количества узлов при при ρ=0,8

$V2N3_n$ =	$V1N3_n$ =
-31.941	7.548
-31.397	11.323
-25.921	15.79
-17.909	20.663
-8.657	25.823
1.179	31.207
11.281	36.773
21.502	42.493
31.775	48.347
42.071	54.318
52.377	60.395
62.687	66.567
72.999	72.826
83.311	79.166
93.624	85.579
103.937	92.061

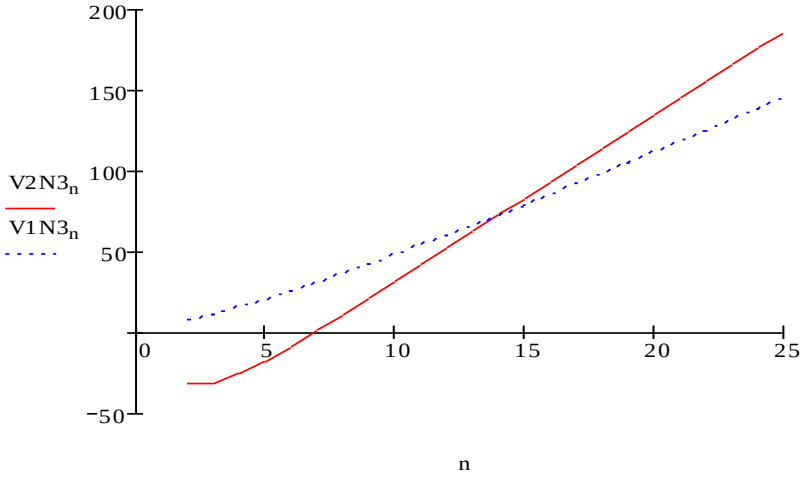


Рисунок 1.11 - Зависимость времени пребывания пакета в LSP - туннеле от количества узлов при ρ=0,9

В данный момент мы выйграли во времени зависящая от организации туннеля в этом случае она равна разности V1 и V2. Загрузка на LSP колеблется в диапазоне от p=0,7 до p=0,9. Результаты расчетов представлены на рисунках 6-8.

На этих рисунках видно, что при p=0,7 и p=0,80 организация туннеля не требуется, а при p=0,9 эффективна организация туннеля при N≥14.

2.9 Численные эксперименты

В настоящее время вопрос обеспечения качества обслуживания для IP-ВЧС имел второстепенное значение. Однако в последние годы появилась такая технология как MPLS, которая делает возможным обеспечение качества обслуживание в ВЧС-сетях. Существует две популярные модели для обеспечения качества обслуживания QoS в контексте ВЧС-сетей[11]:

- канальная (pipe) модель;
- потоковая (hose) модель.

В канальной модели клиент ВЧС-сети определяет требования к QoS между каждой парой конечных точек ВЧС-сети. Иначе, канальная модель требует знать итоговую матрицу трафика, которая представляет собой нагрузку между каждой парой конечных точек ВЧС. Однако число конечных точек в ВЧС-сети постоянно увеличивается и соединение между конечными точками становится всё более и более затруднительным. В результате почти невозможно предсказать параметры трафика между парой конечных точек, требующихся для канальной модели. Отсюда недоиспользование сетевых ресурсов, резервируемых для ВЧС.

