Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Кафедра Телекоммуникационных систем

ДОПУЩЕН К ЗАЩИТЕ
Зав. кафедрой
К.т.н., профессор Байкенов А.С.
(ученая степень, звание, Ф.И.О.)

«____»_____2015 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ
пояснительная записка

на тему: Исследование методов повышение эффективности и качества IP - сетей

Специальность 6М071900 «Радиотехника, электроника и телекоммуникации»

Выполнил Изгуттив К.Е. (Ф.И.О.) _____ (подпись) Группа МТСп-13-1

Руководитель к.х.н., старший преподаватель (ученая степень, звание) _____ (подпись) Кудинова В.С. (Ф.И.О.)

Рецензент к.т.н, зав. кафедры РЭТ КазНТУ (ученая степень, звание) _____ (подпись) Касимова А.О. (Ф.И.О.)

Консультант по ВТ к.т.н. старший преподаватель (ученая степень, звание) _____ (подпись) Ефремова Ю.И. (Ф.И.О.)

Нормоконтролер магистр ассистент (ученая степень, звание) _____ (подпись) Зайцев Е.О. (Ф.И.О.)

Алматы, 2015

Содержание

Аңдатпа

Осы магистерлі диссертацияда трафиктің өзгерісінің ортақ трендтерін және айкынньң микро-мінездемесін айкындауының егжей-тегжейлі акпараттың өңдеуінің аркасында койылған деректерді беру мультисервисті желілерінің трафиктің статистикалық суреті зерттелінген. Өлшеу зерттеулер байланыс операторының бар желіде өткізілді. Зерттеулердің нәтижелері желінің параметрлерін қазіргі үрдістерге одан әрі үндестіруі үшін колданылган. Теория жүзінде кутудің сапасы параметрлері есептелінді. Алынған нәтижелерге сүйеніп сипатта ма сызбалар және корытынды жасалынды.

Аннотация

В данной магистерской диссертации была исследована статистическая картина трафика в мультисервисных сетях передачи данных, которая позволила за счет детальной обработки информации получить общие тренды изменения трафика. Измерения проводились на существующей сети провайдера услуг связи. Полученные результаты исследования были использованы для дальнейшей подстройки параметров сети под существующие тенденции. Были произведены теоретические расчеты параметров качества обслуживания. На основе полученных результатов были построены характеристики и сделаны выводы.

Annotation

The statistical picture of traffic multiservice networks was investigated in this very master’s thesis which allowed to obtain overall trends in traffic at the expense of detailed information processing. Measurements were carried out on the existing network communication service provider. Also were made theoretical calculations of the parameters of quality of service. The characteristics and conclusions were built on the basis of obtained results.

Введение

Интерес к современным интернет-приложениям постоянно растет среди поставщиков услуг и среди клиентов. Некоторые существующие и возникающие услуги требуют высокого уровня качества и требуют высокие качества к сети. Настоящее время приложения (например, видеоконференции), которые очень чувствительны к задержке передачи и дрожание и, как правило, требуют гарантируемую высокую пропускную способность. Многие компнании и организации по всему миру уделяют внимание к качеству обслуживания. Различные сети протоколы и архитектуры, поддерживающие качество обслуживания (QoS) обеспечение теперь доступны и находятся в стадии разработки.

Качество обслуживания и качество обслуживания (QoS) активно исследуется и стандартизированы на протяжении всей истории развития телекоммуникационной отрасли. Огромный вклад в развитие и совершенствование различных принципов качества обслуживания сделал Международный союз электросвязи (МСЭ). МСЭ разработал требования и стандарты для различных параметров QoS, упорно трудился, чтобы стандартизировать несколько сетевых механизмов, которые обеспечивают необходимые QoS производительности, и сформулировать основные понятия и определения.

Мы также представляем обзор сети архитектуры, поддерживающие контроль качества обслуживания в IP-сетях, таких как интегрированные услуги (IntServ) и дифференцированные услуги (DiffServ) модели. Переключение Multiprotocol Label (MPLS) является еще одним методом, часто упоминается в контексте обеспечения качества обслуживания, но его реальная роль в обеспечении QoS не совсем же, как и у моделей IntServ и DiffServ. Этот вопрос будет объяснено в данной работе.

В современных телекоммуникационных сетях постоянно меняющийся характер и обьемы трафика, также предоставляемых информационных и коммуникационных услуг. Решающую роль в этом процессе играет услугами передачи данных, видео, голоса: мультимедийные услуги, такие как IP-телевидение, видео по запросу, IP-телефонии, видео и аудио конференций, и т.д.. Это ясно, что для оказания этих услуг необходимо соблюдать ряд требований к качеству эксплуатационных параметров, таких как потери пакетов вероятности, задержки передачи, джиттер и другие. Часто, статистические характеристики трафика игнорируются и это может привести к неэффективному использованию сетевых ресурсов операторов и, следовательно, более низкое качество услуг, предоставляемых ниже или по количеству абонентов.

1. Исследование качества обслуживания в мультисервисных сетях

1.1 Состояние проблемы, цель и задачи исследования

В последние годы, количество данных, проходящих через глобальную коммуникационную инфраструктуру растет с феноменальной скоростью. Этот рост во многом объясняется ростом популярности мобильных терминалов, социальных сетей и облачных сервисов для бизнеса. Для удовлетворения растущих потребностей общества, операторы стремятся увеличить пропускную способность сети и повысить качество обслуживания. Быстрый рост объема данных сетевого трафика в последний раз, в значительной степени из-за более широкого использования Интернета. В частности, процесс сети материалы с большими объемами данных, а также увеличение трафика с мобильных терминалов, таких как смартфоны и планшетные компьютеры.

Значительный рост использования часто запрашиваемых сайтов социальных сетей и материалов большого объема, например, фильмов и игр, оказывает огромное влияние. Во всем мире ожидается рост общего IP-трафика в среднем на 32% ежегодно, с 2010 по 2015 г., и достижение примерно 80 эксабайт (80 млн терабайт) в месяц к 2015 году. По оценкам Cisco Systems, Inc., к 2015 году глобальный IP-трафик достигнет примерно 80 эксабайт в месяц (на рисунке 1.1)

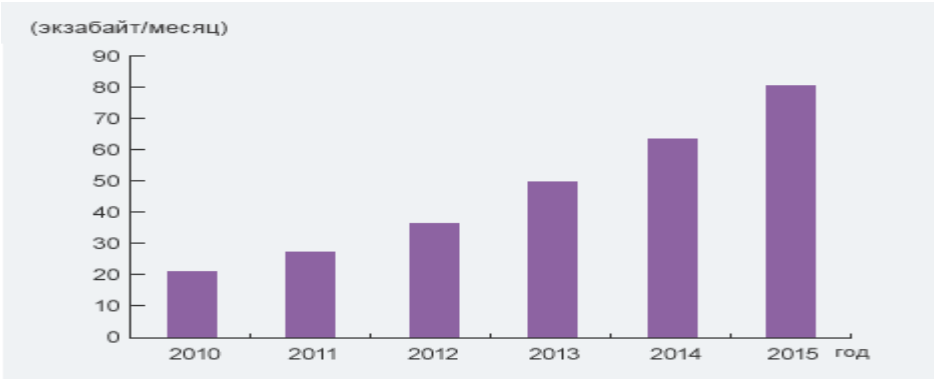

Рисунок 1.1 – Статистика IP-трафик По оценкам Cisco Systems

Основным фактором роста станет видео – к 2014 году его доля в глобальном пользовательском интернет-трафике превысит 91 процент. Расширение сетевой полосы пропускания и скорости передачи данных в Интернете, а также рост популярности телевидения высокой четкости (HDTV) и объемного телевидения (3DTV) станут важнейшими факторами четырехкратного роста IP-трафика, который должен произойти в период с 2009 по 2014 гг [1]

В дальнейшем, это приводит к тому, что пользователи услуг требует, удовлетворяющей требованиям QoS предоставляемых услуг. В связи с тем, что различные службы используют одни и те же каналы и транспортную сеть

с каждого канала службы поднимает его запросы на подключение, существует проблема распределения ресурсов канала связи между различными сетевыми службами. Часто один выделения ресурсов канала приводит к неэффективному использованию канала связи, таким образом, распределение ресурсов в сети должно быть непрерывно, периодически, в зависимости от интенсивности использования различных услуг.

Операторам необходимо расширять полосу пропускания и масштабировать свои сети, поскольку индивидуальные абоненты, корпоративные заказчики и мобильные пользователи демонстрируют неослабевающий интерес к современным видеоуслугам, доставляемым по разным сетям на разные устройства.

В нынешних телекоммуникационных сетях постоянно меняется характер и объем передаваемого трафика и, соответственно, предоставляемых инфокоммуникационных услуг. Важнейшую роль в таком процессе играют услуги передачи данных, голоса, видео: такие мультимедийные услуги, как IP-телевидение, предоставление видео по запросу, IP- телефония, видео- и аудиоконференции и др. Очевидно, что для предоставления перечисленных услуг необходимо соблюдать ряд требований к параметрам качества обслуживания, таких как вероятность потери пакетов, задержка передачи, джиттер и др. Часто незнание статистических характеристик трафика приводит к неэффективному использованию сетевых ресурсов операторов и, следовательно, к низкому качеству предоставляемой услуги или к низкому количеству обслуживаемых абонентов.

Передача трафика в соответствии с качеством обслуживания является одним из самых актуальных задач в современных телекоммуникаций. [2] Неэффективное использование сетевых ресурсов, большое количество абонентов и жесткие требования к параметрам QoS может стать причиной падения качества услуг в мультисервисных сетей передачи данных. Несмотря на большое количество публикаций на эту тему [3,4], сочетание макро-характеристик (количество информации о приложениях, распределение потоков и т.д.) и микрофункций (длина дистрибутив потерь и др.), на практике, никогда не удовлетворяется и та же сеть определенный период времени. В связи с этим, есть проблема получения полную статистическую картину трафика, который будет подробностями лечения, чтобы получить как общие тенденции трафика, а также для уточнения характеристик микро-потока. Полученные результаты могут быть использованы для дальнейшей настройки сетевых параметров под текущие тенденции.

Цель магистерской диссертации является оценка статистических параметров системы для улучшения качества обслуживания в IP - сети передачи данных.

Для того, чтобы достичь поставленной цели необходимо решить следующие задачи:

- проанализировать различные требования QoS услуг, предоставляемых в мультисервисных сетях, к каналу связи;

- исследовать эффективность существующих методов улучшения качества предоставления услуг в мультисервисных телекоммуникационных сетях;

- оценка качества обслуживания в сетях передачи данных;

- сбор статистических данных трафика на действующей сети передачи данных;

- анализ и обработка результатов эксперимента;

- определение структуры и приоритетов трафика;

- разработать метод, позволяющий улучшить качество услуг и эффективно использовать ресурсы канала;

- адаптация параметров системы под существующий трафик мультисервисной сети передачи данных.

1.2 Стандартизация качества обслуживания в мультисервисных сетях

Мультисервисная сеть — это единая телекоммуникационная структура, способная передавать разнородную информацию (голос, видео, данные) со скоростью, превышающей в десятки-сотни раз существующие скорости передачи данных (дословно мультисервисная сеть – это сеть, в которой предоставляется более одной услуги).

Мультисервисная сеть представляет собой универсальную многоцелевую среду, предназначенную для передачи речи, изображения и данных с использованием технологии коммутации пакетов (IP). Мультисервисная сеть отличается степенью надежности, характерной для телефонных сетей (в противоположность негарантированному качеству связи через Интернет) и обеспечивает низкую стоимость передачи в расчете на единицу объема информации (приближенную к стоимости передачи данных по Интернету). Основная задача мультисервисных сетей заключается в обеспечении работы разнородных информационных и телекоммуникационных систем и приложений в единой транспортной среде, когда для передачи обычного трафика (данных) и трафика другой информации (речи, видео и др.) используется единая инфраструктура.

Мультисервисная сеть позволяет поддерживать следующие виды услуг:

- городская компьютерная сеть с постоянной скоростью 100 Мбит/с;

- обмен различной информацией между пользователями сети (музыкой, фильмами, клипами, играми, фотографиями, электронными документами и т.д.);

- доступ к игровым серверам компьютерных клубов города;

- высокоскоростной доступ в Internet ;

- IP-телефония (при подключении к сети пользователь получает возможность подключить IP-телефон с городским номером, и дешевыми междугородними звонками);

- объединение удаленных корпоративных сетей (сетей организаций, компьютерных клубов и т.д.);

- создание виртуальных корпоративных сетей (VPN), коммутируемых и управляемых пользователем;

Определенный из этих сервисов выставляет свои требования, для полноценного функционирования, к каналу связи (см. таблицу 1.1).

Таблица 1.1 - Требования к QoS для разных сервисов

Тип сервиса	Параметры QoS				
	tc, с	B, Мбит/с	$p^{(rj)}$	dT, мс	Dj, мс
VoIP	0,5.1	до 0,085	10^{-3}	< 400	< 150
Видеозвонки	0,5.1	0,512	10^{-3}	30..100	<30
Сетевое «радио»	0,5.1	0,256	10^{-3}	< 1000	-
Видео по запросу	0,5.1	2..20	10^{-3}	30..100	<30
Передача данных	0,5.1	0,128.100	10^{-6}	50..1000	-
IP телевидение	0,5.1	0,512.5	10^{-6}	< 1000	-

В таблице 1.1 приняты следующие обозначения:
t_c - время установления соединения, с;
$p^{(rj)}$ - вероятность разрыва соединения;
dT - задержка, мс;
Dj - джитер, мс;
B - полоса пропускания канала.

Для достижения уровня обслуживания в сетях, сопоставимого с классом обслуживания поставщика услуг, должны быть доступны обширные инструментарии администрирования (Operation, Administration and Maintenance, OAM) для гарантии качества и класса предоставляемых услуг (QoS) и выполнения соглашения об уровне обслуживания (SLA). Осознание потенциала Ethernet как сервиса, обращенного "лицом" к клиенту, и как транспорта в сетях доступа требует от нас рассмотрения ключевых вопросов отделения (демаркации) сети поставщика услуг от сети клиента и предоставление клиенту Ethernet-услуг с качеством поставщика услуг и возможностью управления этими услугами. Поддерживать транспортное администрирование (выполнение проверки по шлейфу, получение статистики производительности, проверку работоспособности и состояния удаленного устройства), они также должны обеспечивать администрирование обслуживания на основе стандартов IEEE 802.lag и ITU-T Y.1731. Данные стандарты позволяют устройству получать информацию и управлять потоками абонентского трафика для обеспечения уровней обслуживания разных бизнес-моделей и возможностью быть использованными на различных рынках.[4]

Предоставление услуг с качеством поставщика услуг требует наличия сложных методов и средств управления, а надлежащее управление требует проведения точных измерений. Обеспечение соответствующего уровня предоставления услуг и последующее повышение их качества подразумевает про-

ведение достоверных измерений и их всестороннего анализа. Данные измерения и анализ не будут давать достоверную информацию, если они не были стандартизированы и не были измерены одинаково, независимо от используемых производителей, сетевого транспорта или протоколов.

