Министерство по развитию информационных технологий телекоммуникации Республики Узбекистан

САМАРКАНДСКИЙ ФИЛИАЛ ТАШКЕНТСКОГО УНИВЕРСИТЕТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Факультет “Телекоммуникационных технологий и профессионального образования”

Кафедра “Телекоммуникационный инжиниринг”

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

для получения академической степени бакалавра по направлению

5311300- “Телекомуникация”

Тема: **ИССЛЕДОВАНИЕ ВЛИЯНИЯ МЕТОДОВ МАРШРУТИЗАЦИИ НА КАЧЕСТВА ОБСЛУЖИВАНИЯ В МУЛТИСЕРВИСНЫХ СЕТЯХ**

Выпускная квалификационная работа

Рекомендовано к защите решением

Кафедры «Телекоммуникационный

инжиниринг» протоколом №__ от

__мая 2015 г.

Заведующий кафедрой

_____доц.Жуманов Х.А

Выполнил: студент 4-го курса

_____Салохитдинов А

Научный руководитель:

_____Рахматов Комил

Самарканд-2015

Содержание

Введение

Правительство Республики Узбекистан уделяет большое внимание развитию информационно-коммуникационных технологий. 18 января состоялось заседание Кабинета Министров Республики Узбекистан, посвященное итогам социально-экономического развития республики в 2012 году и основным приоритетам экономической программы на 2013 год.

В своем докладе Президент Республики Узбекистан Ислам Каримов обозначил задачи по ускоренной реализации мер и проектов в сфере информационно-коммуникационных и телекоммуникационных технологий.

В частности было сказано: «Все большее значение приобретает ускоренная реализация мер и проектов в сфере информационно-коммуникационных и телекоммуникационных технологий. Мы должны отдавать себе отчет, что без кардинального, я бы сказал взрывного продвижения по пути широкого внедрения во все сферы экономики, в нашу повседневную жизнь современных информационно-коммуникационных систем трудно видеть перспективу. Нам необходимо в кратчайшее время не только устранить имеющее место отставание по многим видам оказания информационных услуг, но и выйти в разряд передовых стран с высоким уровнем внедрения информационно-коммуникационных технологий.

Качество обслуживания Quality of Service (QoS) активно исследуется и стандартизируется на всем протяжении истории развития отрасли телекоммуникаций. Огромный вклад в развитие и совершенствование различных принципов качества обслуживания внес Международный союз электросвязи (МСЭ). МСЭ разработал требования и нормы к различным показателям QoS, провел большую работу по стандартизации многочисленных сетевых механизмов, которые обеспечивают необходимые показатели QoS, а также формулируют основополагающие

понятия и определения. В современных телекоммуникационных сетях постоянно меняется характер и объем передаваемого трафика и, соответственно, предоставляемых инфокоммуникационных услуг. Важнейшую роль в таком процессе играют услуги передачи данных, видео, голоса: такие мультимедийные услуги, как IP-телевидение, предоставление видео по запросу, IP-телефония, видео- и аудио-конференции и др. Ясно, что для предоставления перечисленных услуг необходимо соблюдать ряд требований к параметрам качества обслуживания, таких как вероятность потери пакетов, задержка передачи, джиттер и др. Зачастую незнание статистических характеристик трафика может привести к неэффективному использованию сетевых ресурсов операторов и, следовательно, к низкому качеству предоставляемой услуги или к низкому количеству обслуживаемых абонентов. На сегодняшний день в современных телекоммуникациях одной из наиболее актуальных задач является передача трафика с соблюдением ряда требований по качеству обслуживания. Неэффективное использование ресурсов сети, большое количество абонентов, а также жесткие требования к параметрам качества обслуживания могут стать причинами снижения качества предоставляемых услуг в мульти сервисных сетях передачи данных (СПД). Несмотря на то, что по данной тематике существует не одна публикация , совмещение макро-характеристик (объемы информации по приложениям, распределение потоков и т.д.) с микро-характеристиками (распределение длин пакетов, их потерь и др.), практически, никогда не выполняется для одной сети в конкретный отрезок времени. В связи с этим, возникает задача получения полной статистической картины трафика, которая позволила бы за счет обработки детальной информации получить как общие тренды изменения трафика, так и уточнить микро-характеристики потоков.

Актуальность работы. Стремительное развитие современных систем связи, построенных на принципах коммутации пакетов, ставит перед разработчиками телекоммуникационных систем ряд задач. На передний план выходят задачи обеспечения качества услуг, предоставляемых пользователям сети, а также обеспечения высокой степени надежности функционирования современных мультисервисных сетей связи.

Цель работы: Иследование методов маршрутизации для мультисервисных сетей связи, функционирующих в экстремальных условиях, при прохождении по ним самоподобного трафика. Оценка

статистических параметров системы для улучшения качества предоставляемых услуг в мультисервисных СПД.

ГЛАВА 1. Исследование качества обслуживания в мультисервисных СПД

1.1 Состояние проблемы, цель и задачи.

Сегодня активно развиваются различные услуги передачи данных: IP-телефония, IPTV (Internet Protocol Television), видео по запросу, аудио- и видео – конференции, VoIP (Voice over IP) и др. За последнее время объём IP – трафика во всем мире резко увеличится, а большую часть этого объема занимают сервисы реального времени [18]. Впоследствии это приводит к тому, что пользователям услуг требуется, удовлетворяющий требованиям QoS предоставляемых услуг, канал связи. В связи с тем, что различные услуги используют одни и те же каналы транспортной сети и при этом каждая услуга выдвигает к каналу связи свои требования, то возникает задача распределения ресурса канала связи между различными сервисами сети. Зачастую однократное распределение ресурса канала, приводит к неэффективному использованию канала связи, следовательно, распределение ресурсов в сети должно происходить постоянно, периодически, в зависимости от интенсивности использования различных услуг. В современных 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 аудио-конференции и др. Ясно, что для предоставления перечисленных услуг необходимо соблюдать ряд требований к параметрам качества обслуживания, таких как вероятность потери пакетов, задержка передачи, джиттер и др. Зачастую 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 с соблюдением требований по качеству обслуживания является одной из наиболее актуальных задач в современных телекоммуникациях. Неэффективное использование ресурсов сети, большое число абонентов и жесткие требования к параметрам QoS могут становиться причинами падения качества предоставляемых услуг в мультисервисных сетях передачи данных (СПД). Несмотря на большое число публикаций по данной тематике, совмещение макро-характеристик (объемы информации по приложениям, распределение потоков и т.д.) с микро-характеристиками (распределение длин пакетов, их потерь и др.), практически, никогда не выполняется для одной сети в конкретный отрезок времени. В связи с этим, возникает задача получения полной статистической картины трафика, которая позволила бы за счет обработки детальной информации получить как общие тренды изменения трафика, так и уточнить микро-характеристики потоков. Полученные результаты могут быть использованы для дальнейшей подстройки параметров сети под существующие тенденции. 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 СПД

Мультисервисной сетью называют сеть, в которой клиент может получать несколькоразличных услуг по одной абонентской линии (набор различных сервисов): интернет

– доступ до всемирной сети, Web – страницы, FTP (передача файлов), электронная почта и др.;

Тип сервиса	Параметры QoS				
	t_c, с	B, Мбит/с	$p^{(rj)}$	dT, мс	Dj, мс
IP-телефония (голос)	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	-

VPN— виртуальная частная сеть, что позволяет строить сети, или защищенные каналы через Интернет (или арендованные каналы сторонних организаций);
VoIP – IP-телефония, телефонная связь на основе пакетной коммутации;
IPTV – передача видео изображения по сети IP.
Каждый из этих сервисов выдвигает свои требования, для полноценного функционирования, к каналу связи (см. таблицу 1).

Т а б л и ц а 1 – Требования к QoS для разных сервисов

В таблице 1 приняты следующие обозначения:
tc – время установления соединения, с;
p(rj) – вероятность разрыва соединения;
dT – задержка, мс;
Dj – джитер, мс;
B – полоса пропускания канала.

Поскольку физический канал один, а требования услуг различны, то распределение канального ресурса между услугами является важной функцией для обеспечения требования QoS услуг. Среди стандартов, посвященных качеству обслуживания в электросвязи, одно из центральных мест занимает Рекомендация МСЭ E.800. В ней качество обслуживания определяется как «суммарный эффект рабочих характеристик обслуживания, который определяет степень удовлетворенности пользователя данной службой». Расширяя концепцию качества обслуживания, отвечающую Рекомендации E.800, Рекомендация МСЭ G.1000 разделяет рабочие характеристики обслуживания на функциональные компоненты и связывает их с сетевыми характеристиками, определенными в ряде рекомендаций МСЭ – таких как I.350, Y.1540 и Y.1541 [16]. В дополнение к Рекомендации МСЭ G.1000, определяющей структуру связей между рабочими характеристиками (производительностью, надежностью, потерями, задержкой и др.) и

характеристиками сети, Рекомендация МСЭ G.1010 содержит спецификации требований со стороны приложений, ориентированных на конечного пользователя. Исторически, первые системы оценок и механизмов поддержки качества обслуживания были разработаны для традиционных видов электросвязи – телеграфии и телефонии. Понятно, что сегодня при широком применении сетей передачи данных, быстром внедрении широкополосных технологий и замене телеграмм на сообщения электронной почты параметры качества обслуживания и механизмы их поддержки в телеграфных сетях становятся все менее актуальными. В классических IP-сетях применяется метод доставки, который полностью исключает как физическую, так и виртуальную форму организации соединений. Данный метод основан на рассылке пакетов-дейтаграмм. А качество доставки пакетов в традиционных IP-сетях базируется на принципе «наилучшей попытки» (Best effort). Данная концепция предполагает, что пользователи разделяют доступные сетевые ресурсы, трафик передается с максимально возможной в данных условиях загрузки сети скоростью, но при этом обеспечение любого предварительно определенного уровня качества обслуживания не гарантируется. Ясно, что такой подход к обслуживанию означает, что нет гарантии в доставке пакетов в правильном порядке, нет различия между разными видами трафика, и что он будет доставлен в требуемое время или вообще будет доставлен, и т. д.

Принцип «наилучшей попытки» был достаточно эффективен для приложений, где можно данные передавать не в режиме реального времени (передача файлов, электронная почта). Кроме того, с учетом переизбытка сетевых ресурсов в транспортных сетях, построенных на базе волоконно-оптических линий связи, принцип «наилучшей попытки» в определенной степени позволяет обеспечить сегодня требования телефонии (голос поверх IP) и других приложений реального времени. Однако, как только возникает недостаток сетевых ресурсов, который ведет к росту задержек пакетов и увеличению вероятности их потерь, для приложений реального времени уже не могут быть обеспечены необходимые показатели качества обслуживания. Во-первых, это объясняется основным принципом функционирования сетей IP – передачей данных в дейтаграммном режиме, т. е. без управления и без установления соединения.

Во-вторых, с появлением новых приложений, в частности реального времени (интерактивная передача речи, видеоконференции и видеотелефония и др.), одним из наиболее сложных становится вопрос о

гарантированном качестве обслуживания в сетях. Это объясняет, почему качество обслуживания в сетях IP остается предметом постоянного внимания МСЭ, ETSI, IETF и других организаций стандартизации в электросвязи. В рамках работ МСЭ по стандартизации качества обслуживания в IP-сетях предполагаются следующие этапы решения задачи обеспечения качества обслуживания QoS для сетей, построенных на базе протоколов IP: создание согласованного общего набора рабочих характеристик IP-сетей и норм ля него; внедрение сетевых механизмов, которые будут обеспечивать заданные показатели качества обслуживания в конфигурации «терминал-терминал»; вложение нормированных значений показателей качества обслуживания в протоколы сигнализации; разработкаархитектуры сетевых механизмов поддержки. Разделение ресурсов и процессы управления трафиком необходимо скоординировать в условиях наличия большого числа разнообразных приложений, которые существенно отличаются требованиями к рабочим характеристикам сети (см. таблицу 2).

Т а б л и ц а 2 – Чувствительность различных приложений к сетевым характеристикам

Тип трафика	Уровень чувствительности к сетевым характеристикам			
	Полоса пропускания	Потери	Задержка	Джиттер
Голос	Очень низкий	Средний	Высокий	Высокий
Электронная почта	Низкий	Высокий	Низкий	Низкий
Telnet	Низкий	Высокий	Средний	Низкий
Поиск в сети «от случая к случаю»	Низкий	Средний	Средний	Низкий
Транзакции	Низкий	Высокий	Высокий	Низкий
Видеоконференция	Высокий	Средний	Высокий	Высокий
Электронная коммерция	Низкий	Высокий	Высокий	Низкий
Постоянный поиск в сети	Средний	Высокий	Высокий	Низкий
Пересылка файлов	Высокий	Средний	Низкий	Низкий
Мультикастинг	Высокий	Высокий	Высокий	Высокий

В 2008 г. МСЭ-Т опубликовано два международных стандарта, которые отвечают первому из перечисленных этапов. Рекомендация МСЭ Y.1540 [10] описывает стандартные сетевые характеристики для передачи пакетов в сетях IP. Рекомендация МСЭ Y.1541 определяет нормы для параметров, определенных в Y.1540, между двумя граничными сетевыми интерфейсами – точками подключения оконечных терминалов. Также в этой

рекомендации специфицированы шесть классов качества обслуживания в зависимости от используемых приложений.

Эти рекомендации важны для всех участников телекоммуникационного сценария – операторов и провайдеров, производителей оборудования и конечных пользователей. Сетевые операторы и провайдеры будут использовать их при планировании, развертывании и оценке сетей IP в соответствии с требованиями конечных пользователей к качеству обслуживания. Производители будут опираться на эти рекомендации при создании оборудования, которое должно отвечать спецификациям сетевых провайдеров. аконец, конечные пользователи (в первую очередь, корпоративные) смогут применить рекомендации Y.1540 и Y.1541 при оценке характеристик реально функционирующих IP-сетей с позиций соответствия этих характеристик требованиям потребителей. Ниже представлены некоторые детали рекомендаций Y.1540 и Y.1541, касающиеся основных сетевых характеристик, связанных с обеспечением QoS в сетях IP.

Рекомендация МСЭ Y.1540 в Рекомендации Y.1540 рассматриваются следующие как наиболее важные по степени их влияния на сквозное качество обслуживания (от источника до получателя),

сетевые характеристики:

-производительность

-сети;

-надежность

-сети/сетевых элементов;

-задержка;

-потери

-пакетов;

-вариация

-задержки (джиттер).

Производительность сети (или иначе скорость передачи данных) пользователя – это эффективная скорость передачи, которая измеряется в битах в секунду. Необходимо отметить, что значение данного параметра не совпадает с максимальной пропускной способностью сети, которую часто ошибочно называют полосой пропускания. Минимальное значение производительности сети обычно гарантирует провайдер услуг, который, в свою очередь, должен иметь соответствующие гарантии от сетевого провайдера. Однако, в рекомендации Y.1540 не приведены нормативные характеристики производительности сети для различных приложений. В

рекомендации Y.1541 говорится, что параметры, связанные с эффективной скоростью передачи, могут определяться через дескриптор трафика IP-сети, который описан в Рекомендации МСЭ Y.1221. Обычно пользователи ожидают высокий уровень надежности от систем связи. Ее можно определить через несколько параметров, из которых чаще всего используется коэффициент готовности. Данный параметр вычисляется как отношение времени простоя объекта к суммарному времени наблюдения объекта, включающему время простоя и время между отказами. В идеале коэффициент готовности должен быть равен 1, что говорит о 100% готовности сети. На практике коэффициент готовности оценивается числом «девяток». К примеру, «три девятки» означают, что коэффициент готовности составляет 0,999, что соответствует 9 часам времени простоя (недоступности) сети в год. Готовность сети телефонии общего пользования оценивается величиной «пять девяток», что означает 5,5 мин. простоя в год. Нельзя не отметить, что обеспечение коэффициента готовности «пять девяток» в IP- сетях, построенных на традиционном оборудовании данных (маршрутизаторы, серверы), является довольно серьезной проблемой. А причина этого состоит в следующем: обработка информационных потоков в IP-сетях в значительной части базируется на программном обеспечении (а не на аппаратном, как это имеет место в СТОП). К тому же, статистика отказов сетевого оборудования показывает, что надежность программного обеспечения примерно в два раза ниже надежности аппаратного обеспечения. В таблице 3 приведены данные по времени простоя для различного количества «девяток».

Коэффициент готовности	Время простоя
0,99	3,7 дней в год
0,999	9 часов в год
0,9999	53 минуты в год
0,99999	5,5 минут в год
0,99999999	30 секунд в год

Т а б л и ц а 3 – Коэффициенты готовности и соответствующие значения времени простоя оборудования. В общем, сеанс связи состоит из трех основных фаз – установления соединения, передачи информации и разъединения соединения. В Рекомендации Y.1540 из трех фаз сеанса связи описывается только вторая – фаза доставки IP пакетов. Такого рода подход отражает природу IP-сетей, не ориентированных на установление соединений.

Рекомендация МСЭ Y.1541

В данной Рекомендации определены численные значения специфицированных параметров. Они должны выполняться в IP-сетях на международных трактах, которые соединяют терминалы пользователей. Существующие нормы на эти параметры разделяются по различным классам QoS, которые определяются в зависимости от применяемых для обеспечения гарантированного качества обслуживания сетевых механизмов и приложений, В таблице 4 представлены нормы на сетевые характеристики IP-сетей.

Т а б л и ц а 4 – Нормы для характеристик сетей IP с распределением по классам качества обслуживания

Сетевые характеристики	Классы QoS					
	0	1	2	3	4	5
Вариация задержки пакета IP, IPDV	50 мс	50 мс	Н	Н	Н	Н
Коэффициент ошибок пакетов IP, IPER	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	Н
Задержка доставки пакета IP, IPTD	100 мс	400 мс	100 мс	400 мс	1 с	Н
Коэффициент потери пакетов IP, IPLR	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	Н

где Н – не нормировано.

