

УДК 004.732

КАЧЕСТВО ОБСЛУЖИВАНИЯ В МУЛЬТИСЕРВИСНЫХ СЕТЯХ

М.А. АЛИСЕЕНКО, А.А. КОЧЕТКОВА, Б.В. НИКУЛЬШИН

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 20 ноября 2017

Рассмотрены виды трафика в мультисервисных сетях, а также методы и проблемы обеспечения QoS в них. Проведен анализ основных параметров, определяющих качество обслуживания, а также преимуществ и недостатков существующих методов его оценки.

Ключевые слова: мультисервисная сеть, задержка пакетов, джиттер, модель обеспечения QoS.

Введение

Современные мультисервисные сети используют протокол IP и ориентированы на передачу данных и мультимедийной информации, в частности, видеотрафик. При передаче мультимедийных данных по IP-сети возникают задержки, которые влияют на качество предоставляемых услуг.

Требования к характеристикам QoS определяются видом передаваемого по ним трафика, поэтому трафик должен классифицироваться.

Основные характеристики трафика приложений [1]:

- относительная предсказуемость скорости передачи данных (поточковый и пульсирующий трафик);
- чувствительность трафика к задержкам пакетов и их вариациям (трафик реального времени, трафик транзакций, трафик данных);
- чувствительность трафика к потерям и искажениям пакетов (приложения, чувствительные/устойчивые к потере данных).

Особенности пакетной передачи мультимедийных данных

Время прохождения пакета через IP-сеть при относительно высокой нагрузке плохо предсказуемо. Это связано, прежде всего, с пульсирующим характером мультимедийного трафика. Пульсации трафика могут возникать на выходе кодера, что связано с особенностями алгоритмов сжатия медиаданных и контента. Вариация задержки пакета в сети (джиттер пакета) тем больше, чем больше маршрутизаторов и коммутаторов в маршруте, по которому передается пакет. Для успешного декодирования медиаданных в пакетно-ориентированных сетях необходимо устранить джиттер пакетов. Компенсация джиттера в декодере происходит за счет джиттер-буфера [2], который хранит в памяти принятые пакеты в течение времени, определяемого его емкостью (длиной). В функции джиттер-буфера входит восстановление исходной очередности следования пакетов. Сокращение длины джиттер-буфера приводит к слишком частым потерям задержавшихся в сети пакетов, а увеличение его длины – к неприемлемо большой дополнительной задержке. Возможна динамическая настройка длины джиттер-буфера в процессе обслуживания.

Задержка пакетной передачи зависит от общей задержки сквозной передачи соединения IP и рассчитывается по формуле (1):

$$IPTD_{sat} = \sum_{n=1}^{N+1} \{T_{n,propagation} + T_{n,processing}\} + T_{buffer}, \quad (1)$$

где N – число повторных передач, согласно автоматическому запросу на повторение; $T_{n,propagation}$ – задержка на время распространения сигнала по линии связи n -й передачи; $T_{n,processing}$ – задержка обработки для передачи пакета по каналу и адаптация для n -й передачи по линии связи; T_{buffer} – задержка буферизации на интерфейсе соединения линии.

Проблемы, связанные с QoS могут быть разделены на две категории.

1. Не связанные с сетью проблемы, которые заключаются в следующем [3].

1.1. Перегрузка серверов, к которым пытаются получить доступ пользователи. В этом случае путями улучшения QoS являются модернизация серверов или использование дополнительных серверов с оптимальным разделением нагрузки между ними.

1.2. Ошибки работы сети. Например, по ошибке может быть сконфигурирован дублирующий IP-адрес, что приведет к проблемам маршрутизации.

2. Связанные с сетью проблемы, которые заключаются в следующем:

2.1. Проблемы оборудования, основной из которых является быстрое устаревание маршрутизаторов и коммутаторов и их программного обеспечения.

2.2. Недостаток пропускной способности сети доступа, причинами чего являются клиенты с низкоскоростными каналами доступа и перегруженные каналы.

2.3. Неравномерное распределение трафика по причине перегрузки некоторых каналов. Такие перегруженные каналы служат причиной большой задержки пакетов, джиттера или потери пакетов. Причинами этого в сети могут быть:

- непредвиденные события (обрыв волокна или отказ оборудования);
- изменение модели трафика, в то время как сетевая топология и пропускная способность не могут быть изменены так быстро;
- недоступность дополнительной пропускной способности на магистрали в нужное время.