Поставщики услуг, прежде всего, должны четко от начала и до конца понимать, каким образом осуществляется предоставление услуг в неоднородной среде. Для выполнения условий соглашений об уровне обслуживания, они должны иметь точные и непротиворечивые данные относительно надежности и пропускной способности/задержки сети, а также характеристик устройств и сетевых соединений, с использованием которых предоставляются услуги.

Способность проводить стандартизированные тесты в различных ситуациях в любое время суток может предоставить ценную информацию, касающуюся тенденции, которая может использоваться для планирования требуемой пропускной способности, улучшения управления пропускной способностью и составления более подходящих соглашений об уровне обслуживания.

Организации по стандартизации, такие, например, как IEEE и IETF, а также консорциумы поставщиков услуг, например Metro Ethernet Forum (MEF), усиленно работают над определением услуг Ethernet и механизмов по поддержке одновременной передачи видео, голоса и данных с использованием простой и единой инфраструктуры.

Удаленные мониторинг, поиск и устранение неисправностей, а также управление доступны в настоящее время благодаря поддержке протоколов управления промышленного стандарта, таких как SNMP v1/v2/v3, PING и IEEE 802.3ah - но они связаны только с функциями управления транспортного или канального уровней.

Поддержка протокола 802.3ah (OAM), предназначенного для администрирования и обслуживания в процессе эксплуатации, обеспечивает управление передачей данных и работает в режиме "точка-точка". Данный протокол обеспечивает обнаружение и локализацию ошибок, а также обнаружение соседних сетевых элементов. Так как протокол 802.3ah (OAM) является только транспортным стандартом, то поставщики услуг могут по своему усмотрению в соответствии со своими требованиями внедрять управление услугами. К счастью, работы, которые ведутся в MEF, IEEE и IETF, обещают расширить интерфейс управления протокола 802.3ah (OAM) для обеспечения функциональной совместимости оборудования различных поставщиков услуг на уровне управления.[2]

С развитием и объединением стандартов эксплуатации, администрирования и обслуживания услуг IEEE 802.lag, ITU-T Y.1731 и MEF (рисунок 1.2) на сегодняшний день можно ожидать поддержку следующих возможностей.

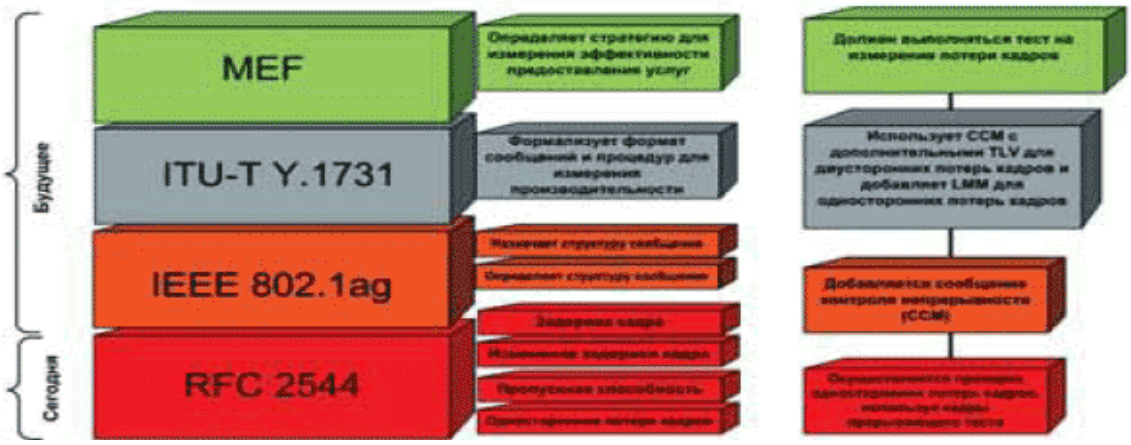

Рисунок - 1.2. Развитие стандартов эксплуатации, администрирования и обслуживания услуг

RFC 2544 позволяет контролировать:

- адресацию;
- обнаружение;
- обеспечение связи;
- сквозное измерение производительности;
- возможность измерения многозвенных линий связи по различным маршрутам;

Мониторинг производительности:

- измерение уровня потери кадров;
- измерение отклонения фазы (jitter);
- измерение среднего уровня задержки;
- единообразную модель данных;

Изоляцию топологии:

- логическая;
- физическая;
- на уровне обслуживания.

Тесты, проводимые в соответствии с методикой, определенной в RFC 2544, предоставляют поставщикам услуг определенный "уровень комфорта", определяя известные процедуры, знакомые поставщикам услуг, а также методологию, которую они знают и которой доверяют. Поставщики услуг, которые так долго привыкали к наличию удаленного доступа к эксплуатационным данным услуг с использованием своих инструментальных средств сетевого управления, теперь требуют аналогичного доступа к данным управления для своих новых Ethernet-услуг.

Проводимые в настоящее время работы на соответствие RFC 2544 создают прочную процедурную основу для дальнейших разработок и более тесную связь с другими развивающимися стандартами для измерения и управления производительности предоставления услуг на основе Ethernet. Важно понимать соответствие каждого стандарта и его связь с другими стандартами.

Стандарт IEEE 802.lag "Управление ошибками соединения (Connectivity Fault Management)" Стандарт IEEE 802.1 ag - управления ошибками соединения (CFM), описывает методологию точной локализации точки, в которой имеет место неисправность, в сетях с множеством поставщиков услуг, обеспечивая сквозное (а не только межканальное) управление обеспечением связи и услугами. Стандарт управления ошибками соединения 802.lag вносит концепцию доменов и поддерживает режим автономности для абонентов, поставщиков услуг, операторов и т.д. Множественные домены могут быть логически интегрированы, или же каждый домен может использовать собственный OAM протокол.

Например, поставщик услуг может использовать его OAM CFM и локализовать проблему для одного оператора. Оператор затем может локализовать проблему в собственной сети посредством использования собственного OAM CFM. Такая возможность является важной для сведения к минимуму затрат на "виртуальные" визиты к клиенту, поскольку она определяет, какому сетевому поставщику услуг в сценарии многочисленных поставщиков услуг принадлежит точка, в которой произошла неисправность.

CFM определяет сообщения и протоколы для всех сетей, в которых он работает, а также отвечает за обнаружение и активность соединений. В дополнение к обнаружению конечных и промежуточных точек обслуживания (MEPS и MIPS), этот стандарт определяет функции трассировки канала связи и кольцевых проверок.

Стандарт ITU-T Y.1731 Ethernet OAM

Стандарт ITU-T Y.1731 Ethernet OAM предназначен для управления неисправностями и производительностью в сети. Данный стандарт связан с управлением неисправностями (способом, аналогичным определенному в стандарте 802.lag) и управлением производительностью на 2-ом уровне (с использованием методологии, аналогично описанной в RFC 2544); он также определяет механизмы проверки уровня потерянных кадров и величину задержки в сети. Данный стандарт добавляет временные метки в тестовые пакеты, определенные стандартом IEEE.

Методики ITU выходят за пределы возможностей тестовых проверок, определенных в RFC 2544, позволяя выполнять измерение величины задержки ее изменения, а также уровень потери кадров в сети, используя реальный трафик пользователя взамен смоделированных пользовательских пакетов, как это имеет место в случае осуществления проверки, основанной на применении RFC 2544.

Стандарты ITU и MEF используют механизмы, лежащие в основе RFC 2544, но не сами процедуры проверки, определенные в RFC 2544. Пакеты сообщений определяются стандартами ITU и IEEE и не рассматриваются инициативами MEF, которые просто требуют, чтобы величина двухсторонней задержки была вычислена.[4]

Стандартизированный инструментарий в сетях доступа Ethernet дает возможность поставщикам услуг увеличивать повсеместное использование

Ethernet, обеспечивая расширенное обслуживание и использование соглашений об уровне услуг (SLA) во всей сети. Способность измерять, управлять и поддерживать разнообразные услуги и дифференцированные уровни обслуживания позволит поставщикам услуг дифференцировать свои предложения на высококонкурентном рынке.

1.3 Оценка качества предоставления сервисов в мультисервисных сетях

Предоставление операторами услуг цифрового телевидения в широкополосных сетях на базе протокола IP (Video over IP, TVoIP, IPTV) является одним из перспективных направлений развития в области услуг связи. Операторы связи на протяжении многих лет работают над внедрением видеоуслуг, и в последнее время наблюдается ускорение этого процесса. Многие операторы Европы и Америки уже внедрили или приступили к внедрению услуг "Triple Play". Казахстанские компании тоже постепенно втягиваются в этот общемировой процесс. К сожалению, первый опыт российских операторов оказался не самым успешным. Данная статья открывает цикл публикаций, предназначенных развеять предубеждения операторов, прояснить сложные вопросы и облегчить им путь к успешному внедрению "Triple Play".

Как показывает практика, внедрение решений "Triple Play" позволяет не только добавить услуги передачи видео и различного вида контент-услуги к голосовым услугам и передаче данных, но и добиться синергетического эффекта, помогая, тем самым, операторам связи эффективно конкурировать на рынке, повышать рентабельность, снижая отток абонентов и ускоряя возврат инвестиций в строительство широкополосных сетей. Данные решения предоставляют абонентам как традиционные услуги сетей кабельного телевидения, так и уникальные сервисы, возможные только в пакетных сетях. Традиционные технологии телевидения (спутниковое, эфирное, кабельное) не обладают интерактивностью, т.е не предусматривают "обратной связи" с абонентом, тогда как услуги "Triple Play", предоставляемые по широкополосным сетям, являются в полной мере интерактивными и позволяют учесть желания абонентов.[3]

Необходим комплекс инструментов, обеспечивающих выполнение вспомогательных задач, возникающих в процессе управления мультисервисными СПД. К этим задачам можно отнести:

- сбор и предоставление оперативной информации о состоянии компонентов сети, нагрузке на компоненты и прогноз на загрузку;
- мониторинг и управление информационными потоками.

Анализ трафика, передаваемого в СПД позволяет решить эти проблемы. Кроме того, учет и анализ трафика позволяет контролировать качество предоставления услуг. Основная цель заключается в обеспечении высокого качества услуг является очень важным для конвергентных сетей передачи голоса и видео трафика каких-либо задержек и технических требований на выделенную

полосу пропускания. Для выявления основных тенденций трафика, его вершины, пики конкретных приложений, а также интероперабельности конкретных типов трафика с различными типами политики и QoS, действуйте следующим образом [23]:

- найти суточные, часовые и иные циклы периодичности в поведении трафика;
- провести анализ потоков данных по длине пакетов передаваемой информации.

1.4 Мультисервисные сети, построенные на базе IP

Основная задача мультисервисных сетей заключается в обеспечении работы разнородных информационных и телекоммуникационных систем и приложений в единой транспортной среде, когда для передачи обычного трафика (данных) и трафика другой информации (речи, видео и др.) используется единая инфраструктура.

Базовыми понятиями мультисервисных сетей являются QoS (Quality Of Service) и SLA (Service Level Agreement), то есть качество обслуживания и соглашение об уровне (качестве) предоставления услуг сети. Переход к новым мультисервисным технологиям изменяет саму концепцию предоставления услуг, когда качество гарантируется не только на уровне договорных соглашений с поставщиком услуг и требований соблюдения стандартов, но и на уровне технологий и операторских сетей.

Архитектурно структуру мультисервисной сети можно представить в виде нескольких основных уровней: магистральный уровень, уровень распределения и агрегирования и уровень доступа.(рисунок 1.4)

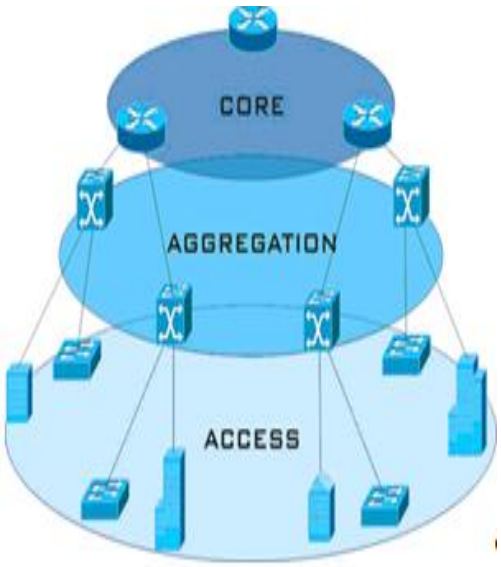

Рисунок 1.4 - Схема структуры мультисервисных сетей.

Магистральный уровень является универсальным высоким уровним, если возможно, единая платформа для передачи информации, осуществляется на основе цифровых каналов связи.

Распределительный уровень включает в себя сетевой узел оператора оборудования, и уровень агрегации выполняет агрегацию задач с уровнем доступа и подключения к позвоночнику (транспортной) сети.

Уровень доступа или внутридомовых корпоративной сети, а также каналов связи для обеспечения их соединения узел (узлы) распределительной сети.

Построение мультисервисных сетей осуществляется на базе самых различных технологий, как на платформе IP (IP VPN), так и на базе выделенных каналов связи. На магистральном уровне наиболее известны сегодня технологии IP/MPLS, Packet over SONET/SDH, POS, ATM, xGE, DWDM, CWDM, RPR.

Сети доступа обеспечивают пользователям доступ корпоративного уровня (или отдельные лица) к операторам связи. Это самая трудная часть телекоммуникационной сети, характеризуется большим набором интерфейсов и терминального оборудования, различных топологий и средств массовой информации, с различными требованиями к надежности и производительности.

