Механизмы качества обслуживания в мультисервисных корпоративных сетях

авторы: Бобров С.И., Корж А.В.

Современные предприятия эффективно функционируют только при постоянном и оперативном информационном обмене между подразделениями. Для эффективного функционирования информационной системы должна быть создана телекоммуникационная инфраструктура. В случае сосредоточенного предприятия эта задача решается относительно просто, путем построения локальной сети (LAN), в случае распределенного предприятия задача становится уже не столь тривиальной и требует построения глобальной сети (WAN) между подразделениями предприятия, но и в том, и в другом случае необходимо обеспечивать качественную передачу технологической информации, электронной почты, трафика ERP и пр.

Основные требования к корпоративным сетям состоят в предоставлении всех необходимых телекоммуникационных и информационных сервисов подразделениям предприятия при оптимизации капитальных затрат на создание сети и минимизации стоимости владения.

Исходя из этого можно сформулировать некоторые базовые принципы построения корпоративных сетей.

– Передача всех типов трафика должна происходить по единым каналам связи (нет нужды строить несколько параллельных сетей, если можно для передачи всего трафика построить и эксплуатировать одну). Другими словами, корпоративная сеть должна быть мультисервисной.

– Для того чтобы иметь возможность наращивать сеть и стыковать ее с другими сетями, она должна строиться на базе открытых стандартов и интерфейсов.

– Исходя из принципа минимизации расходов на создание и эксплуатацию сети корпоративная сеть должна быть сетью с коммутацией пакетов. Обоснованием этого принципа является высокая эффективность использования каналов связи в сетях с коммутацией пакетов по сравнению с сетями с коммутацией каналов. Это особенно важно для минимизации стоимостных показателей корпоративной сети.

Итак, наиболее эффективной будет корпоративная сеть, построенная на таких принципах, как мультисервисность и коммутация пакетов.

Разные типы трафика предъявляют свои специфические требования к характеристикам канала связи. Наиболее жесткие требования по времени доставки у голосового трафика, наименее жесткие – у FTP, SMTP и т.п. Вследствие того что весь трафик передается по одному и тому же каналу, менее приоритетный трафик может создать помеху более приоритетному.

Стоит задача минимизировать необходимую пропускную способность каналов (то есть затраты) и при этом обеспечить каждому типу трафика такие параметры доставки, которые удовлетворили бы его требования без ущерба остальному трафику, обеспечивая, так сказать, симбиоз информационных потоков.

Задача обеспечения требуемых параметров канала для каждого типа трафика в такой мультисервисной сети с коммутацией пакетов решается обеспечением соответствующего качества обслуживания (Quality of service – QoS) всему трафику.

Современные принципы работы QoS может пояснить известный в педагогической психологии пример.

Дети ссорились из-за одного апельсина, каждый хотел его получить. Возможным решением было бы купить еще один, но иногда это невозможно, иногда затруднительно, иногда неудобно, да и просто неэффективно (трата ресурсов). Обычным решением было бы достичь компромисса – выделить каждому по пол-апельсина и разрешить конфликт с частичным удовлетворением запросов каждого.

Когда все же решили узнать, зачем же апельсин нужен детям, то выяснили, что девочке нужна кожура для торта, а мальчик хочет сделать апельсиновый сок. Так, узнав требования каждого, получилось

удовлетворить потребности всех, предоставив искомые части апельсина (специфические ресурсы) так, что полностью выполнили запросы каждого. Таким образом, чтобы эффективно решить задачу, надо на первом этапе узнать и проанализировать конкретные требования претендующих на ресурс.