Модели обеспечения гарантированного обслуживания

Интегрированное обслуживание (Integrated Service, IntServ). Модель интегрированного обслуживания обеспечивает сквозное (End-to-End) качество обслуживания, гарантируя необходимую пропускную способность. IntServ использует протокол сигнализации RSVP (Resource ReSerVation Protocol), который обеспечивает выполнение требований модели ко всем промежуточным узлам [1]. Структурная схема IntServ представлена на рис. 1.

Преимущества модели IntServ заключаются в четко определенной и гарантированной пропускной способности, а значит, в более высокой степени детализации. Этот механизм легко контролировать, поскольку можно следить за каждым маршрутом и каждым соединением. Отличительной особенностью протокола резервирования ресурсов RSVP является универсальность, т.к. отправлять запросы на резервирование может любое приложение, поддерживающее данный протокол. Однако имеется ряд недостатков, препятствующих широкому применению RSVP в пакетных сетях [1]:

- увеличение времени установления соединения;
- выявление отказов в выделении ресурсов для части информационных потоков;
- отсутствие предотвращения потери служебных сообщений RSVP;
- отсутствие высвобождения и резервирования необходимой полосы пропускания для высокоприоритетных потоков;
- недостаточное использование свободной полосы пропускания при резервировании.

Дифференцированное обслуживание (Differentiated Service, DiffServ). Архитектура DiffServ предполагает существование связанных областей сети (DiffServ-доменов), в пределах каждой из которых проводится единая политика по классификации служб передачи пакетов. Классификация проводится на основании анализа заголовков пакетов, но при этом могут приниматься во внимание и другие параметры, предусмотренные производителем маршрутизатора. В результате выполнения классификации каждому пакету ставится в соответствие номер некоторого класса обслуживания, реализованного в данном DiffServ-доме.

Такой номер класса обслуживания называется DiffServ CodePoint (DSCP). Пример сети, построенной согласно модели DiffServ, приведен на рис. 2.

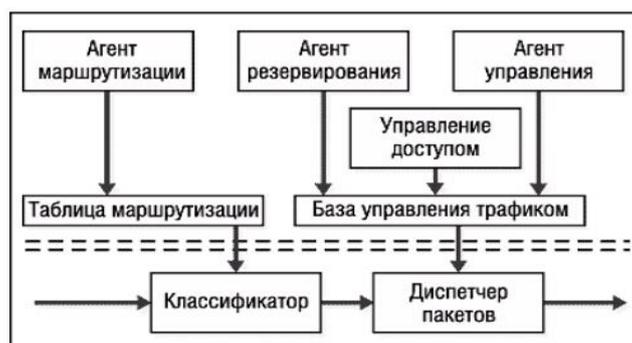


Рис. 1. Структурная схема IntServ

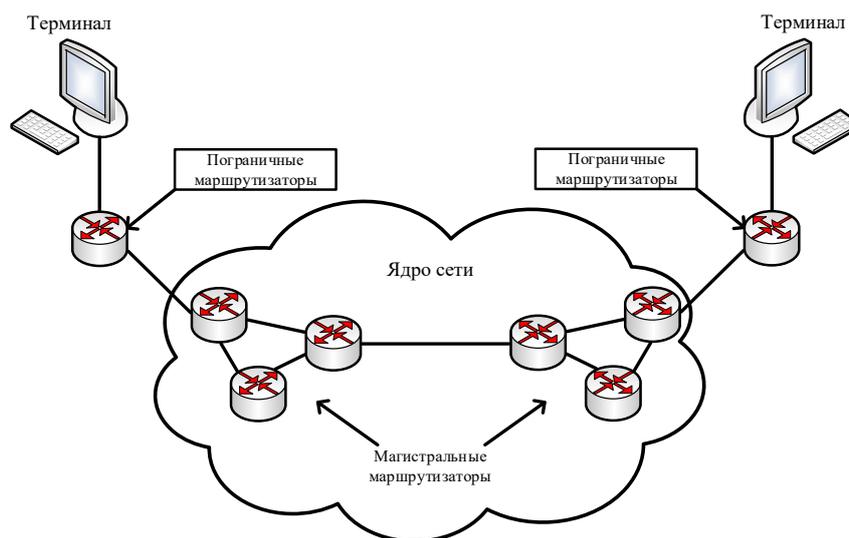


Рис. 2. Пример сети, построенной согласно модели DiffServ

Достоинства DiffServ заключаются в следующем.