Приведенные в таблице, значения параметров представляют собой верхние границы для средних задержек, потерь, ошибок пакетов и джиттера. Здесь представлены спецификации набора параметров, которые связаны с измерением реальных значений характеристик сети – длины тестовых пакетов, периода наблюдений, числа пакетов и т. д. Например, при оценке качества передачи пакетов речи в IP-телефонии минимальный интервал наблюдения должен быть около 1 – 20 с при скорости передачи 50 пакетов в секунду. Согласно Рекомендации интервал измерений для потерь, задержек и джиттера должен быть не менее 60 с. Рекомендация Y.1541 устанавливает соответствие между классами QoS и приложениями:

1) класс 0 – приложения реального времени, чувствительные к джиттеру, для которых характерен высокий уровень интерактивности (видеоконференции, VoIP);

2) класс 1 – приложения реального времени, чувствительные к джиттеру, интерактивные (видеоконференции, VoIP);

3) класс 2 – транзакции данных, для которых характерен высокий уровень интерактивности (к примеру, сигнализация);

4) класс 3 – транзакции данных, интерактивные;
5) класс 4 – приложения, для которых допустим низкий уровень потерь (потоковое видео, массивы данных, короткие транзакции);
6) класс 5 – традиционные применения IP-сетей.

Кроме определения спецификации норм для сетевых параметров ИК 13 МСЭ-Т провел также работы по идентификации и стандартизации сетевых механизмов, обеспечивающих QoS в IP-ориентированных сетях. В 2004 г. была принята Рекомендация МСЭ Y.1291, которая описывает архитектурную модель для поддержки QoS в сетях с пакетной передачей. Сетевые механизмы должны осуществляться в комбинации с характеристиками качества обслуживания, которые формируются в зависимости от приложений. При разработке архитектуры сетевых механизмов учитывалось, что различные услуги будут иметь разные требования к сетевым характеристикам. Допустим, для телемедицины более существенную роль играет точность доставки, нежели джиттер или суммарная средняя задержка, в то время как для IP-телефонии джиттер и задержка должны быть минимальны и являются ключевыми характеристиками.

1.3 Оценка качества предоставления услуг в мультисервисных сетях передачи данных

На сегодняшний день тенденция развития сетей передачи данных представлена конвергенцией голоса, данных, видео, а также учетно-контрольных потоков под единой средой передачи данных. Необходимо четко отделять различные классы потоков трафика друг от друга. Кроме того, делать это необходимо с учетом постоянно изменяющегося характера трафика, его периодичности, «часов пик» и т.д. Необходим комплекс инструментов, обеспечивающих выполнение вспомогательных задач, возникающих в процессе управления мультисервисными СПД. К этим задачам можно отнести:
-сбори предоставление оперативной информации о состоянии компонентов сети, нагрузке на компоненты и прогноз на загрузку;
-мониторинг и управление информационными потоками мультисервисной СПД.

Анализ трафика, передаваемого в СПД, предоставляет возможность решения этих задач. Кроме того, учет и анализ трафика позволяет осуществлять управление качеством предоставления услуг. Основной целью обеспечения высокого качества обслуживания конвергентной сети является критичность голосового и видеотрафика к любым задержкам и требовательность к выделенной полосе пропускания. После выявления требований к какому-либо сегменту сети (количество одновременных вызовов, сетевые приложения, время отклика) необходимо проанализировать возможности оборудования и существующую ситуацию. В ряде случаев это приходится делать уже на существующем сегменте сети. Для выявления основных тенденций трафика, его пиков, пиков конкретных приложений, возможности взаимодействия конкретных типов трафика с различными политиками и типами QoS, необходимо произвести следующие действия:

1) Найти суточные, часовые и иные циклы периодичности в поведении трафика;
2) Снять статистические характеристики трафика по типам протоколов;
3) Проанализировать распределение трафика по приложениям;
4) Провести анализ потоков данных по длине пакетов передаваемой информации.

Модель оценки качества обслуживания в мультисервисных сетях передачи данных, позволяющая описать агрегированный поток информации, потери и задержки при оценке качества различных услуг в сетях передачи данных (СПД) требования к передаче данных зависят от услуги и приложения, ее реализующего. Например, когда в одной сети передаются эластичные данные и неэластичные, их трафик не может обрабатываться одинаково. Тому есть несколько причин:

-пакеты эластичных и неэластичных данных имеют разную длину;
-пакеты эластичных и неэластичных данных передаются с разными скоростями;
-использование различных механизмов и протоколов при обработке в узлах сети и при доставке получателю;
-различная чувствительность к задержкам и потерям.

Поскольку обработка трафика различных типов отличается, методы оценки качества обработки трафика также будут отличаться. Приложения, генерируемые и обрабатывающие трафик, требуют определенных гарантий в доставке данных. Эти гарантии по сложности их обеспечения разделяют

на классы. Задача оценки качества обслуживания в доставке данных определенного класса так или иначе решалась. Однако в мультисервисной сети различные типы трафика оказывают влияние друг на друга, что делает оценку качества обслуживания сети со смешанным трафиком актуальной задачей. Структура трафика в мультисервисных СПД если рассмотреть структуру трафика в мультисервисной сети, то можно выделить три основных типа трафика. Трафик мультисервисной сети можно представить потоками трех основных типов.

Первый тип – это так называемый эластичный трафик (data), т.е. независимый от пропускной способности участка сети. Однако эластичный трафик чувствителен к потерям, но практически не чувствителен к задержкам (до нескольких минут в зависимости от приложения). В качестве транспортного протокола использует TCP. Примером служит трафик таких сервисов, как e-mail, пересылка файлов, web-приложения и т.п.

Второй тип – потоковый трафик (stream). Потоковый трафик можно получить при Интернет-вещании, аудио или видео по требованию. Его отличает допуск достаточно больших задержек и потерь. На приеме обычно используется буфер, позволяющий сглаживать неравномерность задержки путем внесения дополнительной задержки путем внесения дополнительной задержки буфера. Для передачи этого типа трафика вполне возможно использование в качестве транспортных протоколов как UDP, так и TCP.

Третий тип – трафик реального времени (real time). Характеризуется высокой чувствительностью к задержкам и относительно малой чувствительностью к потерям. Это может быть трафик IP-телефонии и видеоконференцсвязи, трафик, передаваемый от систем видеонаблюдения. В зависимости от класса обслуживания оговариваются их конкретные значения потерь и задержек. Трафик транзакций представляет собой сигналы управления различными объектами и процессами, в том числе игры on-line. Такой тип трафика предъявляет высокие требования к задержке, т.е. относится к верхчувствительному к задержкам типу, характеризуется высокой чувствительностью к потерям и переменной битовой скоростью, т.е. отличается высокой степенью непредсказуемости. Трафик реального времени, порожденный такими процессами, как речь или видео, отличается большей устойчивостью к потерям (т.е. относится к малочувствительным к задержкам типам приложений), является

изохронным. Это означает, что он имеет порог чувствительности к задержкам, при превышении которого функциональность приложения резко падает, что характеризует высокая степень предсказуемости порождаемого трафика. Таким образом, в мультисервисной сети можем наблюдать различные комбинации этих трех видов трафика.

ГЛАВА 2. Факторы, влияющие на качество неэластичного трафика в мульти-сервисных сетях

Для удобства оценки влияния факторов их принято делить на две группы: факторы, определяемые влиянием оконечного устройства, и факторы, определяемые влиянием сети.

а) Влияние оконечного устройства.

Под оконечными подразумеваются устройства, в состав которых входит реализация кодека. Например, оконечные устройства IP-телефонии могут быть представлены специализированными ПО, IP-телефоном или шлюзом IP-телефонии. В случае использования ПО или IP-телефона, кодек реализуется непосредственно у абонента, а при использовании шлюза IP-телефонии соединение между шлюзом и абонентом происходит по протоколу, и на этом участке проблема обеспечения качества давно и успешно решена. Кодек может быть представлен как совокупность кодирующего (анализатор) и декодирующего (синтезатор) устройства. В современных системах используются кодеки, обеспечивающие компрессию речи и работающие на основе линейного предсказания. б) Влияние сети рассмотрим в терминах показателей качества QoS:

1) Задержка доставки пакета есть время переноса пакета от источника к получателю. Это время задержки зависит от доступных сетевых ресурсов во время доставки и интенсивности трафика в сети. Речь является трафиком, чувствительным к задержке, однако большинство приложений данных более устойчиво к задержке. В том случае, если задержка доставки речевого пакета больше определенного значения, этот пакет отбрасывается, что приводит к дополнительным потерям. Так, например, в результате исследований качества речевого сигнала было установлено, что человеческое ухо начинает чувствовать задержки передачи речи, больше 150 мс, и ощущает дискомфорт, если задержка составляет более 250 мс. Задержки выше 150 мс осложняют телефонный разговор, а при задержке равной 300 мс разговор начинает распадаться на такие фрагменты, которые невозможно воспринять как слитную речь. Джиттер (вариация задержки доставки пакета) определяется рядом причин, включая такие, как: вариации

времени обработки пакетов при нарушении последовательности их на передаче; вариации длин очередей в узлах сети; наличие в сети трфика данных, конкирирующего с неэластичным трафиком при доступе к общим сетевым ресурсам. Если моменты прибытия в пункт назначения пакетов неэластичного трафика становятся нерегулярными, появляется искажение сигнала. А если джиттер слишком большой и превышает несколько десятков мс, сигнал становится неразборчивым.

2) Потери пакетов. Потери определяются, как процент недоставленных пакетов.
Основные причины потерь пакетов включают в себя:
-ошибки в канале. На данный момент они практически несущественны;
-перегрузка сети. При перегрузках в сети очереди в маршрутизаторах и коммутаторах растут быстро. Если перегрузка продолжается длительное время, буферы переполняются, и пакеты теряются. Пакеты, принадлежащие трафику данных, передаются заново в соответствии с запросом принимающей стороны. Повторная передача пакетов увеличивает их задержку, и они отбрасываются. Если значения коэффициента потерь очень большие в восстановленной на приемной стороне речи появляются «провалы».

2.1 Оценка качества обслуживания неэластичного трафика

Если проблема оценки качества эластичного трафика была решена с большим или меньшим успехом, то оценка качества неэластичного трафика используется два подхода: субъективный и объективный. Субъективный подход предполагает экспертную оценку. Объективный подход использует параметры сети. Рассмотрим объективный метод оценки качества услуг. Результатом вычислений качества обслуживания в соответствии с моделью объективной оценки или E-моделью, является число, которое называется R-фактором. Численные значения R-фактора несомненно сопоставимы с субъективными оценками. соответствии с E-моделью R-фактор принимает значение в диапазоне от 0 до 100, где 100 означает самый высокий уровень качества. Когда рассчитывается R-фактор учитываются различные параметры, в числе которых:
-однонаправленная задержка;
-потери данных, связанные с переполнением джиттер-буфера;
-коэффициент потери пакетов;

-влияние эхо;
-искажения, которые появляются при преобразовании аналогового сигнала в цифровой;
-искажения, вносимые при последующем сжатии данных (обработка сигнала в кодеках) и др.

Значение R определяется как:
R = R0 -Ls -Ld -Le, (1)

где R0=93,2 – базовое значение R-фактора (качество сигнала на входе в систему равно 100 единицам). При его оцифровке и передаче по сети происходит некоторое искажение сигнала, снижающее значение R0, которое обычно округляют до 94;

Ls – искажения, вызванные местным эффектом и процедурой квантования;

Ld – искажения за счет суммарных задержек в сети;

Le – искажения, вносимые оборудованием.

Разберем подробно каждый фактор и дадим методику его оценки.

а) Задержки. Для пакетного трафика можно рассматривать общую задержку t или время доставки пакета как сумму транспортной задержки ttr, задержки распространения tp, задержки коммутации ts и задержки при организации очередей в коммутаторах (задержки на узле) tor.

$$T = ttr + tp + ts + tor \quad (2)$$

Под транспортной задержкой подразумевается время, требуемое для передачи пакета при заданной полосе пропускания и зависящее от размера пакета и ширины полосы пропускания канала и длины пакета, т.е.

$$Ttr=L/B, \quad (3)$$

где L – размер пакета, бит;

B – ширина полосы пропускания, кбит/с.

Задержка распространения (propagation delay) зависит от используемой среды
передачи и расстояния и может составлять десятки миллисекунд.

Задержка коммутации (switching delay) вносится устройствами коммутации и, как правило, составляет менее 10 мс. В случае, если сеть не испытывает перегрузки, задержка при организации очередей в маршрутизаторах отсутствует. В этом случае можно говорить о минимально возможной

задержке при передаче пакетов через заданную сеть. В случае перегрузки сети ta не только может составить значительную величину, но и приводит к джиттеру задержки. Для трафика реального времени джиттер задержки может привести к потере пакетов, т.к. при превышении порогового значения задержки пакеты будут отброшены как не удовлетворяющие требованиям, предъявляемым к режиму реального времени. Для потокового трафика внесение дополнительной задержки не оказывается критичным и не приводит к потерям.

б) Потери сети Pnet обусловлены ошибками в канале (на данный момент ими можно пренебречь) и потерями в узлах сети Ploss.Потери в узлах сети Ploss определяются интенсивностью трафика, размером буфера, применяемой политикой обслуживания очередей и используемыми методами предотвращения перегрузки. Для расчета потерь при известных распределениях, описывающих входной поток, предлагается использовать метод диффузионной аппроксимации:

$$P_{loss} = \frac{1-p}{1-p^{\frac{2}{C_a^2+C_s^2}nb+1}} p^{\frac{2}{C_a^2+C_s^2}nb}$$

где Ca2 и Cs2 - квадратичные коэффициенты вариации соответственно распределений входящего потока и времени обслуживания;

nb - размер буфера;

p - загрузка системы.

Как видно из формулы, случай, когда трафик описывается законом Пуассона, является самым благоприятным для системы. В этом случае квадратичные коэффициенты равны 1, и потери наименьшие по сравнению с другими законами распределения при прочих равных условиях (размере буфера, нагрузке). Наиболее часто встречающиеся законы распределения Парето и для длин протокольных блоков, и для интервалов между их приходами, представляет собой средний вариант. В случае если интервалы между протокольными блоками описываются логнормальным распределением, потери оказываются достаточно велики (при загрузке 0,5 достигают 25%). Из этого можно сделать вывод, что для трафика, тяготеющего к логнормальному закону распределения, необходимо вводить дополнительные механизмы, регулирующие пачечность (например, «корзину маркеров»). При агрегировании различных потоков результирующий поток будет смешанным из различных типов трафика,

генерация и обслуживание которого производится различными приложениями, гарантирующими различное качество связи, напрямую зависящее от факторов, влияющих на него: задержек, потерь, длин очереди на маршрутизаторах и так далее. Выбор методики расчета и оценки влияния этих факторов на качество обслуживания определяется распределением, свойственным определенному типу трафика. Предложена методика, применимая для смешанного типа трафика. Данные расчеты дают наиболее точные результаты при агрегированном потоке в СПД.

Качество обслуживания в сетях, построенных на базе IP-ориентированных протоколов качество доставки в традиционных сетях IP базируется на принципе так называемойN«наилучшей попытки» (Best effort). Концепция «наилучшей попытки» предполагает, что пользователи справедливо разделяют доступные сетевые ресурсы, трафик передается со скоростью, максимально возможной в данных условиях загрузки ресурсов сети, но при этом не гарантируется обеспечение любого предварительно определенного уровня качества обслуживания. Очевидно, что такой подход к обслуживанию означает следующее: отсутствуют различия между разными видами трафика, нет гарантии в доставке пакетов в правильном порядке, и что он будет доставлен в требуемое время или вообще будет доставлен, и т. д.

Концепция «наилучшей попытки» была достаточно эффективной для приложений, где можно передавать данные не в реальном времени (электронная почта, передача файлов). Кроме того, с учетом переизбытка сетевых ресурсов в транспортных сетях, построенных на базе волоконно-оптических линий связи, принцип «наилучшей попытки» в определенной степени позволяет обеспечить сегодня требования телефонии (голос поверх IP) и других приложений реального времени.В последние годы появились и стремительно развиваются новые виды услуг: мобильная связь, услуги сети Интернет, IP-телефония, высокоскоростная передача данных, услуги интеллектуальных сетей.

Внедрение этих услуг стало возможным благодаря появлению оборудования нового поколения, основанного на пакетной коммутации, пришедшей на смену коммутации каналов. В отличие от упомянутых выше технологий в классических сетях IP применяется метод доставки, полностью исключающий любую форму организации соединений – как физических, так и виртуальных. Этот метод основан на рассылке пакетов-дейтаграмм. Технологии пакетной коммутации позволяют предоставить пользователю ряд новых инфокоммуникационных услуг:

-Дистанционное обучение;
-телемедицина;
-передача по запросу видеоинформации;
-удаленный мониторинг и управление объектами;
-участие в интерактивных играх;
-аудио- видео конференции;
-маршрутизация
-вызовов на другие телефонные номера;
-универсальная почта и др.

Сегодня постепенно создается общая конвергированная инфраструктура, базирующаяся на протоколах семейства IP. Инфраструктура, возникшая в результате конвергенции, обеспечивает транспортировку трафика приложений, традиционно использующих сети Интернет, трафика телефонных сетей, а также сетей телевидения. Подобный сценарий конвергенции благодаря объединению технологий экономически выгоден, и определяет развитие сектора телекоммуникаций через создание новых инфокоммуникационных услуг. Однако процесс конвергенции протекает достаточно медленно, так как одним из основных тормозящих факторов в процессе конвергенции сетей и услуг и построении единой сети на базе IP является проблема обеспечения необходимого качества обслуживания. Эта единая сеть рассматривается сегодня как сеть следующего поколения (Next Generation Network – NGN) или ультисервисная сеть. Для того, чтобы полностью реализовать все преимущества конвергенции в IP-ориентированных сетях, разрабатываются новые принципы управления трафиком и распределения ресурсов сетей, которые должны гарантировать определенные показатели качества обслуживания для разнообразного рода и большого числа приложений, реализуемых оконечными пользователями. При этом процессы управления трафиком и разделение ресурсов необходимо скоординировать в условиях большого числа разнообразных приложений, которые существенно отличаются требованиями к рабочим характеристикам сети. В таблице 5 приведена чувствительность различных приложений к сетевым характеристикам.

