Impact Factor: 9.2 ISSN-L: 2544-980X

Управление Трафиком В Мультимедийных Сетях Связи

Камила Шержанова Сапарбаевна [1], Дилнура Шержанова Сапарбаевна [2]

Аннотация: Управление трафиком — это широко распространенная отраслевая практика для обеспечения эффективной работы сетей, включая такие механизмы, как создание очередей, маршрутизация, ограничение или нормирование определенного трафика в сети или предоставление приоритета некоторым типам трафика при определенных сетевых условиях или в любое время. Цель состоит в том, чтобы свести к минимуму влияние перегрузки в сетях на качество обслуживания трафика. Его можно использовать для достижения определенных целей производительности, и его тщательное применение может в конечном итоге улучшить качество работы конечного пользователя технически и экономически обоснованным способом.

Ключевые слова: управление трафиком, джиттер, безопасность, задержка, контроль допуска, эволюция, показатели качества обслуживания.

Несколько механизмов управления трафиком имеют жизненно важное значение для функционирующего Интернета, поддерживающего все виды приложений Over-the-Top (OTT) в режиме «наилучших усилий». Другой набор механизмов управления трафиком также используется в сетях, участвующих в мультимедийном контексте, для обеспечения дифференцированной обработки различных услуг (например, услуга доступа в Интернет, несущая любое приложение OTT, бизнес-VPN, специализированные услуги VoIP или видео), где эти услуги иметь общую инфраструктуру. В этом техническом документе представлена информация об управлении трафиком, а также подробно описаны обоснование и механизмы применения некоторых методов управления трафиком для доступа к сетям в контексте мультимедиа. Продолжаются исследования новых механизмов и методов управления трафиком. Это развивающаяся область исследования. Необходимость развертывания определенного набора методов управления сетью широко признается государственными учреждениями по всему миру.

Управление трафиком в мультимедийных сетях доступа

Введение в управление трафиком. Все сетевые ресурсы ограничены физически (например, количеством и скоростью соединений) и экономическими соображениями. Всегда существовала потребность в оптимизации использования оборудования и других сетевых ресурсов, и это может привести к перегрузке, особенно в больших сетях. Даже в мире с коммутацией каналов ограниченные возможности коммутации и мультиплексирования означали возможность блокировки вызовов при большом объеме вызовов. В IP-мире Интернета с коммутацией пакетов ограниченные возможности канала, маршрутизации и агрегации могут привести к ограничению пропускной способности, увеличению задержки (задержки пакетов), колебаниям задержки (джиттеру) и потере пакетов.

Сетевые операторы несут ответственность за поддержание сети в рабочем состоянии. Для этого необходимо использовать функции управления трафиком. Механизмы управления трафиком представляют собой набор инструментов, которые позволяют сетевому оператору обеспечивать непрерывную работу сети в периоды перегрузки на перегруженных узлах. Эти механизмы также полезны для поддержки соглашений об уровне обслуживания (SLA) и предоставления различных типов услуг. Одна из основных целей состоит в том, чтобы избежать, уменьшить и/или отсрочить неблагоприятное воздействие перегрузки на различные типы трафика, использующего сеть. Эффективное управление трафиком необходимо для минимизации влияния перегрузки на видео в реальном времени, VoIP, потоковое видео и даже просмотр веб-страниц, что, в свою очередь, влияет на работу пользователей. Помимо управления перегрузками, также полезно выявлять и отслеживать перегрузки, как описано в [2].

