Ромасевич Е.П.[1], Ромасевич П.В.[2]

[1]ВолГУ, магистрант, eromasevich2@mail.ru
[2]D-Link, к.т.н., доцент, promasevich@dlink.ru

Исследование процесса потери пакетов при переходе сети MetroEthernet смешанной архитектуры на протокол IPv6

КЛЮЧЕВЫЕ СЛОВА:

Протокол IPv6, сеть MetroEthernet, потеря пакетов, имитационная модель.

АННОТАЦИЯ:

С помощью построенной имитационной модели проведено исследование процесса потери пакетов при передаче самоподобного трафика в сетях IPv4 и IPv6 масштаба города со смешанной архитектурой и выработаны рекомендации телекоммуникационному оператору по качественному предоставлению услуг при переводе сети на IPv6.

Введение

Динамичная информатизация сфер человеческой деятельности обусловила тенденции современного рынка телекоммуникаций, характеризующиеся резким ростом количества сетевых пользовательских устройств, а также масштабным строительством и модернизацией сетевой инфраструктуры, предназначенной для организации различных сервисов – от VoIP до интерактивного телевидения, предполагающих их доступность вне зависимости от местоположения клиента и используемого им интерфейса.

На местах состояние телекоммуникационного рынка характеризуется повсеместным развертыванием сетей широкополосного доступа различной архитектуры и технологий масштаба города MetroEhternet для предоставления комплекса телекоммуникационных услуг TriplePlay (данные, голос, видео) через единую линейную инфраструктуру.

Одним из главных препятствий динамичному развитию телекоммуникационных сетей является недостаточный объём адресного пространства протокола IPv4 из-за быстрого роста количества мобильных устройств, таких как смартфоны и планшетные компьютеры.

Количество устройств, подключаемых к глобальной сети растёт экспоненциально [4], [5]. К серьёзным проблемам использования также относятся проблемы агрегации маршрутов, которые приводят к росту размера таблиц маршрутизации. Задача фрагментации пакета на промежуточных узлах в зависимости от значения MTU канала, в который поступает пакет, и постоянная проверка и пересчёт контрольных сумм

требуют значительных ресурсов маршрутизатора, и, как следствие, растёт время задержки.

Нынешнее состояние сети Интернет обусловлено использованием большого числа сервисов чувствительных ок задержкам, таких как IP-телефония и IPTV. Для обеспечения качества обслуживания в IPv4 предусмотрено поле TypeOfService, однако механизмов обработки пакетов или резервирования канала, в соответствии со значением данного поля, предусмотрено не было. [6]

К сложностям обработки заголовка IPv4 относятся его вариативная длина от 20 от 40 байт, которая опять же приводит к пересчёту контрольных сумм. С другой стороны этой длины недостаточно для добавления необходимого числа дополнительных опций, а многие поля, которые имеются в заголовке, устарели или требуют модернизации. [6]

В 1992 году была поставлена задача создания нового протокола, призванного решить те проблемы, которые имел протокол IPv4. В 1994 году Инженерный совет Интернета IETF утвердил модель протокола Интернет следующего поколения IPng и к 1996 году появилась серия спецификаций описывающих Интернет-протокол версии 6. При создании протокола были учтены недостатки IPv4, а также созданы совершенно новые принципы работы протокола, которые должны обеспечить безопасность и маршрутизацию с сети Интернет прозрачнее и быстрее.

Агентство IANA, управляющая пространствами IP-адресов сети Интернет, распределило 3 февраля 2011 года последние пять блоков IP-адресов между региональными интернет-регистраторами. А по данным [1] на 6 мая 2013, регистратор Европы, Ближнего Востока и Центральной Азии (RIPE NCC) и регистратор Азии и Тихоокеанского региона (APNIC) израсходовали имеющиеся у них IP-адреса 14 сентября 2012 и 19 апреля 2011 года, соответственно. Крупные провайдеры услуг Интернет имеют определённый запас адресов IPv4, но и он в скором времени будет истощён.

Решением проблемы станет переход Интернет на протокол IP версии 6, очевидным преимуществом которого является значительно увеличенное адресное пространство по сравнению с IPv4. Если у протокола IPv4 – 2^{32} адресов, то у IPv6 – 2^{128} адресов.

IPv6 содержит немало функциональных улучшений, прежде всего в области маршрутизации. Адресация теперь имеет иерархическую структуру, что облегчает передачу пакетов по сети. Также на уровне сетевом уровне в IPv6 уже нет подсчёта контрольных сумм, что позволяет маршрутизаторам экономить время обработки. Появились также новые возможности QoS и многоадресное вещание, а IPSec стал обязательным. Максимальный размер пакетов у шестой версии протокола может достигать 4 ГБ, что несомненно приведёт к изменениям принципов передачи данных в будущем. [2]

Большинство специалистов в области Internet-технологий уверены в необходимости перехода на новую, шестую версию протокола IP.

Косвенным свидетельством этому служит постоянно увеличивающееся число организаций, компаний-разработчиков сетевого оборудования и программного обеспечения, принимающих участие в Международном форуме и IPv6 и реализовавшие его поддержку в своем сетевом оборудовании. [3]

В рекомендации МСЭ Y.1540 [21], посвященной технологии IP рассматриваются следующие сетевые характеристики, как наиболее важные по степени их влияния на сквозное качество обслуживания от источника до получателя, оцениваемое пользователем: производительность сети (Мб/сек), задержка (IPTD - IPpackettransferdelay) и потеря пакетов (IPLR - IPpacketlossratio).

Многочисленные зарубежные и отечественные исследования последнего десятилетия показали, что трафик в современных сетях передачи данных проявляет свойства самоподобия [20], которое оказывает негативное влияние на производительность сетей передачи данных ввиду значительно большей потребности в буферной памяти и пропускной способности телекоммуникационных систем, что является одним из основных факторов, влияющих на величину задержки.