Т а б л и ц а 5 – Чувствительность различных приложений к сетевым характеристикам

Тип трафика	Уровень чувствительности к сетевым характеристикам			
	Полоса пропускания	Потери	Задержка	Джиттер
Голос	Очень низкий	Средний	Высокий	Высокий
Электронная коммерция	Низкий	Высокий	Высокий	Низкий
Транзакции	Низкий	Высокий	Высокий	Низкий
Электронная почта	Низкий	Высокий	Низкий	Низкий
Telnet	Низкий	Высокий	Средний	Низкий
Поиск в сети «от случая к случаю»	Низкий	Средний	Средний	Низкий

С появлением нетрадиционных услуг подходы к показателям оценки качества несколько видоизменяются, так как появляются новые потребительские свойства услуги. Одни показатели становятся менее значимыми, другие приобретают большее значение. Кроме того, возникает необходимость в разработке и использовании новых показателей оценки качества. Обеспечение высокого качества услуг отличается от принципов классической телефонии вследствие использования системы и коммутации пакетов. Рассмотрим гарантированное качество обслуживания.

Сущность нового подхода. Новый подход обеспечивает требуемое пользователю качество услуг и получил название QoS (Quality of Service). Он предполагает в отношении качества предоставляемых услуг главным и первостепенным являются требования пользователя: пользователь подает службе заявку на услуги с требуемым ему качеством, в то время как служба либо должна выполнить эту заявку, либо сообщить о невозможности ее реализации, но этот вариант уже является чрезвычайной ситуацией [30].

Требуемое качество услуг при QoS достигается не чрезмерным увеличением пропускной способности сети, а с помощью нижеперечисленных мероприятий: приоритезация пользователей и их заявок; создание системы управления нагрузкой, коммутацией и передачей пакетов. Система управления регулирует и сети, и бизнес, и элементы сетей, и услуги (службы), т.е. является единой. С помощью системы управления обеспечивается управление потоками, сокращение очередей в маршрутизаторах, возможность оптимального распределения полосы частот между заявками с учетом их приоритетов, сокращение времени передачи пакетов и его флуктуации (джиттера), сокращение потерь пакетов и их числа с ошибками.

В результате существования системы управления QoS пользователю гарантируется качество услуг, которое он заказал, независимо от его собственного трафика и трафика других пользователей. Конечно, в ряде случаев это может привести к некоторому снижению качества услуг у

низкоприоритетных пользователей. Понятно, что число высокоприоритетных пользователей должно быть относительно небольшим по сравнению с общим их числом, а услуги для таких клиентов должны предоставляться по более высоким тарифам. Наиболее важным является обеспечение QoS в многофункциональных мультисервисных сетях, по которым одновременно передаются разнотипные сообщения, и в мультимедийных службах по двум основным причинам:

1) сети связи не индифферентны к различным видам информации, и для разных услуг не может быть обеспечено одинаковое качество. Сети связи с разными системами коммутации и передачи имеют различные характеристики по времени распространения сигналов и его флуктуации, достоверности. Используемые в сетях методы коммутации и передачи информации изначально создавались применительно к конкретному виду связи, который предъявляет определенные требования к характеристикам качества услуг;

2) интеграция служб реализуется на основе единой сети с характеристиками, которые более благоприятны для служб одних видов связи и менее - для других. Технология QoS распространена в службах АТМ. На входе в мультиплексор АТМ образуется очередь разного вида сообщений с различными требованиями и характеристиками к системе. МСЭ было определено четыре класса услуг в зависимости от необходимости синхронизации, типа передаваемого трафика и наличия или отсутствия ориентации на соединение:

класс 1 – трафик, ориентированный на установление соединения и требующий синхронизации, с постоянной полосой пропускания (к примеру, режим эмуляции синхронных цифровых каналов);

класс 2 – трафик, ориентированный на установление соединения и требующий синхронизации, с переменной полосой пропускания (к примеру, передача компрессированной речевой и видеоинформации);

класс 3 – трафик, ориентированный на установление соединения и не требующий синхронизации, с переменной полосой пропускания (к примеру, передача кадров X.25, Frame Relay);

класс 4 – трафик, не ориентированный на установление соединения и не требующий синхронизации, с переменной полосой пропускания (к примеру, передача IP- пакетов). Каждому классу обслуживания поставлены соответствующие значения параметров QoS (см. таблицу 6).

Т а б л и ц а 6 – QoS параметры

Класс QoS	QoS параметры						
	CTD	CDV	$CLR_{(0+1)}$	$CLR_{(0)}$	CER	CMR	SECBR
QoS1	400 мс	3 мс	$3 \cdot 10^{-7}$	нет	$4 \cdot 10^{-6}$	1 ячейка в день	10^{-4}
QoS2	Н	Н	10^{-7}	нет	$4 \cdot 10^{-6}$	1 ячейка в день	10^{-4}
QoS3	Н	Н	Н	10^{-5}	$4 \cdot 10^{-6}$	1 ячейка в день	10^{-4}
QoS4	400 мс	6 мс	Нет	$3 \cdot 10^{-7}$	$4 \cdot 10^{-6}$	1 ячейка в день	10^{-4}

где

CTD (Cell Transfer Dalay) – время задержки переноса ячеек;

CDV (Cell Dalay Variation) – отклонение времени задержки переноса ячеек;

CLR (Cell Loss Ratio) – коэффициент потери ячеек;

CER (Cell Error Ratio) – коэффициент ошибочных ячеек;

CMR (Cell Misinsertion Rate) – скорости поступления ячеек;

SECBR (Severely – Errored Cell Block Ratio) – коэффициент ошибочных блоков;

индексы 0 и 1 означают приоритеты потерь – соответственно высокий и низкий;

Н – не определено.

В связи с тем, что на сегодняшний день необходимо удовлетворить каждый запрос пользователя, мультисервисные сети, для которых характерно качество обслуживания QoS, предъявляют к системе управления новые требования. Однако, перед тем как приступить к выполнению очередного запроса пользователя, система управления должна проверить право на получение заказанной им услуги по договору и наличие на его счету достаточных денежных средств для оплаты, т.е. аутентифицировать его. Далее, чтобы удовлетворить запрошенную услугу с требуемым QoS, система управления должна проверить собственные ресурсы. Только после получения положительного ответа система может приступить к обслуживанию пользователя. Вышеизложенные процессы должны осуществляться в минимально короткое время. В случае, если вдруг предлагаемое качество будет недостаточным, то системе управления необходимо мобилизовать все имеющиеся ресурсы, включая выделенные и для других пользователей. Может показаться, на первый взгляд, что переход к QoS будет означать, что не нужно определять оптимальную номенклатуру параметров качества и устанавливать нормы на них. Но эти нормы необходимы для всех (для разработчиков аппаратуры и транспортных систем, для провайдеров и операторов, контрольных органов, проектных и строительных организаций), потому что без них

нельзя обеспечить благоприятное совместное использование однотипных компонентов систем электросвязи. Подтверждением этому служит наличие подобных норм для АТМ сетей, которые построены по технологии QoS. Существуют традиционные методы нормирования качества услуг только для провайдеров и операторов, в связи с этим они должны также дополняться удобными для пользователей характеристиками, как это частично реализовано в АТМ.

2.2 Технология обеспечения QoS в системах IP

В IP-сетях (версия IPV4) сообщения передаются методом «отправь и молись», т.е. без гарантии и уверенности, что сообщение попадет к получателю. При этом нет проверки ни на наличие приоритета у сообщения, ни на готовность сети к его передаче. Независимо от типа пакетов (данные, аудио или видео), они передаются по принципу «первый пришел – первый ушел». Поскольку такое обслуживание для мультимедийного трафика не подходит, сегодня ведутся работы по созданию новых протоколов. Организация по стандартизации в системе Интернет еще в середине прошлого столетия в 1964 г. разработала протокол RSVP (протокол резервирования ресурсов), который содержит в себе основные принципы QoS. Наряду с традиционными услугами он содержит два новых класса обслуживания: контролируемой задержки и гарантированного обслуживания.

Второй гарантирует определенную полосу пропускания, задержку и отсутствие потерь в случае переполнения очередей, но не уменьшает величину разброса задержек (джиттера). Класс контролируемой задержки обеспечивает аналогичное обслуживание, но в отличие от последнего, при увеличении нагрузки QoS остается неизменным. Появились так называемые справедливые модели, обеспечивающие равномерное распределение пропускной способности всем потокам. Следующим этапом рационализации стека протоколов IP стало установление абсолютных приоритетов для пакетов тех видов информации, которые отрицательно реагируют на большие задержки и джиттер. В этом плане отметим протокол взвешенной справедливой очередности – WFQ, согласно которому каждому потоку выделяется доля пропускной способности, пропорциональная заданному весовому коэффициенту.

Для предотвращения перегрузок мультиплексоров вводилась система принудительного сброса пакетов при увеличении трафика выше определенного значения. Эти и другие протоколы хотя и приближали

технологию IP к требованиям QoS, но не отвечали им полностью по двум основным причинам. Во-первых, для их внедрения требуется полная переработка сетевого оборудования и математического обеспечения, а следовательно – много времени и существенные капиталовложения. Во-вторых, в протоколе IP отсутствует механизм маршрутизации, основанный на требованиях QoS. В настоящее время протоколы IP- маршрутизации выбирают маршрут лишь на основе количества переходов или стоимости соединения до точки назначения, а не на базе величины доступной полосы пропускания, значении задержки или ее вариации. Таким образом, протокол RSVP резервирует ресурсы на пути, выбранном без учета параметров, требуемых для обеспечения QoS. Даже если маршрут с оптимальными параметрами QoS существует, протокол маршрутизации не имеет возможности его использовать. Еще один шаг в направлении учета требований QoS был сделан после введения пяти классов обслуживания: с низкой задержкой, высокой пропускной способностью, высокой надежностью, низкой стоимостью, стандартного. Эти протоколы обеспечивают «относительное QoS». Характеристики качества обслуживания в мультисервисных СПД Задержки. Задержка создаёт различные неудобства при ведении диалога, что приводит к перекрытию разговоров и возникновению эха. Эхо возникает, когда отражённый речевой сигнал вместе с сигналом от удалённого конца возвращается опять к говорящему. Эхо становится большой проблемой, когда задержка при передаче больше, чем 50 мс. Когда задержка в одном направлении превышает 250 мс, затруднение диалога и перекрытие разговоров становится серьёзным проблемой качества. Можно выделить следующие источники задержки при передаче речи из конца в конец
(см. рисунок 1):

- задержка накопления (алгоритмическая задержка): эта задержка обусловлена необходимостью сбора кадра речевых отсчётов, выполняемая в речевом кодере;
- задержка обработки: определённые задержки создаются в процессе кодирования и сбора закодированных отсчётов в пакеты для передачи через пакетную сеть;
- сетевая задержка: задержка обусловлена физической средой и протоколами, а также буферами, используемыми для удаления джиттера на приёмном конце. Сетевая задержка зависит от ёмкости сети и процессов передачи в сети.

Рисунок 1 – Составляющие задержки в сетях IP-телефонии

Время задержки можно отнести к одному из трёх уровней:

1) до 200 мс - отличное качество связи. Для сравнения, в СТОП допустимы задержки 150, 200 мс;

2) до 400 мс - хорошее качество связи. Но при сравнении с СТОП разница ощутима;

3) до 700 мс - приемлемое качество связи для неделовых переговоров. Такое качество связи возможно и в спутниковых сетях связи.

Джиттер. В сетях с коммутацией пакетов данные и речь разбиваются на пакеты для передачи через IP-сети, часто бывает так, что пакеты прибывают в пункт назначения в разное время и в различной последовательности. Это приводит к тому, что создается разброс времени доставки IP пакетов – джиттер (или вариация задержки). Джиттер приводит к различным нарушениям передачи речи, они воспринимаются как различного рода щелчки и треск. Можно выделить три основные формы джиттера:

случайный джиттер (Random Jitter - RJ) – результат теплового шума;

джиттер, зависящий от данных (Data Dependent Jitter - DDJ) –происходит при

нарушениях в компонентах сети или в случае ограниченной полосы пропускания;

искажение рабочего цикла (Duty Cycle Distortion - DCD) – возникает из-за задержки распространения между передачей сверху вниз и снизу вверх.

Можно выделить следующие причины появления джиттера:

1) Влияние сети. Время прохождения пакета через сеть неоднозначно. В случае, если нагрузка на сеть небольшая, коммутаторы и маршрутизаторы могут пакеты обрабатывать практически мгновенно, а линия связи бывает доступна практически всегда. Если имеет место большая загруженность сети, пакеты буду довольно длительное время ожидать обслуживания в очередях. Чем больше коммутаторов, маршрутизаторов, линий в маршруте, по которым проходит пакет, тем больше время его задержки и тем больше вариация этого времени, то есть джиттер;

2) Влияние операционной системы. Множество приложений IP-телефонии являются обычными программами, которые выполняются в среде какой-нибудь операционной системы, например, Windows или Linux.

Эти программы обращаются к периферийным устройствам через интерфейс прикладных программ для взаимодействия с драйверами этих устройств, доступ к IP-сети осуществляют через Socket-интерфейс. Зачастую операционные системы не могут контролировать распределение времени

центрального процессора между разными процессами с точностью, превышающей десятки миллисекунд, и не могут обрабатывать за это же время более одного прерывания от внешних устройств. В последствии задержка в продвижении информации между сетевым интерфейсом и внешним устройством речевого вывода составляет, независимо от используемого алгоритма кодирования речи, величину такого же порядка или даже больше;

3) Влияние джиттер-буфера. Проблемы влияния джиттера особенно заметны в пакетно-ориентированных сетях. Речевые пакеты передаются через фиксированные промежутки времени (допустим, через каждые 20 мс), но при прохождении через сеть задержки пакетов оказываются разными, поэтому они прибывают в пункт назначения через различные промежутки времени.

Это показано на рисунке 2.

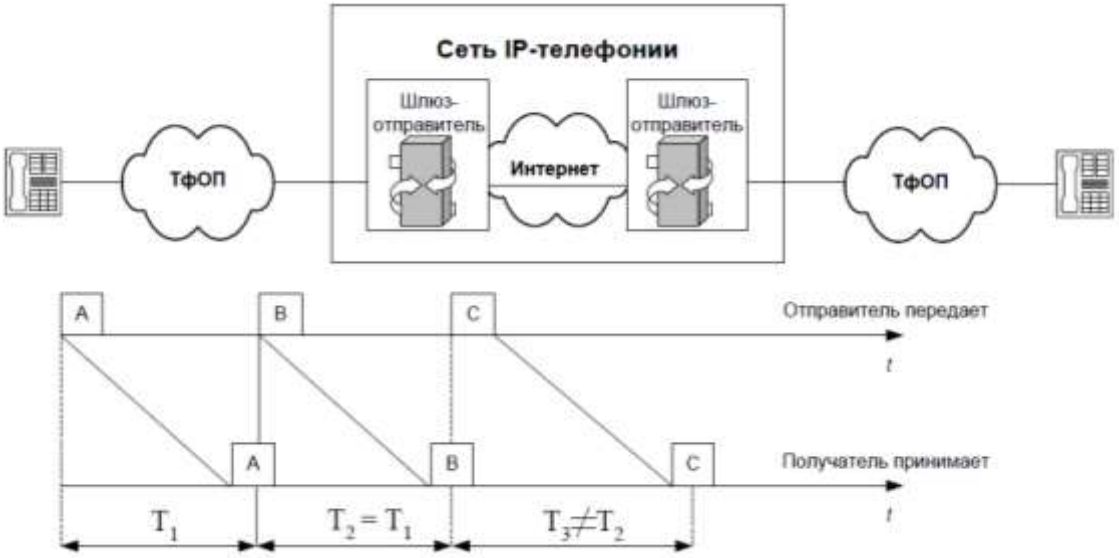

Рисунок 2 – Джиттер

Найдем задержку времени прохождения пакетов через сеть Ti. Она представляет собой сумму постоянной составляющей T (время распространения + средняя длительность задержки в очередях) и переменной величины j, являющейся результатом джиттера:

$$Ti = T \pm j. \quad (5)$$

Чтобы компенсировать влияние джиттера, в терминалах используется так называемый джиттер-буфер. Он хранит в памяти прибывшие пакеты в течение времени, которое определяется его объемом. Когда буфер переполнен, пакеты, которые прибыли слишком поздно, отбрасываются. Интервалы между пакетами восстанавливаются на основе значений временных меток RTP-пакетов. Если при транспортировке по сети пакеты оказались «перепутаны», джиттер-буфер восстанавливает исходную очередность их следования. Чрезмерно короткий буфер может привести к слишком частым потерям «опоздавших» пакетов, а слишком длинный - к нерационально большой добавочной задержке. Обычно предусматривается динамическая подстройка длины буфера в течение всего времени существования соединения. Для выбора наилучшей длины применяются эвристические алгоритмы;

4) Воздействие кодека и числа передаваемых в пакете кадров. Множество современных эффективных алгоритмов кодирования/ декодирования речи ориентировано на передачу данных кадрами, а не последовательностью кодов отдельных отсчетов. Следовательно, в течение времени, пределяемого размером кадра кодека, должна накапливаться