В качестве технологий агрегирования доступа и услуг могут также использоваться совершенно различные подходы, которые определяются, в первую очередь, стоимостью подключения, необходимой пропускной способностью каналов и обеспечением требуемого качества обслуживания, а также уже существующей инфраструктурой, поверх которой создается мультисервисная сеть. Это, например, Fast/Gigabit Ethernet, ISDN, xDSL (HDSL, ADSL, VDSL и др.), сети кабельного телевидения, оптические абонентские сети, беспроводные сети Wi-Fi и WiMAX. В наше время оптимальной, как с точки зрения качества, так и стоимости, принято считать технологию xDSL. Главное ее преимущество заключается в том, что для организации высокоскоростного доступа в сети передачи данных эта технология позволяет использовать уже имеющуюся телефонную сеть.

При большом количестве пользователей в сети с множеством услуг требует сложного и интеллектуальную систему управления. Интернет одновременно передавать различные типы трафика, а также для каждого из них требуется безусловное соблюдение определенных параметров и разрешенных более или менее серьезных уступок, с другой стороны, требует специальных специализированные инструменты, которые мешают перегруженность сети и нарушения требуемого качества.Сеть должна устранить перегрузку сети, автоматически решая, что можно пожертвовать в разных случаях - Полоса пропускания, время доставки или для отдельных потоков целостности информации.

При пренебрежении требований управляемости и мониторинга состояния владельцы сети столкнутся с серьезными трудностями, сопровождающимися критичными для бизнеса сбоями и серьезными финансовыми потерями. Чтобы предоставлять новые услуги, обеспечивать их необходимое качество,

правильно их распределять и маршрутизировать, очень важно, чтобы правильно могли приниматься все необходимые данные, вне зависимости от используемой технологии и типа оборудования. В качестве систем мониторинга и управления сети используются средства диагностики, представляющие собой мощные инструменты (функции анализа протоколов, контроля плана маршрутизации и пр. в современных коммутаторах), а также программные системы OSS/BSS (Operation Support Systems/Business Support Systems).

1.4.1 Обеспечение качества обслуживания сетей на базе MPLS

MPLS (Multiprotocol Label Switching) – это технология быстрой коммутации пакетов в многопротокольных сетях, основанная на использовании меток. MPLS разрабатывается и позиционируется как способ построения высокоскоростных IP-магистралей, однако область применения технологии не ограничивается протоколом IP, а распространяется на трафик любого маршрутизируемого сетевого протокола.

«Многопротокольность» в названии технологии означает, что MPLS - инкапсулирующий протокол и может транспортировать множество других протоколов (рисунок 1.6).

Рисунок - 1.5 Технология MPLS в IP-сетях и модель OSI/ISO

Маршрутизатор, с помощью которого сайт клиента подключается к сети оператора, называется пограничным маршрутизатором клиента (Customer Edge router, CE). Пребывая компонентом сети клиента, CE может быть сведен с магистральной сетью провайдера несколькими каналами. Магистральная сеть провайдера является сетью MPLS, где пакеты IP продвигаются на основе не IP-адресов, а локальных меток.[13]

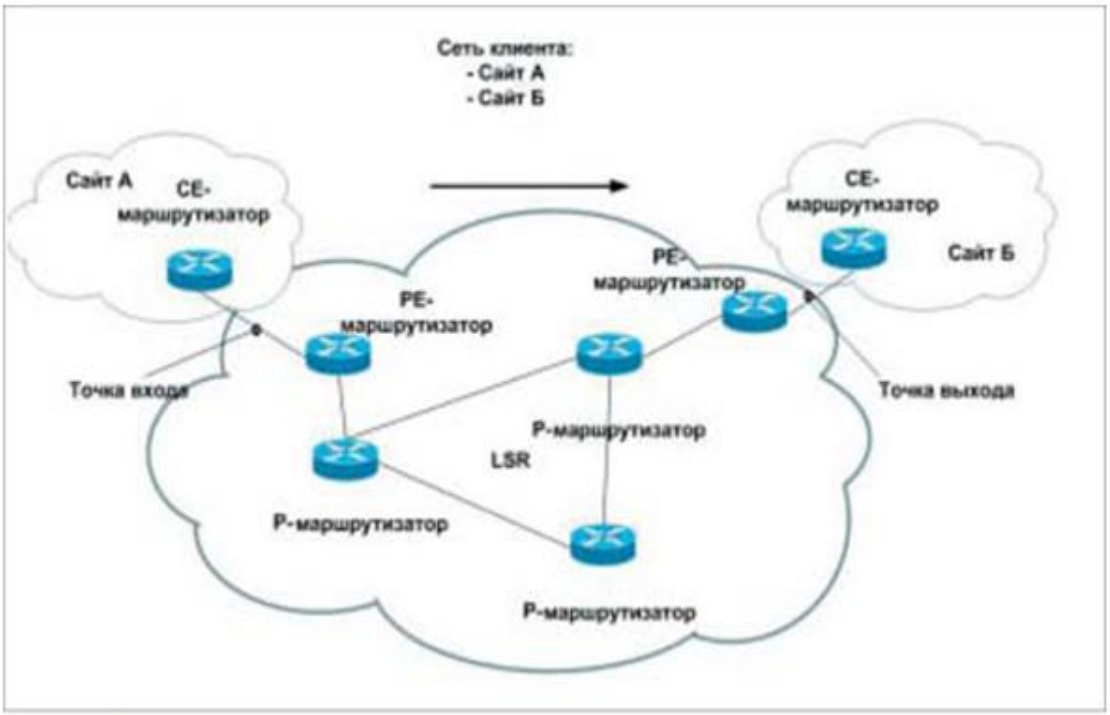

Рисунок 1.6 – технология функционирования MPLS

В изолированной сети пограничных маршрутизаторах (поставщик пограничном маршрутизаторе, PE), которые соединены через маршрутизаторы CE клиентских сайтов, а внутренние маршрутизаторы провайдера позвоночника. Спланировать маршрут-поглотители CE и PE, как правило, непосредственно связанные с физической канала лома под управлением любой протокол канального уровня. В целом, между CE и PE основана на стандартном стека протоколов TCP / IP, поддержка MPLS нужна только для внутренних интерфейсов PE (и всех интерфейсов в-P). В границе края провайдер сети маршрутизаторы PE только быть диссонансом для поддержки виртуальных частных сетей, так что они просто "знать" о существующей VPN. Если мы рассмотрим сеть с точки зрения VPN, поставщик маршрутизатор P непосредственно не взаимодействует с маршрутизаторами CE заказчика, а просто располагаются вдоль LSP между входными и выходными маршрутизация PE-торов.

Функционирование PE-маршрутизаторов

Периферийные маршрутизаторы CE и PE (заказчика и провайдера) обмениваются друг с другом маршрутной информацией одним из внутренних

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

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

К PE-маршрутизатору могут быть подключены несколько VPN-сетей разных заказчиков (рисунок 1.7). В этом случае на каждый интерфейс (int1, int2 и т.д.) PE-маршрутизатора, к которому подключена локальная сеть офиса заказчика, устанавливается отдельный протокол маршрутизации. Для каждого интерфейса PE-маршрутизатора один из протоколов IGP создает таблицу маршрутизации VRF, а каждая таблица маршрутизации VRF соответствует VPN-маршрутам для каждого заказчика.

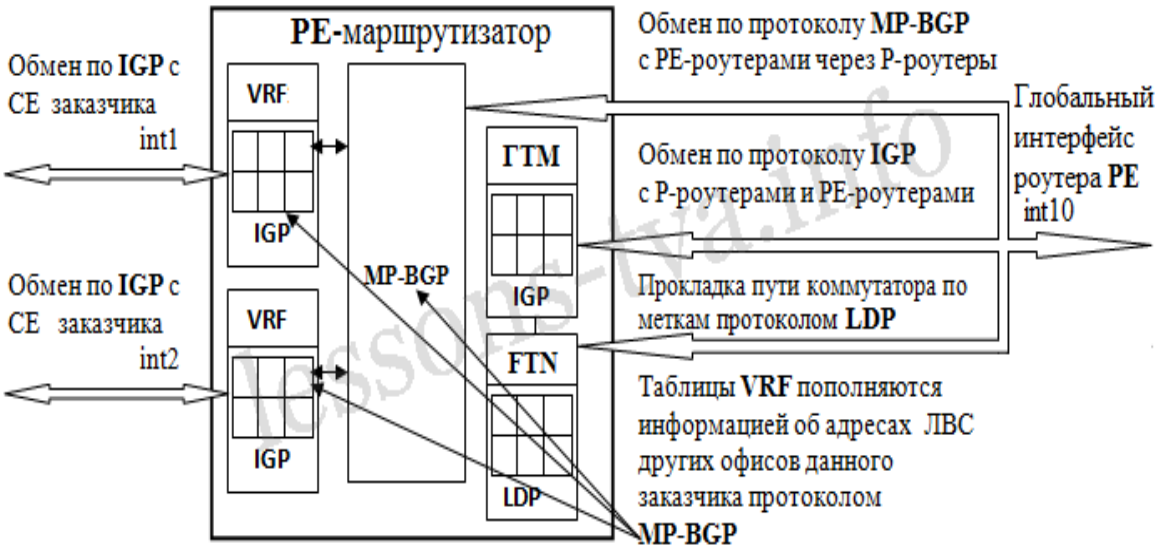

Рисунок 1.7 - PE-маршрутизатор

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

маршрутизаторами с помощью традиционных протоколов внутренней IP-маршрутизации (IGP), например OSPF или IS-IS, и создают свои таблицы маршрутизации.

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

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

Необходимо отметить, что PE направляет входной трафик в определенный виртуальный путь LSP на основании FEC (Forwarding Equivalence Class – класса эквивалентности продвижения). FEC – это группа пакетов к условиям, транспортировки которых предъявляются одни и те же требования. Пакеты, принадлежащие одному FEC, перемещаются по одному LSP. Классификация FEC может осуществляться различными способами, например: по IP-адресу сети (префиксу сети) назначения, типу трафика, требованиям инжиниринга и т.д.

Для корректной работы VPN требует, чтобы информация на rutah идти через провайдера магистральной сети не распространяется за его пределы, а также информацию о маршрутах клиентских сайтов не стали известны за пределами определенной VPN. Барьеры на маршрут объявлений с расширенным ных устанавливаются соответствующим Конфигурации-маршрутизаторов. Протокол маршрутизации содержит информацию о том, как вы можете взаимодействовать с каких-либо объявлений и взять на себя любой интерфейсе распространять их.

Роль таких барьеров в сети MPLS VPN играют пограничные маршрутизаторы PE. Можно представить, что через маршрутизатор PE проходит невидимая граница между зоной клиентских сайтов и зоной ядра сети провайдера. По одну сторону располагаются интерфейсы, через которые PE взаимодействует с маршрутизаторами P, а по другую — интерфейсы, к которым подключаются сайты клиентов. С одной стороны, на PE поступают объявления о маршрутах магистральной сети, с другой — объявления о маршрутах в сетях клиентов.[14]

Аналогичным образом настроены и остальные PE. Маршрутизаторы P принимают и обрабатывают маршрутную информацию IGP, поступающую со

всех интерфейсов. В результате на всех маршрутизаторах PE и P создаются по таблице маршрутизации, где содержатся все маршруты в пределах внутренней сети провайдера. Вместе с тем и сети клиентов ничего не "знают" о маршрутах в сети провайдера. Таблица маршрутизации, создаваемая на пограничных маршрутизаторах PE на основе объявлений из магистральной сети, имеет специальное название "глобальная таблица маршрутизации". В отличие от нее таблицы, которые PE формирует на основе объявлений, поступающих из сайтов клиентов, получили название таблиц VRF (VPN Routing and Forwarding, VRF).

Сайты клиентов представляют собой обычные сети IP, маршрутная информация в которых может передаваться и обрабатываться с помощью любого протокола маршрутизации класса IGP. Очевидно, что этот процесс никак не регламентируется провайдером. Маршрутные объявления свободно распространяются между узлами в пределах каждого сайта до тех пор, пока они не доходят до пограничных маршрутизаторов PE, служащих преградой для их дальнейшего распространения.

Разграничение маршрутов разных клиентов обеспечивает установка на маршрутизаторах PE отдельного протокола маршрутизации на каждый интерфейс, к которому подключен сайт клиента. Этот протокол принимает и передает клиентские маршрутные объявления только с одного определенного для него интерфейса, не пересылая их ни на внутренние интерфейсы, через которые PE связан с маршрутизаторами P, ни на интерфейсы, к которым подключены сайты других клиентов. В результате на маршрутизаторе PE создается несколько таблиц маршрутизации VRF.

Традиционно главными требованиями, предъявляемыми к технологии магистральной сети, были высокая пропускная способность, малое значение задержки и хорошая масштабируемость.

Архитектура MPLS обеспечивает построение магистральных сетей, имеющих практически неограниченные возможности масштабирования, повышенную скорость обработки трафика и высокую гибкость с точки зрения организации дополнительных сервисов. Кроме того, технология MPLS позволяет интегрировать сети IP и ATM, за счет чего поставщики услуг смогут не только сохранить средства, инвестированные в оборудование асинхронной передачи, но и извлечь дополнительную выгоду из совместного использования этих протоколов.

Для обеспечения требуемого качества услуг на сети IP/MPLS применяются четыре класса обслуживания трафика (CoS):

- Best Effort – для передачи некритичных данных;
- Business Critical – для данных, критичных к параметрам передачи;
- Multimedia – для потокового видео или организации видеоконференций;
- Real Time – для передачи особенно критичных к задержкам и потерям данных: голосового трафика (VoIP), видео и ТВ-сигналов высокого качества.

Для соответствующего QoS в IP-сетях международная организация IETF (Internet Engineering Task Force) определила две основные модели: Integrated Services (IntServ) и Differentiated Services (DiffServ). Рассмотрим данные технологии относительно MPLS.

Модель интегрированного обслуживания IntServ обеспечивает сквозное качество обслуживания, гарантируя необходимую пропускную способность. IntServ использует для своих целей протокол резервирования сетевых ресурсов RSVP, который обеспечивает выполнение требований ко всем промежуточным узлам.