Управление трафиком влияет как на показатели качества обслуживания (QoS), так и на показатели качества взаимодействия (QoE). Как описано в [3], QoS — это «мера производительности на уровне пакетов с точки зрения сети», тогда как QoE — это «общая производительность системы с точки зрения пользователей». QoE — это мера сквозной производительности на уровне услуг с точки зрения пользователя и показатель того, насколько хорошо система соответствует потребностям пользователя». QoS — это мера пропускной способности, задержки, изменения задержки пакетов и потери пакетов, а QoE — это субъективная мера восприятия пользователем производительности конкретной услуги. Взаимосвязь между QoS и QoE зависит от типа услуги. Например, пользователи потокового видео могут допустить некоторую задержку, но не потерю пакетов или большие колебания задержки. Пользователи голосовой связи в реальном времени не допускают значительной задержки или изменения задержки, но могут допустить некоторую потерю пакетов. Оба типа приложений имеют минимальные

[1] Отдел подготовки научно-педагогических кадров Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий Ташкент, Узбекистан

[2] Оператор офиса продаж Шовотская телекоммуникационная линия Ташкент, Узбекистан

требования к пропускной способности. Пользователи электронной почты имеют очень высокую устойчивость к задержке, изменению задержки, изменению пропускной способности и потере пакетов (поскольку протоколы, используемые электронной почтой, могут легко восстанавливать потерянные пакеты).

Существует множество механизмов управления трафиком, таких как

- классификация трафика
- учет и формирование трафика,
- маркировка и/или отбрасывание пакетов
- планирование пакетов
- контроль допуска и резервирование ресурсов
- решения о маршрутизации
- кэширование

Эти инструменты можно комбинировать различными способами для достижения политики управления трафиком сетевого провайдера. Но обратите внимание, что нет необходимости или даже пользы применять все эти инструменты вместе в любой части сети. Следующие разделы посвящены использованию некоторых дифференцированных механизмов управления трафиком в контексте мультисервисных сетей доступа.

Перегрузка в сетях доступа

Сети доступа (линии первой мили и узлы, завершающие эти линии) исторически были узким местом. Тем не менее, последовательные волны технологических инноваций привели к огромной эволюции, от модемов коммутируемого доступа к внедрению DSL и кабельных модемов, а теперь еще и к все более глубоким развертываниям FTTx, обеспечивающим подключение к гигабитному доступу. Аналогичный рост происходит и в мобильных сетях с появлением каждого нового поколения. Хотя для значительного улучшения качества широкополосной связи необходимо значительно увеличить скорость доступа, они не устраняют все перегрузки, которые все еще могут возникать по следующим причинам:

Операторы доступа несут ответственность не только за предоставление мобильного или фиксированного доступа, но также за мультиплексирование и агрегирование трафика от всех пользовательских подключений выше в сети. Необходимо найти компромисс между емкостью агрегации и инвестициями, что приведет к приемлемому коэффициенту статистического мультиплексирования с учетом ожидаемого параллелизма, пиковых и средних скоростей. Полное предотвращение перегрузки за счет простого роста пропускной способности (определение всей сети для одновременной непрерывной пиковой пропускной способности (линейной скорости) для всех пользователей) экономически нецелесообразно.

С точки зрения измерения, попытка полностью избежать перегрузки поставит вопрос о том, какая пропускная способность необходима для каждого пользователя. На этот вопрос сложно ответить, так как в любое время могут появиться новые неопределенные приложения, требовательные к полосе пропускания. Кроме того, была продемонстрирована самоподобие интернет-трафика, что означает, что он является скачкообразным во всех временных масштабах; следовательно, чтобы избежать перегрузки, потребуется определение параметров сети для пиковых скоростей для всех пользователей. Важное значение имеет размерность связей между поставщиками. Поскольку сеть доступа подключена к сетям нескольких провайдеров, нереально настроить все эти каналы так, чтобы они поддерживали 100% всего пользовательского трафика в сети доступа. Если такая сеть провайдера отправляет больше трафика, чем рассчитана ссылка, ссылка станет перегруженной. Обратите внимание, что провайдеры знают о размерах ссылок между провайдерами и выбирают, по какой из этих ссылок отправлять свой трафик. Если такая сеть провайдера отправляет больше трафика, чем рассчитана ссылка, ссылка станет перегруженной.