Механизм QoS функционирует сходным образом, обеспечивая надлежащий уровень сервиса для различных типов сетевого трафика при наличии ограниченного канального ресурса. QoS анализирует требования и предоставляет каждому типу трафика удовлетворяющие его значения параметров продвижения трафика по сети: потеря пакетов, задержка, вариация задержки (джиттер). Качество передачи информации напрямую зависит от этих параметров. Так, например, для качественной передачи голоса по сетям с коммутацией пакетов существуют следующие требования: не более 1 % потерь и не более 1 последовательно потерянного пакета: это вызвано тем, что голосовой кодек может скорректировать потерю голосового фрагмента длительностью до 30 мс, а стандартный пакет VoIP несет в себе образец голоса длиной 20 мс; задержка распространения голосовых пакетов в одну сторону из конца в конец описывается рекомендацией ITU-T G.114 и должна составлять для сетей общего пользования величину, не превышающую 150 мс; вариация задержки, определяется величиной буфера и не должна превышать 40 мс.

Требования к параметрам канала для качественной передачи видео намного мягче: не более 2 % потерь; задержка распространения видео в одну сторону из конца в конец должна быть не более 2 сек.; к вариации задержки жестких требований не предъявляется.

Трафик SMTP вообще не имеет сколько-нибудь существенных требований к параметрам канала.

Существуют следующие модели обслуживания трафика:

– Best-effort services model (модель услуг скорейшей доставки);

– Integrated services model – IntServ (модель интегрированных услуг);

– Differentiated services model – DiffServ (модель дифференцированных услуг).

Best-effort – это единственная модель, в которой приложение высылает информацию когда хочет, какую хочет, сколько хочет и без какого-либо уведомления или запроса, да и сетевые устройства не обеспечивают выделения ресурсов сети. В этой модели сеть пересылает информацию без оценки доступных ресурсов, пропускной способности и какой-либо приоритизации трафика, используется построение очередей по умолчанию – FIFO (первый вошел – первый вышел). Эта модель подходит и используется для информационного обмена основной массы сетевых приложений: передача файлов, электронная почта и т.д., но не для высокоприоритетного и мультимедийного трафика.

IntServ – мультисервисная модель, которая может учесть и обеспечить множественные требования QoS. В рамках этой модели конечные приложения запрашивают определенные ресурсы сети для передачи трафика по сети и требуют обеспечения необходимой пропускной способности и задержки. Информация будет выслана через сеть только после подтверждения выделения в сети необходимых ресурсов для трафика. Вполне естественно и логично, что для работы этой модели нужны QoS-совместимые приложения.

Сетевые ресурсы выделяются в соответствии с требованиями приложений и остаются занятыми до тех пор, пока трафик движется через сеть.

IntServ предусматривает использование приложением протокола Resource reservation protocol (RSVP – протокол резервирования ресурсов) для информирования сетевых устройств о параметрах трафика и требуемых ресурсах сети.

В модели IntServ рассматривается два типа услуг:

1) guaranteed service (гарантированный сервис) позволяет приложениям резервировать пропускную способность для обеспечения гарантированного времени задержки передачи информации;

2) controlled load (управляемая нагрузка) осуществляет доставку трафика через сеть с минимальными помехами со стороны низкоприоритетного трафика и обеспечивает лучший контроль за сетевыми ресурсами, чем тот, что реализован в модели услуг скорейшей доставки.

Модель IntServ требует выделения служебных сетевых ресурсов для каждого потока информации. Для миллионов потоков информации в Интернете, количество служебной информации в рамках этой модели является чрезмерным. Это, а также необходимость пользоваться только QoS-совместимыми приложениями делает затруднительным распространение этой модели в больших сетях с разнородным оборудованием и ПО. Глобальным примером такой сети является Интернет.

Модель DiffServ занимает промежуточное положение между моделью Best-effort services с ее неспособностью управлять сетевыми ресурсами и моделью IntServ с ее значительными требованиями к сетевому окружению.

В этой модели каждый пакет классифицируется (маркируется) на коммутаторах или маршрутизаторах на границах сети, пакеты или кадры объединяются в группы (классы) на основе сходных требований к ресурсам сети. На базе этого на каждом узле сети таким группам или классам предо- ставляются соответствующие ресурсы сети на основании приоритетности класса трафика и наличия ресурсов.