Качество обслуживания QoS в сетях IP определяется в рекомендации МСЭ Y.1541 и зависит от множества факторов и может варьироваться в значительных пределах в зависимости от функционала телекоммуникационного оборудования, параметров трафика и сети.

Поэтому для непрерывного оказания услуг телекоммуникационным операторам необходима предварительная оценка работоспособности при проектировании новой или модернизации существующей телекоммуникационной сети, работающей на базе протокола IPv6 или осуществляющей миграцию на него [19]

По причине трудности постановки эксперимента и сложности аналитического моделирования, имитационное моделирование может быть наиболее рациональным способом решения подобной задачи.

Поэтому целью данной работы является построение имитационной модели сегмента сети MetroEthernet и исследование различий процесса потери пакетов самоподобного трафика при использовании протокола IPv4 и IPv6 при прочих равных условиях.

Имитационная модель

При анализе действующих телекоммуникационных систем с помощью моделирования определяют границы работоспособности системы, выполняют имитацию экстремальных условий, которые могут возникнуть в процессе ее функционирования. Искусственное создание таких условий на действующей системе затруднено и может привести к катастрофическим последствиям, если система не справится со своими функциональными обязанностями. Целесообразность использования моделирования для действующей системы состоит также в том, что можно

опытным путем проверить адекватность модели и оригинала и более точно определить те параметры телекоммуникационной системы и внешних воздействий на нее, которые служат исходными данными для моделирования. Это позволяет выявить ее резервы и прогнозировать ее работу.

Имитационная модель – совокупность описания системы и внешних воздействий, алгоритмов функционирования системы или правил изменения состояния системы под влиянием внутренних и внешних возмущений. Эти алгоритмы и правила не дают возможности использования имеющихся математических методов аналитического и численного решения, но позволяют имитировать процесс функционирования системы и производить измерения интересующих характеристик. [14]

За основу была взята телекоммуникационная сеть одного из операторов Волгограда. Сеть представляет собой топологию смешанного типа. Здесь представлена сложная звездообразная топология, а также кольцевая на уровне распределения, как показано на Рис.3.

Для создания модели сети был выбран новый инструмент в этой сфере – сетевой симулятор NS-3. Этот симулятор представляет собой совершенно новый продукт со своей архитектурой и подходом к построению моделей. NS-3 полностью написан на языке C++, а сетевые модели становятся его составляющими. В симуляторе NS-3 достигается более детальная симуляция сети, по сравнению со своими предшественниками. Необходимо отметить, что данный программный продукт позволяет моделировать телекоммуникационные сети на основе IPv6, что особенно актуально ввиду уже начавшегося перевода опорных сетей федеральных операторов на этот протокол. Кроме того, в данном программном продукте есть возможность моделирования беспроводных сетей различного типа, что при современной мобильности клиентских устройств весьма актуально.

Симулятор NS-3 в отличие от своего предшественника включает приложение NetAnim – визуализатор, разработанный на кроссплатформенной библиотеке Qt4. Он предназначен для анимации событий, происходящих в модели. Входными данными для визуализатора являются трассировочныеXML-файлы. Файлы этого формата создаются в ходе симуляции, если в коде модели присутствует специальная функция. Данное приложение помогает быстро оценить правильность построения модели, в течение времени просмотреть движение данных по моделируемой сети.

Интерфейс программы представлен на Рис.1

В пакет NS-3 также входит анализатор TraceMetrics – инструмент для анализа трассировочных файлов симулятора NS-3. Польза данной программы в том, что она делает практический анализ трейс-файлов, созданных в ходе симуляции и, как результат, показывает некоторые

интересные данные из выполненного скрипта. Вид данной программы представлен на Рис.2.

Для адекватного моделирования необходимо учесть свойство самоподобия (фрактальности) сетевого трафика. Наиболее часто для моделирования фрактального трафика используется распределение Парето. Достоинством такого распределения является возможность определения фрактальности трафика по его параметрам. Недостатком является то, что оно имеет бесконечную дисперсию, что означает высокую изменчивость входного трафика. Это создает определенные трудности использования данного распределения при моделировании реальных процессов в телекоммуникационных системах.

Наряду с распределением Парето, наиболее часто используется распределение Вейбулла, которое хорошо подходит, в частности, для моделирования процессов потери пакетов при переполнении буфера сетевых интерфейсов [17].

Распределение Вейбулла – это также распределение с так называемым «тяжёлым хвостом», широко применяемое при моделировании сетевого трафика, с функцией распределения

$$F(x) = 1 - e^{-\left(\frac{x}{\beta}\right)^{\alpha}}$$

Генерировать значения для трассы с плотностью распределения вероятностей Вейбулла можно так же, как для экспоненциального распределения, используя инверсию функции распределения Вейбулла. [18]