С технической точки зрения природа IP-трафика (UDP и TCP) и современные механизмы управления означают, что некоторая перегрузка всегда будет происходить. Каждое TCP-соединение по своей природе пытается заполнить доступную пропускную способность канала, отправляя все больше и больше пакетов, пока не будет обнаружена перегрузка, активируя механизмы контроля перегрузки и приводя к реакции задержки. Существуют разные разновидности TCP, и все они пытаются оптимизировать пропускную способность, контролировать перегрузку и быть справедливыми по отношению к другим потокам. На эти три цели напрямую влияет длина очереди и механизм отбрасывания/маркировки пакетов, используемый в очереди. Независимо от глубины очереди, текущие разновидности TCP всегда будут приводить к заполнению очереди и перегрузке. Когда TCP смешивается с трафиком UDP без каких-либо различий, неограниченный трафик UDP (приложения без управления потоком) приводит к перегрузке и отбрасыванию пакетов как для данных UDP, так и для данных TCP, что может привести к голоданию потоков TCP. В сети доступа обычно имеется несколько каналов с высокой пропускной способностью (например, 1, 10 Гбит/с) на сетевой стороне узла доступа, которые перенаправляют трафик на множество пользовательских каналов с меньшей пропускной способностью (например, ~ 100 Мбит/с для VDSL). В нисходящем направлении входящий импульсный высокоскоростной трафик необходимо буферизовать на

низкоскоростных пользовательских линиях. Несоответствие скоростей входящего и исходящего трафика может привести к заполнению очереди даже для потоков ниже скорости линии отдельного пользователя.

Приложения, переносимые по сетям доступа, расширились в масштабах и значительно увеличили объем трафика, перейдя от базовой услуги доступа к Интернету к Triple Play и конвергенции фиксированной и мобильной связи к облачным приложениям. Такие приложения также предъявляют новые требования к QoS. Например, мобильная передняя связь может иметь очень строгие требования к задержке и джиттеру при транспортировке между распределенными и централизованными узлами, составляющими блок основной полосы частот. Кроме того, будущие приложения следующего поколения, такие как сверхнадежная связь с малой задержкой, будут обеспечивать очень низкую сквозную задержку на уровне приложений (порядка 1 мс). Сохранение перегруженности и расширение количества услуг, нагрузки на них и ожидаемого качества обслуживания иллюстрируют постоянную важность применения надлежащих методов управления трафиком в сетях доступа. Текущее использование управления трафиком в сетях с мультисервисным доступом

Как описано в разделе 4.1 документа [4], мультисервисная сеть доступа «поддерживает различные IP-услуги в дополнение к доступу в Интернет, включая бытовые услуги, такие как IPTV и голосовая связь. Трафик для этих услуг может поступать от сетевых провайдеров (NSP) или поставщиков приложений (ASP) через [интерфейс провайдера к провайдеру] в виде IP-трафика или (для таких услуг, как бизнес-связность уровня 2) от другого сетевого провайдера в виде Ethernet или другого Трафик второго уровня. Этот трафик может быть мультиплексирован с трафиком доступа в Интернет в региональной сети или сети доступа, как показано, и может быть запланирован вместе с трафиком доступа в Интернет для создания желаемого QoS для каждой услуги». В таких сетях общепринятой практикой является применение дифференцированной обработки трафика путем его классификации по разным потокам пакетов для каждого пользователя и/или для каждого приложения, а также путем применения предписанного набора действий к разным потокам. Подробную информацию об управлении трафиком и дифференциации трафика см. в [4] и [5].

Пример структуры и функциональных блоков типичной сети доступа FTTx приведен на рисунке 1. На нем показано подключение для сочетания интернета и услуг, управляемых оператором, с типичным примером мер управления трафиком, используемых в различных точках сети. . В этом разделе основное внимание уделяется части доступа к сети (от узла доступа до резидентного шлюза конечного пользователя). Аналогичные механизмы могут использоваться и в других частях сети (пограничный сетевой шлюз, промежуточные коммутаторы агрегации). Дополнительную информацию об архитектуре фиксированных широкополосных сетей см. в [6], [7], [8], [9], [10], а дополнительную информацию об участии Residential Gateway см. в Приложении A в[11].