Применительно к MPLS расширения протокола RSVP могут быть использованы для распределения меток в качестве части процесса резервирования ресурсов и установить маршрут LSP с зарезервированными ресурсами. Такие LSP-маршруты называются LSP-маршрутами с гарантированной полосой пропускания (guaranteed bandwidth LSP). Данные маршруты должны удовлетворять требованиям к ширине полосы пропускания на всех каналах для поддержки резервирования, а также иметь достаточное буферное пространство на промежуточных узлах для того, чтобы вместить возможные всплески в зарезервированном потоке данных. После того как маршрут установлен, поддерживающее коммутацию по меткам устройство LSR вставляет объект явного маршрута (Explicit Route Object) в сообщение PATH протокола RSVP, обеспечивая тем самым создание LSP-маршрута вдоль выбранного пути. Пакеты, для которых было сделано RSVP-резервирование, могут рассматриваться как эквивалентные классы FEC. При этом каждый класс FEC идентифицируется своей меткой .

Тем не менее, предоставление качественных услуг с механизмом IntServ, применяются к каждой отдельной расширения потока и не может быть трудно реализовать. Таким образом, новый подход для обеспечения качества путем адаптации Обь-за совместной моделей для движения, в котором различные потоки объявление ся в интегрированных классах и обеспечить надлежащее качество услуг для объявлений потоков.

Архитектура DiffServ предполагает существование связанных областей сети (DiffServ-доменов), в пределах каждой из которых проводится единая политика по классификации служб передачи пакетов. В результате выполнения классификации каждому пакету ставится в соответствие номер некоторого класса обслуживания, реализованного в данном DiffServ-домене. Такой номер класса обслуживания называется DiffServ CodePoint (DSCP). Выбранное значение DSCP записывается в заголовок IP-пакета в поле ToS. Для каждого класса обслуживания администратор DiffServ-домена может установить набор требований к параметрам QoS. После классификации пограничные устройства приводят параметры информационных потоков, поступающих в DiffServ-домен в соответствие с требованиями, устанавливаемыми для выбранных классов обслуживания [3].

Поле DSCP определяет уровень обслуживания пакета в данном сетевом узле. Для этого уровня обслуживания используется термин режим пересылки

PHB (Per-Hop Behavior), который определяет порядок обработки пакета в узле в плане очередности его диспетчеризации и отбрасывания. То есть PHB определяет очередность пересылки пакетов, вероятность отбрасывания пакетов в том случае когда очередь становится длиннее заданного порога.

Всего определенно 14 стандартных классов обслуживания трафика. Возможны варианты срочной пересылки Expedited Forwarding (EF) при котором трафик встречает минимальную задержку и низкую вероятность потерь, пересылки по возможности Best Effort (BE) при котором трафик не проходит никакой специальной обработки, и 12 классов гарантированной пересылки Assured Forwarding (AF) с различными номерами очереди и очередности отбрасывания пакетов [1].

Заметим, однако, что для данной этикетке QoS в соответствии с самодостаточной движения. Если трафик на маршруте не должно име-ющему адекватные ресурсы для выполнения требований к качеству функции-нирования, это гарантирует качество передачи физически не в состоянии быть выполнена.

MPLS — TE позволяет создавать коммутируемые по меткам тракты через звенья имеющие надлежащие ресурсы, тем самым гарантируя, что для обслуживания потока всегда будет иметься достаточная полоса пропускания.

Однако простое совмещение DiffServ и MPLS–TE не позволяет добиться желаемого результата. Так как MPLS-TE не имеет информации о разделении потоков по классам обслуживания CoS и функционирует в доступной полосе пропускания одинаково для всех классов. Для объединения Diffserv и Traffic Engineering была разработана новая модель QoS, объединяющая все лучшее из них — Diffserv-Aware Traffic Engineering [2].

LSR-устройства сети MPLS не анализируют содержание IP-заголовка и значение его поля DSCP, как требует механизм DiffServ. Это означает, что соответствующее значение PHB должно быть получено из значения метки. Промежуточный заголовок MPLS имеет 3-битовое поле Exp. Первоначально оно рассматривалось как экспериментальное. Данное поле может содержать до восьми значений и используется в коммутации MPLS для поддержки до 8 классов DiffServ. Поэтому биты приоритета отбрасывания пакетов или первых 3 бита поля DSCP на границе сети копируются в поле Exp заголовка MPLS. Каждое LSR-устройство на маршруте LSP преобразует биты поля Exp в значения PHB. Провайдер службы может также установить другое значение CoS пакета MPLS, определенное при предоставлении службы. Данная функция позволяет провайдеру устанавливать поле Exp MPLS вместо того, чтобы переписывать значение пользовательского поля IP-приоритета отбрасывания, что предоставляет возможность сохранить IP-заголовок в первоначальном состоянии и использовать его в дальнейшем. При движении пакета по MPLS-магистрали сконфигурированный пользователем класс CoS не изменяется. Маршруты LSP, созданные таким образом, известны как маршруты E-LSP или Exp-LSP. Маршруты E-LSP могут поддерживать до восьми классов PHB на каждом LSP-маршруте .

Если в сети MPLS требуется более 8 значений PHB, то используются маршруты L-LSP (меточный маршрут — Label LSP), и в этом случае значение PHB LSR-устройства определяется по значению метки. Преобразование метки в функции PHB должно быть передано по протоколу сигнализации. Для каждого маршрута L-LSP возможен только один параметр PHB, или нескольких PHB, которые имеют одинаковый режим диспетчеризации, но различные приоритеты отбрасывания пакетов. Приоритеты отбрасывания трафика кодируются в битах поля Exp промежуточного заголовка.

Маршруты E-LSP более эффективны, чем маршруты L-LSP, поскольку модель E-LSP аналогична стандартной модели DiflServ. На одном маршруте E-LSP может поддерживаться несколько значений PHB. Таким образом можно ограничить общее количество создаваемых маршрутов LSP, что позволяет экономить пространство меток [2].

Так как базовым требованием к DiffServ –TE быть в состоянии отдельно резервировать полосу пропускания для трафика каждого класса, то необходимым является отслеживание во всех маршрутизаторах сети того какая полоса пропускания доступна для трафика каждого класса в любой момент времени. Для этого вводится понятие класс типа CT (Class of Type), которое определяется как совокупность ограничений по полосе пропускании звена данных. С помощью CT производится маршрутизация с учетом ограничений полосы пропускания звена и управления доступом. Предусмотрено до восьми CT, где негарантированному обслуживанию соответствует CT0. Один LSP может передавать трафик только одного и того же CT и использовать при этом одинаковые или разные приоритеты вытеснения трактов потоков. Информация о CT для LSP передается в составе сообщения Path протокола RSVP.

Одним из самых важных аспектов расчета доступной полосы пропускания является назначение полосы пропускания для разных CT. Доля пропускной способности звена, которую может занимать данный CT называется ограничением по полосе пропускания BC (bandwidth constraint) [2].

Одна из моделей ограничений по полосе пропускания ставит в соответствие одному BC один CT. Она называется моделью максимального назначения MAM (Maximum Allocation Model). Согласно модели MAM пропускная способность звена просто распределяется между разными CT без возможности распределения неиспользуемой полосы пропускания, так что эта полоса может непроизводительно простаивать вместо того чтобы использоваться для других CT. К достоинствам данной модели можно отнести полную развязку трактов LSP, переносящих трафик от разных CT, в связи с чем нет необходимости задавать приоритеты.

Модель назначения полосы пропускания, называемая моделью матрешек RDM (Russian Dolls Model), улучшает эффективность использования пропускной способности звеньев по сравнению с моделью MAM благодаря тому, что позволяет классам CT совместно использовать полосу пропускания. В данной модели на одном конце спектра BC7 мы имеем фиксированную долю пропускной способности звена, которая резервируется только для трафика

CT7. На другом конце спектра BC0 предоставляет полную пропускную способность звена, которая совместно используется всеми CT. Недостатком модели RDM по сравнению с моделью MAM является отсутствие развязки разных CT, и поэтому должна использовать механизм приоритетного вытеснения для того чтобы соответствующему CT в любом случае гарантировать его пропускную способность.

Уведомления об используемой модели BC и о полосе пропускания, назначенных для каждого BC, передаются с помощью протоколов IGP. Возможен вариант с различными моделями BC в разных звеньях сети, однако такой вариант усложняет конфигурирование, обслуживание и эксплуатацию.

В данной работе были рассмотрены существующие методы обеспечения качества обслуживания в мультисервисных сетях передачи данных основанных на технологии MPLS. Были выявлены их преимущества и недостатки, что позволяет провайдерам обеспечивать заданное качество обслуживания более эффективно на широком спектре платформ.

2.Экспериментальная часть

2.1 Описание исследуемой системы

В исследовании была применена СПД «Казтелепорт» построенный на MPLS. СПД предоставляет услуги виртуальных выделенных сетей (VPLS, IP VPN) и виртуальных выделенных линий (virtual leased line). Интеллектуальные функций урпавление трафиком, предоставляемые протоколом IP/MPLS, позволяет организовывать, удалять и менять маршруты по мере необходимости для поддержки тех или иных услуг и соглашений об уровне обслуживания (SLA).

IP/MPLS успешно применяется в крупнейших операторских сетях в Казахстане о во всем мире. Международные организации по стандартизации (IETF, Metro Ethernet Forum) разработали спецификации, обеспечивающие совместимость и взаимодействие оборудования разных производителей, включая совместимость на уровне протоколов сигнализации (LDP, RSVP), услуг (IP-VPN, VPLS, VLL) и диагностических утилит.

В соотвествии с типовым архитектурой, в сети выделяется несклько уровней иерархии, как показоно на рисунке 2.1:

- ядро сети
- уровень агрегации
- уровень доступа

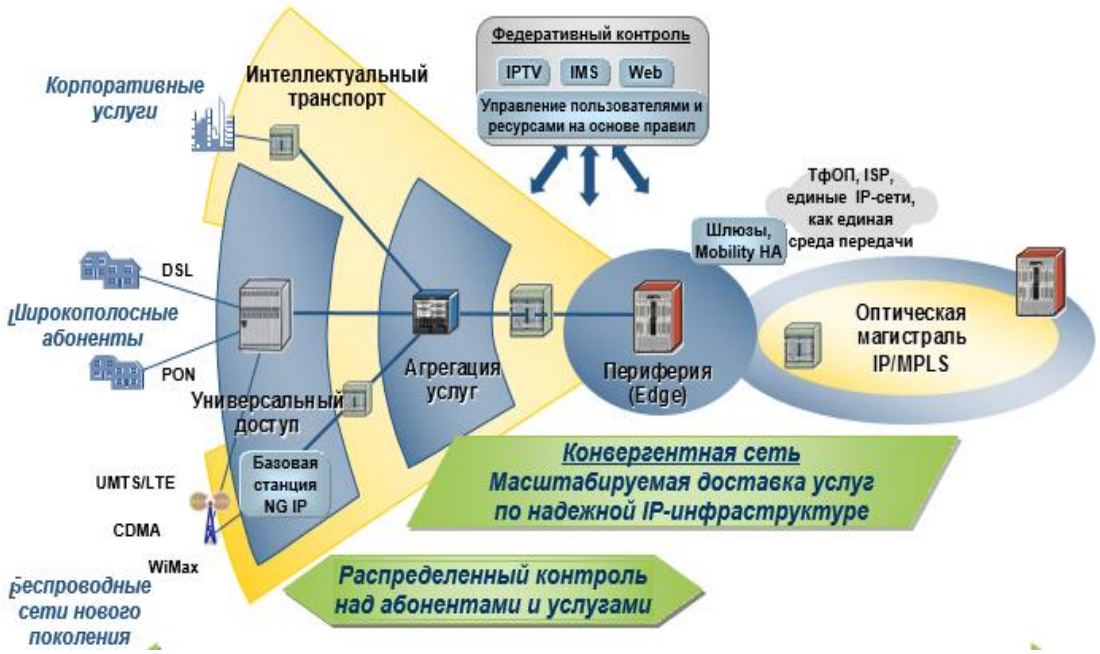

Рисунок 2.1- Архитектура транспортной сети IP/MPLS

В ядре СПД и на уровне агрегации используется новый тип сетевого оборудования – сервисных коммутаторов/маршрутизаторов операторского класса, ориентированных на использование технологии IP/MPLS и ее развитые сервисные возможности, с тем , чтобы добиться полной поддержки IP-услуг нового поколения. Благодаря использованию IP/MPLS в качестве основной транспортной среды возможно предоставлять сервисы (VLL,VPLS,IP VPN) одновременно с Triple Play сервисами для клиентов.

Верхний уровень иерархии – ядро сети – состоит из узлов, объединенных в кольцо по технологиb 10 Гбит/с Ethernet. Ядро сети выполнено на сервисных маршрутизаторах с полной поддержкой IP/MPLS. Маршрутизаторы ядра выполняют функции PE/P устройств, предоставляют сервисы L3/L2 и являются L3 границей сети. Используется MPLS Fast Reroute для быстрого восстановление в течение времени, не превышающего 50 мсек, на уровне агрегации с резервными маршрутизаторами, т.е. кольцевое и частично связанные топологии. Благодаря использованию механизмов , как резервный маршрут (LSP) и быстрого переключение (MPLS Fast Reroute), сеть агрегации обеспечивает время восстановления, не превышающего 50 мсек даже при переключении тысячи клиентских сервисов, затронутых отказом.

За счет использования механизмов интеллектуального управления трафиком (Traffic Engineering) и быстрой перемаршрутизации (Fast Reroute). Это позволяет в автоматическом режиме мгновенно переключать потоки данных на резервные направления при авариях на физических средах и выходе из строя сетевого оборудования, а также в случае существенного повышения за-

грузки основных маршрутов. Автоматизация процесса обеспечивается протоколами маршрутизации и сигнализации MPLS.

На уровне агрегации используется сервисные коммутаторы с полной поддержкой IP/MPLS и сервисов второго уровня. Межузловые связи на уровне агрегации выполнены оптоволоконным кабелем по технологии 1 Гбит/с Ethernet. Сегменты агрегации представляют собой линейные, древовидные и кольцевые топологии.

Ethernet сети на основе протокола MPLS имеют отличные характеристики масштабируемости и взаимодействия оборудования различных производителей. При использовании MPLS инкапсуляции и коммутации по меткам, VLAN-ы имеют только локальную значимость, обеспечивая работу десятков тысячи заказчиков.Блогодоря отображению номеров VLAN в LSP, клиентский трафик эффективно разделяется и прозрачно передается через сеть операторов.