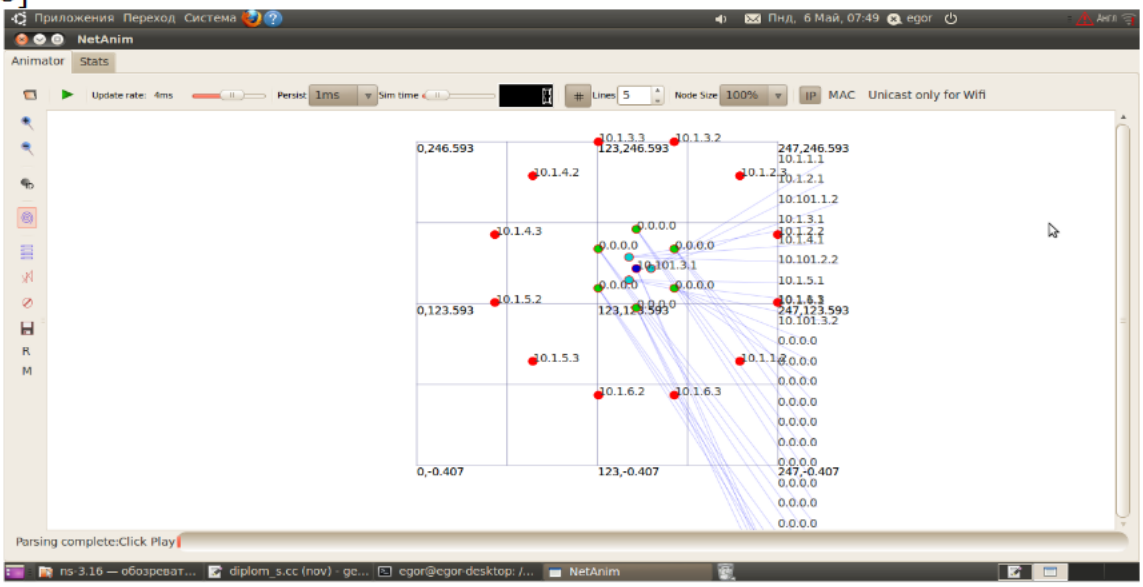

Рис.1. Визуализатор NetAnim (экранная копия)

Основой имитационной модели стала архитектура сети широкополосного доступа в Интернет одного из операторов города Волгограда. Сеть представляет собой топологию смешанного типа. Здесь

представлена сложная звездообразная топология, а также кольцевая на уровне распределения, как показано на Рис.3.

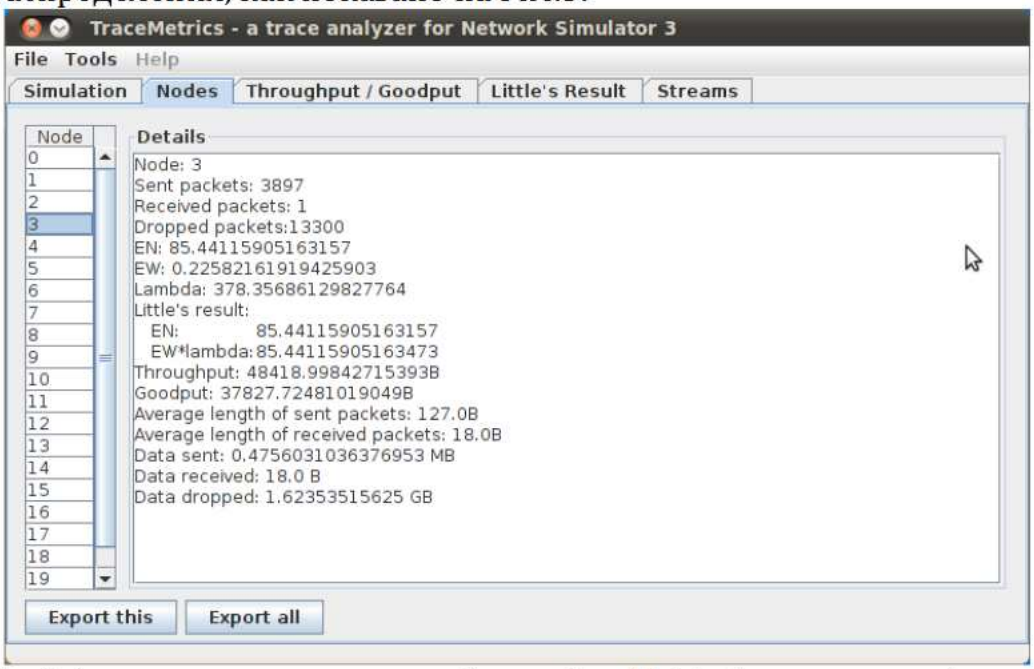

Рис.2. Анализатор трассировочных данных TraceMetrics (экранная копия)

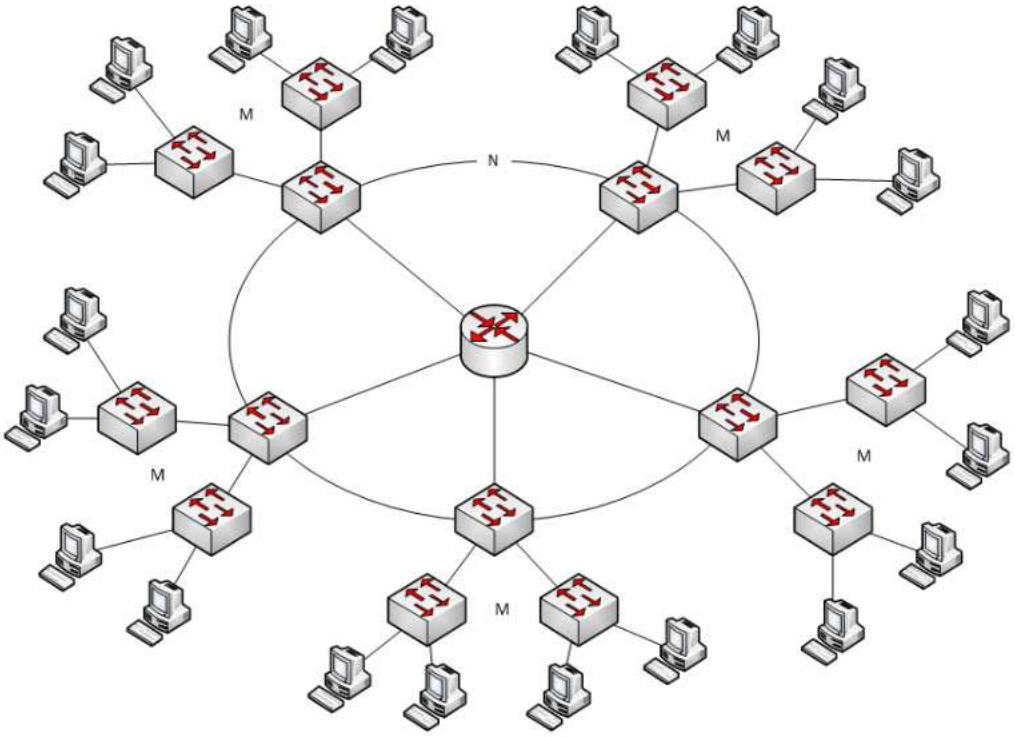

Рис.3. Топология моделируемой сети

В модели используются узлы, имитирующие как коммутаторы L2, так и коммутаторы L3. Программа модели написана таким образом, что исследователь может легко менять такие параметры как количество