Дифференцированное управление трафиком в сетях с мультисервисным доступом состоит из классификации трафика, за которой следуют такие действия, как активное управление очередями (AУО) с отбрасыванием/перемаркировкой пакетов, планирование очередей, управление скоростью (формирование, применение политик) и, возможно, управление допуском к общие ресурсы. Классификация по пакетам заключается в распознавании определенного трафика как отличного от другого трафика для предоставления ему дифференцированной обработки. Обычно это делается на границе сети или на самом устройстве конечного пользователя (если оператор доверяет этому устройству, например, собственному сервисному ящику оператора). Классификация может основываться на различных характеристиках трафика, включая исходный, целевой, транспортный или прикладной протокол, а также на значениях определенных битов в заголовках различных протоколов (например, кодовая точка diffserv или DSCP в заголовке IP или биты приоритета в заголовке IP). Заголовок кадра Ethernet). Некоторые операторы используют управление трафиком как часть продуктовых приложений и услуг.

К разным классам трафика может применяться разная обработка. Приоритизация — это практика, при которой некоторый трафик обрабатывается лучше, чем другой трафик (например, пакеты отправляются раньше других пакетов или не отбрасываются при перегрузке). К разным классам трафика можно применять разные политики. Основными механизмами, используемыми для приоритизации, являются организация очередей и планирование, при которых пакеты из разных классов трафика обслуживаются (измеряются, маркируются или отбрасываются, а затем пересылаются путем формирования очереди и планирования между очередями) с учетом приоритета или взвешенным циклическим способом. Контроль скорости путем формирования или применения политик не позволяет любому конкретному пользователю загружать сеть сверх своего профиля коммерческого обслуживания (таким образом, также влияя на обслуживание других пользователей). По этой же причине доступ к сетевым ресурсам (мощность сети, мощность сервера приложений) может контролироваться для специализированных сервисов. Контроль доступа также может предотвратить неосознанное снижение пользователями своих собственных услуг, запрашивая слишком много экземпляров приложений для их скорости соединения. Важно подчеркнуть, что методы управления перегрузкой всегда должны быть активны. Нецелесообразно активировать их только при обнаружении заторов, поскольку они могут иметь и профилактический эффект. Например, формирование трафика посредством буферизации сглаживает пики трафика и позволяет избежать жесткого ограничения (контроля) данных; пики невозможно предсказать, и, следовательно, формирование всегда должно оставаться включенным.

Наконец, обратите внимание, что сеть также может косвенно улучшать QoS с помощью других средств;

- Путем перемещения контента ближе к конечному пользователю. Сети доставки контента (CDN) помогают распространять контент по всему миру масштабируемым образом. В сетях доступа прозрачные кэши снижают задержку, уменьшают потребность в повторных передачах и снижают нагрузку трафика в точках соединения. Конечно, кэширование не отвечает потребностям интерактивных приложений.
- путем построения деревьев IP-многоадресной рассылки как способа ограничения нагрузки в частях сети по сравнению с эквивалентным набором одноадресных потоков, оставляя больше возможностей для других приложений и потоков, тем самым косвенно улучшая качество обслуживания.