последовательность цифровых представлений отсчетов определенной длины. Помимо этого, некоторым кодекам необходим предварительный анализ большего числа речевой информации, чем должно быть в кадре. Это неизбежное время накопления и предварительного анализа входит в общую длительность задержки пакета. Можно предположить, что чем меньше длина кадра, тем меньше должна быть задержка. Но из-за значительного объема служебной информации в RTP/UDP/IP-пакетах, передача маленьких пакетов данных очень неэффективна, так как при применении кодеков с маленькой длиной кадра приходится упаковывать несколько кадров в один пакет. Помимо этого, кодеки с большей длиной кадра более эффективны, так как они могут «наблюдать» сигнал в течение большего периода времени и, следовательно, могут более эффективно моделировать этот сигнал. Сети передачи данных на основе протокола IP не обеспечивают гарантированную полосу пропускания, так как не гарантируют доставку пакетов. Для тех приложений, для которых не важен интервал и порядок прихода пакетов, размер задержек между отдельными пакетами не имеет существенного значения. IP- телефония как одна из областей передачи данных, является услугой, в которой важна динамика передачи сигнала, которая обеспечивается современными способами передачи и кодирования информации, а также важен порядок прихода пакетов. Транспортные протоколы стека TCP/IP, работающие поверх протокола IP, не гарантируют высокое качество обслуживания IP трафика, чувствительного к задержкам. А протокол TCP, хоть и гарантирует достоверную доставку данных, однако переносит ее с различными задержками. В свою очередь, протокол UDP, который, как известно, используется для переноса информации для приложений реального времени, обеспечивает меньшее время задержки, по сравнению с протоколом TCP, но, как и протокол IP, не имеет никаких механизмов обеспечения качества обслуживания. Потеря пакетов может иметь место из-за перегрузок или вследствие ошибок при маршрутизации. Вероятность потери пакета (Packet Loss Rate, PLR) представляет собой отношение количество потерянных пакетов к общему числу переданных за достаточно большой интервал наблюдения. Редко пакеты могут поступить пользователю, которому они не были предназначены. Такие случаи называются доставкой пакета не по адресу (вставкой пакета). Вероятность доставки пакета не по адресу (Packet Insertion Rate, PIR) -это количество пакетов, которые доставлены не по адресу, за достаточно большой промежуток времени. Природа этих ошибок в большинстве случаев

определяется техническими устройствами, где они возникают. Ошибки, зависящие от систем передачи, в основном определяются физической средой (волоконно-оптическая линия, коаксиальный кабель и др.) и рядом других факторов (видом скремблирования, кодирования и т. д.). Под временной прозрачностью сети понимается её свойство поддерживать значение времени задержки и джиттера (разброса задержки), при которых обеспечивается требуемое качество обслуживания. Ее принято оценивать двумя основными показателями: временем задержки и джиттером задержки:

Время задержки есть разница во времени между началом передачи пакета источником и окончанием приема этого же пакета получателем. Она может быть разной для каждого пакета и представляет собой случайную величину (СВ). Числовыми характеристиками этой СВ являются среднее время задержки и дисперсия времени задержки. В отличие от упомянутых выше технологий в классических IP сетях применяется метод доставки пакета, который полностью исключает любую форму организации соединений – как виртуальных, так и физических. Данный метод основан на рассылке пакетов-дейтаграмм. В традиционных сетях IP качество доставки базируется на принципе «наилучшей попытки» (Best effort). Концепция так называемой «наилучшей попытки» предполагает, что пользователи разделяют доступные сетевые ресурсы, а трафик передается с максимально возможной в данных условиях загрузки ресурсов сети скоростью, но при этом не гарантируется обеспечение предварительно определенного уровня качества обслуживания. Ясно, что такой подход к обслуживанию говорит о следующем: отсутствуют различия между различными видами трафика, нет гарантии доставки пакетов в правильном порядке, и что пакет будет доставлен в нужное время или вообще будет доставлен, и т. д.

Принцип «наилучшей попытки» был достаточно эффективен для приложений, где можно передавать данные не в режиме реального времени (передача файлов, электронная почта и т.д.). Кроме того, с учетом переизбытка сетевых ресурсов в транспортных сетях, построенных на базе волоконно-оптических линий связи, концепция «наилучшей попытки»

в определенной степени позволяет обеспечить сегодня требования телефонии (голос поверх IP) и других приложений реального времени. Но в случае возникновения недостатка ресурсов, ведущего к увеличению росту задержек пакетов и вероятности их потерь, необходимые для приложений реального времени показатели качества обслуживания не могут быть

обеспечены. Прежде всего, это объясняется главным принципом функционирования IP-сетей – передачей данных в дейтаграммном режиме, т. е без управления и без установления соединения.

С появлением новых приложений реального времени (интерактивная передача речи, видеоконференции и видеотелефония), вопрос о гарантированном качестве обслуживания в IP - сетях становится одним из наиболее сложных. Это и объясняет, почему качество обслуживания QoS в сетях IP остается предметом пристального и постоянного внимания МСЭ, ETSI, IETF и других организаций стандартизации в электросвязи.

Производительность сети - это скорость передачи данных пользователя. Она определяется как эффективная скорость передачи, которая измеряется в битах в секунду. Необходимо подчеркнуть, что значение данного параметра не совпадает с максимальной пропускной способностью сети. Провайдер услуг обычно гарантирует минимальное значение производительности, также он, в свою очередь, должен иметь соответствующие гарантии от сетевого провайдера. Надежность сети/сетевых элементов. Обычно пользователи ожидают высокий уровень надежности от систем и сетей связи. Надежность сети может быть охарактеризована рядом параметров, из которых наиболее часто используется коэффициент готовности сети, определяемый как отношение времени простоя объекта к суммарному времени наблюдения объекта, включающему время простоя и время между отказами. В идеале коэффициент готовности должен быть равен 1, что означало бы стопроцентную готовность сети. Однако, на практике коэффициент готовности оценивается количеством так называемых «девяток». Например «три девятки» означают, что коэффициент готовности равен 0,999, что соответствует 9 часам времени недоступности (простоя) сети в год. А готовность сети телефонии общего пользования оценивается величиной «пять девяток», что означает 5,5 мин. простоя в год. Средняя задержка доставки IP пакета – это параметр (Рекомендация Y.1540), который определяется как средняя арифметическая величина задержек пакетов в выбранном наборе принятых и переданных пакетов. Ее значение зависит от передаваемого по сети трафика и доступных ресурсов сети, в том числе и от пропускной способности. Уменьшение доступных сетевых ресурсов и рост нагрузки ведут к росту очередей в узлах сети и, следовательно, к увеличению величины средней задержки доставки пакетов. Наиболее чувствительной к задержкам является речевая информация и, частично,

видеоинформация. А приложения передачи данных зачастую менее чувствительны к задержкам. Если задержка доставки пакета превышает определенное значения Tmax, то такие пакеты отбрасываются. Это ведет к ухудшению качества речи в приложениях реального времени, таких как IP-телефония. Такие ограничения, связанные со средней задержкой IP - пакетов, играют важнейшую роль для успешного внедрения технологии Voice over IP (VoIP), видео-конференций и других приложений с трафиком реального времени. Данный параметр во многом определяет готовность пользователя принять такого рода приложения.

Джиттер или вариация задержки IP - пакета (IP packet delay variation, IPDV). Вариацию задержки характеризует параметр Vk. Для пакета IP с индексом k данный параметр между входной и выходной точками сети определяется в виде разности между абсолютной величиной задержки Xk при доставке пакета с индексом k, и определенной эталонной величиной задержки доставки IP - пакета d1,2, для тех же точек сети:

$$Vk = Xk – d1,2 \quad (6)$$

Эталонная (опорная) задержка доставки пакета IP, d1,2, между источником и получателем вычисляется как абсолютное значение задержки доставки первого IP - пакета между данными точками сети. Джиттер проявляется в том, что последовательные IP - пакеты приходят к получателю в нерегулярные моменты времени. В IP-телефонии это, например,
ведет к искажениям звука и впоследствии к тому, что речь становится непонятной. Коэффициент потери пакетов IP (IP packet loss ratio, IPLR) есть отношение уммарного числа утерянных пакетов к общему числу принятых пакетов. Возникают потери пакетов в сетях IP в тех случаях, когда значение задержки при передаче превышает нормированное значение Tmax. При потере пакетов во время передаче данных не исключена их повторная передача по запросу принимающей стороны. Пакеты в системах VoIP, которые пришли к получателю с задержкой, превышающей Tmax, отбрасываются, что в принимаемой речи ведет к провалам. Среди вызывающих потери пакетов причин, важно отметить рост очередей в сетевых узлах, возникающих при перегрузках сети. Коэффициент ошибок пакетов IP (IP packet error ratio, IPER) определяется как суммарное число пакетов, принятых с ошибками, к суммарному числу успешно принятых и пакетов, принятых с ошибками.

2.3 Описание программного обеспечения, использованного в исследовании

Для получения точных результатов, отражающих реальное состояние мультисервисной СПД, необходимо проводить статическую обработку эксперимента. Экспериментом в данном случае является запись показаний параметров при реальной работе сети. В качестве средства записи используются инструменты, построенные по принципу анализатора протоколов . Анализатор протоколов представляет собой аппаратный либо программно-аппаратный комплекс, который позволяет захватывать и обрабатывать данные, передаваемые в конкретной мультисервисной СПД. По расшифровке полученной таким образом информации наблюдатель может делать вывод о реальном состоянии сети. Для полного понимания работы анализатора протоколов, конечно, необходимо обладать знаниями о физическом распространении сигналов в канале связи, о форме их представления, о методах кодировки, о структуре передачи данных. Во многих приложениях такого класса эти сведения бывают неполными, поэтому часто приходится придумывать методики, позволяющие выражать требуемые параметры анализатором протоколов. Если структурная топология мультисервисной СПД позволяет получать данные от каждого активного узла в любой точке системы, то накопленная анализатором протоколов в любом месте статистика отражает реальное состояние сети. для определения параметров сети использовалось программное обеспечение Wireshark 1.8. Обзор программы представлен на рисунке 3.

Рисунок 3 – Обзор программы Wireshark

Wireshark является программой-анализатором сетевых пакетов с исходным кодом. Без какого-либо специального оборудования или перенастройки эта программа может перехватывать входящие и исходящие данные на любом сетевом интерфейсе компьютера: Ethernet, Wi-Fi, PPP, loopback и даже USB. Обычно Wireshark применяется для выявления проблем в сети, таких, как перегруженность, слишком долгое время ожидания или ошибки протоколов. Wireshark написан на библиотеках GTK+ и имеет графический интерфейс (GUI). Ядром Wireshark является библиотека libpcap, с помощью которой и производится перехват данных. Программа имеет встроенную поддержку очень большого количества сетевых устройств. Все современные Ethernet и Wi-Fi карты не имеют каких-либо проблем с совместимостью в этой программе. Запуск новой сессии перехвата производится в окне программы из меню «Capture». Чтобы увидеть весь список сетевых интерфейсов, которые смогла обнаружить Wireshark, необхдимо перейти по пути в меню «Capture > Interfaces». Появится диалоговое окно, в котором, помимо физических устройств, будет присутствовать псевдоустройство «any», которое перехватывает данные со всех других устройств этого списка. Перед началом можно задать некоторые опции, с которыми будет запускаться перехват. Перейдя по «Capture > Options», достаточно выбрать:

-фильтры для выборочного анализа трафика (например, по определенному протоколу или диапазону адресов);

-автоматическиостановить перехват по достижении указанного в настройках времени;

-отсортировать полученные данные по указанному размеру или дате.

Первое, что можно увидеть при запуске новой сессии – окно лога, где показывается основная информация о выполняемом программой процессе: источник, приемник, протокол, время и т.п. Вся информация организована в виде таблицы с заголовками. Для большей читаемости Wireshark выполняет цветовое выделение фрагментов текста, изменение цвета фона или пометку наиболее «интересных» пакетов с помощью флагов (см. рисунок 4).

Продолжительность перехвата зависит от того, какую информацию необходимо получить в результате. Например, для анализа и решения трудноопределимых проблем, связанных с работой Интернет-сервисов, потребуется несколько часов. Зато для ознакомления с основными возможностями программы будет достаточно всего нескольких минут. Для анализа любого полученного пакета достаточного выбрать его в окне

логов. Однако, делать это целесообразно после остановки перехвата данных. Подробная деталировка интересующего пакета будет представлена в отдельном древовидном окне, в котором все его составляющие будут рассортированы по сетевым уровням.

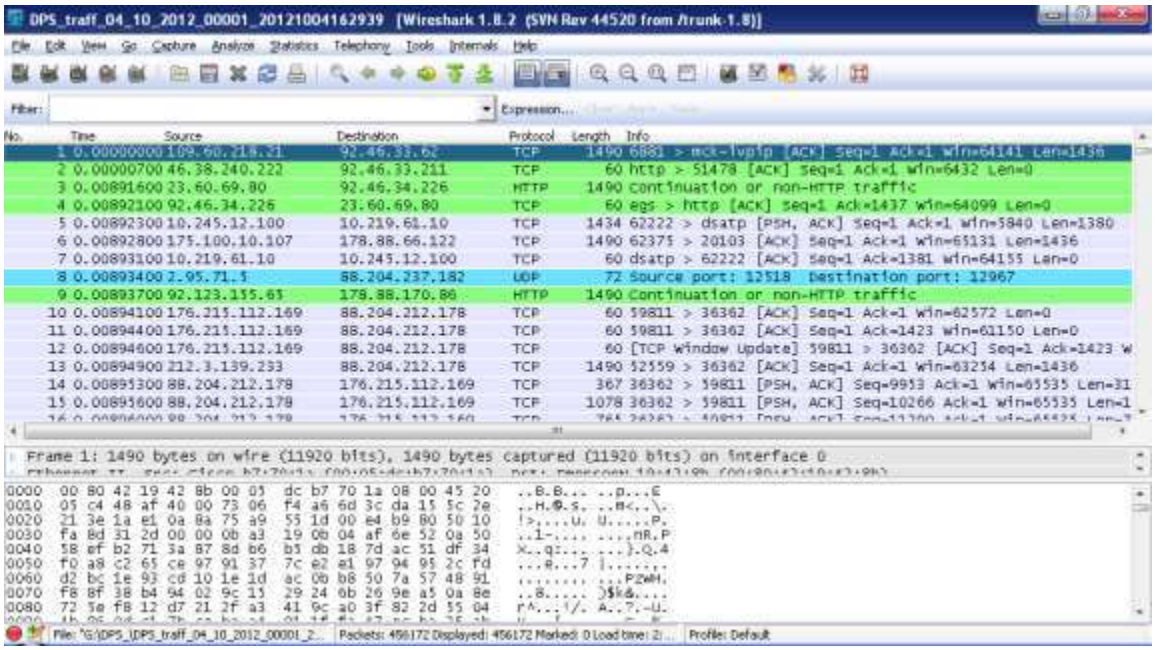

Рисунок 4 – Основная информация при сканировании

Всегда можно сохранить перехваченные данные для их дальнейшего анализа. Wireshark сохраняет полученные данные в файл с расширением .pcap. Однако этот файл может быть достаточно большим. Поэтому, если необходима картина только определенной части всего сетевого трафика, можно воспользоваться фильтрами Wireshark для урезания объема этого файла. Система фильтров располагается в том же окне, что и общая таблица перехватываемых данных. Система фильтров является основным способом преобразования полученных данных в нужный вам формат. Для того, чтобы выбрать нужный фильтр, необходимо щелкнуть на кнопку «Filter» в окне программы. Появится окно с опциями на выбор: только TCP; только UDP; все IP-адреса, кроме локальных; все, кроме DNS и ARP; и многие другие. При выборе любого фильтра из списка в окне синтаксиса Wireshark будет отображена полная команда, представляющая собой фильтр в его «развернутом» виде. Это полезно для изучения синтаксиса Wireshark при написании собственных фильтров. Wireshark позволяет вручную выбрать логические операторы и известные поля, которые вы можете использовать при составлении своих собственных фильтров.
Меню «Анализ» («Analyze») содержит набор более сложных заранее предустановленных опций фильтрации.

-« Enable Protocols» предоставляет возможность включить или отключить протоколы;
-« Specified Decodes» позволяет декодировать определенные протоколы, что может быть полезным при диагностике конкретно выбранного приложения;
-«Follow TCP Stream» поможет выбрать отдельное соединение по TCP-протоколу и проследить его состояние от начала и до конца; подобные опции имеются для UDP и SSL- соединений;
-«Expert Infos» извлекает сообщения об ошибках и флаги предупреждения (такие, как потерянный или не в очереди сегмент) для быстрого обнаружения проблемы.
Меню «Статистика» («Statistics») предоставляет более общий обзор всего набора перехваченных данных. Это меню содержит предустановленные функции для анализа общих параметров сети и предоставляет их в удобном табличном виде. Здесь можно проанализировать такие данные, как время ответа; размеры фрагментов, на которые разбиты пакеты; трафик на уровне ссылок и приложений. Wireshark также может выводить полученную информацию в графическом режиме, что облегчает ее восприятие. Перейдя в «Graphs tool» в меню «Статистика» («Statistics»), можно выбрать пять фильтров для сравнения файлов позаголовочно с помощью выделения различными цветами. Обучающие материалы по этой программе на сайте проекта Wireshark являются незаменимым подспорьем. Wiki имеет несколько страниц, посвященных основным проблемам сети, а также ссылки на другие источники с подобной информацией. Представлена информация по другим программам сетевого анализа и анализа безопасности, таким как Nagios, EtherApe, NMap и tcpdump. Большинство исследований проблем в сети требуют понимания сути стеков протокола TCP/IP. В Wireshark включено множество возможностей по анализу сети, когда необходимо исследовать ее в поисках источника проблем. Например, можно запустить статистическое сравнение между двумя сохраненными файлами перехвата трафика. Это позволяет выполнить захват, когда проблема только изучается, а затем сравнить их снова.