коммутаторов распределения, количество коммутаторов доступа на каждом коммутаторе распределения, количество пользовательских компьютеров на каждом коммутаторе доступа, а также размер пакета генератора трафика. Таким образом, модель является масштабируемой. Количество узлов в модели можно подсчитать как

$$S = 1 + N + N * M + N * M * K$$

где S – общее количество узлов в модели,

N – количество узлов на уровне распределения,

M – количество узлов на уровне доступа,

K – количество хостов, подключённых к одному узлу на уровне доступа.

Каждый сегмент сети имеет своё адресное пространство. Скорость передачи данных в каждом сегменте одинакова, и имеет задержку 2 мс. В процессе исследования данный параметр изменяется. Скорость в кольце, связывающем коммутаторы распределения – 1 Гбит/с с задержкой 1 мс, а скорость до маршрутизатора ядра – 10 Гбит/с с аналогичной задержкой.

Код программы имеет два варианта. Первый вариант программы основан на передаче пакетов с помощью Интернет-протокола версии 4, а второй – на передаче пакетов с помощью IPv6. Так как данные протоколы Интернет имеют отличные друг от друга механизмы работы, они требуют также разный код при программировании их в имитационной модели.

Предметом исследования в данной работе является потеря пакетов в сети оператора, при использовании им протоколов IPv4 и IPv6 при прочих равных условиях.

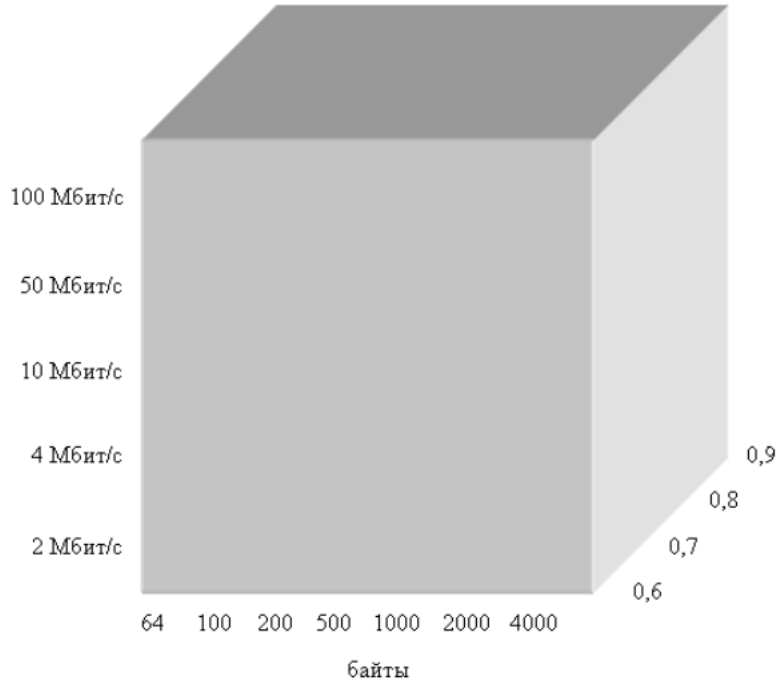

Рис.4. Масштаб экспериментов с помощью имитационной модели

Трафик в имитационной модели является самоподобным, и передаётся по протоколу транспортного уровня UDP. Создаёт трафик OnOff-генератор. Параметр On в течении которого генерируется трафик находится на основании распределения Вейбулла, а параметр Off является постоянным, и составляет 0,25.

Эксперименты шли в нескольких направлениях. Для наглядности это было представлено на Рис 4.

Из рисунка видно, что в ходе данной работы изменяется скорость доступа (скорость от хостов к узлам, имитирующем коммутаторы доступа) от 2 Мбит/с до 100 Мбит/с, размер пакета принимает семь значений от 64 байт до 4000 байт. Каждый из вариантов этих экспериментов проходит при четырёх значениях параметра Хёрста – от 0,6 до 0,9.

Такой «трёхмерный» эксперимент проводится четыре раза: для случая, когда между узлами агрегации существует кольцо при двух протоколах, и для случая, когда кольца нет при двух протоколах.

Всего в процессе работы было предусмотрено более пятиста экспериментов, в ходе которых изменялись различные параметры сети и поведения трафика, чтобы сравнить работу двух протоколов. Однако, учитывая ограничения по объему публикации, здесь приведены лишь наиболее характерные результаты.

Результаты всех экспериментов представлены в магистерской научно-исследовательской работе и находятся на кафедре «Телекоммуникационных систем» ВолГУ.

Исследование потерь пакетов при передаче данных на основе IPv4 и IPv6

Для исследования были созданы две модели сети. Топология в обеих моделях одинаковая – используется один код. Одним кодом также запрограммирован генератор трафика. Разница заключается в сетевом уровне. В первом случае используется Интернет-протокол версии 4, в другом – его шестая версия.

Топология моделируемой сети представлена на Рис.3. Эксперименты проводились с тремя L3 коммутаторами распределения, двумя L2 коммутаторами доступа на каждом L3 коммутаторе и двумя пользователями на каждом коммутаторе доступа.

Данная модель имеет следующие характеристики:

- от ядра сети до уровня распределения канал – 10Гб/с;
- на уровне агрегации канал – 1 Гб/с;
- использование стека Интернет;
- использование протокола UDP для передачи данных;
- масштабируемость модели;
- учёт самоподобия трафика;
- использование OnOff-генератора с распределением Вейбулла.