1. Обеспечение единства обработки трафика определенного класса.
2. Разделение всего трафика на относительно небольшое число классов без необходимости анализа каждого информационного потока отдельно.
3. Отсутствие необходимости в организации предварительного соединения и резервировании ресурсов.
4. Отсутствие требования к высокой производительности сетевого оборудования.
5. Исключение необходимости использования вспомогательных протоколов сигнализации (т.е. проблема совместимости оборудования разных производителей неактуальна).

Недостатки модели DiffServ заключаются в следующем.

1. В условиях однородного трафика (например, только голосового) принцип применения приоритетов становится неактуальным, и сеть начинает работать в режиме Best Effort Service.
2. Отдельные внутренние маршрутизаторы могут отреагировать неоднозначно на значения битов в поле ToS или даже изменить их.
3. Поскольку DiffServ работает за счет выборочного сброса пакетов в периоды сетевой перегрузки, то соединения с низким приоритетом могут разорваться во время высокой сетевой активности.

Одной из реализаций модели DiffServ является технология многопротокольной коммутации на основе меток Multiprotocol Label Switching (MPLS), которая на сегодняшний день стала одной из основных для построения крупных сетей операторов, предоставляющих услуги с обеспечением качества обслуживания. Данная технология предназначена для ускорения коммутации пакетов в транспортных сетях. Основное ее отличие в том, что MPLS изначально не

является технологией обеспечения качества и становится таковой только при использовании протокола RSVP-TE.

Преимущества технологии MPLS:

- выбор маршрута на основе анализа IP-адреса;
- ускоренная коммутация (сокращает время поиска в таблицах);
- гибкая поддержка QoS, интегрированных сервисов и виртуальных частных сетей;
- эффективное использование явного маршрута;
- сохранение инвестиций в уже установленное АТМ-оборудование;
- разделение функциональности между ядром и граничной областью сети.

Однако внедрение технологии MPLS, как правило, связано с организацией высокоскоростной магистрали, что требует установки высокопроизводительного оборудования и, как следствие, серьезных финансовых затрат. Дополнительная гарантия доставки пакетов может создать проблемы в области масштабируемости.

Интегро-дифференцированное обслуживание (Integrated Services Operation over Diffserv Networks, Int-DifServ). Стандарт RFC2998 описывает принципы организации взаимодействия IntServ/RSVP и DiffServ для предоставления QoS от источника получателю. Слабые места одной модели компенсируются соответствующими решениями другой. С одной стороны, плохо масштабируемая IntServ на магистральных участках сети может быть заменена на более простую DiffServ. С другой стороны, с помощью RSVP решается вопрос с неопределенностью получаемого сервиса в DiffServ-сети. Основная проблема при взаимодействии DiffServ и RSVP – соответствие ресурсов, запрашиваемых через RSVP и предоставляемых в DiffServ-регионе (непрерывная последовательность DiffServ-доменов, в пределах которых могут оказываться дифференцированные услуги). Модель DiffServ представлена на рис. 3.

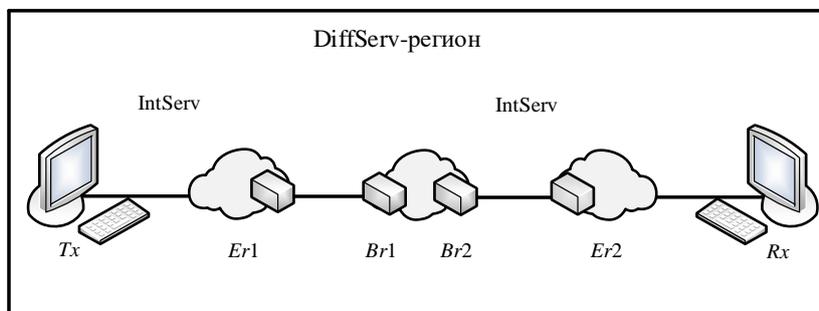


Рис. 3. Модель интегро-дифференцированного обслуживания IntDifServ

Сравнительные характеристики обеспечения QoS представлены в таблице.

Параметр	IntServ	DiffServ	MPLS	Int-Difserv
Метод обеспечения QoS	Резервирование	Приоритезация	Перемаршрутизация	Резервирование, приоритезация
Необходимость использования дополнительных протоколов	RSVP	Нет	LDP, CR-LDP, RSVP	RSVP
Требования к производительности маршрутизаторов	Высокие	Низкие	Средние	Средние
Эффективность масштабирования сети	Невысокая	Высокая	Высокая	Высокая
Совместимость оборудования разных производителей	Средняя	Высокая	Средняя	Средние
Гарантированность обеспечения качества	Высокая	Средняя	Высокая с использованием RSVP	Высокая

Практический подход к обеспечению QoS

Подход к обеспечению QoS включает в себя следующие шаги.