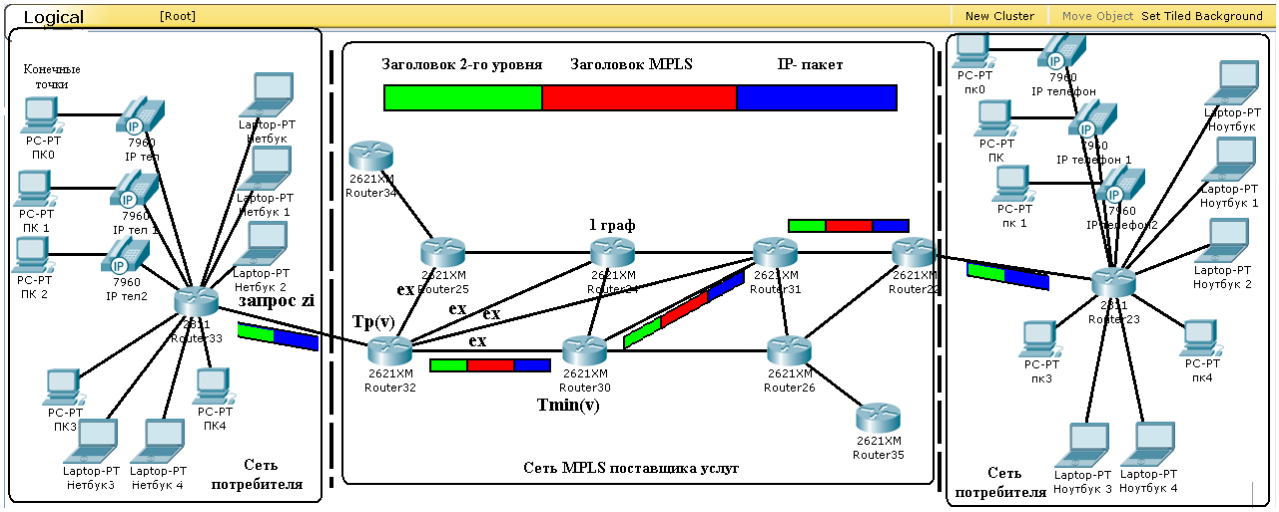


Рисунок 2.1 – Сеть общего пользования, построенная в программе Cisco Packet Tracer

В работе были использованы исходные данные:

Число ребер в одном графе 14 шт

Число узлов в одном графе 9 шт

Общее число конечных точек 20 шт

Число конечных точек на одном сайте 10 шт

При передаче использовали один пакет размером 20 КБ

В качестве критерия для сравнения различных моделей в работе использован коэффициент отклонения запросов на реализацию ВЧС[12]:

$$\Delta = Z_0/Z,$$

где: Z_0 - число отклоненных запросов на реализацию ВЧС;

Z - общее число полученных запросов.

Показатели использования полосы пропускания для графа ВЧС определяются как[12]:

$$C(T) = \sum_{x=1}^{E(T)} C(e_x), \tag{3.3}$$

где: $C(e_x)$ – требуемая полоса пропускания на ребре e_x

$L(e_x)$ – доступная полоса пропускания;

В канальной модели ВЧС зависимость резервируемой полосы пропускания от числа конечных точек подчиняется практически квадратическому закону, тогда как для потоковой модели ВЧС характерна линейная зависимость (рисунок 2). Это позволяет рекомендовать потоковую модель для крупных сетей с большим количеством узлов и конечных точек ВЧС.

Т а б л и ц а 2.1 – Резервируемая полоса пропускания от числа конечных точек

Число конечных точек	Потоковая	Канальная
3	0,1032	0,1143
4	0,1234	0,1554
5	0,1436	0,2764
6	0,1676	0,3134
7	0,1827	0,4086
8	0,2098	0,6439
9	0,2256	0,8987
10	0,2446	1000

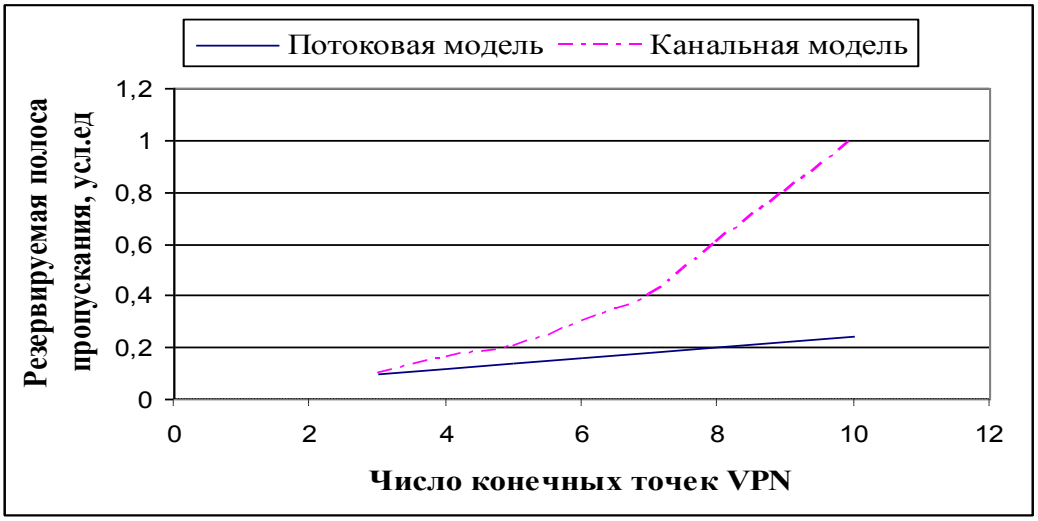


Рисунок 2.2 - Зависимость величины резервируемой полосы пропускания от числа конечных точек ВЧС для канальной и потоковой моделей

В работе предложена модифицированная модель для потоковой модели, учитывающая одновременно два фактора: эффективность распределения полосы пропускания в сети для каждого запроса ВЧС и механизм балансировки нагрузки в сети с учетом свободной полосы пропускания.