Другими словами, можно собрать и сравнить файлы захватов с разных машин, например, в различных сегментах сети или с различными конфигурациями. Это тем более полезно, так как имеются сборки Wireshark для проприетарных операционных систем: при выяснении проблем с производительностью может потребоваться собрать информацию с различных источников. Несмотря на то, что инструменты

анализа и фильтрации, заложенные в графическом интерфейсе Wireshark, редоставляют большие возможности для перехвата трафика, возможности GUI этим не ограничиваются. Имеется множество примеров того, что представление отчетов в графическом режиме выдает информацию в таком виде, который никогда не смогут представить таблицы. Имеются множество инструментов, расширяющих возможности Wireshark в качестве визуализации, написанных для этой программы. Wireshark может экспортировать захваченные данные в файл формата CSV, который в дальнейшем вы можете открыть в любом другом приложении, например, в обыкновенной электронной таблице, наподобие Gnumeric или OpenOffice, или в таком статистическом пакете, как R или gnuplot. Хорошие приложения для анализа можно найти на forensicswiki.org. Список этих приложений постоянно меняется. К примеру, популярный движок анализа Freebase Gridworks был преобразован в проект Google Refine, который может визуализировать сетевой трафик значительно более удобным способом. И последнее, но не менее важное. Хотя Wireshark почти всегда позиционируется как сетевой инструмент для анализа, правда заключается в том, что он может анализировать и другие устройства, такие как USB-трафик и даже Unix-сокеты между приложениями. С помощью программы облегчается процедура распознавания и анализа трафика, анализ позволяет отделять потоки приложений друг от друга, автоматически определять их статистические характеристики. Эти характеристики также используются для прогнозирования основных показателей качества сети.

ГЛАВА 3. Проведение экспериментальной части

3.1 Обоснование исследования

На сегодняшний день на современном этапе развития отрасли телекоммуникаций всё больше и больше возрастает спрос на инфокоммуникационные услуги. Данные услуги связи предполагают автоматизированную обработку и хранение информации, а также предоставление еепо запросу, используя средства вычислительной техники, как на исходящем, так и на входящем конце соединения. В мультисервисных сетях передачи данных должна передаваться многокомпонентная информация (данные, речь, видео) с гарантированными параметрами качества обслуживания и необходимой синхронизацией всех компонент в реальном времени.Одновременноэксплуатировать несколько сетей (передачи голоса, передачи данных, передачи видео) с экономической точки зрения не выгодно. Сегодня вместо использования большого количества проводов или кабелей с набором радиотерминалов или уплотненной «цифрой» телефонной проводки, уже эксплуатируются новые единые мультисервисные сети, которые позволяют получать все услуги с помощью одного универсального телекоммуникационного терминала. Таким образом, с помощью конвергенции различных сетей образована на базе протокола IP единая сетевая инфраструктура, обеспечивающая предоставление услуг Ethernet, ATM/FrameRelay, IP-VPN, Internet. Такой инфраструктурой и является мультисервисная сеть.

Мультисервисная сеть передачи данных – это сеть с пакетной коммутацией, способная предоставлять различные услуги электросвязи и в которой возможно использование нескольких широкополосных транспортных технологий, позволяющих обеспечить требуемое качество обслуживания. В данной сети функции служб не зависят от нижележащих транспортных технологий. Она предоставляет пользователям свободный доступ к операторским сетям и другим поставщикам услуг. Здесь поддерживается обобщенная подвижность, предоставляющая возможность повсеместного и постоянного и обеспечения пользователей услугами связи. Согласно исследованиям, за 2008 год объём трафика Интернет вырос на 61%, а за 2011 год на 85% . В ногу с развитием телекоммуникационных сетей связи развиваются различные IP – услуги: Voice over IP (VoIP),

Internet Protocol Television (IPTV), видео по запросу и т.д. Согласно этим тенденциям, могу предположить, что в мире в ближайшие годы объём IP – трафика резко возрастет, и основную часть этого объема будут занимать сервисы реального времени. Все эти факты приводят к тому, что для пользователей требуется, удовлетворяющий требованиям QoS услуг, канал связи. Требования к каналу связи каждая услуга выдвигает свои, но при этом различные услуги используются в одних и тех же каналах транспортной сети. В связи с этим перед нами встает задача распределения канального ресурса между различными услугами сети. В большинстве случаев, однократное распределение канального ресурса приводит к неэффективному использованию ресурсов канала. Следовательно, ресурсы должны распределяться в сети периодически, зависимо от того, с какой интенсивностью используются различные услуги. Целью оптимизации на канальном, сетевом и транспортном уровнях модели OSI является эффективность упаковки пакетного трафика. Также необходимо отметить, что снижение накладных расходов максимально в случае передачи маленьких пакетов, что обычно имеет место в голосовых приложениях. Очевидным способом снижения объема передаваемого IP- трафика является его сжатие. Однако оно эффективно далеко не для всех типов трафика: *например* голосовая и видеоинформация обычно сжимается соответствующими кодеками, поэтому ее дополнительная компрессия практически ничего не дает. В то же время для типичного Web-трафика эффект может оказаться весьма значителен. Дополнительный эффект обеспечивает компрессия заголовков различных протоколов сетевого и транспортного уровней (IP, TCP, UDP, RTP). Функции качества обслуживания в сетях IP (IP QoS) заключаются в обеспечении гарантированного и дифференцированного обслуживания сетевого трафика путем передачи контроля за использованием ресурсов и загруженностью сети ее оператору. QoS представляет собой набор требований, предъявляемых к ресурсам сети при транспортировке потока данных. QoS обеспечивает сквозную гарантию передачи данных и основанный на системе правил контроль за средствами повышения производительности IP-сети, такими, как механизм распределения ресурсов, коммутация, маршрутизация, механизмы обслуживания очередей и механизмы отбрасывания пакетов. Именно за счет описанных выше функций IP QoS позволит обеспечить необходимое качество услуг реального времени в условиях перегрузок магистрального канала. На рисунке 5 показаны

показатели суточной нагрузки абонентов в течение 3 суток, записанные на действующих пользователях в системе NMS – Network Management System. На графике заметно, что часы наибольшей нагрузки (ЧНН) по времени приходятся на 16:00-18:00 ч., но распределение входящего и исходящего трафика существенно различается. Такой же ЧНН был зафиксирован программой Wireshark (см. приложение А). Абоненты в основном являются пользователем услуги, и их трафик в основном – входящий, относительно реже предоставляет услугу, и меньшая часть трафика соответственно – исходящая. В то же время с точки зрения потребителя WEB- услуга более требовательна к качеству – транспортные задержки вызывают заметный дискомфорт. Услуга IP-телефонии, хотя и требует значительно меньшего трафика, еще более требовательна к качеству – потери и задержки сверх допустимого уровня делают связь вообще невозможной.

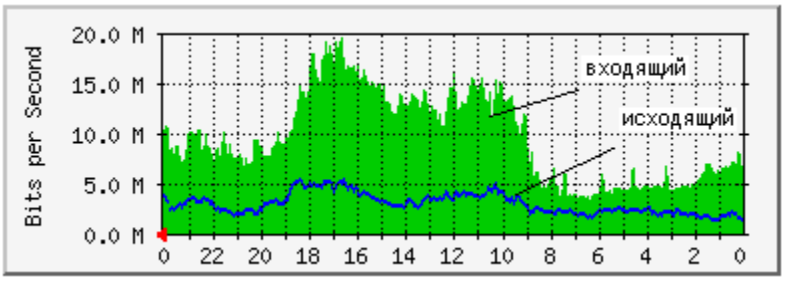

Рисунок 5 – Суточный трафик по системе NMS

Таким образом, формулируется идея основной задачи: обеспечить приоритетное прохождение небольшого по объему, но требовательного к показателям качества трафика перед большим, но нетребовательным пиринговым трафиком. WEB-трафик занимает промежуточное положение между ними. Описание исследуемой системы в исследовании была использована система управления сетью NMS (Network Management System). Используя протокол TCP/IP, NMS взаимодействует с оборудованием через LAN. Также NMS соединен с одним из IP портов инкапсулятора (IPE). Эти соединения позволяют оператору NMS производить проверку и контролировать состояние оборудования, собирать статистические данные, загружать программное обеспечение для всех компонентов сети. Оператор NMS может контролировать и инициировать все возможные действия в сети. Сервер протокола данных (Data Protocol Server (DPS)) выступает в качестве интерфейса между IP сетью пользователя и поставщиком услуг (оператором). Он соединен с одной стороны с IP сетью пользователя и опционально сетью Интернет, с другой стороны с IPE. Сервер DPS построен на карте PowerPC. Для преодоления

проблемы производительности сервер DPS локально обрабатывает пользовательские протоколы (например, TCP), удаляет протокольные заголовки и инкапсулирует только пользовательские данные. В дополнении к ускорению трафика TCP/IP , опционально сервер DPS имеет программный модуль для поддержки улучшенных возможностей, таких как шифрование и сжатие, а также поддержки Virtual Private Network (VPN). На рисунке 6 показана схема
соединения сервера с IP – сетью пользователей.

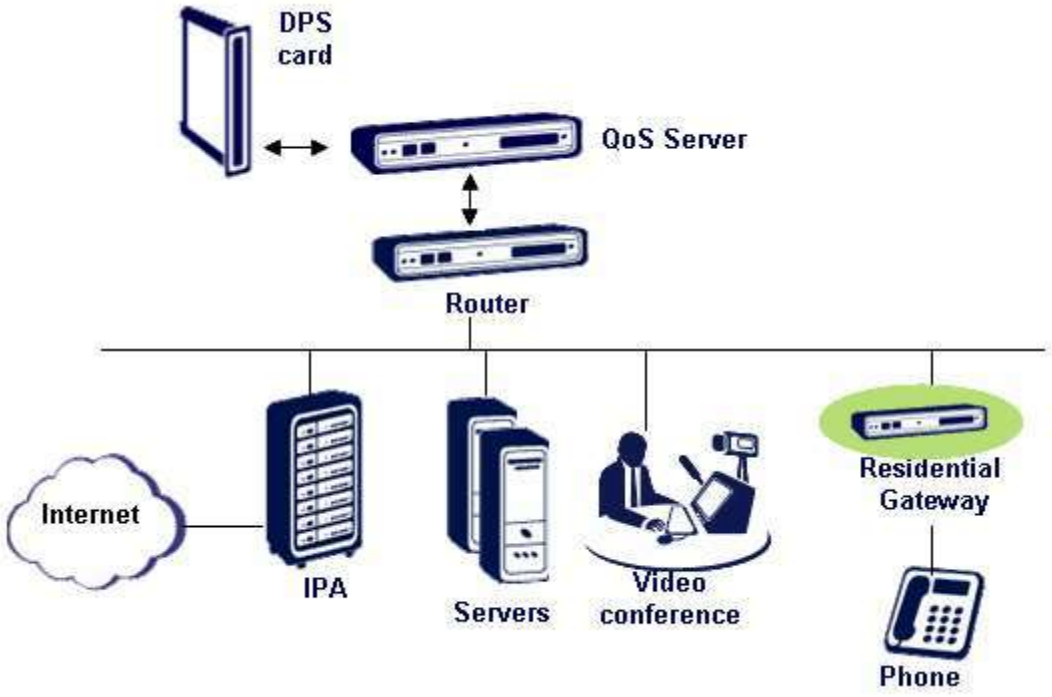

Рисунок 6 – Схема соединения сервера с IP-сетью

DPS направляет пакеты в сеть Интернет через сервер QoS (FairShare) и маршрутизатор. Данные из сети Internet/Intranet проходят через сервер QoS (FairShare) иВпопадают в DPS.

DPS некоторые внутренние служебные протоколы, позволяя системе быть в среде TCP/IP.

Система поддерживает широкий диапазон протоколов связи. Такие общие протоколы маршрутизации, как RIP v1 и v2, протокол DHCP, NAT, IGMP и IRDP. Она также включает набор IP функций позволяющий работать в среде с несколькими IP-устройствами, включая установление приоритетов IP, входящее/исходящее QoS, IP Access Lists и логическую группировку IP.

Сервер DPS представляет собой интерфейс между IP-сетью клиента и сетью
оператора.

Сеть Интернет базируется на “наборе протоколов TCP/IP”. Фактически, его популярность может быть объяснена наличием этих разнообразных протоколов. Разрабатываемый в течение последних трех десятков лет TCP/IP позволяет различным компьютерам (называемым «хосты» на языке TCP/IP), подсоединенным к различным сетям, поддерживать связь друг с другом и обмениваться информацией. Для поддержания всех этих различных сетей, TCP/IP состоит из нескольких протоколов (вот почему он называется набором протоколов), которые работают в модульном режиме. Например, для поддержания сети нового типа должен быть разработан только такой модуль, который имеет прямой доступ в аппаратное обеспечение сети. Также могут быть разработаны новые приложения, обеспечивающие подсоединение к другим модулям. Эта модульность частично несет ответственность за широкое использование TCP/IP. Рассмотрим физическое соединение устройств сети. Интерфейсы DPS и терминала поддерживают IP с использованием подключения к локальной сети Ethernet. В DPS соединение представляет собой интерфейс 100 Base T. В терминале встроенный RJ-45 обеспечивает соединение 100BaseT. Опционально, в некоторые модели терминалов, может быть установлена плата расширения 4-портовый LAN коммутатор, обеспечивающий 4 соединения 100Base T RJ-45. Маршрутизация. Каждый маршрутный компонент, т.е. DPS или терминал, инициирует свою таблицу маршрутизации при запуске. Для каждого маршрутизатора таблицы маршрутизации могут конфигурироваться статически или динамически с использованием протокола RIP. Статическая маршрутизация и динамическая маршрутизация не являются взаимно исключающими.

Протокол маршрутной информации (Routing Information Protocol) – один из самых простых протоколов маршрутизации. Применяется в небольших компьютерных сетях, позволяет маршрутизаторам динамически обновлять маршрутную информацию (направление и дальность в хопах), получая ее от соседних маршрутизаторов.

Протоколом в наборе протоколов TCP/IP, ответственным за надежную сквозную передачу данных, является протокол TCP. Протокол TCP предназначен для предотвращения перегрузки сети, при которой сеть временно не может производить обработку всего трафика от всех хостов, требующих доступа. Для предотвращения перегрузки сети, протокол TCP исследует сеть путем отправки ограниченного количества данных и определения времени, в течение которого эти данные достигают своего места назначения, а потом отправляет дополнительные данные.

TCP предполагает, что большая задержка указывает на затор в сети и для того, чтобы избежать усиления затора, он направляет новые данные в сеть с более медленной скоростью. Каждый терминал действует как маршрутизатор групповой рассылки, периодически отправляя отключенным к нему хостам запросы IGMPv2. DPS действует как хост, реагирующий на запросы IGMP от маршрутизаторов в IP-сети клиента или сети Интернет.

В IGMP DPS составляет список всех поддерживаемых Multicast групп. Для обновления этого списка DPS периодически широковещательно пересылает сообщение с информацией обо всех группах, поддерживаемых в данный момент. Это сообщение по цели схоже с обычным запросом о ринадлежности IGMP. Если терминал получил отчет о принадлежности IGMP (внешнего IGMP) от хоста, направляющего отчеты о принадлежности группе, которая не была включена в сообщение DPS, терминал (после случайного периода времени) направляет сообщение с запросом IGMP.

Система управления сетью (NMS) – это центральный пункт управления,
позволяющий полностью контролировать сеть как локально (на стороне ЦУС), так и удаленно с помощью программного обеспечения «клиент управления».

Все компоненты Центра Управления Сетью имеют «горячий» резерв. Состояние всех компонентов ЦУС отслеживается программным обеспечением с интеллектуальным алгоритмом, которое автоматически переключает управление на резервный компонент в случае выхода из строя основного. Поддержка автоматического резервирования обеспечивает бесперебойное функционирование сети с минимальными перерывами в случае возникновения неисправности. Радиочастотное оборудование и составные компоненты имеют резерв по схеме 1:1, остальные основные компоненты ЦУС резервируются либо по схеме 1:1, либо по схеме 1:N.

Модульное исполнение ЦУС позволяет системному оператору производить замену неисправных компонентов без прерывания трафика в сети. Если какой-нибудь компонент вышел из строя, система управления сетью (NMS) выдаст соответствующее предупреждение, и неисправный компонент может быть заменен в режиме горячей замены (hot-swap), без необходимости выключения всей сети. Нисходящий процесс разработки, уделял огромное внимание вопросам гибкости и модульности всей сети. При разработке и тестировании различных алгоритмов использованы

процедуры соответствия стандарту ISO-9000. Это относится как к алгоритмам передачи голоса, так и к алгоритмам передачи данных, а также и к алгоритмам управления. Разработчики основывались на очень существенной базе, полученной от существующих линий продуктов – хорошо зарекомендовавших себя технологий, которые прошли испытания на разнообразных сетях, в различных конфигурациях и с различными приложениями. Возможности нового программного обеспечения стали результатом добавленных возможностей в NMS, которые заботятся о передаче через систему голоса и данных. Особенности программного обеспечения включают:

1) программное лицензирование - теперь нужно только купить необходимую функцию, и Вы получаете новые возможности и способности системы;

2) удаленная активация лицензии - избавляет от необходимости посещения удаленных станций в случае обновления или добавления новой функции;

3) восстановление предыдущей конфигурации - позволяет вернуться к предыдущей конфигурации рабочей системы, в случае если что-нибудь пойдет не так в момент обновления программного обеспечения.