Модель предоставление Ethernet услуг на основе протокола MPLS базируется на широко признанных и используемых стандартах IETF и Metro Ethernet Forum, таких как Ethernet Virtual Leased Line (draft-Martini) VPLS(draft –ietf-l2vpn-vpls-ldp).

Для доступа в интернет использован пограничный маршрутизатор Cisco.

Для управление сетевым оборудованием, а также для облегчение работы оператора по запуску и поддержке различных сервисов, диагностике, поиску и устранению неисправности используется система управление сетью Service Aware Manager. Это эффективная система управления сетью и услугами в конвергентной среде IP/MPLS, от уровня доступа до ядра быстрое конфигурирование сервисов сокращает срок предоставления услуг конечным пользователям и повышает уровень гибкости при запуске новых сервисов.(рисунок 2.2)

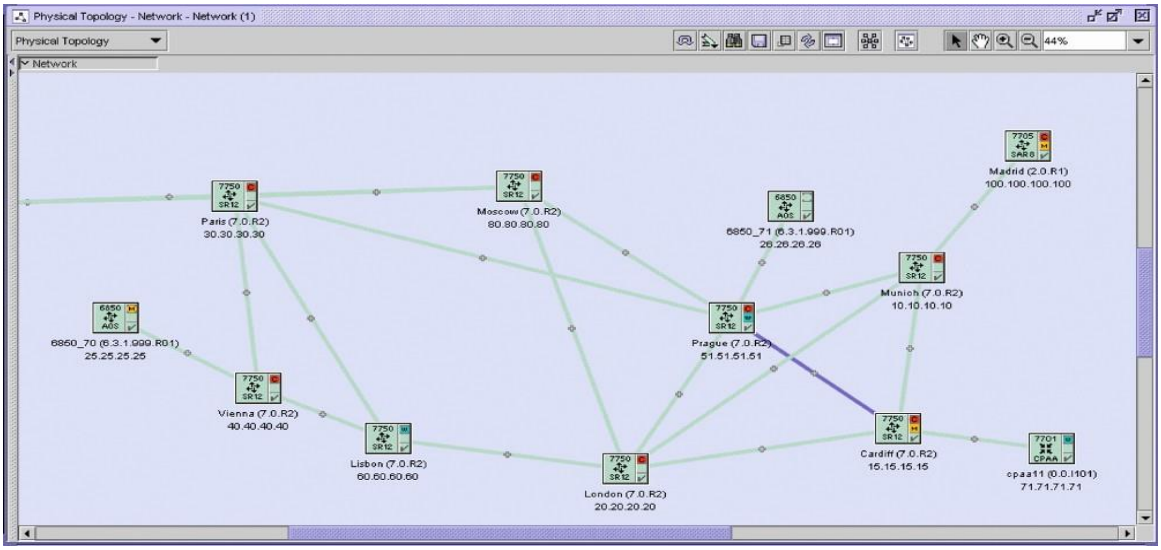

Рисунок 2.2- Управление сетью

SAM имеет архитектуру клиент-сервер и позволяет управлять всеми сетевыми элементами и сервисами из единого центра управление сетью, а также с удаленных терминалов. Система управление может работать с любым сетевым оборудованием, поддерживающим протокол SNMP.

Возможности:

- Простой графический интерфейс упрощает настройку и конфигурирование услуг. Автоматизация предоставления услуг ускоряет работу и снижает риск ошибок при использовании интерфейса командной строки
- Общее конфигурирование услуг VLL/VPLS и IPVPN сокращает затраты на внедрение услуг разных типов
- Расширенные возможности обеспечения гарантированного качества услуг выявляют различные нарушения конфигурирования услуг до того, как они станут заметны потребителям
- Эффективные средства диагностики помогают быстро выявлять основные причины проблем и ускоряют их устранение
- Гибкие шаблоны настроек упрощают интеграцию с существующими процессами
- Открытые интерфейсы, поддерживающие интеграцию со специализированными веб-порталами, системами поддержки эксплуатации (OSS) и системами поддержки бизнес-процессов (BSS)

Приемущество:

- Быстрое внедрение новых услуг и технологий
- Ускоренное и надежное конфигурирование, минимизирующее риск неправильной настройки и сокращающее ввод системы в эксплуатацию
- Проактивное устранение проблем до того, как они станут заметны потребителям
- Результативный сбор статистических данных для организации гибкого биллинга и опций SLA (соглашений об уровне предоставляемых услуг)
- Непревзойденная эксплуатационная масштабируемость для обеспечения поддержки роста сети и увеличения объема предоставляемых услуг
- Повышение производительности и гибкость за счет использования системы управления позволяет экономически эффективно интегрироваться в существующие операционные среды, оптимизируя бизнес-процессы
- Внедрение системы 5620 SAM повышает производительность и гибкость управления сети, что обеспечивает эффективную интеграцию с существующей инфраструктурой и улучшает процессы управления.

Услуга виртуальная частная сеть (IP VPN)

Услуга IP VPN - это создание виртуальных частных сетей связи на базе IP-сети, с применением технологии MPLS (Multi Protocol Label Switching), которая позволяет объединять удаленные офисы Клиента в единую защищенную корпоративную сеть с полным спектром телекоммуникационных услуг и гарантией качества обслуживания.

Предоставление доступа к сервису осуществляется по выделенным каналам, что позволяет передавать любые объемы информации.

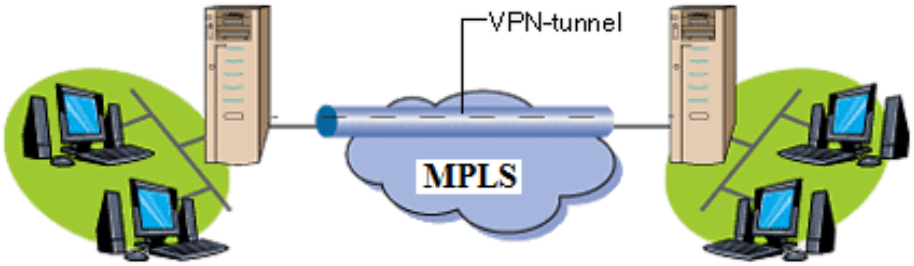

Рисунок – 2.3 IP VPN

Важнейшие задачи, которые можно решить с помощью услуги IP VPN:

- создание защищенной корпоративной сети, невзирая на географическую удаленность офисов компании друг от друга
- высокая безопасность передачи информации
- интеграция различных бизнес-приложений, которая обеспечивается тремя классами обслуживания, каждый из которых предназначен для соответствующего типа трафика. При этом гарантировано качество передачи трафика для каждого класса:
- "Передача данных": обмен файлами и сообщениями, совместная работа над документами и базами данных, доступ к корпоративным информационным http -серверам
- "Голос": телефония - удобная и недорогая внутрикорпоративная телефонная связь с использованием короткого набора номера
- "Видео": видеоконференцсвязь, телемедицина.

Преимущества организации VPN на базе MPLS

Основными преимуществами организации VPN на базе MPLS можно назвать:

- масштабируемость;
- возможность пересечения адресных пространств, узлов подключенных в различные VPN;
- изолирование трафика VPN друг от друга на втором уровне модели OSI.

Масштабируемость достигается за счет того, что подключение нового узла в имеющийся VPN производиться только перенастройкой одного PE, к которому подключается данный узел.
В разных VPN адресные пространства могут пересекаться, что может быть крайне полезным, в случае если оператору надо предоставить VPN нескольким клиентам, применяющим одинаковое приватное адресное пространство, например адреса 10.0.0.0/8. Устройства P (LSR) при коммутации рассматривают только внешнюю метку, определяющую LSP между PE, и не анализируют заголовок IP пакета, то справедливо говорить о том, что P устройства вы-

полняют 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 VPN полностью разделяются, и обеспечивается разделение трафика от разных VPN на втором уровне модели OSI.

На рисунке 2.4 показана схема соединения сервера с IP – сетью пользователей.

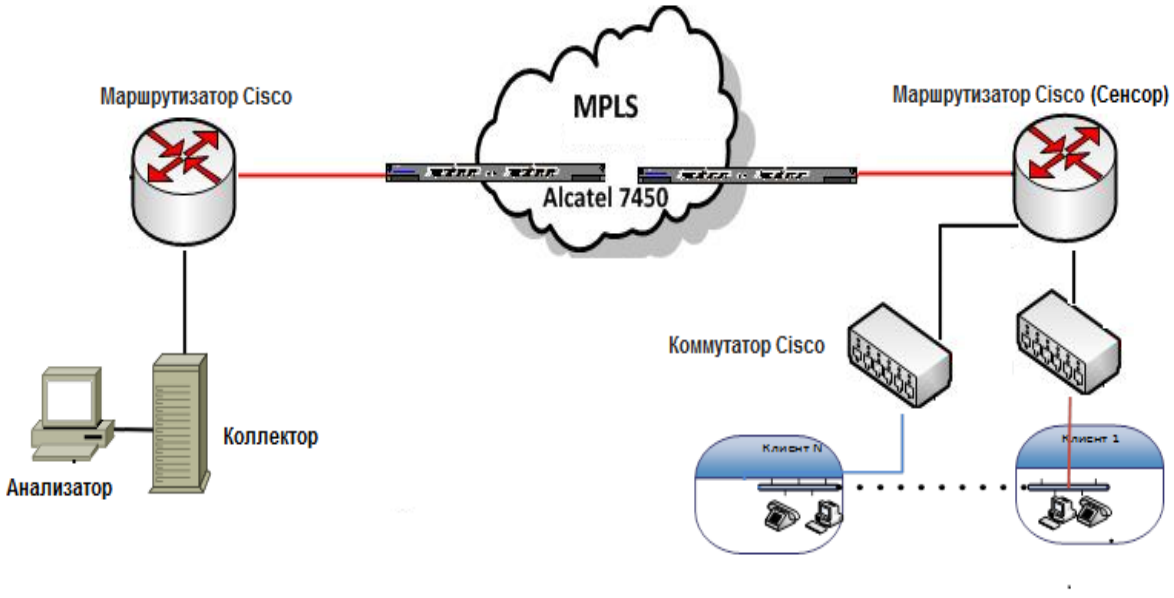

Рисунок 2.4 - Структура сети

2.3 Описание программного обеспечения, используемого в исследовании

В работе рассматривается реализация протокола для мониторинга сетевого трафика на третьем уровне (уровень IP). NetFlow — проприетарный открытый протокол, разработанный Cisco для мониторинга трафика в сети. Netflow предоставляет возможность анализа сетевого трафика на уровне сеансов, делая запись о каждой транзакции TCP/IP.

Назначение протокола NetFlow — это сбор, обработка данных и управление физическими интерфейсами. Можно получить информацию о нагрузке, в некоторых случаях информацию о температуре и других климатических условии.

Для пересылки заголовков IP-пакетов, проходящих через маршрутизатор разработано много протоколов, однако стандартом де-факто стал протокол Netflow, разработанный компанией Cisco для своих маршрутизаторов. Суть протокола Netflow в том, что заголовки транзитных IP-пакетов накапливаются в специальном буфере и аггрегируются (т.е. пакеты с одинаковыми характеристиками объединяются в одну запись) что позволяет существенно

сэкономить на объеме пересылаемых данных по протоколу Netflow. Таким образом, для экспериментального исследования можно применить данный протокол.

В процессе эксперимента с NetFlow протоколом можно выполнить анализ пакетов, проходящих через определенный интерфейс сетевого устройства, на основе чего формируется информация в определенном формате о параметрах различных сетевых потоков, проходящих через этот интерфейс, и эта информация передается по IP сети специальной программе, называемой NetFlow коллектором (NetFlow collector). Программа NetFlow коллектор, устанавливается на каком-то компьютере (сервере) сети, и занимается сбором и первичной обработкой информации от одного или группы сетевых устройств, передающих данные в формате NetFlow. Далее уже используются программы, анализирующие собранные данные и предоставляющие пользователю требуемые ему отчеты о работе сети.

Если используется UDP, то потерянная из-за проблем в сети запись не будет получена коллектором. Коллектор может определить потери пакетов по значениям номера записи, которые по стандарту должны быть возрастающими.

Суть работы с Netflow заключается:

- Получаем данные с сенсоров и передаем их на коллектор.
- Обрабатываем и передаем на анализатор.

Архитектура системы основана на датчике, коллектора и анализатора:

- Сенсор собирает статистику проходящего через него трафика. Датчики установлены в сети «узловой точки", такие как пограничные маршрутизаторы сети сегментов.

- Коллектор собирает информацию с датчиков. Полученные данные-ные сбрасывает в файл для дальнейшей обработки. Различные коллекторы хранить данные в различных форматах.

- Анализатор или система обработки читает эти файлы и генерирует ruet-отчеты в форме более удобной для людей. Система должна быть совместима с форматом данных, предоставляемых коллектором. В современной переменных системы, коллекционер и анализатор, часто в сочетании в единую систему.

(рисунок 2.5)

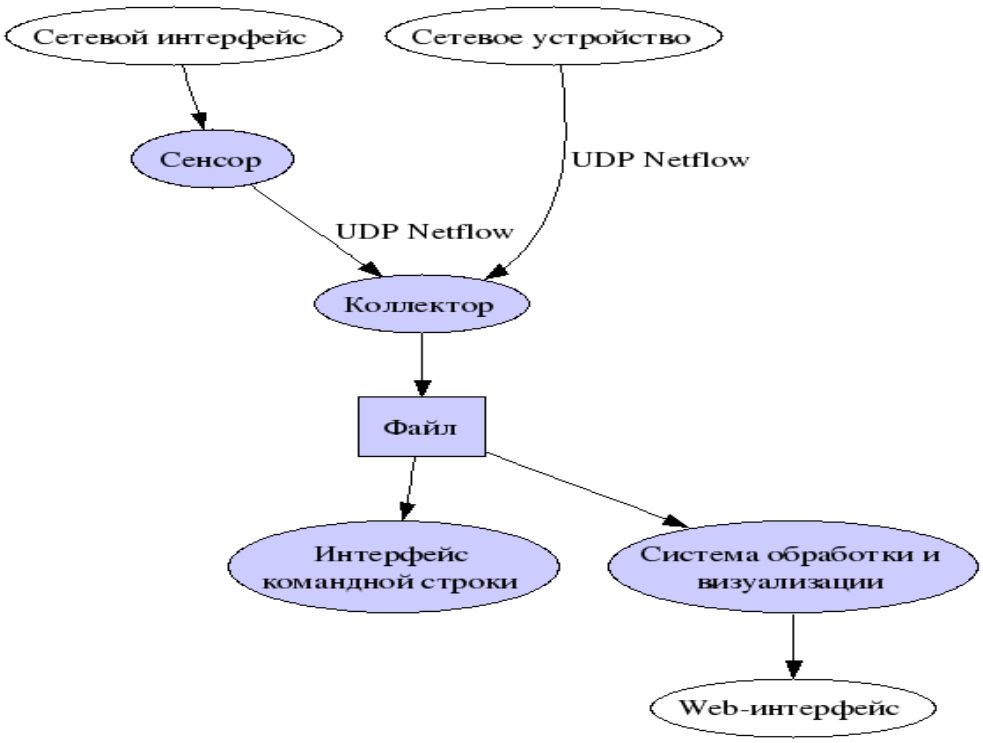

Рисунок 2.5 - Архитектура протокола

Коллектор и стоящий за ним анализатор являются «пассивными» элементами системы. Сенсор шлет на коллектор отчеты о трафике, коллектор принимает, анализатор анализирует, и заполняет свою базу данных на сервере. Если сенсор выключен, он «исчезает» из текущей «он-лайн» статистики, но при этом сохраняется данные о трафике.