Преимуществом метода DiffServ является то, что он не требует QoS-совместимых приложений.

Маркирование может быть осуществлено модификацией одного из следующих полей:

– три старших бита в байте IP ToS (поле IP Precedence);

– шесть старших битов в байте IP ToS (поле DSCP (Differentiated services code point);

– три бита поля Class of service (CoS) кадра Ethernet;

– три бита MPLS Experimental;

– один бит Cell loss probability ячейки ATM.

В связи с тем что функции QoS обеспечиваются самой технологией ATM, которая редко используется при построении корпоративной сети, в дальнейшем будем рассматривать три первых способа маркирования трафика как наиболее часто используемых в корпоративных сетях и считать, что при классификации трафика модифицируются либо поле Type of service (ToS) заголовка IP-пакета, либо поле CoS заголовка ISL/802.1q кадра.

На сетевом уровне IP-пакеты можно классифицировать двумя способами: установкой полей IP Precedence или DSCP в байте ToS, а на канальном уровне кадры Ethernet, а именно кадры IEEE 802.1q – установкой поля CoS.

Поскольку маркирование трафика – одна из важнейших составляющих применения QoS, то выбор метода классификации требует более детального описания:

– классификация на канальном уровне может быть применена при любом протоколе сетевого уровня модели ISO;

– классификация на канальном уровне – это единственный вариант классификации для не-IP-трафика;

– классификация на сетевом уровне позволяет QoS-маркирование вне зависимости от технологии канального уровня, то есть применима для межсетевого взаимодействия;

– устаревшее оборудование может не понимать DSCP;

– может быть установлено до 8 значений IP Precedence и до 64 значений DSCP;

– может быть установлено до 8 значений поля CoS.

И хотя сначала кажется удивительным наличие трех опций для маркирования, в реальных сетях со всем многообразием оборудования и технологий наличие трех вариантов оказывается совсем не лишним.

В общем случае для маркирования трафика в маршрутизируемой сети (WAN) на сетевом уровне используют DSCP, поле CoS используется для маркирования кадров в коммутируемой сети (LAN).

Классификация на канальном уровне обеспечивает маркирование пакетов при помощи поля CoS. Значение изменяется от нуля для наименьшего приоритета до семи для наивысшего. Порты коммутатора устанавливают входящему трафику соответствующее поле CoS. Маршрутизаторы могут преобразовать значение поля CoS в соответствующие значения поля IP Precedence или DSCP.

Классификация на сетевом уровне выполняется устройствами третьего уровня (маршрутизаторами); такая классификация воспринимается всеми сетевыми устройствами IP-сети и может быть ими изменена при прохождении пакета через сеть. Одинаковое значение поля соответствует одинаковым требованиям трафика к параметрам сети. Поскольку DSCP занимает старшие 6 бит байта ToS, а IP Precedence старшие 3 бита, то одновременно DSCP и IP Precedence не могут быть использованы; при их совместном использовании DSCP будет иметь преимущество и, кроме того, он обеспечивает более гибкую настройку QoS за счет наличия 64 возможных значений. К сожалению, если хоть одно устройство в сети не понимает DSCP, то в сети для классификации на сетевом уровне можно использовать только IP Precedence.

Современные методы маркирования строятся на базе классов с использованием политик. Рекомендуемой моделью построения QoS считается MQC (Modular QoS CLI). Наиболее важным преимуществом этой модели является модульность и независимость каждого модуля-этапа применения QoS друг от друга. MQC описывает следующую последовательность применения механизма QoS:

– идентификация трафика;

– маркирование трафика или определение принадлежности трафика к тому или другому классу;

– назначение политики QoS классам;

– применение политик на интерфейсы.

Модульность MQC позволяет повторно использовать определенные классы и политики, а также упростить внесение изменений и поиск ошибок. Именно с этой целью была разработана модель OSI и объектно-ориентированное программирование.