Шаг 1. Своевременное исправление уязвимостей. Отдельные точки неисправностей, узлы с низкой пропускной способностью и ошибки конфигураций должны быть устранены. Пропускная способность должна быть увеличена таким образом, чтобы даже отказ наиболее критичных маршрутов и каналов не приводил к перегрузкам сети. Должны быть оценены и перенастроены метрики внутреннего протокола шлюза (Interior Gateway Protocol, IGP), протокол граничного шлюза (Border Gateway Protocol, BGP) и политики равноправного информационного обмена.

Шаг 2. Деление трафика на классы. Предлагаются три класса обслуживания [4].

2.1. Premium-обслуживание, которое обеспечивает надежное обслуживание с низкой задержкой и малым джиттером. При таком обслуживании может обрабатываться, как трафик реального времени (например, видеоконференции), так и трафик, критичный к потерям (например, трафик управления сетью).

2.2. Assured-обслуживание, которое обеспечивает надежное и предсказуемое обслуживание. При таком обслуживании может обрабатываться трафик нереального времени виртуальных частных сетей (Virtual Private Network, VPN).

2.3. Обслуживание Best effort (подход «наилучшей попытки») – традиционное Интернет-обслуживание, эффективное для поддержки приложений нереального масштаба времени (передача файлов) и близких к реальному масштабу времени (аудио, видео).

Шаг 3. Защита Premium трафика и инжиниринг трафика. В предлагаемом подходе для защиты и инжиниринга используется многопротокольная коммутация по меткам (Multiprotocol Label Switching, MPLS).

Сначала в сети конфигурируются пути коммутации по метке (Label Switched Path, LSP). Каждый входной маршрутизатор будет иметь два LSP по отношению к выходному маршрутизатору. Один LSP используется для Premium трафика, а второй – для Assured и Best effort трафика. Premium LSP будет иметь разрешение на быструю перемаршрутизацию (защищенный канал, маршрутизатор или сегмент), которая необходима приложениям, не допускающим потери пакетов. Когда в защищенном сегменте происходит отказ, маршрутизатор непосредственно предшествующего защищенного сегмента (называемый защитным маршрутизатором) получит уведомление от второго уровня. Для обхода неисправности будет использоваться временное соединение LSP. Эта защита может вступить в силу в течение 50...100 мс. Во время быстрой перемаршрутизации путь, принятый за LSP, может быть условно оптимальным. Для исправления этого защитный маршрутизатор отправит сообщение входному маршрутизатору LSP, который вычислит новый путь для LSP и переключит трафик на новый LSP. Однако быстрая перемаршрутизация делает сеть значительно сложнее.

Для того чтобы избежать концентрации Premium трафика на любом канале, для каждого канала устанавливается верхний предел относительно того, сколько пропускной способности может быть задействовано для Premium трафика. Когда данная часть пропускной способности не используется, она при необходимости может быть использована трафиком других классов.

Инжиниринг трафика реализуется в целях предотвращения случаев перегрузок, вызванных неравномерным распределением трафика, и быстрого устранения перегрузки в случае ее возникновения.

При выполнении инжиниринга трафика на основе DiffServ появляется еще одна цель – держать долю Premium трафика для каждого канала на обоснованно низком уровне так, чтобы задержка и джиттер Premium трафика были низкими. При необходимости Premium трафик может занимать ресурсы низкоприоритетного трафика, доставка которого становится невозможной, если весь трафик является высокоприоритетным.

По сравнению с управлением трафиком в соответствии со схемами policing, shaping, а также буферизацией данных, инжиниринг трафика позволяет управлять как трафиком, так и работой сети в гораздо более широком масштабе. Он может быть рассмотрен как общий механизм управления.

Шаг 4. Организация очередей и планирование на основе деления на классы. На основании поля EXP (experimental) заголовка MPLS пакеты различных классов помещаются в различные очереди. Конфигурирование производительности и размера очередей является трудной задачей. Рассмотрим один из возможных подходов.

Скорость входного потока каждой очереди на интерфейсе может быть найдена путем суммирования скоростей всех проходящих в данной очереди LSP, используя протокол SNMP. Выходные скорости этих очередей должны регулярно устанавливаться (например, еженедельно). Необходимо отметить, что корректировка скоростей влияет только на производительность трафика, проходящего через определенный интерфейс.