В ходе исследования было проведено 560 экспериментов, по каждому из которых был получен и обработан файл трассировки. Каждый трейс-файл несёт в себе информацию о 10 секундах модельного времени. Работа модели представлена на Рис.5.

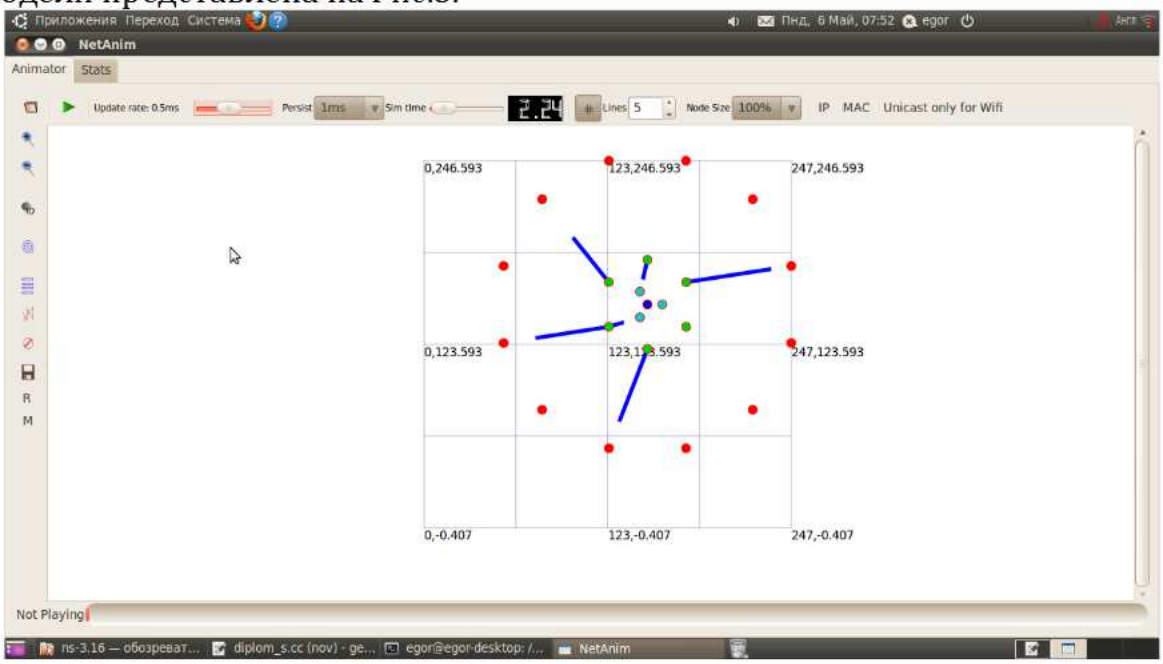

Рис.5. Работа модели в визуализаторе NetAnim (экранная копия)

В модели использовались значения размеров передаваемых пакетов из разных диапазонов, а именно 64, 100, 200, 500, 1000, 2000 и 4000 байт. Эти значения были взяты, чтобы охватить весь диапазон значений «вокруг» минимально допустимого, и вероятного наиболее применимого, значения MTU для протокола IPv6. Это необходимо для того, чтобы посмотреть, как ведёт себя новый протокол при различных условиях.

На сегодняшний день рынок широкополосного доступа в Интернет предлагает пользователям довольно большой выбор скоростей. Поэтому в данной работе не было остановки на одной конкретной скорости, а промоделированы пять скоростей: 2, 5, 10, 50 и 100 Мбит/с.

Помимо стороны пользователя, в модели была затронута и сторона оператора. Модель была исследована при двух вариантах. В первом варианте коммутаторы распределения были объединены в кольцо. Во втором варианте «кольца» не было, и коммутаторы взаимодействуют друг с другом через маршрутизатор ядра.

Так как современные IP-сети обладают свойством самоподобия, параметры генерации трафика подбирались таким образом, чтобы исследовать сеть при четырёх значениях параметра Хёрста: 0,6 , 0,7 , 0,8 и 0,9.

Как видно из графиков, при размере пакетов до 500 байт, скорость не сильно влияет на потери, которые почти одинаковы на этом отрезке. На следующем отрезке, от 500 байт до 1000 байт, кривые расходятся. А дальше

наблюдается интересный момент: на отрезке от 1000 байт до 4000 байт скорость доступа практически не влияет на потери у протокола IPv6, в отличие от IPv4. Если второго потери стремятся к нулю при увеличении скорости, что логично, то у первого потери находятся на уровне около 20%.