Идентификация трафика позволяет одним из известных способов определить интересующий нас трафик, чтобы в дальнейшем выделить классы трафика и применить к нему механизмы QoS. Хотя возможны различные методы идентификации, но чаще всего для идентификации трафика применяют списки доступа (ACL).

В процессе маркирования идентифицированный на предыдущем этапе трафик назначается классам, что позволяет строить механизм QoS на базе классов и политик.

Назначение политики QoS классам описывается построением и управлением очередями, методикой опроса очередей (queuing) и отбрасывания пакетов.

Основными методами построения очередей считаются следующие.

FIFO (First IN – First Out) – пакеты поступают в очередь и покидают ее в одной и той же последовательности. Не обеспечивается ни приоритизация трафика, ни гарантированная пропускная способность. Наименее подходит для обеспечения механизмов QoS.

CQ (Custom queuing) – потоки трафика размещаются в 16 очередей (с 1 по 16) с определенной глубиной очереди. Существует еще так называемая нулевая очередь для служебного трафика (управляющие пакеты, keepalive и т.д.), информационный трафик не может быть помещен в эту очередь. Трафик помещается в определенную очередь по критериям: входящий интерфейс, списки доступа, размеры пакетов и типы приложений. Данные выбираются последовательно из каждой очереди. Размер выборки для каждой очереди определяется средней величиной пакета, MTU и необходимой пропускной способностью. Размер выборки вычисляется для каждой очереди отдельно, обеспечивая заданную пропускную способность. Надо заметить, что за каждую выборку из очереди выбирается не заданное количество байт, а то количество

пакетов, которое вмещает не меньше, заданного количества байтов. Гарантированная пропускная способность обеспечивается весьма приблизительно.

PQ (Priority queuing) – трафик выделяется в четыре очереди с высоким, средним, нормальным и низким приоритетами. Трафик в очередях обслуживается в следующей последовательности: сначала из очереди с высоким приоритетом, потом средним, затем нормальным и т.д. Если есть хоть один пакет в очереди с более высоким приоритетом, то будет обслуживаться именно он, вне зависимости от количества пакетов в менее приоритетных очередях. Это приводит к тому, что данные в очереди с высоким приоритетом, вероятнее всего, будут доставлены без потерь и задержек, но при этом данные из других очередей могут быть потеряны или доставлены с большой задержкой. При переполнении сети трафик из высокоприоритетной очереди может занять весь канал, отказывая таким образом в обслуживании остальному трафику.

WFQ (Weight fair queuing – справедливое весовое построение очередей) может быть построена на базе потоков трафика (Flow-based WFQ) и классов трафика (Class-based WFQ). Если говорить о FBWFQ, то потоки трафика размещаются в соответствующих очередях. В простейшем случае каждая очередь обслуживается на общих основаниях, получая равную часть пропускной способности канала. При этом количество бит, передаваемых за одну выборку, у всех очередей одинаково, и, соответственно, пакеты небольшого размера покидают очередь быстрее, чем пакеты большого размера. Вследствие того что голосовой трафик обычно передается короткими пакетами, пакеты такого трафика покидают очередь быстрее, чем большие пакеты, характерные для FTP, SMTP и др. В отдельных случаях механизм QoS требует предоставления некоторым очередям больше ресурсов сети. Распределения ресурсов сети между очередями производится на базе веса очереди: чем меньше вес, тем больше приоритет очереди. Вес очереди

может быть определен на базе значения поля IP Precedence из выражения: Вес= , а пропускная способность для потока, соответственно, пропорциональна величине IP Precedence+1. Поток трафика с большим значением IP Precedence получает большую часть пропускной способности.

CBWFQ может более гибко выделять трафик в очереди. В этом случае принадлежность трафика к очереди может определяться администратором на базе IP Precedence, DSCP, интерфейсов и списков доступа (ACL). CBWFQ обеспечивает гарантированную пропускную способность. Весь трафик выделяется в несколько очередей с гарантии- рованной пропускной способностью или без ее резервирования. Для классификации используется MQC.