Важно также предотвратить влияние перегрузок низкоприоритетного трафика, на работу высокоприоритетного трафика. Это полезно, когда пропускная способность сети становится недостаточной по причине обрыва волокна или другого отказа оборудования.

Шаг 5. Внедрение других схем управления трафиком (Policing и Shaping). Уровень обслуживания клиента SLA (Service Level Agreement) определяет величину трафика (если надо, то для каждого класса), который пользователь может отправить/принять. Однако схема Policing и Shaping могут оказывать влияние на работу устройств доступа. В таком случае есть альтернатива – агрегировать трафик от многих клиентов и следить/ограничивать его совместно.

Когда отказывает канал или маршрутизатор, IGP, MPLS и BGP необходимы для переконфигурации в течение временного промежутка от секунд до минут. В этот период пакеты будут испытывать большую задержку или теряться. Быстрая перемаршрутизация MPLS может защитить Premium трафик на период переконфигурации, что сделает сеть более доступной для Premium трафика, чем для Assured трафика. Кроме того, высокое значение отношения выходной скорости ко входной для Premium очереди позволяет Premium трафику иметь более низкие задержки и джиттер. Поскольку Assured трафик может использовать в три (или любое другое установленное значение) раза больше ресурсов, чем трафик Best effort, условия для его доставки будут лучше, чем для трафика Best effort, особенно, при возникновении отказа и большой загрузке канала.

В случае неисправности узла или канала инжиниринг трафика автоматически перемаршрутизирует трафик и позволит избежать любых перегрузок. Это может привести к небольшому увеличению задержки для некоторых видов трафика, т.к. выбирается более длинный путь, но предотвратит потерю пакетов и обеспечит низкий джиттер после восстановления сети.

Заключение

Рассмотрены основные проблемы обеспечения качества обслуживания (QoS) в мультисервисных сетях, а также технологии и рекомендации к его обеспечению. Основными параметрами, определяющими качество обслуживания, являются полоса пропускания, задержка пакетов, джиттер, потери пакетов. Для соблюдения характеристик QoS следует классифицировать трафик в зависимости от его назначения.

Проведен анализ технологий QoS, исходя из которого можно заключить, что ни одна из них не является универсальной. Однако стоит выделять несколько основных критериев QoS, а остальными пренебрегать.

Определено, что модель DiffServ подходит для применения в крупных ЛВС и территориально распределенных сетях (WAN), а также на стыке сетей провайдеров, в каналах с малой пропускной способностью. т.к. эта технология обеспечивает относительное увеличение полосы пропускания для приоритетных потоков.

Модель IntServ приемлема для использования в корпоративных сетях с целью решения ограниченного круга задач, но плохо пригодна для использования в высокоскоростных магистральных сетях и Internet. Этот механизм легко контролировать, однако уменьшается надежность передачи служебных сообщений и могут возникнуть проблемы совместимости оборудования в глобальных сетях.

Наиболее перспективными и сбалансированными технологиями QoS являются MPLS RSVP-TE и Int-DiffServ, в связи с тем, что они объединяют в себе лучшие стороны обеих моделей. Так, в MPLS за счет маршрутизации по меткам возможно более гибкое распределение ресурсов сети, что позволяет использовать несколько альтернативных путей доставки трафика для создания высокоскоростных магистралей, объединения локальных сетей. Однако эти технологии требуют высоких затрат на реализацию.

QUALITY OF SERVICE IN MULTISERVICE NETWORKS

M.A. ALISEYENKA, A.A. KACHATKOVA, B.V. NYKULSHYN

Abstract

The types of traffic in multiservice networks, as well as the methods and problems of providing QoS in them are considered. The main parameters that determine the quality of service, as well as the advantages and disadvantages of existing methods of its evaluation are analyzed.

Keywords: multiservice network, delay, jitter, QoS assurance model.

Список литературы

1. Листопад Н.И., Величкевич И.О. // Веснік сувязі. 2009. №2. С. 25–32.
2. Конопелько В.К., Лапшин С.М., Цветков В.Ю. Измерение и анализ трафика IP-телефонии. Минск, 2011.
3. Шувалов В.П., Крук Б.И., Попантонолуло В.Н. Телекоммуникационные системы и сети. М. 2005.
4. Xiao X. *et al.* // IEEE Commun. Mag. Dec. 2002. P. 38–43.