NetFlow использует UDP или SCTP для передачи данных о трафике коллектору. Как правило, коллектор слушает порт 2055, 9555 или 9995 (или тот, который Вы укажете при настройке коллектора и сенсора). Сенсор выделяет из проходящего трафика потоки, характеризуемые следующими параметрами:

- адрес источника;
- адрес назначения;
- порт источника для UDP и TCP;
- порт назначения для UDP и TCP;
- тип и код сообщения для ICMP;
- номер протокола IP;
- сетевой интерфейс (параметр ifindex SNMP);
- IP Type of Service.

Потоком считается набор пакетов, проходящих в одном направлении.

Когда датчик обнаруживает, что поток завершается (изменить пакет, или для сброса TCP - сессия), он посылает информацию на кол лектора. В зависимости от настроек он может также периодически отправлять информации коллектору все еще достигая потоков. Это очень важный момент - при

настройке датчика мы решаем по каким параметрам отправлено на информацию коллектора будут объединены в отчетах.

На границе установлены маршрутизаторы, с которых собственно и собираться данные о трафике, причем со внешних интерфейсов. Мы сможем увидеть только общую картину и констатировать, что действительно каналы у нас загружены. Как показывает практика, даже один пользователь способен полностью загрузить 100 Мбит-ный канал.

Эксперимент был проведен на сети компании казтелепорт провайдера доступа в мультисервисную сеть передачи данных. Компания обеспечивает доступ в Интернет, оказывает услуги передачи речи по протоколу IP, видеоуслуги (видеоконференции по протоколу IP) для корпоративных клиентов.

Рассмотрим механизм, того, как происходит сбор информации о сетевых потоках и их экспортирование в оборудовании Cisco Systems. Программный модуль на сетевом устройстве просматривает пакеты, проходящие через сетевой интерфейс, и на основании их анализа формирует данные по каждому сетевому потоку, проходящему через этот интерфейс в формате NetFlow протокола. Эти данные в виде отдельных записей по каждому сетевому потоку временно складываются в кэш (кэшируются). Каждая запись о потоке имеет уникальный идентификатор. Периодически данные из кэша пересылаются через сетевой интерфейс на компьютер (сервер), на котором установлена программа NetFlow коллектора (рисунок 2.6).

Таким образом, использование NetFlow протокола несколько дополнительно загружает сетевой интерфейс. Однако, благодаря очень высокой эффективности протокола, передаваемые с помощью него данные занимают всего около 1,5% от трафика коммутатора или маршрутизатора. NetFlow протокол подсчитывает практически все пакеты и обеспечивает сжатый, но достаточно информативный обзор о всем сетевом трафике по заданному сетевому интерфейсу. Экспортирование данных из кэша выполняется по определенным правилам:

- Записи о сетевых потоках хранятся в кэше заданный промежуток времени. По истечению этого времени они удаляются. По умолчанию в устройствах Cisco Systems записи могут храниться 30 минут.
- Если кэш полностью заполняется, то часть записей удаляется.
- TCP соединения, у которых прекратился поток (FIN) или к которым применена перезагрузка (RST), будут считаться утратившими силу.

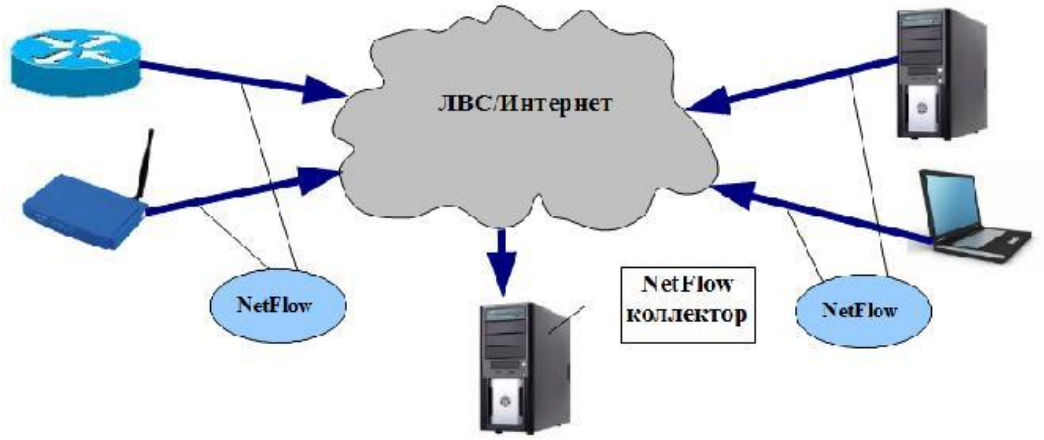

Рисунок 2.6 - Схема построения IP-сети с использованием Netflow

Записи о сетевых потоках, которые утратили силу группируются в "NetFlow Export" дейтаграммы и экспортируются на сетевое устройство (компьютер), с установленным NetFlow коллектором. Такие дейтаграммы могут содержать до 30 записей для NetFlow протоколов версий 5 или 9. Настройка NetFlow протокола выполняется для каждого интерфейса сетевого устройства. Для экспорта информации требуется указать IP адрес и номер порта устройства, где будет работать NetFlow коллектор.

2.2 Проведенные исследования

Эксперимент был проведен на сети алматинского провайдера доступа в мультисервисную сеть. Компания обеспечивает доступ в Интернет, оказывает услуги передачи речи по протоколу IP, видеоуслуги (видеоконференции по протоколу IP) для корпоративных клиентов.

Целью эксперимента является: сбор статистических данных трафика на действующей сети передачи данных; оценка статистических параметров системы для предоставления услуг в мультисервисных сетях.

Для анализа трафика, поступающего от абонентов, рассматривался входящий трафик клиентов телекоммуникационной сети компании казтелепорт, при этом измерялась скорость передачи и объем трафика.

Ежесуточно данные о трафике, поступающие от клиентов, собирались с интервалом в 1 час. На рисунке 2 представлена информация о суточном изменении скорости передачи информации за неделю.

Т а б л и ц а 2.1 - Статистические данные изменение скорости передачи в течении суток

8.00	9.00	10.00	11.00	12.00	13.00	14.00	15.00	16.00	17.00	18.00	19.00	20.00	21.00
1,51	1,76	2,45	2,64	2,1	2,7	1,51	1,64	2,8	2,9	2,4	2,1	1,2	1,105
1,36	1,88	2,01	2,63	1,27	1,84	1,79	1,42	3,6	2,8	2,81	2,65	3,44	1,74
1,05	1,95	2,67	2,89	3,06	3,04	2,94	1,489	2,45	2,947	4,036	2,84	2,094	1,42
1,19	2,28	6,37	3,63	3,2	4,8	4,6	3,84	2,5	2,94	6,12	4,32	3,78	2,64
0,104	1,95	2,67	2,29	5,01	5,75	9,88	8,36	2,55	3,01	5,19	2,24	3,51	3,038
1,03	2,08	4,28	1,87	2,5	4,42	4,37	7,45	6,21	2,87	2,41	3,89	3,15	1,77
1,005	1,02	1,12	1,92	1,52	1,97	1,61	2,94	3,28	4,5	5,56	3,01	2,89	2,76

На рисунке 2.6 последовательно отражены суточные изменения скорости передачи по дням недели, то есть ряд 1 – понедельник, ряд 2 – вторник, ряд 3 – среда, ряд 4 – четверг, ряд 5 – пятница, ряд 6 – суббота, ряд 7 – воскресенье.

Как видно из рисунка 2 наибольшая поступающая нагрузка приходится на пятницу, а наименьшая на понедельник.

Значение входящего трафика возрастает с начала рабочего времени с 8.00 и до 11.00. Час наибольшей нагрузки (ЧНН) приходится на интервал 12.00 -16.00. В интервале 16.00 – 17.00 нагрузка падает и опять возрастает. После 20.00 резко убывает.

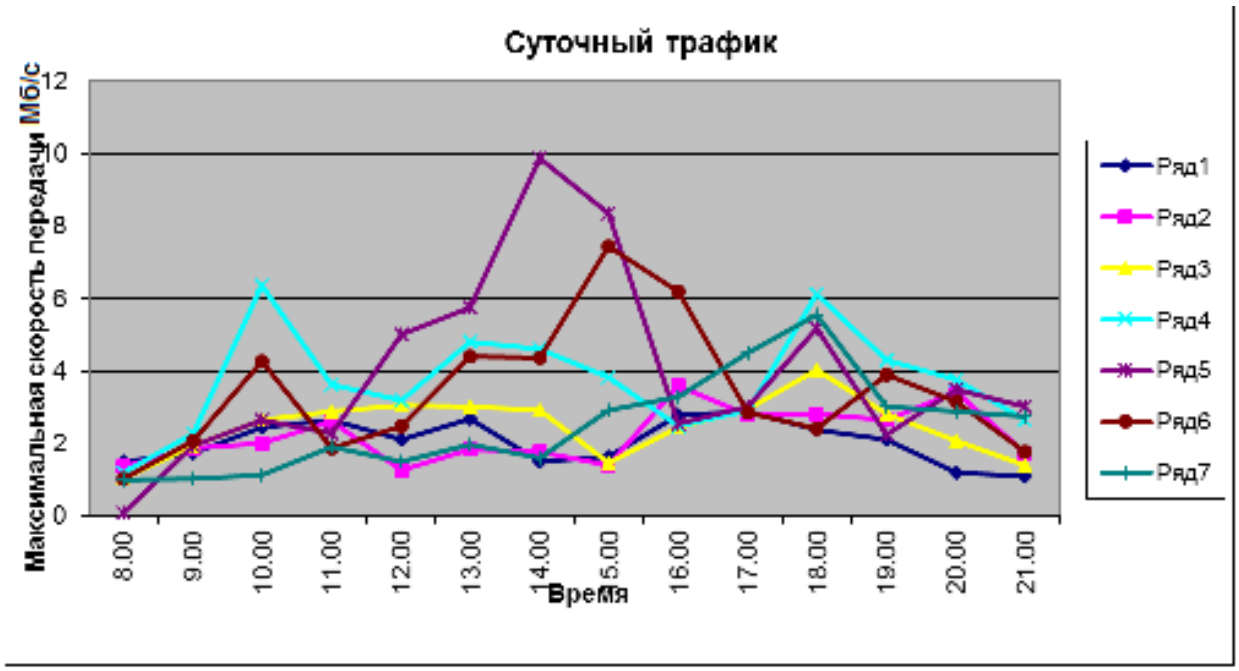

Рисунок 2.6 – Суточный трафик

По результату обработанных статистических данных, было высчитано математическое ожидание и дисперсия.

Математическое ожидание:

$$M[X] = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{2.1}$$

Дисперсия случайной величины:

$$D[X] = M\left[(X - M[X])^2\right] \tag{2.2}$$

Т а б л и ц а 2.2 – Расчет математического ожидание

Дни	Пн	Вт	Ср	Чт	Пт	Сб	Вс
M(x)	2,058	2,231	2,491	3,729	3,968	3,45	2,5075

Т а б л и ц а 2.3 – Расчет дисперсии

Дни	Пн	Вт	Ср	Чт	Пт	Сб	Вс
D(x)	0,344	0,537	0,601	1,937	6,464	2,98	1,667

3.Расчетная часть

3.1 Определение скорости передачи данных при оказании услуги доступа в сеть интернет

Согласно примечанию 7 технического регламента ТР 2007/003/BY [7] и международного стандарта IEC 60027-2 [8] единицей количества информации является бит (русское обозначение «бит», международное – «bit») и байт (русское обозначение «Б», международное – «B»). Соответствие между этими единицами отражается в равенстве:

1 Б = 8 бит.

Скорость передачи данных определяется как отношение числа бит данных (L) ко времени (t), за которое переданы эти биты, т. е.

C = L / t , бит/с. (3.1)

Согласно таблице 2 технического регламента ТР 2007/003/BY [7] множителями и приставками, используемыми для образования наименований и обозначений кратных единиц СИ, формируемыми на основе единицы «бит/с», являются следующие русские и международные приставки:

1 кбит/с = 1000 бит/с; 1 kbit/s = 1000 bit/s;
1 Мбит/с = 1000 кбит/с; 1 Mbit/s = 1000 kbit/s;
1 Гбит/с = 1000 Мбит/с; 1 Gbit/s = 1000 Mbit/s;
1 Тбит/с = 1000 Гбит/с; 1 Tbit/s = 1000 Gbit/s.

На основе единицы байт, обозначенной «Б», имеются обозначения в русских и международных приставках в десятичной системе:

1 кБ/с = 1000 Б/с = 8000 бит/с;
1kB/s = 1000 B/s = 8000 bit/s;
1 МБ/с = 1000 кБ/с = 8000000 бит/с;
1MB/s = 1000 kB/s = 8000000 bit/s.

Программисты и компьютерщики используют множители и приставки в двоичной системе счисления:

1 Кибит/s = 210 бит/s = 1024 бит/s;
1 Kibit/s = 210 bit/s = 1024 bit/s;
1 Мибит/с = 210 Кибит/с = 210 . 210 бит/с = 1048576 бит/с;
1 Mibit/s = 210Kibit/s = 1048576 bit/s.