Влияние оконечных устройств на конечное QoS

Различные механизмы на самих конечных точках (одноранговые узлы или клиент и сервер) также будут влиять на конечное QoS и QoE в дополнение к механизмам управления трафиком, используемым оператором в своих сетевых элементах. Как мы можем сравнить влияние конечных точек и промежуточной сети? С точки зрения конечной точки промежуточная сеть представляет собой черный ящик, который может иметь различную пропускную способность и задержку. Хотя конечные точки могут исследовать поведение сети, они не могут контролировать его. Конечные точки могут адаптировать способ отправки своего трафика на другой конец только следующим образом:

Маркировка пакетов (хотя обычно такая маркировка считается недоверенной операторами и перезаписывается в сети)

1. Адаптация скорости передачи к обратной связи с другого конца (например, медленный запуск TCP и предотвращение перегрузки, например, версия UDP для QUIC от Google)
2. Распределение трафика по нескольким параллельным потокам TCP, что позволяет конечной точке использовать больше ресурсов, чем конечным точкам, пытающимся использовать только один поток, что приводит к конкуренции между конечными точками.
3. Настройка поведения сервера (например, запуск более агрессивной версии TCP на стороне сервера в некоторые критические моменты). Но это приводит к конкуренции между потоками, кто-то выигрывает, а кто-то проигрывает, так что это не приведет к глобальному улучшению.

Использование оконечных устройств на конечном QoS

Различные механизмы на конечной конечной точке (одноранговые узлы или клиент и сервер) также включают в себя конечное QoS и QoE в соответствии с механизмом управления трафиком, часто используемым оператором в своих элементах сети. Как мы можем оценить влияние конечных точек и промежуточной сети?

С точки зрения конечной точки зрения промежуточная оценка представляет собой черный ящик, который может иметь различную пропускную способность и поддержку. Несмотря на конечные точки наблюдения за поведением сети, они не контролируют его. Конечные точки зрения представляют собой способ передачи своего трафика на конец другого пути:

- Обычно такая маркировка пакетов (обычно такая маркировка недоверенной операторами и перезапуск в сети)
- Адаптация скорости передачи к точке наблюдения с другой стороны (например, медленный запуск TCP и отклонение перегрузки, например, версия UDP для QUIC от Google)
- Распределение трафика по калориям потока TCP, что позволяет конечной производительности использовать больше ресурсов, чем конечными точками, пытающимися использовать только один поток, что приводит к конкуренции между конечными точками.
- настройка поведения сервера (например, запуск более агрессивной версии TCP на стороне сервера в некоторых случаях). Но это приводит к конкуренции между потоками, кто-то выигрывает, а кто-то проигрывает, так что это не происходит к глобальному миру.

Управление трафиком в контексте мультимедиа

Приложения будут отличаться требованиями к производительности QoS. Дифференцированная обработка классов трафика с приоритетом и контролем использования пропускной способности может улучшить качество обслуживания для чувствительных приложений, не нанося ущерба качеству других приложений, при условии, что классы с более низким приоритетом защищены от истощения классами с более высоким приоритетом. Перегрузка по-прежнему означает, что те пакеты, которые больше не могут быть обслужены в данный момент времени, отбрасываются или задерживаются. Но пакеты могут быть отброшены без драматических последствий при правильном выполнении, а задержки не всегда критичны. Некоторые приложения (такие как связь в реальном времени) очень чувствительны к задержкам, но более устойчивы к потерям, чем другие, в то время как другие (например, потоковое видео) нетерпимы к потере пакетов, но могут выдерживать большие задержки. Вот почему имеет смысл группировать приложения, чувствительные к задержкам, в классы трафика с мелкими буферами, а более чувствительные к потерям приложения — в классы трафика с глубокими буферами. Веб-приложения не в режиме реального времени, передаваемые по TCP, не чувствительны ни к задержкам, ни к потерям, но требуется

большая буферизация, чтобы обеспечить справедливую и стабильную пропускную способность TCP для потоков с разным временем прохождения туда и обратно (Round Trip Times).

Без дифференциации на любое приложение может повлиять потеря пакетов или заполнение буфера. Без контроля использования полосы пропускания некоторым пользователям или приложениям может быть нанесен ущерб из-за «неправильного поведения» других пользователей или приложений.