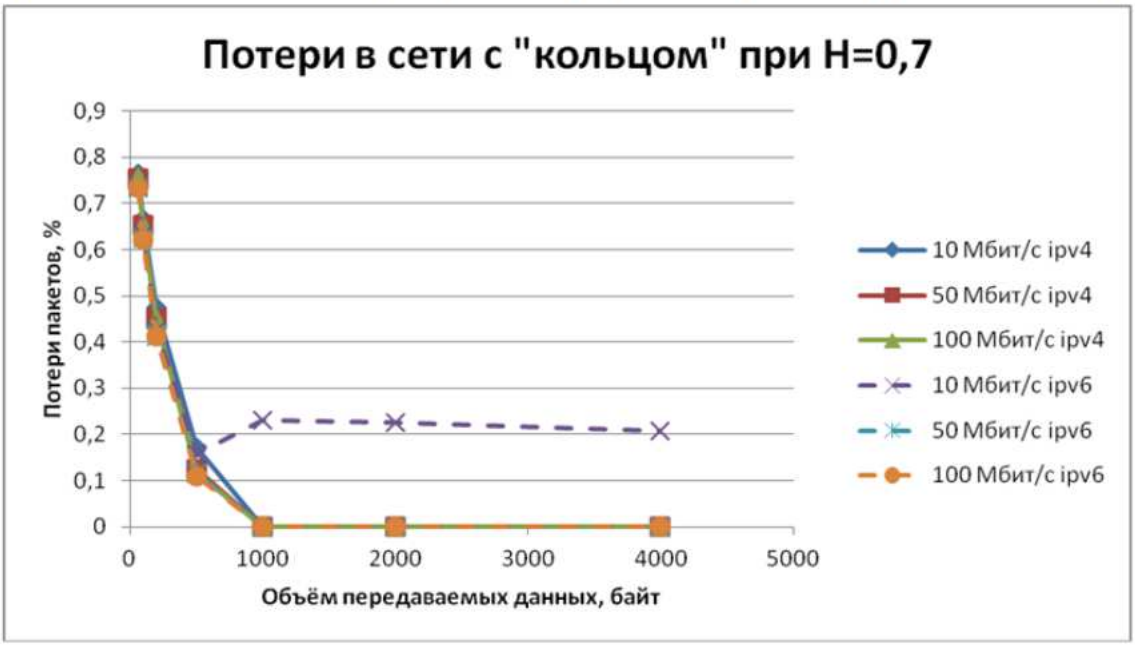

Рис.6. Случай кольца на уровне распределения (агрегации)

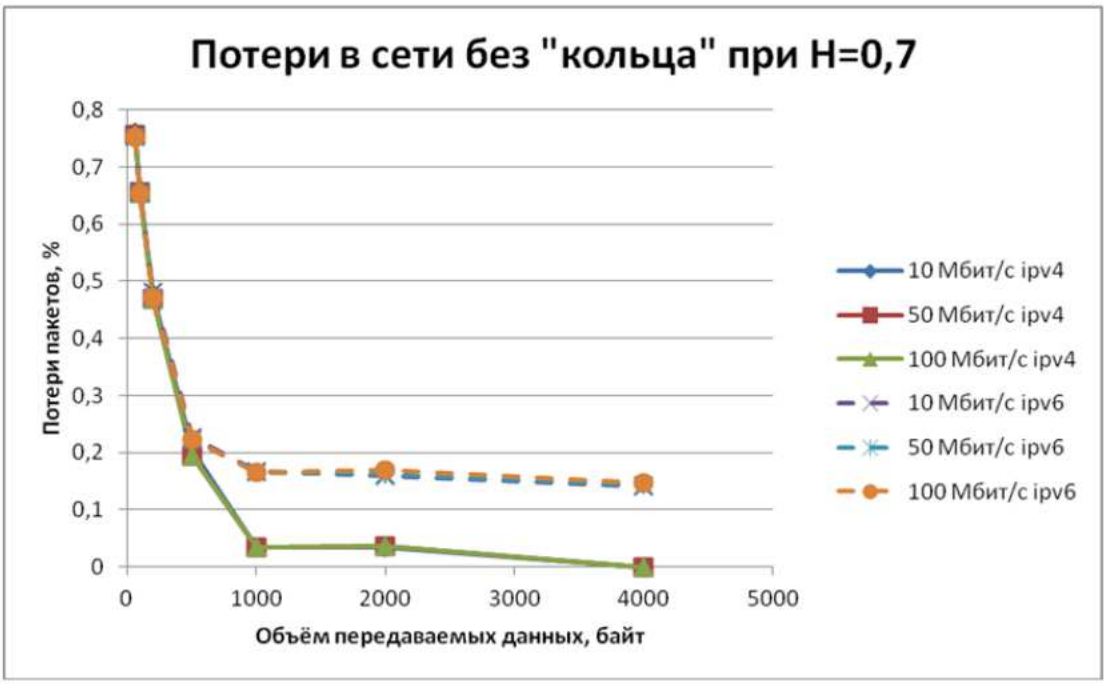

Рис.7. Случай отсутствия кольца на уровне распределения (агрегации)