Система управления сетью (NMS) охватывает каждый компонент системы. Объединяя обе стороны (данные и голос) на одной общей платформе, были улучшены функции управления NMS. Среди мощных функций управления NMS:

1) объединенная, на основе стандарта, архитектура клиент-сервер;

2) годы эксплуатационного опыта стали результатом внедрения следующих средств управления:

-«Template» шаблон - легкое и быстрое копирование существующей конфигурации терминала и любого другого элемента сети;

-«Commit» - определите обновленные параметры, сохраните их и определите

время, когда система применит обновления;

-«Compare» сравнить - сравнение новой и существующей конфигурации элементов и шаблонов;

-полное, непрерывное качество сервиса (End-to-end QoS);

-сосуществование нескольких SLA;вывод

аварийных и информационных сообщений на основе предопределенных правил позволяет производить анализ первичных ошибок на всех компонентах сети;

детализированный CDR—для формирования данных, необходимых биллинговым системам. Компьютер, с установленным программным обеспечением клиента NMS подключается к серверу NMS через локальную сеть LAN. NMS позволяет оператору управлять и контролировать телекоммуникационную сеть. С помощью NMS можно просматривать и модифицировать отдельные компоненты сети. Модель клиент-сервер позволяет осуществлять доступ к системе нескольким операторам.
NMS сервер расположен на стороне оператора, в то время как NMS клиент может работать удаленно. Пользовательский интерфейс NMS используется для конфигурации сети, управления пользователями, контроля и управления сетью, предоставляет аварийные сообщения и события сети, сбор статистики, сбор сообщений сети и генерирование LOG и CDR файлов.

Администратор сети может настроить разные уровни доступа для операторов, позволяя различным операторам осуществлять операции контроля и конфигурации сети согласно их уровню доступа.

NMS позволяет оператору конфигурировать и контролировать DPS.

Система NMS имеет иерархический, объектно-ориентированный удобный пользовательский графический интерфейс GUI (Graphical User Interface). Иконки и окна представляют сетевые компоненты и группы. При необходимости оператор может переносить сетевые элементы между группами. Иконки используются для взаимодействия с компонентом, включая конфигурацию, передачу команд, опрос статуса, сбор статистики и предоставление отчетов. Если компонент состоит из подкомпонентов, доступ к этим компонентам происходит через компонент верхнего уровня. Цвет иконки сообщает текущий статус компонента.

Очень высокий уровень эффективности передачи поддерживается автоматической адаптацией к изменениям в типе трафика и загрузке (без вмешательства оператора). Этот механизм адаптации также помогает поддерживать стабильность канала, несмотря на увеличение загрузки трафика.

Клиент-серверная система управления сетью (NMS) дает операторам возможность осуществлять централизованное многозадачное управление и контроль над всей сетью связи. Оператор может просматривать, модифицировать и загружать отдельные элементы конфигурации сети. Доступ к серверу NMS осуществляется через однородный пользовательский интерфейс, запускаемый на удаленном клиенте сети. Функциональные возможности NMS обеспечивают конфигурацию сети,

управление со стороны оператора, мониторинг и контроль сети, отображение аварийных сигналов и событий, сбор статистики, журнальную регистрацию событий, а также сбор Записей Данных о Вызове (CDR) для биллинга.

Сетевой администратор назначает уровни авторизации, таким образом операторы выполняют только разрешенные действия по мониторингу, контролю или конфигурированию сети. Они могут просматривать, модифицировать или загружать конфигурационные элементы для системы.

Репозиторий программного обеспечения - сохраняет все определенные в системе версии программного обеспечения в NMS. Информация о версии программного обеспечения состоит из: номера версии, программного обеспечения и файлов XML, в которых описана конфигурация сети.

Все конфигурационные изменения элементов сети хранятся в базе данных NMS. Оператор может редактировать эти изменения, по необходимости, а операция Commit (выполнить) приводит их в исполнение. Функциональные возможности включают в себя операцию отмены изменений и возможность планирования времени выполнения операции. Каждый элемент имеет показатель состояния выполнения.

Дополнительные инструменты конфигурирования:

- экспорт/импорт - конфигурация элемента в/из файла;
- дублирование - возможность дублирования элемента сети;
- сравнение - позволяет производить сравнение определений и значений между: существующими элементами, версиями, конфигурации существующих и новых элементов, выполненных конфигурационных изменений с невыполненными изменениями;
- «Мастер» конфигурации (Configuration wizards)— позволяет легко и просто конфигурировать элементы сети.

NMS предоставляет данные о параметрах конфигурации телеметрии и состоянии элементов сети, позволяя идентифицировать конфигурационные ошибки и изменения состояния компонентов сети. Статистическая информация о трафике и порте может быть собрана NMS и предоставлена оператору.

Мультисервисная СПД включает в себя улучшенную систему управления неисправностями (см. рисунок 7), которая позволяет наблюдать за сетью и сообщениями в NMS.

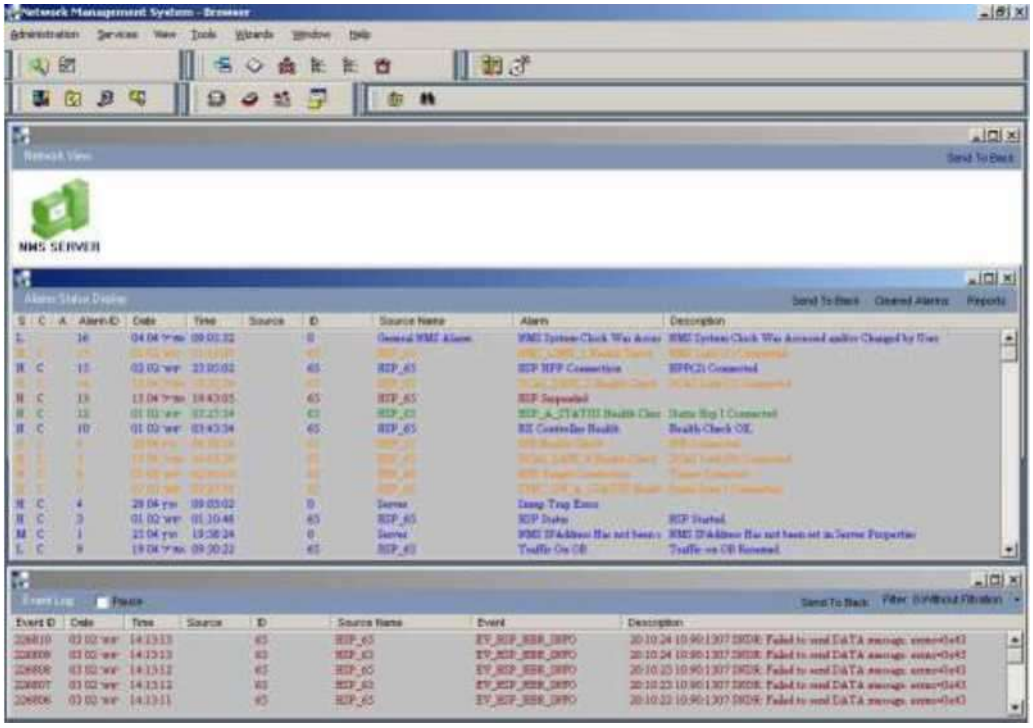

Рисунок 7 - Управление неисправностями в системе NMS

Некоторые характеристики системы управления неисправностями:

- аварийные сообщения и события показывают любые изменения в состоянии элемента сети в виде графической иконки с цветовой кодировкой и текста;
- основанный на системе правил (rule-based reasoning (RBR)) метод состоит из фактов (событий) и правил (базы знаний);
- анализ основных причин определяет взаимоотношение между событиями на основании правил, анализируя основную причину, и инициирует только соответствующие аварийные сообщения;
- фильтрация отображения событий браузера упрощает просмотр и управление браузером, используется в тех случаях, когда скорость происхождения событий высока, либо администратор желает отфильтровать несущественные или не имеющие отношения события.

Клиент может выбрать приобретение различных вариантов, исходя из нужд конечного пользователя. После первичного развертывания сети можно с легкостью добавить дополнительные опции, просто активизируя их посредством соответствующего ключа для лицензирования программного обеспечения. Механизм лицензирования программного обеспечения использует файл лицензии для идентификации NMS основного компьютера и лицензирования опции программы.

Автоматическое резервирование базы данных планируется на определенное время и с частотой, удобной для каждого пользователя. Подобное резервирование прозрачно (выполняется без вмешательства оператора или прерываний в сети). Резервирование рекомендуется осуществлять в ночное время для получения надежной и новейшей конфигурации на случай необходимости перезагрузки старой базы данных.

Поддержка Простого Протокола Управления Сетью (Simple Network Management Protocol (SNMP)) позволяет сети взаимодействовать с управляющими системами сторонних сетей и создавать единую точку управления.

Сервер NMS работает под управлением операционной системы Windows 2003 на базе cPC1. Клиент NMS работает под управлением операционной системы Windows XP Professional на базе ПК. Отличительной чертой NMS является наличие ReportEdge - сервера отчетов на основе Web, который запускается на выделенном компьютере:

- предоставляет Web-доступ к комплексу отчетов, которые могут быть активированы через базу данных NMS. Отчеты можно просмотреть, распечатать или сохранить в файл в нескольких стандартных форматах;
- отчеты включают в себя данные анализа состояния сети, событий, аварийных сообщений и статистику;
- активация отчета может быть инициирована пользователем или запланирована;
- ReportEdge отличается наличием базы данных с историей отчетов.

Всегда имеются пакеты, которые слишком маленькие или слишком большие для точного соответствия размеру оптимизированного временного интервала. При использовании улучшенного формирования пакета фактический фактор заполнения временных интервалов увеличивается на 5% - 15%, в зависимости от трафика сети. Улучшение особенно эффективно в сетях с несколькими приложениями в каждом узле или в сетях доступа к Интернет с несколькими ПК в узле.

Для поддержания приложений с большим потоком данных, например, видеоконференцсвязь или загрузка файлов, система поддерживает режим потока данных. Пакеты пользователя располагаются каскадом один за другим и затем фрагментируются так, что они точно соответствуют величине временного интервала. Последние байты одного пользовательского пакета могут быть включены в начало следующих

пакетов, тем самым, уменьшая общее количество пакетов и удельный вес служебной информации в потоке пользовательских данных.

Для приема IP пакетов от компонентов сети, маршрутизатор использует четыре типа интерфейсов (портов):

- IP Forwarding - стандартный порт, который действует также как и любой коммутатор 3-го уровня - направляет пакеты по из назначению, основываясь на сконфигурированных подсетях или таблице маршрутизации;
- Ethernet IP Forwarding In - этот порт принимает IP пакеты. Основываясь на таблице перенаправления, определяется, какие пакеты инкапсулировать в формат MPE. Порт IP Forwarding In выступает входящим портом для перенаправления трафика типа: Sync и MC&C (Management, Command & Control);
- UDP-In - этот порт использует UDP туннель для передачи потока данных, очень схоже с взаимодействием между DPS и HSP. Отправитель посылает трафик на специфический UDP порт. Порт UDP In служит логическим портом для приема голосовых пакетов для последующей их передачи;
- TCP-In - принимает данные, которые будут переданы через TCP соединение. Это обеспечивает надежность передачи данных и контроль потока данных через стандартные механизмы TCP.

Если происходит конфликт, пакеты данных передаются повторно (при отсутствии подтверждения получения через определенный промежуток времени) на произвольно выбранной частоте в последующий временной интервал для целей максимального уменьшения вероятности второго конфликта. Этот режим работы с использованием произвольного доступа подходит для интерактивного трафика, который характеризуется короткими сообщениями и небольшой загрузкой канала.

Полоса пропускания, выделенная для сети, первоначально основывается на анализе трафика и пересматривается по мере необходимости в целях соответствия новой нагрузки сети или требованиям производительности.

Рассмотрим, как устанавливаются IP приоритеты.

В то время, как желательно предоставление всем пользователем в сети наилучшего качества услуг, ресурсы для этой цели могут быть не всегда доступны. В этих случаях качество ухудшается. Система позволяет оператору сети устанавливать приоритеты IP- трафика так, что приложения, наиболее восприимчивые к ухудшению качества (или более

важные) будут иметь приоритет по сравнению с остальными приложениями.

Поддерживается два уровня приоритетов: высокий и низкий. Когда для доступа к каналу соперничают трафик высокого и низкого приоритета, DPS передаст вначале некоторое количество пакетов с высокой приоритетностью, а затем меньшее количество пакетов с низкой приоритетностью.

IP-трафик может получить высокий приоритет на основе различных критериев:

- протокол: TCP, UDP, ICMP и IGMP;
- номер порта назначения TCP или UDP, или диапазон портов;
- до десяти комбинаций исходного IP-адреса и протокола.

При установлении соединения TCP ведет себя как хороший игрок, он не хочет наводнять сеть данным, которые могут не поступить на другой конец соединения, известно под названием «зондирование сети».

Сначала, как только установлено соединение, TCP отправляет один пакет данных и ожидает их подтверждения. Размер окна передачи устанавливается равным 1 (размер окна в TCP выражается в байтах, таким образом, фактическим значением является количество отправленных байтов; в большинстве случаев максимальный размер сегмента, разрешенный канальным уровнем (для ясности, размер окна) будет выражен в пакетах). Если прием первого пакета подтверждается, TCP направляет два пакета, устанавливая окно передачи равным 2 и ожидает АСК. По мере продвижения процесса размер окна увеличивается вдвое каждый раз. Как видно, «медленный старт» не является таким уж медленным, увеличиваясь экспоненциально. Для передачи файлов большого размера или других приложений это может быть несущественным, но при работе интерактивных приложений такая задержка весьма досадна. Например, web-браузер открывает новое TCP соединение для каждого объекта на странице; для небольших графических файлов передача будет завершена до того, как окно достигнет своего максимального размера. В конце концов, все эти миллисекунды складываются вместе к неудовольствию пользователя.

Если утери пакетов не происходит, окно будет увеличиваться до размера, который готов принять принимающий конец соединения с возможным ограничением размером буфера. Количество данных, которое готов принять принимающий конец соединения называется окном приема; оно используется TCP для контроля потока. Окно приема это не только

счетчик, поддерживаемый каждым хостом, но фактически это 16-битное поле в заголовке TCP (где оно называется просто окном).

Если пакеты были утеряны или повреждены, для исключения проблемы перегруженности размера окна используется второй метод. Это другой, более сложный и медленный способ увеличения размера окна, который замедляется длительными задержками, связанными с подтверждением приема. Так как TCP является сквозным протоколом, этот механизм применяется тогда, когда пакеты утеряны где-либо на всей протяженности канала.

3.2 Описание проделанных экспериментов

Эксперимент был проведен на сети алматинского провайдера доступа в мультисервисную СПД. Компания обеспечивает доступ в Интернет, оказывает услуги передачи речи по протоколу IP, видеоуслуги (видеоконференции по протоколу IP) для корпоративных клиентов. Схема измерений трафика представлена на рисунке 8.

Рисунок 8 - Схема измерений трафика на СПД провайдера

Поступающий на маршрутизатор трафик зеркалируется на порт, к которому подключен сервер с активированной программой Wireshark 1.8.0. Общая продолжительность измерений на сети провайдера составила 3 суток, в течение которых были зафиксированы данные о восьми миллиардах пакетов. Файлы данных размером по 200 Мбайт поочередно обрабатываются утилитой TShark, входящей в состав пакета Wireshark. Для суточного интервала собранной статистики был выбран час наибольшей нагрузки (ЧНН) по количеству передаваемых байт по протоколу http.

На рисунке 9 представлено распределение объемов трафика по

типам транспортных протоколов (OSI Layer4). Как видно из рисунка, наибольший объем трафика передается с использованием стека TCP/IP (67,88%), на долю UDP/IP приходится 31,23%. Эти данные были также сняты программой Wireshark (см. приложение Б).

Дальнейший анализ проведен раздельно по приложениям, использующим TCP/IP и UDP/IP (приложение В). Картина распределения протоколов использующих стек TCP/IP представлена на рисунке 10.

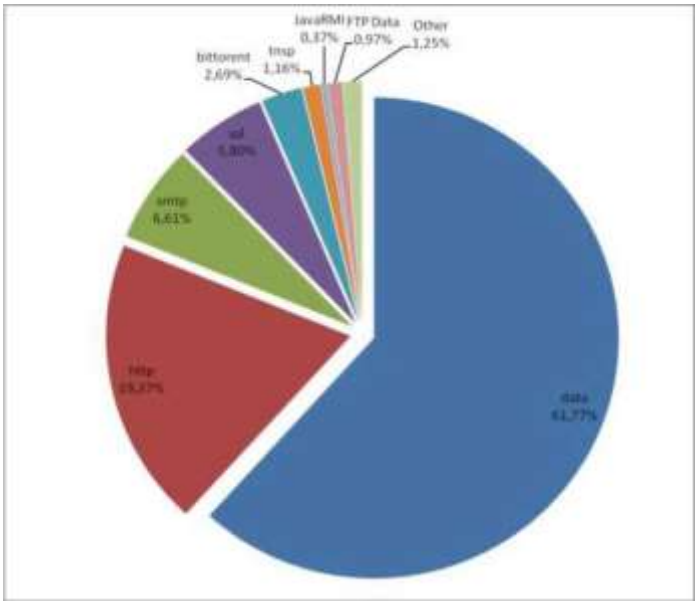

Рисунок 10 - Распределение объемов данных по приложениям, использующим стек TCP/IP

Из представленной диаграммы видно, что электронная почта занимает в общем объеме 12,41% (по протоколам smtp и ssl), данные (data) - 61,77%, объемы данных обмена сетей класса Peer-to-Peer (bittorrent) - 2,69%, тогда как данные по протоколу прикладного уровня передачи данных http составляют по меньшей мере 19,37%, доля http-трафика превысила долю Peer-to-Peer-сетей, из которых почти половина - это передача потокового видео и звука. Основную часть данных такого трафика составляет просмотр пользователями www страниц и передача файлов при помощи протокола http.