Обратите внимание, что трафик высокоскоростного Интернета (High Speed Internet) переносит любое приложение Over-The-Top (OTT), от просмотра до потоковой передачи и связи в реальном времени. HSI — это единый класс трафика с максимальной эффективностью. Следовательно, любые требования QoS приложений OTT (например, видео через HTTP) не могут быть удовлетворены сетью. Это означает, что даже для HSI-трафика Best Effort должен быть определен хотя бы некоторый минимальный уровень поддержки. Дифференциальное управление трафиком направлено на оптимизацию для каждого класса трафика четырех параметров QoS: пропускная способность, задержка, изменение задержки пакетов и потеря пакетов2. На рис. 2 дается обзор важности параметров качества для HSI, VoIP, IPTV и мобильной транспортной сети. Можно отметить, что, несмотря на то, что HSI оценивается как «максимальное усилие», все же существуют некоторые минимальные требования к качеству (например, подключение к Интернету не должно быть полностью маргинализировано другими услугами с более высоким приоритетом). С помощью управления трафиком каждому классу трафика можно назначить относительный приоритет и соответствующую обработку буфера, что позволяет сосуществовать различным классам в одной инфраструктуре с ограниченными общими ресурсами.

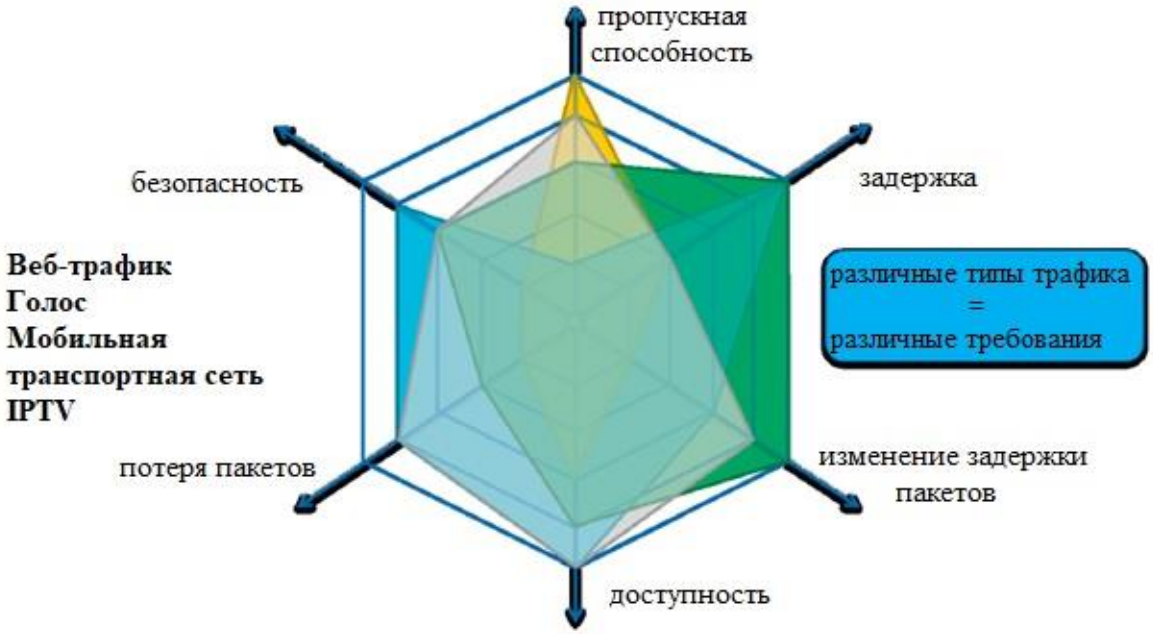

Рис.1-Типы трафика и их соответствующие требования к качеству

Дифференцированное управление трафиком иногда может принести пользу клиентам, например:

- Приоритизация аварийно-спасательных служб по сравнению с другими видами дорожного движения гарантирует доступность услуг для спасения жизней.
- Адекватная организация очередей и приоритетное планирование для видеотрафика (IPTV) снижает потери пакетов и защищает его пропускную способность и, следовательно, может дать оператору возможность обеспечить хорошее качество восприятия для своих клиентов.
- Бизнес-клиенты обычно имеют строгое SLA (соглашение об уровне обслуживания) с операторами, и операторы должны соблюдать это SLA, не влияя на качество, воспринимаемое всеми другими клиентами.