Однако существуют единицы, которые используются на различных сайтах, но не относятся к международной системе единиц (СИ).

Неправильное обозначение единиц скорости передачи данных ведет к недостоверным результатам измерения. Например, на некоторых страницах web-сайтов приводят сокращенные обозначения: вместо единицы СИ «Кибит/с» записывают «Кбит/с», или «Кб/с», что вносит путаницу у пользователей и разработчиков сайтов. Можно, например, единицу «MB/s» принять за единицу СИ «MiB/s», опуская букву «i». Но в СИ это разные размерности. Если сравнивать их, то они имеют следующие значения:

1 MB/s = 1000000 B/s = 800000 bit/s;
1 MiB/s = 1048576 bit/s.

Сравнивая полученные значения, можно увидеть, что, принимая единицу «MB/s» за «MiB/s», значение скорости будет увеличено в 1048576/800000 = 1,31 раза по сравнению с истинным.

Поэтому рекомендуется приводить единицы измерения скорости передачи данных в соответствии с ТР 2007/003/BY [7]. Тогда можно гарантировать объективность и достоверность измерений.

Расчет скорости передачи представлен в общем виде. Задача оценки скорости передачи данных при оказании услуги доступа в сеть интернет сводится к «вычленению» из общего потока данных физического уровня числа

бит L, относящегося к потоку данных пользователя (рисунок 3.1).

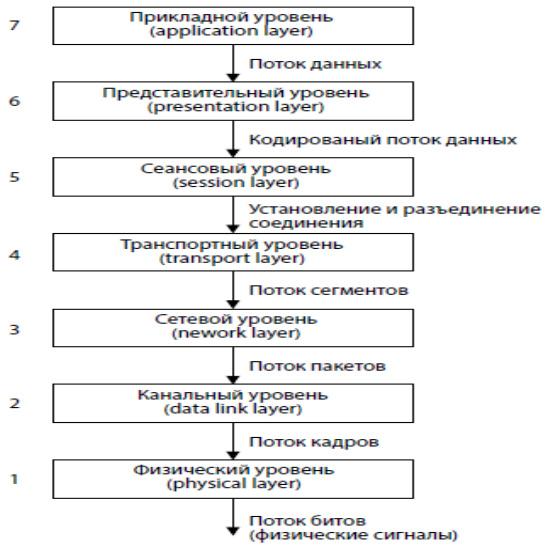

Рисунок 3.1 – Сетевая модель OSI

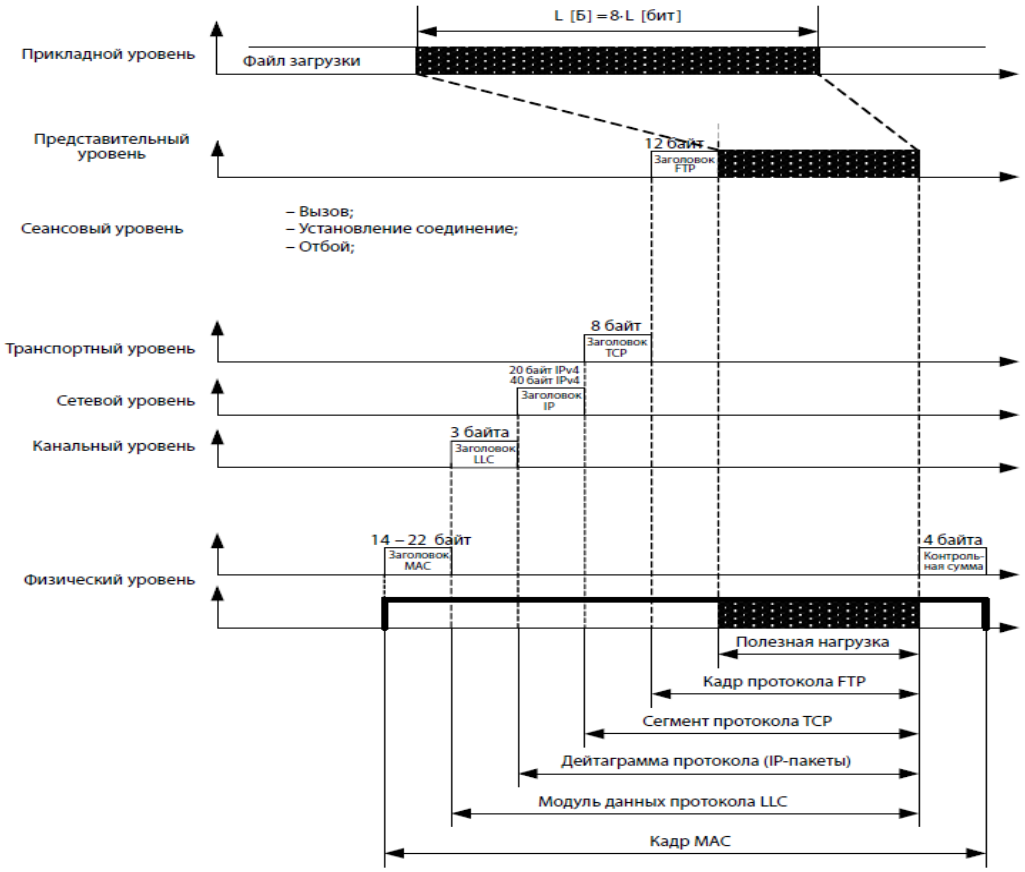

Рисунок 3.2 - Временная диаграмма, поясняющая процесс формирования потоков данных от прикладного уровня до физического

Произведем расчет исходя и имеющихся договоров на предоставление услуг от провайдеров. Средняя скорость загрузки канала в офисе казтелепорт на исходящий трафик 3мбит/сек, входящий 4мбит/сек.

1мб=1024кб=1кб=10254байт=1байт=8бит
8*1024*1024=8388608 бит

Расчет средней скорости передачи данных при исходящем трафике через канал от провайдера

1мбит=1048576 бит
1048576*3=3145728 бит

$$C_1 = \frac{314572}{3600} = 873{,}3 бит/сек$$

Расчет средней скорости передачи данных при входящем трафике через канал от провайдера

1мбит=1048576 бит
1048576*4=4194304 бит

$$C_2 = \frac{4194304}{3600} = 1165{,}08 бит/сек$$

Рассчитаем среднюю скорость передачи данных входящего и исходящего трафика по формуле

$$C_1 = \frac{C_1 + C_2}{2} = 1019{,}19 бит/сек \qquad (3.2)$$

$$C_1 = \frac{C_1 + C_2}{2} = \frac{873{,}3 + 1165{,}08}{2} = 1019{,}19 бит/сек$$

Средняя скорость загрузки канала в головном офисе составляет на исходящий трафик 1,5 мбит/сек, входящий 2,3 мбит/сек.

Расчет средней скорости передачи данных при исходящем трафике через канал от провайдера

1 мбит=1048576
1048576*1,5=1572864 бит

$$C_1 = \frac{1572864}{3600} = 436{,}9 бит/сек$$

Расчет средней скорости передачи данных при входящем трафике через канал от провайдера

1 мбит=1048576 бит

1048576*2,3=2411724,8 бит

$$C_1 = \frac{2411724,8}{3600} = 669,9 бит/сек$$

Рассчитаем среднюю скорость передачи данных входящего и исходящего трафика по формуле

$$C_{ср} = \frac{C_1 + C_2}{2}, бит/сек$$

$$C_{ср} = \frac{C_1 + C_2}{2} = \frac{436,9 + 669,9}{2} = 553,41 бит/сек$$

3.2 Расчет скорости передачи полезной нагрузки

Отличие полезной пропускной способности от полной пропускной способности зависит от длины кадра. Технология GE является развитием технологии Ethernet, поэтому формат кадра практически не отличается. Различие лишь во временных параметрах. Межкадровый интервал составит 0,096 мкс. Для его учета в расчете это время переводится на избыточную информацию. Так как скорость физической среды составляет 1 Гбит/с (т.е. Bt = 1 073 741 824 бит/с), то межкадровый интервал (IPG) будет равен:

$$IPG = 1073741824 \cdot 0,096 \cdot 10^{-6} = 13, байт.$$

При расчете количества полезных данных (MSS) следует учитывать, что в технологии GE максимальный размер пакета 1526 байт, из которых 18 байт занимает служебная информация (заголовок GE), и 8 байт – преамбула.

То есть доля пользовательской информации на информацию пакета, сформированного по технологии GE составляет:

$$\gamma_{GE} = \frac{1526 - 18 - 8}{1526 + IPG} = \frac{1500}{1539} = 0,975.$$

Также необходимо оставить место для меток MPLS (Nметк.) и заголовков TCP/IP (Nзаг.). В сетях MPLS, при использовании VPN, требуется использовать стек из 2 меток по 32 бита (Nметк = 8 байт), где верхняя будет определять маршрут следования, а нижняя будет использована выходным граничным маршрутизатором для выбора необходимого сайта VPN. Заголовки TCP/IP занимают каждый 20 байт (Nзаг.=40 байт).

Учитывая вышеописанный состав пакета, получим количество полезных данных в сети с технологиями MPLS и GE:

$$MSS = 1526 - 18 - 8 - 2 \cdot 4 - 2 \cdot 20 = 1452, байта.$$

Рассчитаем максимальный размер пакета в канале (MTU) с учетом межкадрового интервала:

$$MTU = 1526 + IPG = 1539, \text{байт}.$$

Т а б л и ц а 2 – Состав пакета на магистральном участке

Преамбула	8байт
Заголовок GE	18 байт
Стек из 2 меток	8 байт
Заголовок IP	20 байт
Заголовок TCP	20 байт
Межкадровый интервал (IPG)	13 байт

При идеальных условиях максимальная пропускная способность для пользовательских данных Сп будет равна:

$$C_{П} = \frac{MSS}{MTU} \cdot B_t = \frac{1452}{1539} \cdot 1073741824 = 966,1, \text{Мбит/с}. \quad (3.3)$$

Доля пользовательской информации на информацию пакета составляет:

$$\gamma_{MPLS-GE} = \frac{MSS}{MTU} = \frac{1452}{1539} = 0,943. \quad (3.4)$$

Следовательно, теоретически можно передать следующее количество пакетов (Р) размером 1539 байт:

$$P = \frac{B_t}{8 \cdot MTU} = \frac{1073741824}{8 \cdot 1539} = 87211, \text{пакетов/с}. \quad (3.5)$$

Время передачи одного пакета или задержка (Тп) на один шаг (1 539 байт) составит:

$$T_{П} = \frac{8 \cdot MTU}{B_t} = \frac{8 \cdot 1539}{1073741824} = 11,5, \text{мкс}. \quad (3.6)$$

При расчетах не учитывается время необходимое для получения подтверждений о доставке пакетов, не учитывается время на установление и разрыв соединения, не учитывается задержки сети GE (так как они не значительны, 0,01-0,4 мс), а так же служебный трафик (протоколы управления, маршру-

тизации и т.д.). Служебные протоколы будут учтены при расчетах пропускной способности услуг сети.

Заключение

Исследование приводит к выводу, что для обеспечения требуемого качества обслуживания в мультисервисной сети может быть достигнуто путем повышения эффективности работы сетевых устройств - маршрутизаторов, шлюзов, обеспечивая гарантированную полосу пропускания, использование магистральных сетей с высокой пропускной способностью. Тем не менее, наиболее подходящим является использование более гибких методов предоставления необходимых показателей качества обслуживания, такие как использование протокола Netflow. В то же время эффективно используется сетевым ресурсам для огромного спектра различных приложений и сервисов, в том числе наиболее важных параметров для сетевых, аудио и видео приложений реального времени.

В данной магистерской диссертации был получен полную статистическую картину движения, которая позволила деталями лечения, чтобы получить общие тенденции в скорости движения. Измерения проводились на существующем у оператора сотовой сети. Исследования показали, общую картину изменений в клиентской сети трафика в режиме реального времени в течение недели.

Перечень сокращений

QoS Quality of service – Качество обслуживания
IP Internet Protocol - Межсетевой протокол
VoIP - Voice over IP
Virtual Private Networks — Виртуальные частные сети
Class of Service - Класс обслуживания.
HDTV - Телевидения высокой четкости
OAM (Operation, Administration and Maintenance,) - обширные инструментарии администрирования
СПД - Сети передачи данных
MPLS Multiprotocol Label Switching - Многопротокольная коммутация по меткам
МСЭ - Международный союз электросвязи
MOS - Mean Opinion Score
PE(Provider Edge router) - Пограничные маршрутизаторы
CE(Customer Edge router) - Пограничным маршрутизатор клиента
VRF (VPN Routing and Forwarding, VRF) - Поступающих из сайтов клиентов, получили название таблиц
DSCP (DiffServ CodePoint) - номер класса обслуживания
NMS Network Management System – Система управления сетью
DPS Data protocol server – Сервер протокола данных
CTD Cell Transfer Dalay – время задержки переноса ячеек
MAM (Maximum Allocation Model) - Модель максимального назначения
SLA Service-level Agreement - Соглашение об уровне обслуживания
OSI (open systems interconnection basic reference model) - базовая эталонная модель взаимодействия открытых систем
CMR Cell Misinsertion Rate – скорость поступления ячеек
SNMP (Simple Network Management Protocol) - простой протокол сетевого управления
TCP (Transmission Control Protocol) - протокол управления передачей
UDP (User Datagram Protocol) — протокол пользовательских датаграмм
SECBR Severely – Errored Cell Block Ratio – коэффициент ошибочных блоков
IPTV - Internet Protocol Television
DDJ - Data Dependent Jitter
VPLS (Virtual Private LAN Service)— сервис виртуальной частной сети
PPP (Point-to-Point Protocol) — двухточечный протокол канального уровня
RJ - Random Jitter
RFC Request for Comments - Запрос комментариев
RTD Round-trip Delay - Круговая задержка
STM Synchronous Transport Module - Синхронный транспортный модуль
СМО Система массового обслуживания
FIFO First Input - First Output - первым пришел первым обслужен

LIFO Last Input - First Output - последним пришел первым обслужен
ЧНН - Час наибольшей нагрузки
MTU (maximum transmission unit) - означает максимальный размер полезного блока данных одного пакета
Maximum segment size (MSS) — максимальный размер полезного блока данных TCP сегмента.
LSP (Layered Service Provider) - многоуровневый поставщик услуг
L2TP (Layer 2 Tunnelling Protocol) — используется в продуктах компаний

Список литературы

1. Gartner, "Прогноз: Общедоступные облачные сервисы, всемирные и региональные, отрасли промышленности, 2010-2015 гг., обновление 2011 г." (29 июня 2011 г.)
2. McDysan. QoS and Traffic Management in IP and ATM Networks // McGraw-Hill.2000.
3. Телемультимедиа № 4 (32) сентябрь 2005
4. IEEE 802. lag. Connectivity Fault Management (CFM). Стандарт описывает протокол мониторинга состояния соединений, в какой-то степени это аналог протокола BFD.ITU-T Y.1731. Стандарт комитета ITU-T воспроизводит функции стандарта IEEE 802.lag и расширяет их за счет группы функций мониторинга параметров QoS.IEEE 802.3ah. Стандарт тестирования физического соединения Ethernet. MEF E-LMI. Интерфейс локального управления Ethernet.