Рассмотрение потоков на уровне пакетов проведено с учетом используемого стека протоколов. Выяснилось, что в численном выражении короткие пакеты составляют большую долю от общего числа переданных пакетов, поэтому целесообразно отнормировать количество пакетов конкретной длины в соответствии с объемом переносимых данных. На

рисунке 11 представлена диаграмма распределения длин пакетов приложений, использующих стеки TCP/IP и UDP/IP.

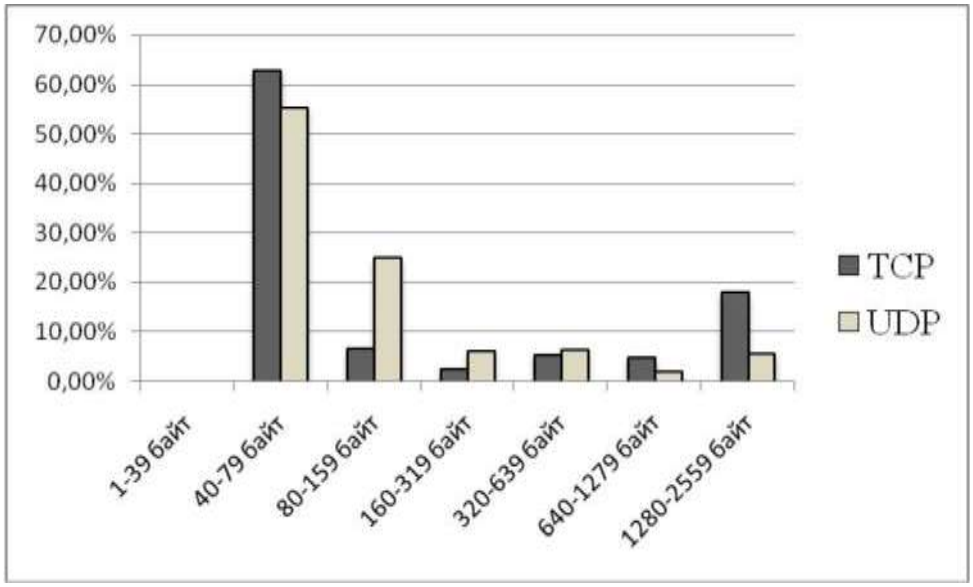

Рисунок 11 - Распределение передаваемого трафика по длинам
IP пакетов для стека
TCP/IP и UDP/IP

Как видно из представленной диаграммы, более 60% передаваемых объемов данных по стеку TCP/IP переносится пакетами размером 40 - 80 байт. Анализ распределения длин пакетов для приложений, использующих стек UDP/IP, показывает, что большая часть данных (более 50%) переносится пакетами длиной также 40-80 байт, а в целом около 80 % переносится пакетами размером 40-160 байт. Действительно, большую часть потока этих приложений составляют телефонные вызовы VoIP с применением кодека G.723.1, длина пакета для которого составляет: 20-24 байт (речь - 30 мс) + 20 байт (заголовок RTP) + 16 байт (заголовок UDP) + 20 байт (заголовок IP) = 80 байт. Таким образом, при определении политик обеспечения QoS следует ориентироваться на длины пакетов, переносящих большую долю трафика данного приложения.

Влияния длины блока данных на качество передаваемых пакетов данных. Для этого длину окна для приема блока данных уменьшили до 160 байт. Длина окна устанавливается на сервере DPS (Data Protocol Server - сервер протокола данных) посредством системы управления сетью NMS (Network Management System). Проведен анализ влияния размеров блока данных на количество ошибочных пакетов. В приложении Г представлено,

какого типа наблюдаются ошибки. Результаты эксперимента приведены на рисунке12.

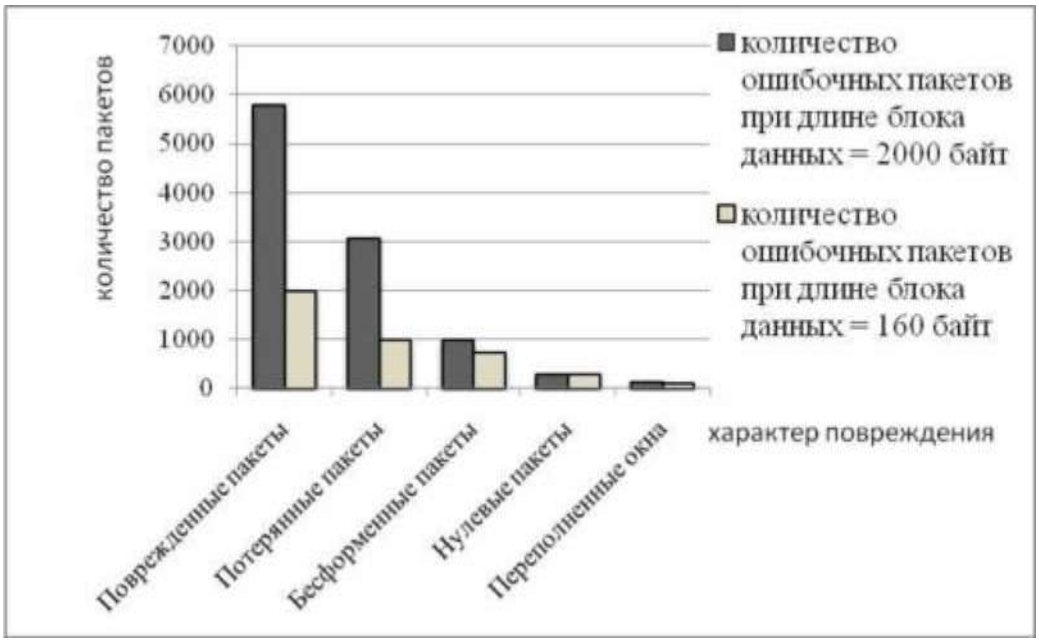

Рисунок 12 - Анализ влияния размеров блока данных
на количество ошибочных
пакетов

Из рисунка 12 видно, что с уменьшением размеров блока данных количество поврежденных и потерянных пакетов снизилось почти в три раза.

Исследования показали, что около 80% передаваемых объемов данных по стекам TCP/IP и UDP/IP переносится короткими пакетами (40 - 160 байт), основную часть которых составляет передача потокового видео и звука при помощи протокола http. Количество ошибочных пакетов заметно сократилось при уменьшении размеров блока данных. В результате можно утверждать, что наблюдается улучшение качества предоставляемых услуг в мультисервисных СПД.

3.3 Расчет теоретических значений параметров QoS работы сети

Современная тенденция конвергенции различных типов сетей привела к необходимости переноса сетью различного вида трафика.

Характеристики QoS (Quality of Service) особенно важны в случае, когда сеть передает одновременно трафик различного типа, например, голосовой трафик и трафик web- приложений. Это связано с тем, что различные типы трафика предъявляют разные требования к характеристикам QoS.

В связи с тем, что постоянно увеличивается объем мультисервисной

информации (данные, голос, видео), передаваемой в современных мультисервисных СПД, возрастают требования к качеству обслуживания трафика, генерируемого пользователями, абонентскими системами и самой сетью.

Значимыми характеристиками в тесте QoS являются следующие параметры:

- Круговая задержка (round trip delay);
- Колебание пакетов (jitter);
- Потеря пакетов (packet lost).

Для расчета временной задержки на сети учитываются такие параметры как длина оптического кабеля и его тип, потери в волокне, данные по дисперсии, отношение оптический сигнал/шум, частота и уровень канала, тип и параметры оборудования, в том числе транспондеров, количество сетевых элементов и точек регенерации.

Основная величина задержки вносится длиной оптического кабеля. Задержка, вносимая оборудованием, незначительно отражается на общей величине временной задержки канала.

Измерение указанных параметров может производиться для разных классов сервиса: real-time (реального времени), business critical (критичный для бизнеса) и best effort (наилучшей попытки).

Рассчитаем теоретические значения параметров QoS. Расчетные параметры QoS могут быть использованы при заключении соглашения об уровне обслуживания (SLA) со сторонними операторами в обеспечении заданного качества обслуживания в сквозном соединении (end-to-end) для различных видов трафика.

Необходимо определить следующие параметры:

- круговая задержка;
- задержка распространения;
- время ожидания пакета в очереди на маршрутизаторе;
- задержка, вносимая активным оборудованием;
- потеря пакетов;
- колебание пакетов (jitter).

1) Круговая задержка

Круговая задержка (RTD - round-trip delay) - это суммарное время, требуемое для передачи пакета от источника до получателя и обратно.

В общем случае круговая задержка включает в себя следующие виды задержек:

- задержка распространения сигнала;
- ожидание пакета в очереди на маршрутизаторе;

- задержка, вносимая активным оборудованием.

При условии, что маршрутизация симметричная (использование одного маршрута от источника до получателя и обратно) и проходит по кратчайшим путям, круговая задержка рассчитывается следующим образом:

RTD = 2(Op + EDQi + XOa.eO, (7)

где RTD - круговая задержка;

Df, - задержка распространения;

DQ - время ожидания пакета в очереди на маршрутизаторе;

Da.a - задержка, вносимая активным оборудованием.

1) Сначала рассчитаем задержку распространения (D_p).

Задержка распространения сигнала зависит от протяженности маршрута и скорости распространения светового потока в оптическом волокне. Таким образом, задержка распространения равна:

Dp = Rk/C, (8)

гдеDp - задержка распространения (с);

C - скорость света в вакууме (м/с);

R - протяженность маршрута (м);

k - коэффициент преломления материала сердечника оптического волокна, значение которого лежит в пределах от 1,45 до 1,55 (ближе к 1,5).

Рассчитаем задержку распространения на 3000 км, при k= 1,5:

$$D_p = Rk/C = 310^6 \text{ м } 1{,}5 / 310^8 \text{ м/с} = 1{,}5 \bullet 10^{-2} \text{ с} = 15 \text{ мс},$$

В случае если протяженность маршрута R неизвестна, то значение R можно рассчитать с использованием коэффициентов, которые оцениваются из D (air distance - прямое расстояние между узлами), в соответствии с рекомендацией ITU (G.826), в которой указано (см. таблицу 7):

Т а б л и ц а 7 - Расчет R в соответствии с рекомендацией ITU (G.826)

D	R
D<1000 км	R=1,5D
1000 км < D < 1200 км	R=1500 км
D > 1200 км	R=1,25D

1) Рассчитаем время ожидания пакета в очереди на маршрутизаторе (DQ)

Время ожидания пакета в очереди на маршрутизаторе (DQ) рассчитывается по формуле:

$$Dq = (b/r) \bullet (1/1\text{-}u), \quad (9)$$

где b - средняя длина пакета (бит);

r - скорость передачи канала (бит/с);

u - средний коэффициент использования канала.

При скорости 100 Мбит/с, длине пакета 2000 байт = 16 000 бит и среднем коэффициенте использования канала равным 0,9 время ожидания пакета в очереди составляет:

$$D_q = (16\ 10^3/10^8) \bullet (1/(1\text{-}0{,}9)) = (16/10^5)\ 10 = 1{,}6 \text{ мс}$$

При скорости 100 Мбит/с, длине пакета 160 байт = 1280 бит и среднем коэффициенте использования канала равным 0,9 время ожидания пакета в очереди составляет:

$$Dq = (1280/10^8) \bullet (1/(1\text{-}0{,}9)) = (128/10^7)\ 10 = 0{,}128 \text{ мс}$$

Чем меньше длина пакета, тем меньше время ожидания пакета в очереди.

Это относится к одному маршрутизатору на пути от источника до получателя. В целом, задержки на маршрутизаторах всегда меньше 1 мс, если каналы не перегружены.

2) Найдем задержку, вносимую активным оборудованием (D_{ae}).

Задержка, вносимая активным оборудованием (Da.e.) - это суммарное значение задержек вносимых следующим оборудованием:

- компенсаторами дисперсии;
- транспондерами;
- 3R регенераторами;
- другим активным оборудованием.

Значения задержек, вносимые активными элементами сети и используемые для расчета, приводятся поставщиками в технической документации к оборудованию.

$$^{D}\text{a.e. общ.} = {}^{D}\text{a.e. 1} + {}^{D}\text{a.e. 2} + \bullet\bullet\bullet + {}^{D}\text{a.e. n} = \wedge\ {}^{D}\text{a.e.i} \quad (10)$$

Например, для оборудования Cisco данные по задержке, вносимой компенсаторами дисперсии следующие (см. таблицу 8):

Т а б л и ц а 8 - Задержка в волокне компенсаторов дисперсии

DCM module	Propagation delay (ps)
DCM-2.5	1
DCM-5	3
DCM-7.5	5
DCM-10	7
DCM-20	15
DCM-30	22
DCM-40	30
DCM-50	38
DCM-60	45
DCM-70	53
DCM-80	61
DCM-90	68
DCM-100	76

Задержка, вносимая транспондером, зависит от того, является ли транспондер одновременно и концентратором (мукспондер - TRBC) и характера клиентского сигнала (размещен ли клиентский сигнал в OTU или нет). Вносимая задержка берется из следующих данных:

- TRBD UNI = 150 ps (пример OTU2 линейный интерфейс, STM64/10GE клиентский интерфейс);
- TRBC UNI = 150 ps (пример OTU2 линейный интерфейс, STM16 клиентский интерфейс);
- TRBD NNI = 160 ps (пример OTU2 линейный интерфейс, OTU-2 клиентский интерфейс);
- TRBC NNI = 175 ps (пример OTU2 линейный интерфейс, OTU-1 клиентский интерфейс);
- Задержку на транспондере нужно считать на всех транспондерах от клиентского до клиентского интерфейса: на приеме, на передаче, на промежуточных R3 регенераторах.

3) Рассчитаем потерю пакетов. Уровень потери пакетов определяется количеством пакетов, отбрасываемых сетью во время передачи. Одними из основных причин потери пакетов являются перегрузка сети и повреждение пакетов во время передачи по линии связи. Также отбрасывание пакетов может быть вызвано недостаточным размером входного буфера.

$$K_{потерь} = N_{потерь}/(N_{потерь}+N_{получ}) \cdot 100\%,$$

Коэффициент потери пакетов определяется следующей формулой:

Где $N_{отерь}$ - количество потерянных пакетов;

$N_{олуч}$ - количество пакетов, полученных успешно.

Количество переданных пакетов 115303, потерянных (или поврежденных) - 488, при этом количество доставленных пакетов 114800 (Приложение Г), то коэффициент потери пакетов будет следующий:

$$K\ потерь = 488/(488+114800) \bullet 100=0{,}004 \bullet 100\% = 0{,}4\ \%$$

4) Колебание пакетов (jitter)

Параметр определяется в RFC 3393 как разница сквозных задержек прохождения двух пакетов. Значение jitter для i-ого и j-того пакетов будет рассчитываться как:

$$Dij = (Rj - Ri) - (Sj - Si) = (Rj - Sj) - (Ri - Si), \quad (12)$$

где R - время отправки пакета (с);

S - время его доставки (с).

3.4 Определение скорости обслуживания с применением теории массового обслуживания

Модель системы массового обслуживания (СМО) является одной из основных моделей, которые используются инженерами-связистами. Она рассматривается в теории очередей или в теории массового обслуживания. В этой области первые работы были вызваны потребностями практики, особенно широким развитием телефонных сетей. Следовательно, в теории массового обслуживания распространена терминология, заимствованная из телефонии (заявки, требования, каналы обслуживания, вызовы и т.д.).

Теория СМО связана непосредственно с математическими моделями (с их разработкой и анализом), описывающими процесс обслуживания некоторых объектов, которые поступают в виде некоторого потока на входное устройство обслуживающего прибора, и в общем случае

образующего там очередь.

В связи с тем, что рассматриваются абстрактные (математические) модели, природа обслуживаемых объектов абсолютно не важна, а также их физические свойства (будут ли это вызовы, информационные кадры в сетях связи либо покупатели в магазине). Важным являются правила и математические законы обслуживания этих объектов, моменты их появления, так как от этих законов и моментов зависит, адекватно ли отобразится эволюция моделируемого объекта во времени. Следовательно, методы анализа очередей предполагают абстрактные (математические) модели, а из контекста мы всегда должны понимать, исследуя какую реальную систему необходимо применять эти модели.

Использование системы массового обслуживания как модели преследует цель анализа качества функционирования вышеуказанных оригинальных систем.

Сети массового обслуживания (СеМО) используются для определения наиболее важных системных характеристик инфокоммуникационных систем: времени доставки пакетов, производительности, вероятности блокировки в узлах сети и потери сообщений, допустимые значения нагрузки, при которых выполняется обеспечение требуемого качества обслуживания QoS и др.

Фундаментальным в теории СеМО является понятие состояния сети. Важнейшей характеристикой СеМО являются вероятности их состояний. Чтобы определить вероятности состояний СеМО необходимо исследовать случайный процесс, протекающий в сети. За модели протекающих процессов в СеМО чаще всего используются марковские и полумарковские.

Функционирование экспоненциальных СеМО описывает марковский процесс с непрерывным временем. Экспоненциальная сеть - это сеть, в которой входящие в каждую СМО потоки требований пуассоновские, а время всех этапов обслуживания, которое реализуется на любой СеМО, имеет экспоненциальное распределение. Следовательно, можно считать, что этапы обслуживания не зависят друг от друга, от параметров входящего потока, от состояния сети, даже от маршрутов следования требований.

Теория экспоненциальных СеМО наиболее разработана. Она широко применяется как для исследования СПД, так и для исследования мультипроцессорных вычислительных систем (ВС). Глубокий анализ немарковских моделей систем связи представляет собой значительные трудности, которые обусловлены, прежде всего, отсутствием независимости длительности требований в различных узлах модели систем связи с нестандартными дисциплинами. При достаточно реалистической, на первый

взгляд, догадке о том, что длина требования сохраняется постоянной в процессе передачи его через сетевые узлы, необходимо отслеживать путь каждого требования, что представляет невозможным аналитический расчет характеристик для сети с количеством узлов M>2.