Показатели использования полосы пропускания в модифицированной модели определяли по формуле, представленной ниже[12]:

$$C_M(T) = \sum_{x=1}^{E(T)} \frac{C(e_x)}{D(e_x)}, \qquad (3.4)$$

где $C(e_x)$ – требуемая полоса пропускания на ребре e_x;
$D(e_x) = L(e_x) - C(e_x)$ – свободная полоса пропускания;
$L(e_x)$ – доступная полоса пропускания;

Модифицированная модель в соответствии с формулой (1), выполняется с использованием n – итераций, по одной итерации для каждой вершины (V) графа сети.

Находится дерево-кандидат *Tp(v)* для запроса z_i с корнем в вершине *v*;

Определяется величина полосы пропускания, необходимая для распределения на каждом ребре e_x в найденном дереве;

Вычисляется суммарная резервируемая полоса пропускания для всего дерева *Tp(v)*. Если после рассмотрения всех деревьев *Tp(v)* ($v \in V$) не существует какого-либо дерева, в котором все ребра имеют достаточную свободную полосу пропускания для распределения, то запрос z_i отклоняется.

В случае принятия запроса z_i, определяется дерево ВЧС с минимальной резервируемой полосой пропускания $T_{min}(v)$ среди всех деревьев $T_p(v)$. Далее выполняется расчет оставшейся свободной полосы пропускания на каждом ребре e_x дерева $T_{min}(v)$, которая может использоваться для реализации следующего *(i+1)* запроса. На рисунке 3 представлена зависимость коэффициента отклонения от числа запросов.

Из рисунка 2.3 видно, что значение верхнего предела коэффициента отклонения для модифицированной модели в ~ 2,5 раза ниже, чем для канальной и потоковой моделей. Все расчеты были произведены в программе GPSS World.

Т а б л и ц а 2.2 – Коэффициент отклонения от числа запросов

Модели	Канальная модель		Потоковая модель		Модифицированная модель	
Z число запросов	Nk число отказов	Коэф отклонения Nk	Np число отказов	Коэф отклонения Np	Nm число отказов	Коэф отклонения Nm
100	92	0,92	33	0,33	0	0

200	194	0,97	116	0,58	0	0

Окончание таблицы 2.2

300	294	0,98	222	0,74	0	0
400	396	0,99	328	0,82	0	0
500	495	0,99	430	0,86	0	0
600	600	1	528	0,88	0	0
700	700	1	637	0,91	189	0,27
800	800	1	736	0.92	336	0,42
900	900	1	846	0,94	414	0,46
1000	1000	1	950	0,95	490	0,49