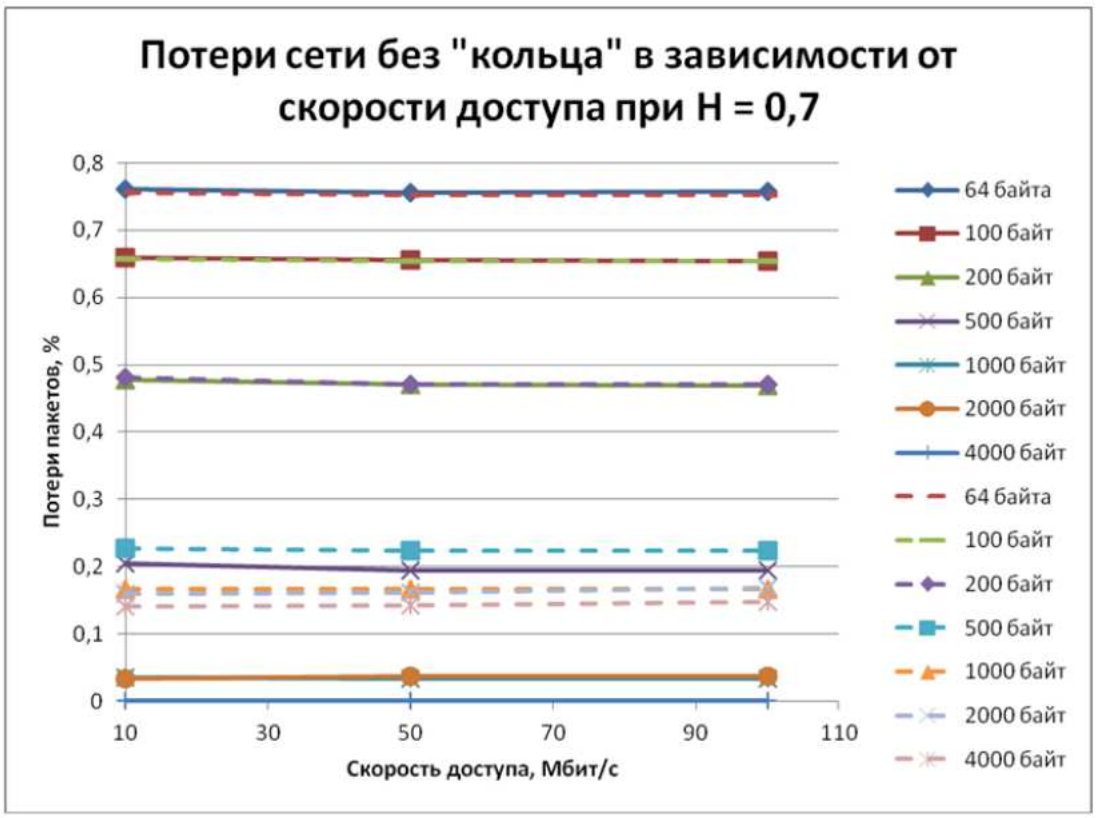

Рис.8. Случай отсутствия кольца на уровне распределения (агрегации)

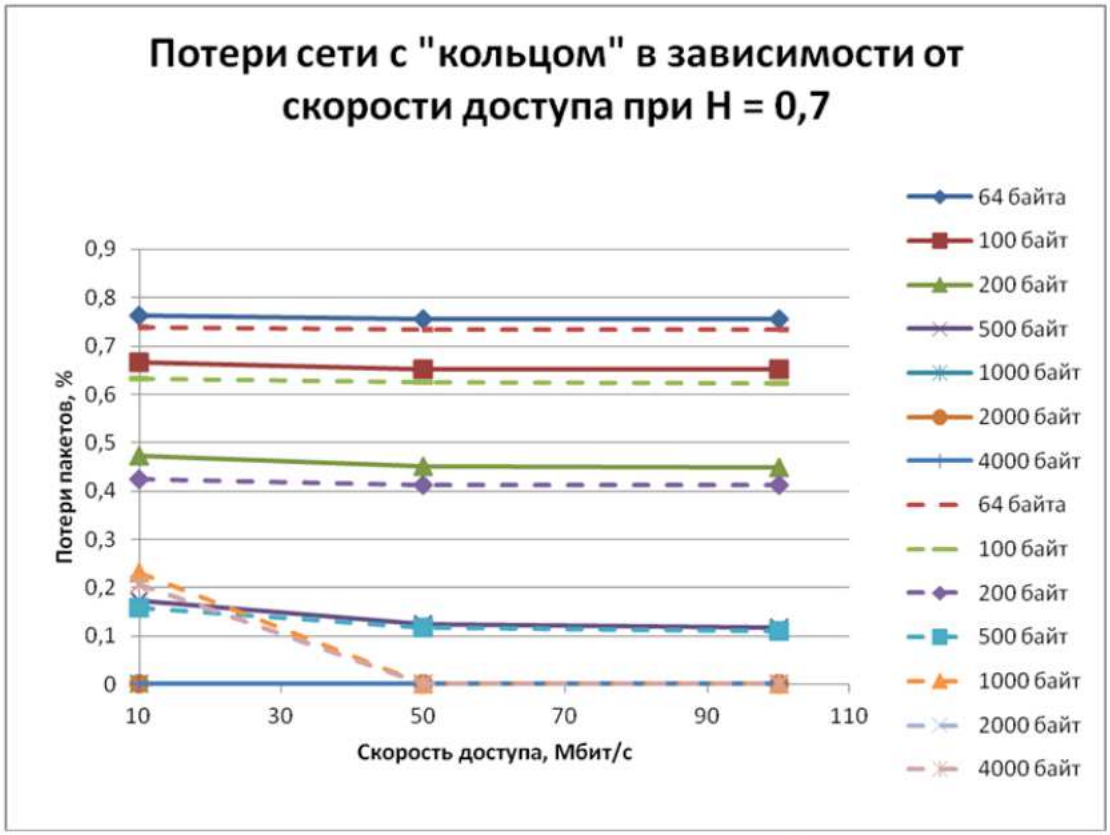

Рис.9. Случай кольца на уровне распределения (агрегации)

На Рис.6-7 показаны проценты потери пакетов в зависимости от величины передаваемых пользовательских данных. Соответственно нужно иметь в виду, что реальный размер пакета на различных уровнях модели OSI будет больше.

Различие потери пакетов при разных версиях Интернет-протокола объясняется различием механизмов маршрутизации реализованных в симуляторе для этих протоколов. Для IPv6 в NS-3реализована пока только статическая маршрутизация, что, впрочем, адекватно отражает реальную ситуацию при неизменности топологии сети и скоростей каналов в ней. В случае варианта сети без «кольца» на уровне распределения ситуация стабильна - потери пакетов IPv6 снижаются до уровня примерно 15% при достижении объёма передаваемых данных в 1000 байт и далее от размера передаваемых данных не зависят. Ситуация с IPv4 в случае звездообразной топологии выглядит лучше – потери составляют около 3%, и опускаются до нуля при дальнейшем увеличении до 4000 байт.

Ситуация явно улучшается при объединении коммутаторов распределения в кольцо. При разных объёмах данных, передаваемых в пакете, и скоростях доступа 50 Мбит/с и 100 Мбит/с протокол IPv6 показывает результат даже лучший, чем протокол IPv4 на 1-2%. В обоих случаях трафик проходит по «кольцу» распределения, не затрагивая маршрутизатор ядра, в который поступают только служебные ICMP-пакеты IPv6. Исключение составляет случай, когда скорость доступа имеет значение 10 Мбит/с. Если с IPv4 ситуация соответствует двум другим скоростям, то с IPv6 потери начинают возрастать после объёма передаваемых данных в 500 байт, затем наблюдается рост потерь до 23% при длине данных 1000 байт и далее снижаются по мере увеличения объёма данных пакетов до 20% при 4000 байт. При детальном изучении трассировочных файлов становится понятно, что данные начинают также проходить через маршрутизатор ядра и процент потерь в «ядре» составляет 80% от всех потерь в сети, а остальные потери относятся к уровню распределения.