Анализ, посвященных расчету или исследованию немарковских моделей, работ показал, что решения алгоритмически получаются, применяя сложные численные расчеты с методом преобразований Лапласа-Стилтьеса. Реализация программная, решения очень трудоемкие, при большой и средней нагрузке имеют место значительные погрешности при оценке показателей производительности инфокоммуникационных систем (ИС). В связи с вышеизложенным, для моделирования СеМО, которые выходят из класса мультипликативных, используются приближенные методы.

Аналитические методы расчета характеристик инфокоммуникационных систем базируются на анализе экспоненциальных СеМО. Используя данный математический аппарат, можно прийти к аналитическим моделям для решения большого круга задач исследования СМО.

СеМО, прежде всего, представляют собой совокупность взаимосвязанных СМО. Вспомним основные особенности этих систем.

Требования (заявки) на обслуживание поступают через случайные или постоянные интервалы времени. Каналы (приборы) используются для обслуживания этих заявок. Процесс обслуживания длится некоторое постоянное или случайное время. Когда заявка поступает и в это время все каналы заняты, то она отправляется в буфер и ожидает начала обслуживания. Заявки, которые находятся в буфере, образуют очередь на обслуживание. В случае если ячейки буфера все заняты, то система отвечает заявке отказом в обслуживании и она теряется. Одной из основных характеристик СМО является вероятность отказа (вероятность потери заявки). Существуют также и другие характеристики СМО, такие как коэффициент загрузки прибора (доля времени, в течение которого прибор занят обслуживанием), средняя длина очереди, среднее время ожидания начала обслуживания и т.д.

СМО различают по объему буфера: СМО смешанного типа, где буфер имеет конечное число заявок, СМО с ожиданием, где буфер не ограничен и с отказами, где отсутствует буфер. В СМО с ожиданием - нет потерь заявок, в СМО с отказами отсутствуют очереди, в смешанном СМО возможно и то и другое.

Заявки также различают по их важности, т.е. по приоритету. В первую очередь обслуживаются заявки с более высоким приоритетом. Абсолютный приоритет дает возможность остановить на некоторое время обслуживание

неважной заявки, а также в приборе или в буфере занять ее место. Вытесненная заявка теряется или в буфере ждет, когда ее обслужат. Но при этом уже нужно возобновить обслуживание ранее вытесненной заявки сначала, не продолжая с точки прерывания. Однако, если заявка из буфера вытеснена, она, конечно, теряется. В вычислительных системах, к примеру, абсолютный приоритет имеют команды оператора. Относительный же приоритет дает право первым занять освободившийся прибор. Однако он не дает право вытеснять заявку из буфера или прибора. Относительный и абсолютный приоритеты различаются также моментом действия: относительный реализуется, когда освобождается прибор,а абсолютный - в момент поступления.

Бывают фиксированные и динамические приоритеты. Чаще всего фиксированные приоритеты называются дисциплиной обслуживания. Она задает порядок выбора заявок одинакового приоритета в освободившийся прибор из очереди. Выделим следующие основные дисциплины: RAND (Random): случайный выбор из очереди, LIFO (Last Input - First Output): последним пришел - первым обслужен, FIFO (First Input - First Output): первым пришел - первым обслужен. В бытовых условиях чаще всего имеет место дисциплина FIFO.

LIFO осуществляется в буфере, который организован по принципу стека. Эта дисциплина может быть целесообразной, к примеру, при передаче информации, если ее ценность со временем быстро падает.

В теории СМО немаловажное место занимает понятие случайного потока. Случайный поток - это некоторая последовательность событий, наступающих в случайные моменты времени. Он обычно задается функцией распределения величины интервала (промежутка) между временами наступления событий.

Отметим, что в пуассоновском потоке отсутствуют последействия. Если помимо этого выполняются условия ординарности и стационарности, то пуассоновский поток считается простейшим.

Известно, что распределение для стационарного потока не зависит от положения интервала на оси времени и зависит только от его длительности. Отсутствие последействия говорит о независимости количества событий в неперекрывающихся интервалах. Свойство ординарности состоит в том, что вероятность появления больше одного события на бесконечно маленьком интервале имеет порядок малости выше, нежели вероятность появления одного события на этом же интервале.

В сети передачи данных, не ориентированной на соединение, каждый пакет доставляется индивидуальным маршрутом, и передача пакета

считается завершенной только после получения подтверждения о его приеме. Сеть состоит из двух узлов и соединяющих их дуплексных каналов. Для сопоставимости результатов с сетью с коммутацией каналов будем считать полную интенсивность потока во входящем узле, равной X, пропускную способность дуплексного канала между узлами положим равной $Ст=NC_L$ в каждом направлении, где величина ^ определяет максимальную скорость доступа к узлу от индивидуального абонента (пропускная способность абонентской линии). В этой сети принципиально отсутствуют расходы времени на установление соединения, однако, в качестве накладных расходов выступает время на получение подтверждений о приеме пакета.

Рассмотрим два способа передачи подтверждений. Первый состоит в передаче от узла. В отдельных пакетах с информацией о подтверждении, а второй предполагает, что в информационные пакеты обратного направления встраиваются специальные поля битов подтверждения о приеме пакетов встречного направления.

Рассмотрим сначала первый способ. Пусть каждый принятый пакет генерирует отдельное подтверждение фиксированной длины L_I бит. Тем самым в каждом узле образуется поток пакетов переменной длины, состоящих из некоторого фиксированного поля длины L_I и поля случайной длины со средним значением m_c. Такие пакеты поступают в очередь на входном узле и обслуживаются в порядке поступления.

Очевидно, что здесь мы должны использовать модель СМО с произвольным распределением времени обслуживания в силу специфики структуры пакетов. Поставим задачу: найти среднее время отклика T_D от узла до узла, используя модель M/G/1.

Техника безопасности

Охрана здоровья трудящихся, обеспечение безопасных условий труда, ликвидация профессиональных заболеваний и производственного травматизма – одна из главных забот нашего государства. Состояние условий труда, при котором исключено воздействие на работающих различных опасных или вредных производственных факторов, принято называть безопасностью труда. Охрана труда – это система социально-экономических, технических, санитарно-гигиенических и организационных мероприятий обеспечивающих безопасность, сохранение здоровья и работоспособности человека в процессе труда.

Организует работу по охране труда на предприятии инженер по технике безопасности. Он назначается выше стоящим органом, подчиняется главному инженеру и руководителю предприятия. В его обязанности входят следующее:

разрабатывать мероприятия по охране труда;

обучение персонала и принятие экзамена по технике безопасности;

расследование несчастных случаев;

проведение инструктажей по технике безопасности и контроль за вопросами охраны труда;

допуск к работе и проверка наличия соответствующих документов, и т.д.

на предприятиях проводятся в установленное время инструктажи по технике безопасности, которые делятся на:

вводный инструктаж, проводится при приёме на работу нового человека;

инструктаж по ТБ на рабочем месте, проводятся с вновь поступающими на работу под роспись в журнал;

повторный инструктаж по ТБ, проводится через определённый период времени;

внеплановый инструктаж по ТБ, проводится как правило в отрасли в целом при несчастных случаях со смертельным исходом и направлен на предупреждение подобных фактов в отрасли;

целевой инструктаж по ТБ, проводится с работниками, которым выдаётся задание не связанное с их должностными обязанностями.

Вводный инструктаж проводится в кабинете по ТБ в форме лекции-беседы в течение 2-2,5 ч. Инструктаж должен проводится по программе разработанной с учётом требований стандартом, ССБТ, а также всех особенностей

производства, утверждённой главным инженером, по согласованию с комитетом профсоюза. О проведении инструктажа и проверке знаний должна быть сделана запись в “Журнале регистрации вводного инструктажа”, личной карточке инструктажа, с обязательной подписью инструктируемого и инструктирующего.

Обучения на предприятии осуществляется двумя способами:
Обучение без отрыва от производства по специальной программе (на час короче рабочий день и занятия в классе которые проводит инженерно-технический персонал завода).
обучение с отрывом от производства. Рабочий направляется в учебно-курсовой кабинет, где проводятся занятия и сдаётся экзамен на разряд и группу допуска.

На предприятиях периодическая проверка знаний правил ТБ, действующих инструкций и других нормативных документов по охране труда, ТБ, производственной санитарии и противопожарной технике производится:
ежегодно: у рабочих всех специальностей и любой квалификации, у линейных ИТР монтажных и наладочных организаций, мастеров цеха;
1 раз в 2 года: у руководящего состава монтажных и наладочных организаций;
1 раз в 3 года: у административного, технического и хозяйственного персонала.

После обучения и экзамена специальной квалификационной комиссией присваивается рабочим специальная квалификационная группа допуска по электробезопасности. Таких групп пять:
I группа: для отнесения к группе I достаточно пройти инструктаж по электробезопасности с оформлением его в журнале. Выдача удостоверения лицам с группой I не требуется;
II группа: Необходимо элементарное знакомство с электроустановкой, представление об опасности электрического тока. Следует знать основные меры предостережения и правила первой помощи. К этой группе относятся монтёры со стажем 1 месяц и практиканты электрики;
III группа: Требования в этой группе те же, что и к IV, но достаточно элементарное знание электротехники. Стаж работы требуется не менее 6 месяцев.

IV группа: Необходимо знать электроустановку в объёме специализируемого профтехучилища, правила первой помощи, все разделы ПТБ, электроустановку настолько, чтобы свободно производить переключения. Вести надзор за работающими, членами бригады, организовать безопасное проведение работы в электроустановках напряжением до и выше 1000 В. К

этой группе относятся начинающие инженеры и техники оперативной и оперативно-ремонтный персонал со стажем работы в электроустановках не менее одного года;
V группа: Необходимо знать схемы и оборудование своего участка и правила безопасности. Уметь организовать безопасное выполнение работы и вести надзор. Знать правила первой помощи пострадавшему от электрического тока и уметь её оказать. Уметь обучать персонал ПТБ и оказанию первой помощи. К этой группе относятся мастера, техники, инженеры в возрасте не моложе 19 лет с законченным специальным образованием и стажем работы в электроустановках не менее полгода, а также электромонтёры, электрослесари, инженеры-практики в возрасте не моложе 20 лет с большим стажем работы в электроустановках.
В электроустановках запрещается самовольное производство работ. Работы необходимо выполнять: по наряду, допуску, составленному по специальной форме по устному или письменному распоряжению; с записью в оперативный журнал.
К работам на линиях связи и проводного вещания допускаются лица, достигшие 18-летнего возраста.
Электромонтер проходит обязательное медицинское освидетельствование при поступлении на работу и в дальнейшем не реже одного раза в год.
Электромонтер до назначения на самостоятельную работу должен пройти обучение безопасным методам труда в объеме:
Правил техники безопасности при работах на линиях связи и проводного вещания.
Инструкции по охране труда предприятия.
Дополнительных правил и нормативных документов, действующих на предприятии.
По окончании обучения электромонтер проходит обязательную проверку знаний, после чего ему должна быть присвоена соответствующая квалификационная группа по электробезопасности и выдано удостоверение. В дальнейшем проводится периодическая проверка не реже одного раза в год.
При прохождении курса обучения безопасным методам труда каждый работник должен получить навыки оказания первой доврачебной помощи.
Все работы на линиях связи и проводного вещания производятся не менее, чем двумя лицами, одно из которых назначается старшим, ответственным за соблюдение требования безопасности. Лицо, назначенное старшим должно иметь квалификационную группу по электробезопасности не ниже IV, остальные члены бригады (звена) – не ниже III.

Нарядом для работы в электроустановках называется составленное, на специальном бланке задание на её безопасное производство, определяющее содержание, место, время её начало и окончания, необходимые меры безопасности, состав бригад и лиц, ответственных за безопасности выполнения работы.
Наряд выписывают в двух, а при передаче его по телефону или радио в трёх экземплярах. В последнем случае лицо, давшее наряд оставляет один экземпляр у себя. Записи о наряде должны быть разборчивыми. Исправление текста не допускается. Допускающий вручает наряд производителю работ после допуска бригады к работам. При перерывах в работе наряд остаётся действительным, если не изменились условия, относящиеся к подготовке и состоянию рабочего места. Изменение и расширение рабочего места возможны только в том случае, если будет выписан новый наряд.

Заключение

В заключение можно отметить следующее. Решение задачи обеспечения требуемого качества обслуживания в мультисервисных СПД, конечно, можно достигнуть прямым путем – на основе повышения

производительности сетевых устройств – маршрутизаторов и шлюзов, предоставления гарантированной полосы пропускания, использования магистральных сетей с высокой пропускной способностью. Однако, наиболее целесообразным, считается использование более гибких методов, обеспечивающие требуемые показатели качества обслуживания, при этом эффективно используются ресурсы сети для огромного набора различных приложений и услуг, включающие и наиболее критичные к параметрам сети аудио- и видео-приложения реального времени. В данной работы была получена полная статистическая картина трафика, которая позволила за счет обработки детальной информации получить общие тренды изменения трафика, уточнить микро-характеристики потоков. Измерения проводились на существующей сети оператора связи. Проведенная работа показали, что около 80% передаваемых объемов данных по стекам TCP/IP и UDP/IP переносится короткими пакетами (40 - 160 байт), основную часть которых составляет передача потокового видео и звука при помощи протокола http. Полученные результаты были использованы для дальнейшей подстройки параметров сети под существующую картину трафика. В итоге было уменьшено количество ошибочных пакетов, время ожидания пакета в очереди на маршрутизаторе, увеличена скорость обслуживания кадров. В результате можно утверждать, что наблюдается улучшение качества предоставляемых услуг в мультисервисных СПД. Была построена зависимость среднего времени отклика сети от поля случайной длины кадра. В ходе работы были произведены необходимые расчеты параметров качества, представлены графические результаты измерений и расчетов.

Список литературы

1. Яновский Г.Г. Качество обслуживания в сетях IP// Вестник связи - 2008. - №1.

2. Трещановский П.А. Оптимизация стохастической модели трафика для мультисервисных сетей // Инженерный вестник Дона. - 2011. - № 3. - С. 1-8.

3. Crovella M., Krishnamurthy B. Internet Measurement: Infrastructure, Traffic and Applications. John Wiley&Sons, Ltd., 2006. — 495 p.
4. Деарт В.Ю., Пилюгин А.В., Маньков В.А. Оценка влияния реальных характеристик веб-трафика на качество обслуживания в мультисервисной сети доступа // T-Comm. Специальный выпуск по итогам 3-й отраслевой научной конференции «Технологии информационного общества» в 3-х частях. - М.: Медиа паблишер, 2009. - Ч.1. - С.8-13.
5. 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
6. Г.Г. Яновский.Г.Г. Качество обслуживания в сетях IP - СПб.: Вестник связи № 1,
2008
7. McDysan. QoS and Traffic Management in IP and ATM Networks // McGraw-Hill.
2000.
8. Е.А. Кучерявый. Управление трафиком и качество обслуживания в сети Интернет//СПб, Наука и Техника. 2004.
9. Р. Кох, ГГ. Яновский. Эволюция и конвергенция в электросвязи//М., Радио и связь.
2001.
10. МСЭ-Т Recommendation Y.1540. IP Packet Transfer and Availability Performance Parameters//December 2002.
11. МСЭ-Т Recommendation Y.1541. Network Performance Objectives for IP-Based Services//May 2002.
13.ТрещановскийП.А. Методика расчета коэффициента использования мультисервисных сетей // Инфокоммуникационные технологии. - 2011. - Т. 9, № 3. - С. 47-52.
14.ТрещановскийП.А. Методы управления качеством обслуживания в мультисервисных сетях абонентского доступа // Известия высших учебных заведений. Электроника. - 2010. - № 3(83). - С. 68-73.
15. Трещановский П.А. Метод управления ресурсами мультисервисной сети на основе стохастического подхода // Труды 66-ой Всероссийской конференции, посвященной Дню радио. - М.: РНТОРЭС имени А.С. Попова, 2011. - С. 23-25.
Global Bandwidth Research Service [Электронный ресурс] - Режим доступа к статье: http://www.telegeography.com/product-info/gb/index.php

Перечень сокращений

QoS	Quality of service - Качество обслуживания
СПД	Сети передачи данных
МСЭ	Международный союз электросвязи
MOS	Mean Opinion Score
NGN	Next Generation Network - Сеть следующего поколения
SLA	Service-level Agreement - Соглашение об уровне обслуживания
NMS	Network Management System - Система управления сетью

DPS	Data protocol server - Сервер протокола данных
CTD	Cell Transfer Dalay - время задержки переноса ячеек
CDV	Cell Delay Variation - отклонение времени задержки переноса
CLR	Cell Loss Ratio - коэффициент потери ячеек
CER	Cell Error Ratio - коэффициент ошибочных ячеек
CMR	Cell Misinsertion Rate - скорость поступления ячеек
SECBR	Severely - Errored Cell Block Ratio - коэффициент ошибочных
IPTV	Internet Protocol Television
VoIP	Voice over IP
DDJ	Data Dependent Jitter
DCD	Duty Cycle Distortion
RJ	Random Jitter
MPLS	Multiprotocol Label Switching - Многопротокольная коммутация
IP	Internet Protocol - Межсетевой протокол
OTU	Optical Transport Unit - Оптический транспортный блок
RFC	Request for Comments - Запрос комментариев
RTD	Round-trip Delay - Круговая задержка
STM	Synchronous Transport Module - Синхронный транспортный
СМО	Система массового обслуживания
FIFO	First Input - First Output - первым пришел первым обслужен
LIFO	Last Input - First Output - последним пришел первым обслужен
RAND	Random - случайный выбор из очереди
ЧНН	Час наибольшей нагрузки