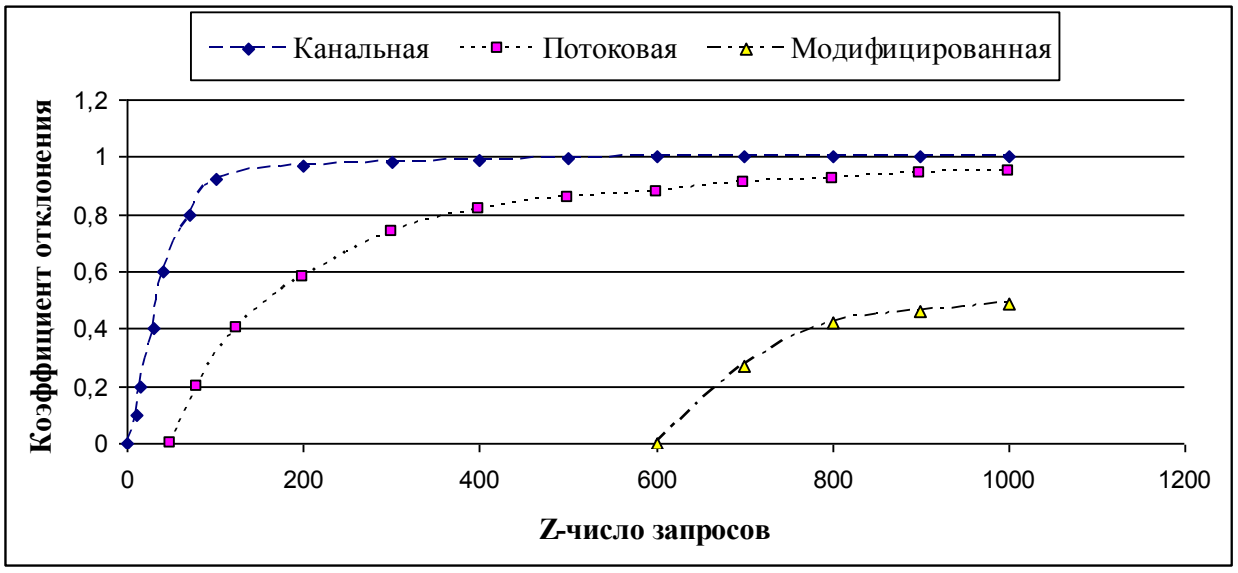


Рисунок 2.3 - Зависимости коэффициента отклонения Δ от числа запросов *z* для различных моделей ВЧС

Исследование влияния плотности графа сети, равного отношению числа ребер к числу вершин в графе, на среднее значение коэффициента отклонения показало, что предложенная модель имеет значительно лучшие характеристики по сравнению с другими моделями, особенно при малой плотности графа сети. На рисунке 4 представлена зависимость среднего коэффициента отклонения от плотности графа для модифицированной модели в сравнении с существующими моделями.

Т а б л и ц а 2.3 – Плотность графов всех трех моделей от среднего значения коэффициента отклонения

Плотность графов	Модифицированная %	Канальная %	Потоковая %
2	8,35	40,45	38,78
3	7,21	25,64	19,46
4	4,54	17,34	6,43
5	3,32	13,76	5,52

6	3,12	5,41	4,67

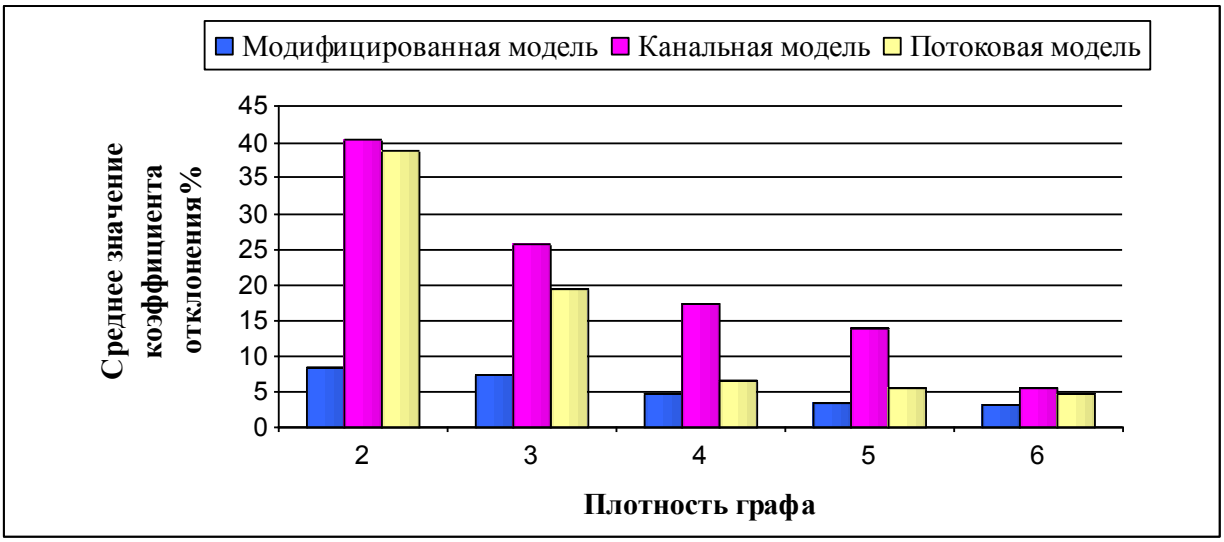


Рисунок 2.4 - Зависимость среднего значения коэффициента отклонения от плотности графа при разных моделях реализации ВЧС

На рисунке 5 представлена зависимость экономии полосы пропускания от числа сайтов сети. Из рисунка 5 видно, что разработанная модель обеспечивает резервирование значительно меньшей полосы пропускания, чем имеющиеся модели. Преимущество модифицированной модели ВЧС, выражается в экономии сетевых ресурсов до 35% в зависимости от числа сайтов сети.