Как упоминалось ранее, причиной перегрузки и, следовательно, ухудшения качества обслуживания является потребность в ресурсах, превышающих доступные ресурсы, а также технико-экономическая реальность размеров сети. Давайте возьмем пример дифференциации трафика в действии. Предположим, что управляемая видеоконференция между двумя сторонами и сеанс FTP через доступ в Интернет осуществляются через одно и то же пользовательское соединение.

- Применяя общее ограничение скорости, общий трафик пользователя приводится в соответствие с его тарифом на подписку на услугу.
- Оператор управляет сеансом видеоконференции. Контроль допуска на прикладном уровне применяется для проверки подписки на услугу.

- Поток видеоконференций классифицируется как класс трафика в реальном времени и имеет приоритет над интернет-трафиком Best Effort. Трафик буферизуется в неглубоких очередях, что обеспечивает низкую задержку. Когда в соединении возникает перегрузка (например, из-за увеличения трафика TCP), поток видеоконференции будет поддерживать низкую задержку и пропускную способность благодаря своей мелкой очереди и классу трафика, обслуживаемому со строгим приоритетом. Кроме того, объем трафика в этом классе трафика контролируется (управляемыми приложениями и ограничением скорости), чтобы избежать потерь из-за несоответствующих пользовательских потоков.
- Оператор не управляет сеансом FTP, он классифицируется как Best Effort и имеет более низкий приоритет, но обслуживается более длинными очередями, что поддерживает пропускную способность TCP. Механизм TCP попытается максимально использовать доступную полосу пропускания, вплоть до перегрузки. Когда возникает перегрузка, в сеансе TCP происходит отбрасывание пакетов и снижается скорость. Поскольку пакеты видеовызовов получают более высокий приоритет, поток TCP будет испытывать большую перегрузку при наличии видеовызова и снизит его скорость, но как только высвободится больше пропускной способности (например, видеовызов завершен), он снова увеличится до попытаться заполнить только что освободившуюся емкость.

Будущие эволюции

Эволюция телекоммуникационной отрасли с новыми парадигмами требует сети со сверхнизкой задержкой [12]. В зависимости от приложения может потребоваться или не потребоваться дифференцированная обработка для обеспечения достаточной производительности QoS. Эти новые сетевые и сервисные разработки включают в себя;

- Виртуальная реальность — для этого требуется очень высокая пропускная способность и низкая задержка, чтобы избежать неприятного взаимодействия с пользователем.
- Переход к виртуализации сетевых функций (NFV) и программно-определяемым сетям (SDN). Подход SDN/NFV открывает возможность переноса функций с сетевых элементов на облачную серверную инфраструктуру NFV, а также возможность программирования сети за счет использования NETCONF/YANG в плоскости управления. Что касается управления трафиком, такая программируемость может охватывать правила QoS (например, правила классификации) и совместное использование или резервирование ресурсов между службами или виртуальными операторами (например, разделение оборудования или мультиарендность на основе управления). Broadband Forum активно участвует в определении моделей YANG. Правила и политики QoS могут стать более сложными из-за более динамичной среды.

«Промышленный Интернет» представляет собой переход от сети, ориентированной на человека (с задержками порядка одной цифры мс), к сети, совместимой с машинами (Интернет вещей), с некоторыми приложениями, требующими гораздо меньшей задержки (в 100 раз меньше, чем порядка мкс).