WFQ применяется по умолчанию на последовательных интерфейсах с пропускной способностью до 2 Мб/с. По умолчанию количество очередей ограничено значением 256. С одной стороны, каждая зарезервированная очередь – это использованный ресурс памяти устройства, с другой, если количество сформированных потоков (классов) больше, чем очередей, то несколько потоков (классов) будут вынуждены разделять одну очередь, что может отрицательно сказаться на качестве передачи трафика.

LLQ (Low latency queuing) – поступающий трафик размещается в таких очередях: приоритетной, в несколько очередей с зарезервированной пропускной способностью или в очередь по умолчанию без резервирования пропускной способности. Для классификации используется MQC.

Трафик, помещенный в приоритетную очередь, обслуживается в первую очередь аналогично обслуживанию высокоприоритетного трафика в Priority queuing, но в пределах заданной для этой очереди пропускной способности, чтобы не позволить высокоприоритетному трафику узурпировать весь канал. Приоритетная очередь используется для такого чувствительного к задержке трафика, как голос.

Трафик, помещенный в одну из нескольких очередей с зарезервированной пропускной способностью, обслуживается после высокоприоритетного трафика наравне с трафиком из других очередей с зарезервированной пропускной способностью. Трафику в этих очередях гарантируется пропускная способность, но не гарантируется приоритетное обслуживание, поэтому не рекомендуется использовать их для передачи такого весьма критичного к задержке трафика, как голос.

По умолчанию эти два вида очередей не могут использовать более 75 % канала, оставляя для неклассифицированного трафика, помещенного в незарезервированную очередь, 25 % пропускной способности канала.

Можно сказать, что LLQ – это своего рода симбиоз PQ и CBWFQ.

LLQ наиболее подходит для обеспечения механизмов QoS. Существует приоритетная очередь с гарантированной пропускной способностью для критичного к задержке трафика и очереди с гарантированной пропускной способностью, но без приоритета, для трафика, критичного к пропускной способности, но не столь критичного к задержке и к вариации задержки. Неклассифицированный трафик передается в очереди без гарантированной пропускной способности и без приоритета.

Итак, для эффективной передачи по корпоративной сети разнородного трафика с предоставлением каждому типу трафика тех ресурсов сети, которые требуются для него, необходимо применять механизмы QoS. Использование MQC и LLQ дает возможность добиться наилучшего результата при построении мультисервисных корпоративных сетей. Построение сети с пакетной коммутацией позволяет эффективно использовать пропускную способность каналов, а применение на такой сети механизма QoS обеспечивает качественную передачу всех типов трафика сети.

Необходимо отметить, что применение механизмов QoS имеет смысл при средней загрузке канала с пиками до 100 %. При загрузке канала в среднем менее 30 % и отсутствии пиков до 100 % в применении QoS нет нужды, так как он все равно не работает. При постоянной загрузке канала, близкой к 100 %, работа QoS будет тоже малоэффективна, в этом случае рекомендуется увеличивать пропускную способность канала.

Рассмотрим возможную реализацию изложенных принципов в корпоративных сетях на примере территориально-распределенного предприятия, подразделения которого объединены каналами WAN. Требуемые услуги: передача критически важных технологических данных, передача электронной почты, web-трафика и пр.

Корпоративный трафик генерируется приложениями и поступает в сеть. На границе сети (в маршрутизаторе или коммутаторе) критически важные данные и голосовой трафик (в случае мультисервисной пакетной сети – VoIP) могут быть определены по параметрам: логический адрес источника/назначения, протокол транспортного уровня, его порты, входящий интерфейс. Идентификация трафика может быть осуществлена списками доступа (ACL) или по значению полей CoS, ToS. Списки доступа могут выделить трафик, опираясь на его параметры сетевого и транспортного уровня, так, VoIP-пакеты – это UDP-сегменты с номерами порта 16384-32767, сигнализация передается TCP, номер порта 1720; технологический трафик может иметь какой-то выделенный IP-адрес источника/назначения (например, серверов ERP) или специфический порт протокола транспортного уровня. Что касается CoS и ToS, если их значение выставило приложение, то сетевое устройство может согласиться с установленными значениями или модифицировать их. Например, IP-телефоны выставляют IP Precedence=5 и могут устанавливать поле CoS. А если, например, приложение (web-сервер) генерирует трафик с завышенным значением CoS, то коммутатор может и должен, если на него возложены функции маркирования трафика, установить это поле в соответствующее значение.