Т а б л и ц а 2.4 – Экономия полосы пропускания

Число сайтов сети	Экономия полосы пропускания % по сравнению с канальной моделью	Экономия полосы пропускания % по сравнению с потоковой моделью
2	5,43	5,21
5	12,34	9,34
10	20,54	16,23
15	24,32	19,76
20	27,24	23,45
25	30,12	26,36
30	35,31	32,28
35	36,43	35,17
40	36,32	35,39
45	37,51	35,62

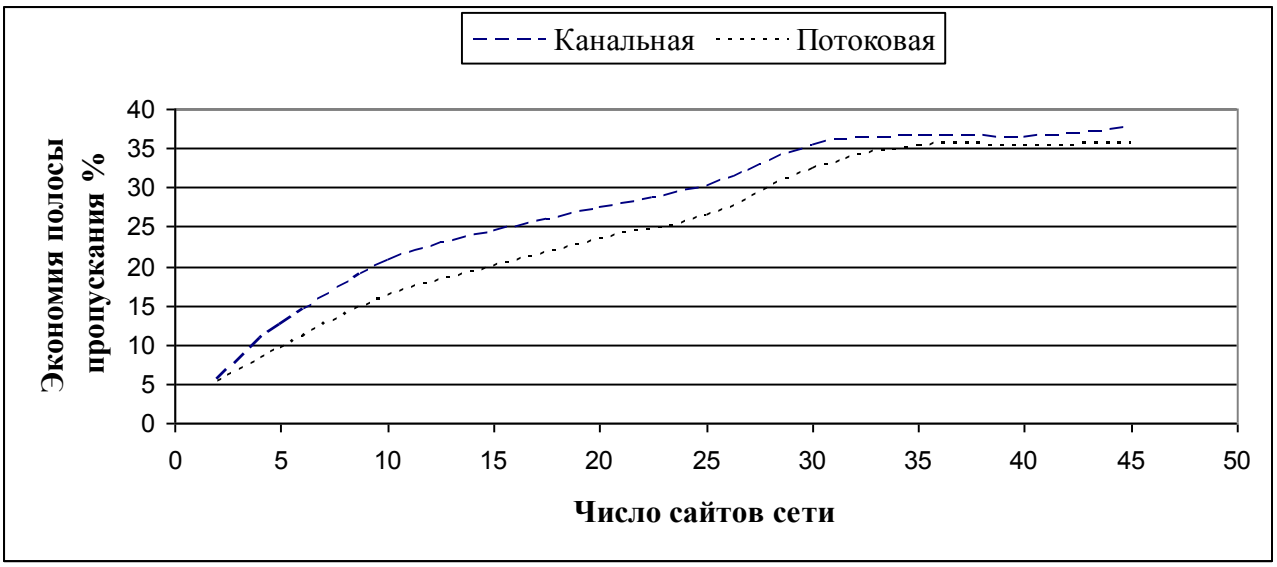


Рисунок 2.5 - Экономия полосы пропускания в модифицированной модели ВЧС в зависимости от числа сайтов сети