Если посмотреть на полученные результаты под другим углом зрения, то видно, что потери пакетов при звездообразной топологии (Рис.8) так или иначе имеют место при обоих версиях протокола IP и при различных длинах передаваемых данных, которые, однако, снижаются при увеличении их длины. Напротив, при топологии с кольцом на уровне распределения (Рис.9) лучших результатов достигает протокол IPv6 при размерах данных более 2000 байт при том, что у протокола IPv4 на этих же длинах потери пакетов всё же имеют место.

При детальном анализе файлов трассировки становятся понятны возможные причины описанных явлений.

При анализе заголовка пакетов в трассировочных файлах, видно использование заголовка расширений Fragment Header. Размер пакета на данном отрезке больше размера MTU, но транзитные узлы теперь при IPv6

пакеты уже не фрагментируют. Соответственно данные должны фрагментироваться либо уровнем выше сетевого, либо однократно на стороне отправителя, и передаваться фрагментами до пункта назначения. Так как фрагментации на уровне приложения в модели не происходит, она выполняется на узле-отправителе, используя дополнительный заголовок Fragment Header. Недостатком этого механизма является то, что при потере одного фрагмента, получатель уже не сможет собрать пакет, и он фактически теряется и процент потери пакетов растет, и приходится высылать весь пакет заново, что создает дополнительную нагрузку на сеть.

На основании полученных результатов можно дать следующие рекомендации операторам:

1. Архитектура сети должна иметь «горизонтальные» связи коммутаторов уровня распределения (агрегации) для обеспечения дополнительных путей движения пакетов в обход устройств ядра. Это не только разгрузит оборудование ядра, но и исключит единую точку отказа всей сети в случае, если ядро состоит из одного устройства, что по нашей жизни бывает нередко.
2. Увеличение MTU в своей сети. Современное телекоммуникационное оборудование и каналы связи позволяют сделать этот параметр больше. Это избавит источник, не имеющий своих инструментов, от фрагментации на сетевом уровне, а также положительно повлияет на увеличение пропускной способности, благодаря уменьшению количества заголовков.
3. Увеличение скорости доступа конечного пользователя. На Рис.9 видно, что потери в данной архитектуре сети сводятся к нулю при использовании обоих версий протокола IP при тарифах более 50 Мбит/с и соответствующих длин пакетов, которые уже являются обычными в крупных городах в сетях операторов федерального уровня.
4. Целесообразно использовать пакеты большой длины, дабы уменьшить нагрузку транзитных узлов и передавать больше информации за один акт обработки заголовка.

Результаты данной работы могут быть использованы телекоммуникационными операторами для предварительной оценки ресурсов и действий, необходимых для успешной миграции телекоммуникационных сетей с IPv4 на IPv6.

Литература

1. Материалы сервера http://www.potaroo.net/tools/ipv4/
2. Дериев И. IPv6, не дожидаясь провайдера. 28.07.2011. Материалы сервера http://www.ixbt.com/soft/ipv6.shtml
3. Алексеев И. Переход на IPv6. Журнал «LAN», №07-08, 2001 год // Издательство «Открытые системы». Материалы сервера http://www.realcoding.net/article/view/636
4. Материалы сервера http://www.ipv6.ru/russian/history/ipv4.php
5. Материалы сервера http://do.gendocs.ru/docs/index-242882.html
6. Материалы сервера http://ipv6.ispras.ru/article.html
7. Материалы сервера http://cdo.bseu.by/library/ibs1/net_l/tcp_ip/net/frmp_ipv6.htm

8. RFC 2374. Материалы сервера http://tools.ietf.org/html/rfc2374
9. RFC 4291. Материалы сервера http://tools.ietf.org/html/rfc4291
10. RFC 2373. Материалы сервера http://tools.ietf.org/html/rfc2373
11. RFC 3587. Материалы сервера http://tools.ietf.org/html/rfc3587
12. RFC 2460. Материалы сервера http://tools.ietf.org/html/rfc2460
13. RFC 4303. Материалы сервера http://tools.ietf.org/html/rfc4303
14. Построение широкополосной телекоммуникационной сети пакетной коммутации с интеграцией услуг с учётом свойств сетевого трафика [Текст]: учеб. Пособие / П.В. Ромасевич; Гос. образоват. учреждение высш. проф. Образования «Волгогр. гос. ун-т», Каф.телекоммуникац. систем. – Волгоград :Изд-во ВолГУ, 2009. – 92 с.
15. Материалы сервера http://www.nsnam.org/docs/release/3.16/tutorial/ns-3-tutorial.pdf
16. Столлингс В. Современные компьютерные сети. 2-е изд. – СПб.: Питер, 2003. – 783 с.
17. Ю.И.Лосев, К.М.Руккас. Анализ моделей вероятности потери пакетов в буфере маршрутизатора с учетом фрактальности трафика // Вісник Харківського національного університету, серія «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління» – 2008, №833, с.163-169
18. Фрактальные процессы в телекоммуникациях. Монография. / Под ред. О.И. Шелухина. – М.:Радиотехника, 2003. – 480 с.
19. П.В.Ромасевич. Исследование сети MetroEthernet на основе её имитационной модели//Известия ОрелГТУ, Информационные системы и технологии – 2010, №2/58 (585)
20. W.E.Leland, M.S.Taqqu, W.Willinger, D.V.Wilson., On the self-similar nature ofethernettaffic , IEEE/ACM Transactions of Networking, 2(1):1-15,1993
21. МСЭ-Т Recommendation Y.1540. IP Packet Transfer and Availability Performance Parameters//December 2002.