Необходимо упомянуть, что одна и та же рабочая станция может генерировать как ERP-трафик, так и SMTP, а устанавливать для всех типов трафика, генерируемых рабочей станцией, одно и тоже поле CoS в общем случае неправильно. Рекомендуется производить маркирование на устройствах сетевого уровня (маршрутизаторах, коммутаторах 3-го уровня), модифицируя по- ле ToS.

В результате идентификации трафика каждому или нескольким типам трафика назначается свой класс. Так может быть определен класс VoIP для голосового трафика, класс ERP для приоритетного технологического трафика и т.д.

После этого к каждому классу применяются политики, которые описывают выделение ресурсов сети для данного класса трафика, гарантируемую пропускную способность, предоставление приоритета. Так, допустим, голосовому трафику выделяется (на основании анализа максимальной требуемой пропускной способности) 512 кб/с, и такой трафик определяется как приоритетный, трафику ERP выделяется 1 Мб/с без приоритета. Трафику СУБД, маркированному в класс DataBase на базе значения CoS, равного 3, гарантировано выделяется 256 кб/с. Неклассифицированному трафику предоставляется оставшаяся пропускная способность, естественно, такой трафик – неприоритетный.

Заключительным этапом внедрения QoS является назначение политики на интерфейс маршрутизатора.

В результате выполнения изложенного комплекса мероприятий обеспечивается качественная передача всего корпоративного трафика по сети.

Рассмотрим ситуацию, когда высокоприоритетный трафик поступает на интерфейс, а в это время большой пакет низкоприоритетного трафика покидает его, это приводит к задержке. Задержка рассчитывается элементарно: Задержка =  . Так, если кадр размером 1500 байт покидает интерфейс в канал 64 кб/с, то задержка составит до 187 мс, что неприемлемо для голосового трафика. Это будет ощущаться при задержке во множестве очередей при прохождении по сети.

Поэтому для каналов с пропускной способностью ниже 2 Мб/с рекомендуется использовать технологию фрагментации и интерливинг (чередование) (fragmentation and interleaving).

Представим часть конфигурации граничного маршрутизатора подразделения, которая реализует описанный пример.

…

{Идентификация голосового трафика (ACL 101) и трафика ERP (ACL 102)}

access-list 101 permit udp any any range 16384 32767

access-list 101 permit tcp any any 1720

access-list 102 permit ip any host 10.36.17.18

!

{Маркирование (классификация) трафика: голосового в класс voip и ERP-трафика в класс ERP, трафика СУБД с установленным полем CoS в 3 классе DataBase}

class-map voip

  match access-group 101

class-map ERP

  match access-group 102

class-map DataBase

  match cos 3

!

{Применение политики к классам, задание llq-очереди}

policy-map llq

  class voip

       priority 512

  class ERP

       bandwidth 1024

  class DataBase

```
        bandwidth 256
  class class-default
        fair-queue
!
{Применение политики на интерфейс}
interface serial0/0
  bandwidth 2048
service-policy output llq
```

Хотелось бы отметить, что применение механизма QoS в сети с коммутацией пакетов позволяет эффективно и качественно передавать весь трафик корпоративной сети. При этом ресурсы сети предоставляются требовательному к задержке трафику на приоритетной основе, а остальной трафик получает назначенную для него пропускную способность. Таким образом, каждый информационный сервис получает желаемую часть ресурса.