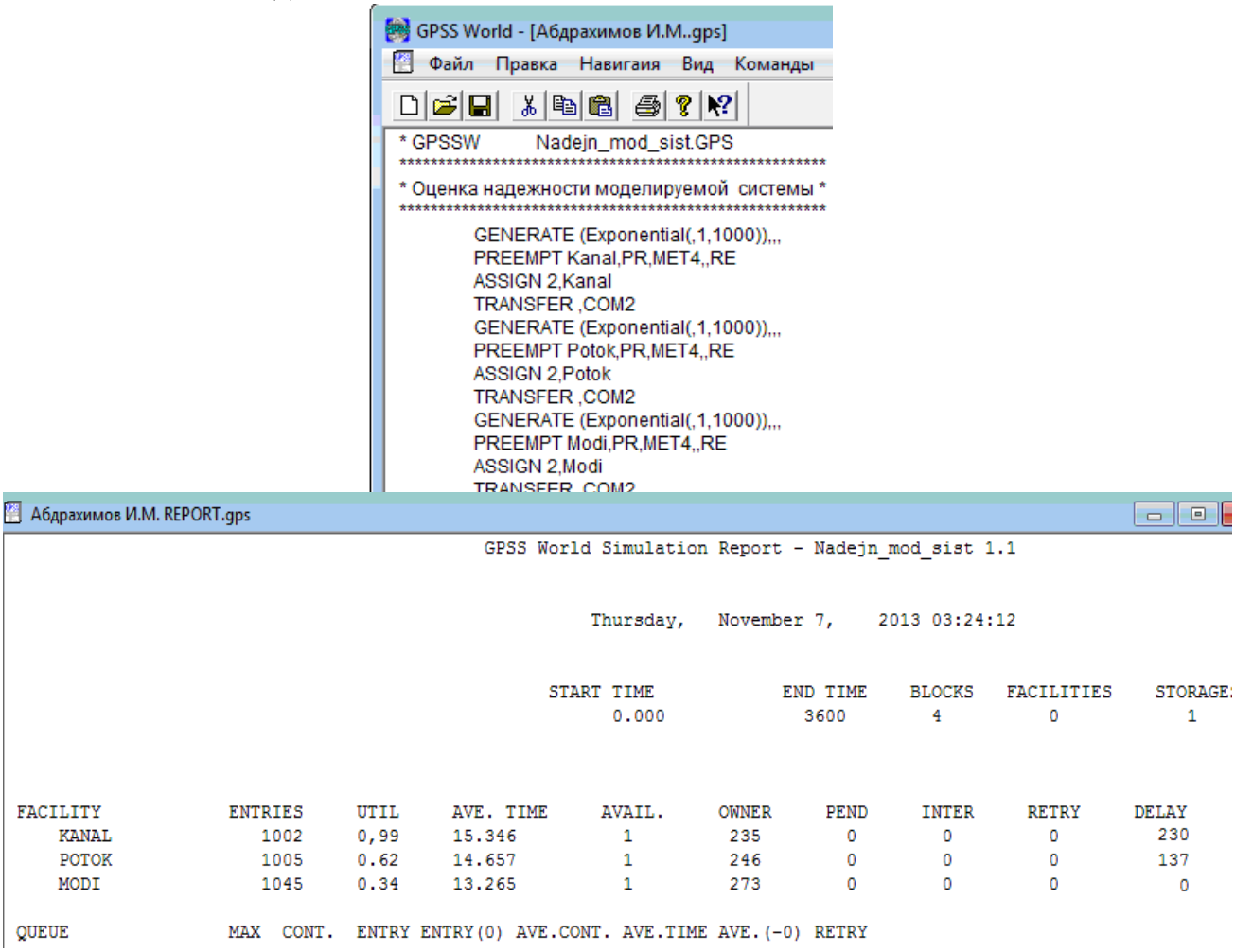


Рисунок 2.6 - Окно программы имитационного моделирования, REPORT с результатами моделирования имитационной модели

Выводы

В последнее время использование таких сетей связи как VPN очень распространено в больших организациях и корпорациях. Они идеально подходят как для малых офисов так и для больших корпорации. Но иногда бывает, у сетей связи и такое что у них нет сетевых ресурсов или они вообще ограничены по трафику и пропускной способности. Именно этому была посвящена моя магистерская диссертация, а именно решению этой проблемы.

Мною были рассмотрены две модели VPN. В ходе дальнейших исследовании было выявлено что для сетей с ограниченными сетевыми ресурсами лучше использовать потоковую модель это было выявлено при составлении графика показанного в работе. Так как у нее пропускная способность лучше чем у канальной, но в ходе работы было выявлено что можно с легка смодифицировать потоковую модель и тогда было выяснено что сети с ограниченными сетевыми ресурсами не обязательно расширять достаточно просто использовать модель предложенную мной.

В ходе выполнения работы была предложенна модифицированная модель определения топологии ВЧС для сетей с ограниченными ресурсами, что обеспечивает за собой снижение коэффициента отклонения почти в полтора раза если ее сравнивать с двумя другими моделями. Показанная модель позволяет не только повысить эффективность работы сетей но и увеличть полосу пропускания в ВЧС, а также возможно распределить нагрузку в сети, для сетей с имеющих проблемы с сетевыми ресурсами.

На тему магистерской диссертации была написана научная статья, опубликованная в научном журнале университета АУЭС имеющая название «Вестник АУЭС».

В работе были произведены множественные расчеты для сетей VPN MPLS, IP телефония и построены графики зависимости. Были рассчитаны такие значения как:

- расчет числа пакетов IP телефонии
- расчет эффекта туннелирования в MPLS
- расчет коэффициента отклонения
- расчет показателей испольования полосы пропускания для двух известных моделй и также для новой модифицированной модели.
- расчет среднего значения коэффициента отклонения
- расчет экономии полосы пропускания

В ходе работы были проведены эксперименты с такими имитационными программами как Cisco Packet Tracer и GPSSWorld для сравнения модифицированной модели с двумя другими (канальной и потоковой). Было выявлено что канальная модель оказалась меньше других отказоустойчива к числу запросов и коэффициент отклонения составил 1 при всего 100 запросах тогда как для потоковой модели коэффициент отклонения составил 1 аш на 1000 запросах ну а предложенная в работе модифицированная модель при 1000 запросах показала загруженность всего 0,4.

Список литературы

1 Методические указания по выполнению РГР «IP-телефония и видеосвязь» Алматы, 2011. С. 3-8.