5 C. Fraleigh, S. Moon, B.Lyles, C. Cotton, M. Khan, D. Moll, R. Rockell, T.Seely and C. Diot. Packet-level traffic measurements from the Sprint IP backbone. IEEE Network, 2003.

6 Маньков В.А., Пилюгин В.А. Особенности работы TCP в мультисервисных сетях ADSL доступа//Труды конференции «Телекоммуникационные и вычислительные системы» –
М.: МТУСИ, 2009.-С.15

7. Олвейн, Вивек. Структура и реализация современной технологии MPLS. : Пер. с англ. – М. : Издательский дом «Вильямс», 2004. – 480 с

9 Е.А. Кучерявый. Управление трафиком и качество обслуживания в сети
Интернет//СПб, Наука и Техника. 2004.

10 Р. Кох, ГГ. Яновский. Эволюция и конвергенция в электросвязи//М., Радио и связь. 2001.

11 МСЭ-Т Recommendation Y.1540. IP Packet Transfer and Availability Performance Parameters//December 2002.

12 МСЭ-Т Recommendation Y.1541. Network Performance Objectives for IP-Based Services//May 2002.

13. Advanced MPLS Design and Implementation. Структура и реализация современной технологии MPLS. Руководство Cisco

14. A. Malis, RFC-2917, *A Core MPLS IP VPN Architecture*, September 2000.

15. Андрей Вишняков. Сигнализация VPLS: LDP или BGP [Электронный ресурс].

16. Семенов Ю.А. (ГНЦ ИТЭФ). Сервис виртуальной локальной сети VPLS (RFC-4761). [Электронный ресурс]. – Режим доступа:http://book.itep.ru/4/4/rfc4761.htm

17. Базовые сервисы технологии MPLS. [Электронный ресурс]. – Режим доступа: http://nag.ru/articles/reviews/15448/bazovye-servisy-tehnologii-mpls.html

18. Дуглас Э. Камер - Сети TCP/IP. Принципы, протоколы и структура. Том 1. Четвёртое Издание. - 2003.

19. Wendell Odom - CISCO Официальные руководства по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 640-822, ICND2 640-816

Приложение А

Измерение трафика по программе Netflow

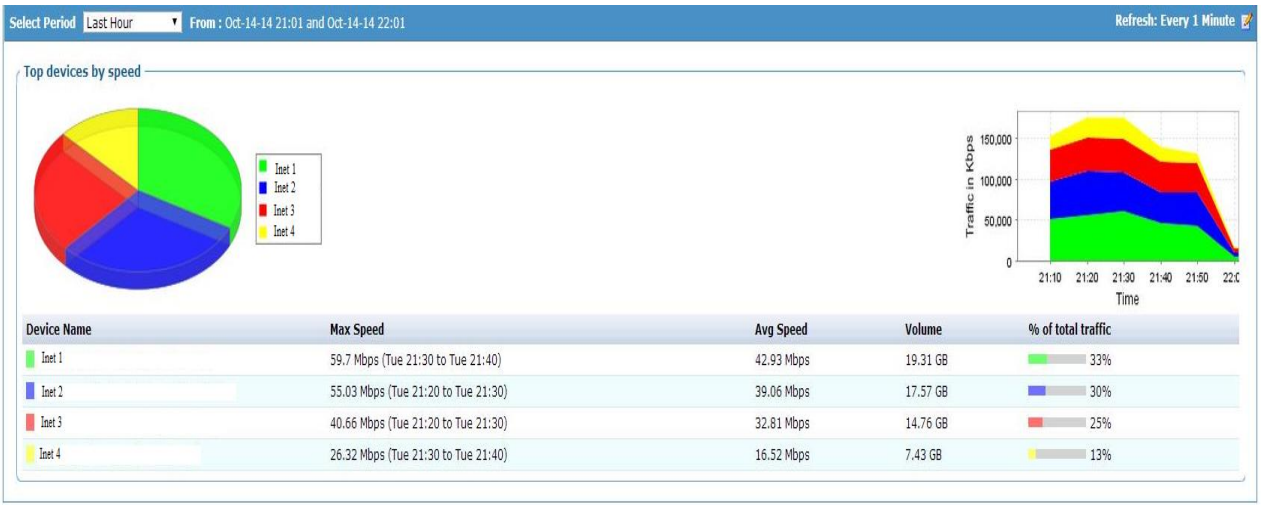

Рисунок А1 – График измерения

Приложение Б
Листинг программы MathCad14

Нахождение времени отклика сети в программе MathCad14

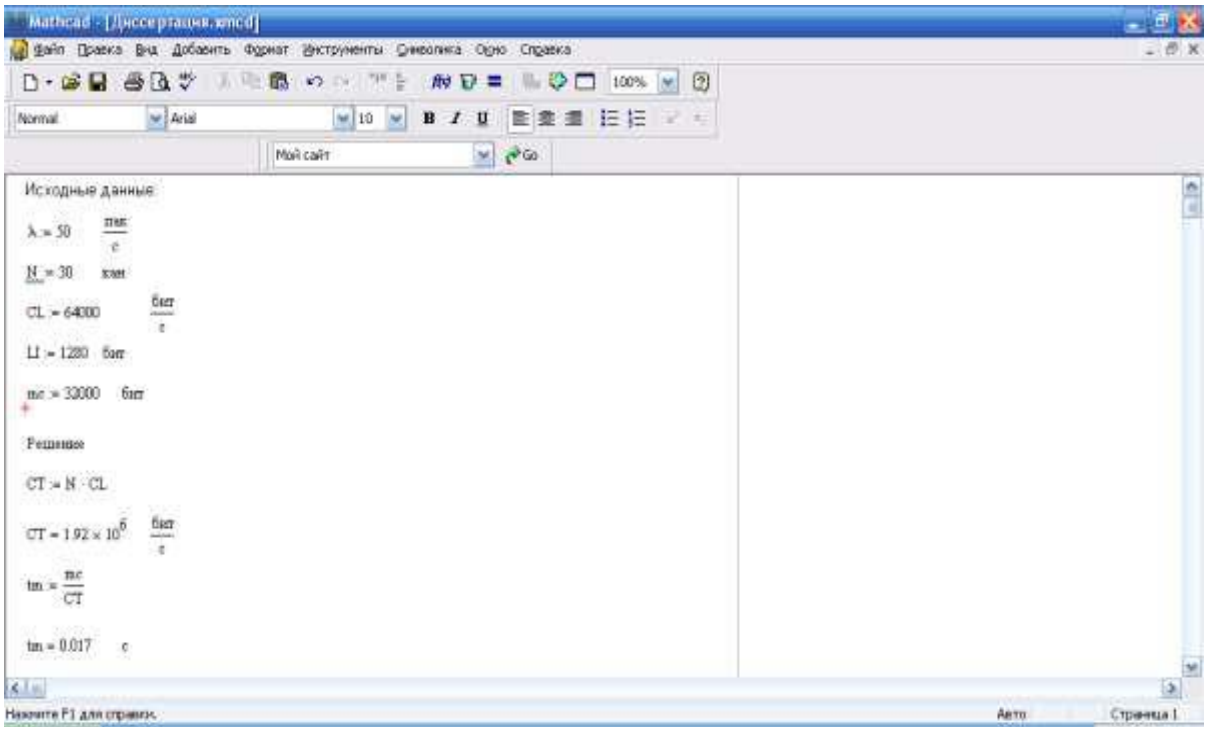

Рисунок А1 – Нахождение tm

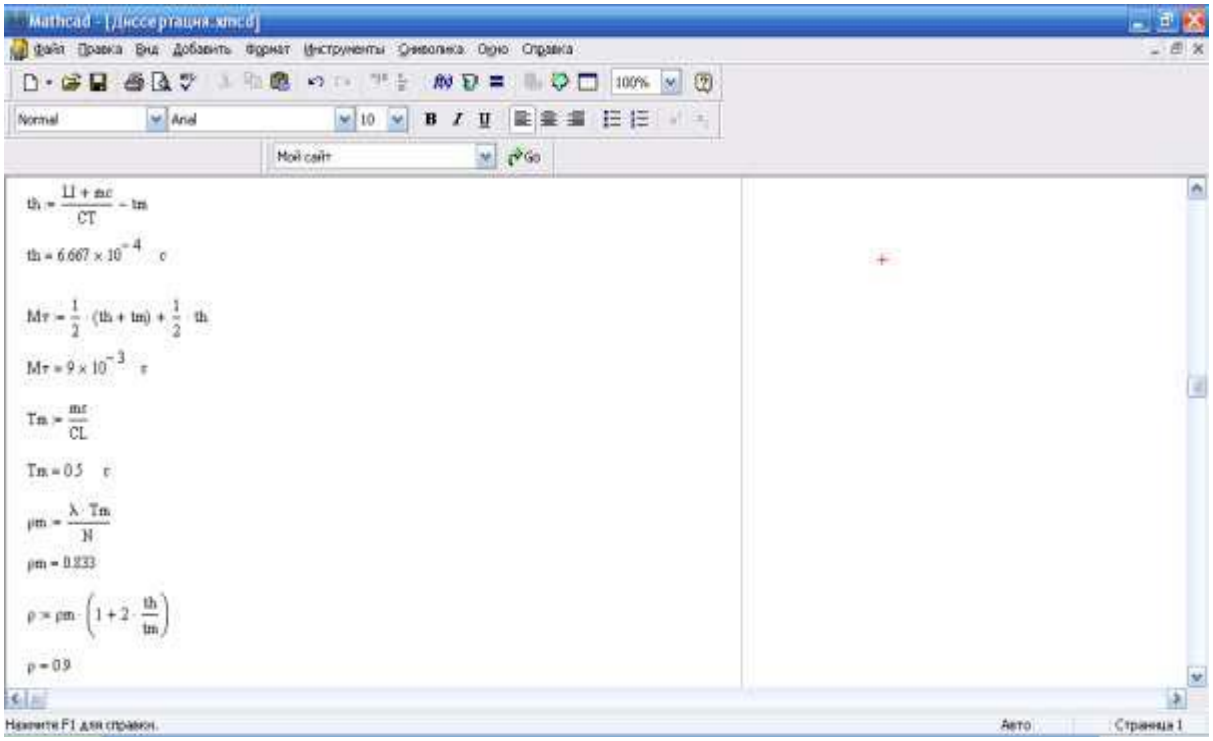

Рисунок А2 – Нахождение p

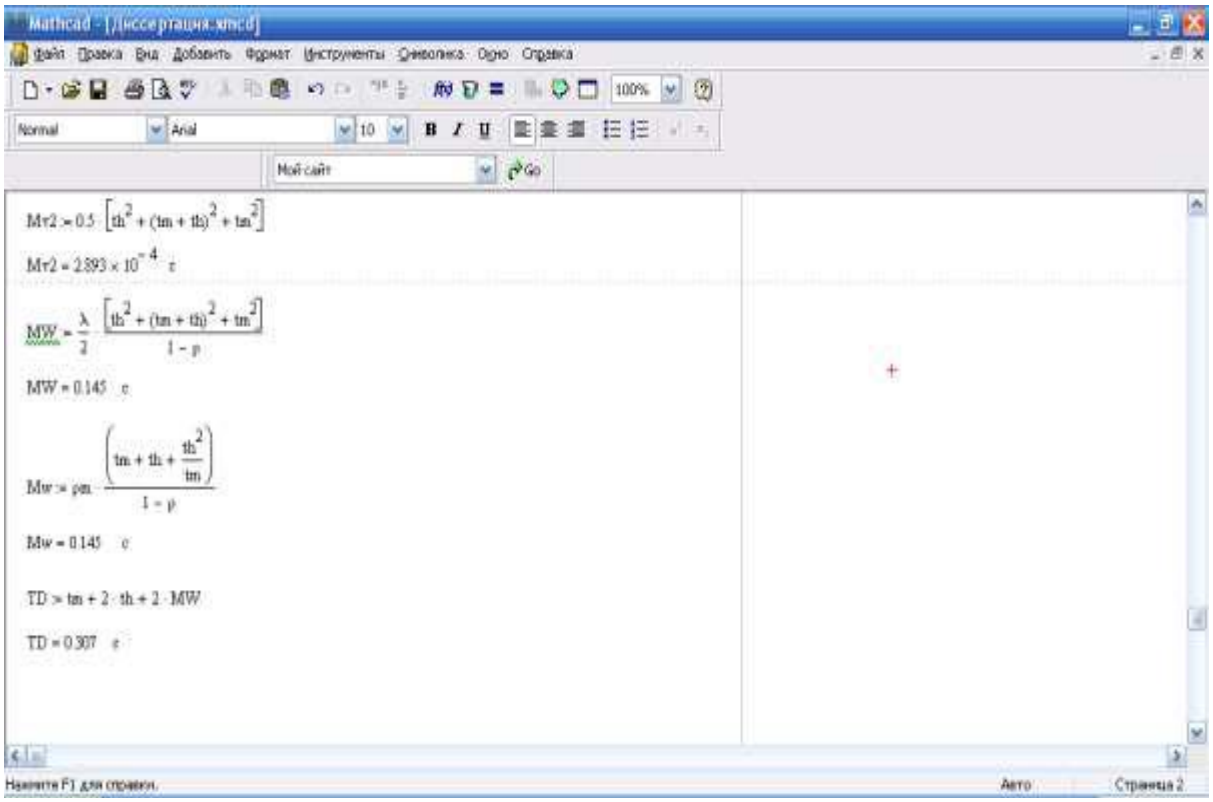

Рисунок А3 – Нахождение времени отклика