- Мобильная обратная и передняя связь будет все больше использовать части тех же активов доступа и агрегации, что и фиксированные услуги. Новые поколения мобильных устройств (5G) будут предъявлять еще более строгие требования к задержке и колебаниям задержки пакетов.
- Устранение задержек в очереди является фундаментальным фактором такого развития, однако разновидностям TCP, используемым в настоящее время в Интернете, требуется организация очередей для достижения стабильно высокой загрузки канала. Были предложены новые варианты TCP, которые могут работать при почти нулевом заполнении очереди, такие как TCP центра обработки данных (DTCCP). DTCCP может поддерживать низкую задержку в очереди без ущерба для использования канала. Но DTCCP не используется в Интернете, потому что это привело бы к голоданию устаревших разновидностей TCP. Недавно в IETF (Dual Queue Coupled AQM) обсуждался новый AQM, который мог бы решить эту проблему. Внедрение такого механизма управления трафиком AQM в сетевые узлы позволит Интернету развиваться для поддержки службы TCP с малой задержкой и низкими потерями без ущерба для производительности классического трафика, тем самым обеспечивая «справедливость» обслуживания или нейтральность в производительности потока. независимо от разновидности TCP.

Выводы

Мы изучили ценность и механизмы применения некоторых методов управления трафиком в мультимедийных сетях доступа. Дифференциация трафика обычно используется для управления трафиком от нескольких сервисов в точках перегрузки, с назначением приоритетов для балансировки потребностей QoS различных сервисов, а также для управления скоростью и доступом для справедливого управления общими ресурсами. Перегрузка не может быть устранена как таковая из-за ограниченного и общего характера сетевых ресурсов и их использования требовательными к скорости приложениями и протоколами. Преимущество дифференцированного управления трафиком заключается в обеспечении обработки QoS для конкретного класса трафика, что, в свою очередь, позволяет чувствительным приложениям обеспечивать требуемое качество обслуживания без блокировки других типов приложений даже в случае перегрузки.

Соответствующее управление трафиком требуется как для специализированных сервисов, так и для HSI, что позволяет им сосуществовать в общей мультимедийной сетевой инфраструктуре. Операторы используют такое

управление трафиком для предоставления услуг с добавленной стоимостью как частным, так и бизнес-пользователям, включая транзитную (и переднюю) мобильную связь. Хотя в такой схеме доступ в интернет, как правило, относится к самому низкому классу трафика, минимальный уровень обслуживания может быть обеспечен за счет адекватного определения параметров сети и управления ресурсами.

Простое устранение узких мест в доступе и увеличение скорости линии для всех не будет решением без выбранных методов управления трафиком. Такие методы играют важную роль в оптимизации использования пропускной способности сети, но это не избавляет от необходимости вкладывать средства в дополнительную пропускную способность, когда начинают возникать длительные периоды перегрузки.

Исследовательская работа по новым механизмам управления трафиком все еще продолжается, поэтому ожидается дальнейшее развитие.

Литературы

1. Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32015R2120&from=EN
2. "Broadband Access Service Attributes and Performance Metrics", Broadband Forum TR-304
3. "Triple Play Services Quality of Experience (QoE) Requirements", Broadband Forum TR-126
4. "Differentiated Treatment of Internet Traffic", Broadband Internet Technical Advisory Group Technical Working Group Report – BITAG, October 2015
5. "Real-time Network Management of Internet Congestion", Broadband Internet Technical Advisory Group Technical Working Group Report – BITAG, October 2013
6. "Broadband Remote Access Server (BRAS) Requirements Document", Broadband Forum TR-92
7. "Migration to Ethernet-Based DSL Aggregation", Broadband Forum TR-101
8. "Using GPON Access in the context of TR-101", Broadband Forum TR-156
9. "GPON-fed TR-101 Ethernet Access Node", Broadband Forum TR-167, "
10. "Multi-service Broadband Network Architecture and Nodal Requirements", Broadband Forum TR-178
11. "Internet Gateway Device Data Model for TR-069", Broadband Forum TR-098
12. ITU-T Technology Watch Report (August 2014) - The Tactile Internet