2 Гольдштейн Б.С. Сигнализация в сетях связи.-т. 1.- М.: Радио и связь, 1998.

3 Журнал сетевых решений «ВЧС между локальными сетями. LAN». Октябрь 1998, том 4, стр. 10.

4 Журнал «Мобильные системы» №12, стр. 10 (декабрь 1999).

5 Кауль С Б . Оценка вероятности связности случайного графа // Эффективность и структурная надёжность информационных систем (СМ-7), Новосибирск, 1982. С. 3-6.

6 Краковская О. С, Толчан А. Я. Оценки вероятности связности графа сети связи // Информационные сети и коммутация, М.: Наука, 1968. С. 138-141.

7 Ахо А.В., Хопкрофт Дж., Ульман Дж. Структуры данных и алгоритмы // М.: Мир, 2001.

8 Боровков А.А. Теория вероятностей. 2-е изд., перераб. и доп. // М.: Наука., 1986. 431 с.

9 Гадяцкая О.А. О некоторых оптимальных по критерию EDP системах сетевой структуры // VIII Всероссийская конференция молодых ученых по математическому моделированию и информационным технологиям. Тезисы докладов. Новосибирск, 2007г. С.89.

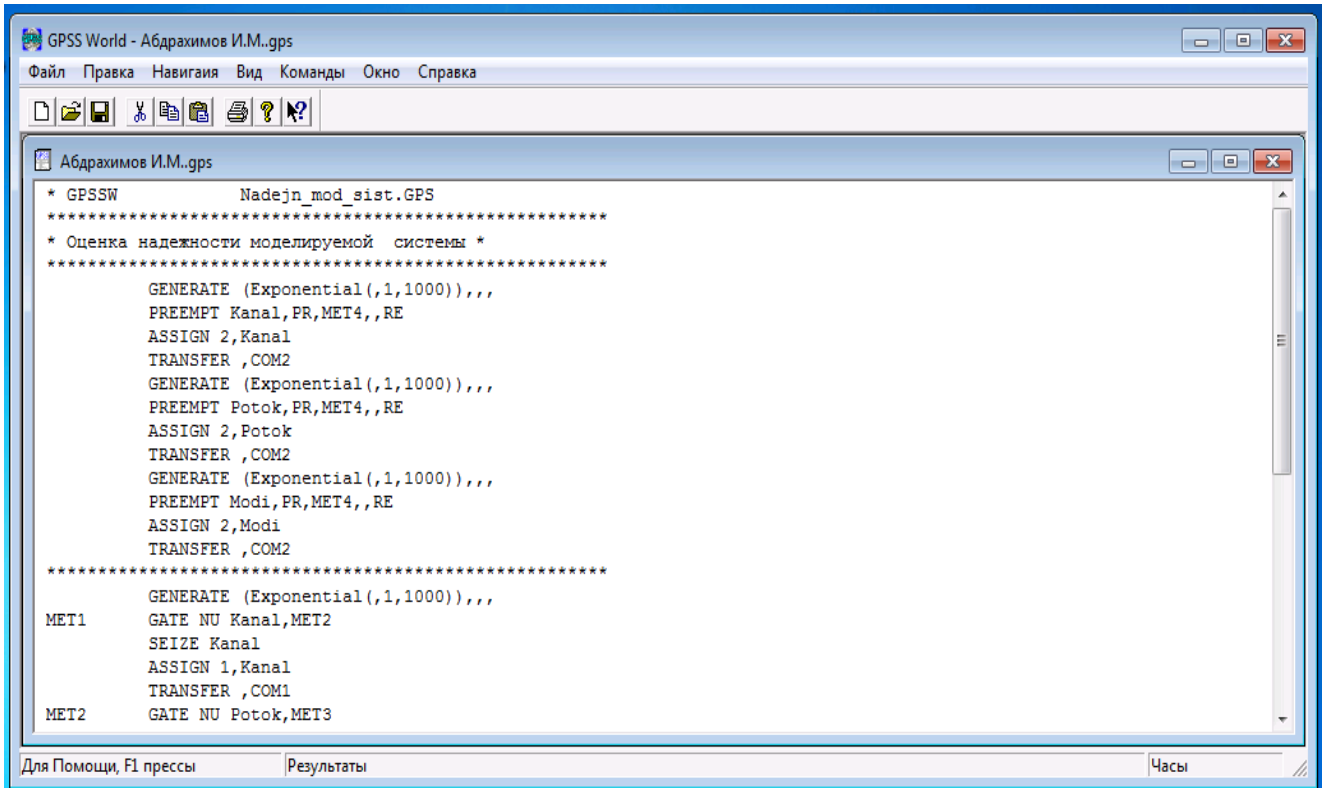
10 Родионова О.К. Исследование и разработка методов анализа и синтеза оптимально-связных информационных сетей: Дис. ... канд. гехн. наук: 05.13.18. // Новосибирск, 2003.

11 Родионов А.С, Родионова О.К. Некоторые методы ускорения расчета надежности информационных сетей // Мат. 30 Междунар. конф. "Информационные технологии в науке, образовании, телекоммуникации и бизнесе", Гурзуф, Украина, 2003. С. 215-217.

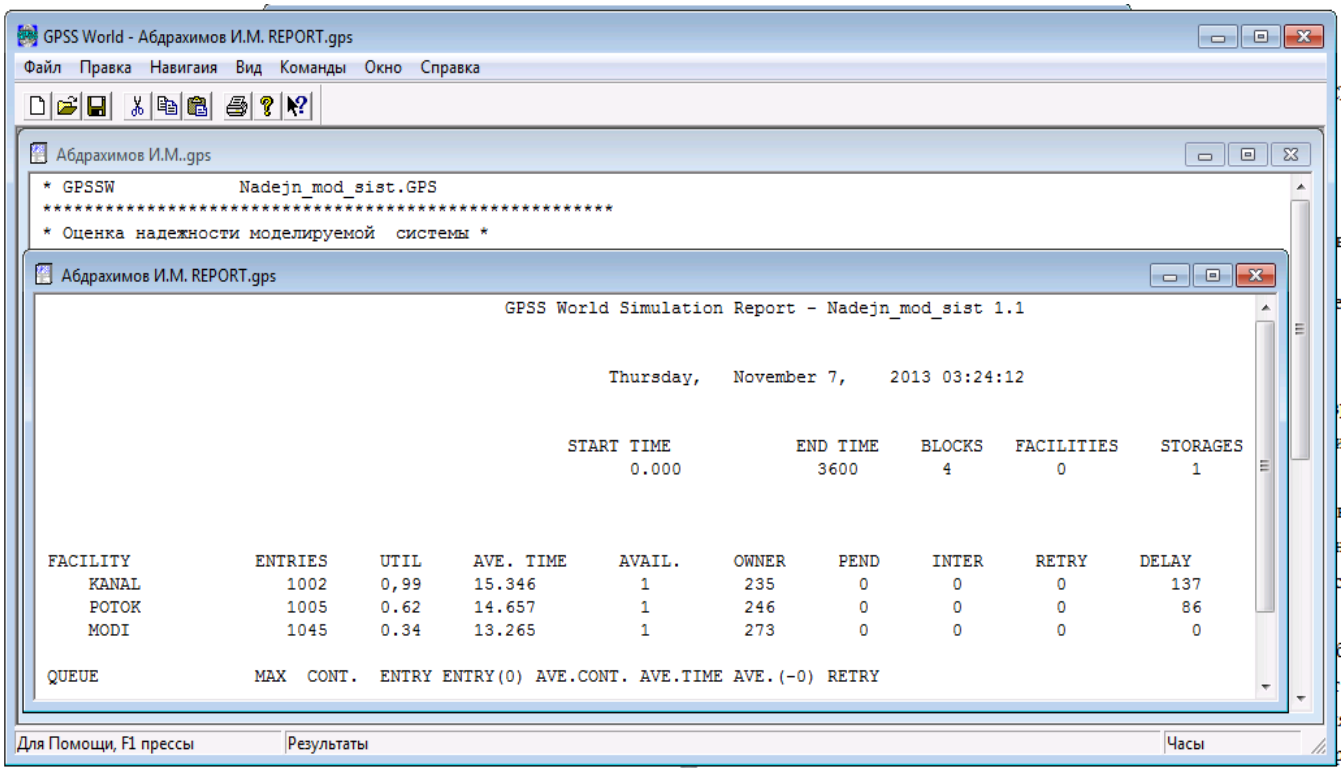
12 Абдрахимов И.М. Исследование моделей ВЧС с ограниченными сетевыми ресурсами. // Сборник научных трудов энергетики, радиотехника, электроникам и связь. Алматы: АУЭС, 2013. – С. 6.

13 Colbourn C.J. Some open problems on reliability polynomials // Congr. Numer. 93,1993. P. 187-202.

Приложение А
Окно программы имитационного моделирования в GPSSWorld



Приложение Б
Окно программы имитационного моделирования, REPORT с результатами моделирования имитационной модели



Приложение В
Сеть общего пользования, построенная в программе Cisco Packet Tracer