КАЧЕСТВО ОБСЛУЖИВАНИЯ ТРАФИКА РЕАЛЬНОГО ВРЕМЕНИ В МУЛЬТИСЕРВИСНОЙ СЕТИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Аникеев А.И.,[1] Репин Б.Г.,[2] Селезнев А.В.[3]

DOI:10.21682/3034-40-50-2024-2-13-20

Ключевые слова: *сеть с пакетной коммутацией, соглашение о качестве обслуживания, сетевой трафик, качество передачи, доступность услуг, приоритезация трафика, точки контроля, сеть доверенного оператора.*

Аннотация.

Цель статьи: *на основе анализа особенностей обеспечения качества обслуживания трафика реального времени в мультисервисной сети специального назначения разработать подходы к реализации механизмов контроля.*

Метод исследования: *при проведении исследования применялись методы теории телетрафика.*

Результат: *в работе проведен анализ механизмов маркировки и обработки трафика реального времени в мультисервисной сети специального назначения, которая является составной VPN MPLS сетью. Предложены подходы к реализации механизмов контроля качества. Сформулирована проблема обеспечения требуемого качества обслуживания трафика, связанная с особенностями маркировки, перемаркировки и настройки механизмов обработки трафика реального времени при продвижении его через составную сеть, поскольку именно туннелирование трафика в сети IP/MPLS порождает эту проблему. Определен метод корректировки ситуации, опирающийся на мутацию поля DSCP пакета, в частности, предлагается маркировать трафик классом EF, обеспечивающим сервис с низкой задержкой и сводящий к минимуму джиттер задержки.*

Практическая ценность *состоит в том, что в статье предложена реализация механизмов QoS с учетом существующей практики маркировки трафика реального времени на конечных узлах и перемаркировки трафика в сети IP/MPLS доверенного оператора. В частности, для маркировки исходного потока трафика реального времени предлагается использовать класс DSCP, обеспечивающий сохранение исходной кодировки при переходе из домена IP в домен MPLS. Процессы обработки трафика в сети доверенного оператора находятся вне зоны контроля системы управления связью мультисервисной сети специального назначения, поэтому в работе определены точки контроля качества, поскольку в случаях, когда сложно провести измерение, актуальным является анализ текущих характеристик качества обслуживания трафика.*

Введение

С точки зрения современных тенденций развития телекоммуникаций специального назначения актуальной задачей является построение конвергентной мультисервисной сети. Такая сеть должна обеспечивать неограниченный набор услуг, предоставлять гибкие возможности по управлению и созданию новых видов сервиса. Последнее требует реализации универсальной транспортной сети с распределенной коммутацией, где взаимодействие между устройствами и приложениями осуществляется с помощью создания виртуальных соединений, на управление которыми заметно влияют особенности стохастической динамики процессов пакетной коммутации [1].

Одной из наиболее актуальных проблем исследования вероятностно-временных характеристик сетей является адекватный учет особенностей сетевого трафика.

Традиционный трафик локальных и глобальных сетей состоит из передачи файлов приложений, не требующих принятия специальных мер или применения специальной обработки. Однако, при передаче голоса, видео и других приложений реального времени по сети с пакетной коммутацией, ситуация кардинально меняется и без реализации механизмов обеспечения качества обслуживания (Quality of Service, QoS) уже не обойтись [2].

Адекватно настроенные механизмы приоритезации и обработки трафика позволяют соответствующим образом распределить доступную

[1]Аникеев Александр Иванович, преподаватель кафедры «Сетей связи и систем коммутации» Военной академии связи, г. Санкт-Петербург, Россия. E-mail: aai1956@yandex.ru

[2]Репин Борис Григорьевич, кандидат военных наук, доцент, доцент кафедры «Сетей связи и систем коммутации» Военной академии связи, г. Санкт-Петербург, Россия. E-mail: rbg@inbox.ru

[3]Селезнев Андрей Васильевич, кандидат технических наук, научный сотрудник Военной академии связи, г. Санкт-Петербург, Россия. E-.mail: andrsel@mail.ru

пропускную способность канала и обеспечить требуемый уровень качества обслуживания разноприоритетного трафика. Здесь следует отметить, что приоритезация требуется в основном только в узких, загруженных местах, когда пропускной способности канала не хватает для передачи всех поступающих пакетов и нужно каким-то образом дифференцировать их обработку. Кроме того, приоритезация необходима для предотвращения влияния всплесков сетевой активности на чувствительный к задержкам трафик.

Современная мультисервисная сеть специального назначения представляет собой сеть VPN IP/MPLS. Следовательно, для обеспечения требуемого качества предоставляемых услуг необходимы соответствующие настройки маркировки туннелированного трафика и механизмов QoS для эффективной обработки туннелированного трафика. Туннелирование является важной особенностью обработки трафика в таких сетях, поскольку передача приоритезированного трафика осуществляется через виртуальные каналы или туннели для обеспечения конфиденциальности, целостности и безопасности передаваемой информации и гарантировать приемлемый уровень обслуживания для каждого приложения

Туннелирование трафика позволяет объединить удаленные сегменты в единую сеть, в которой могут использоваться различные технологии и ресурсы. В случае использования VPN IP/MPLS сети, основным преимуществом является возможность обеспечения требуемого уровня качества обслуживания (QoS), что особенно важно для приложений реального времени.

Исследование вопросов конфигурирования механизмов QoS является важным аспектом обеспечения оптимальной производительности и надежности такой сети. В данном контексте, разработка подходов к настройке параметров QoS, специально адаптированной для управления туннельным трафиком имеет большое значение и включает в себя определение оптимальных параметров, учитывающих специфику сетей специального назначения, а также обеспечение баланса между эффективностью и степенью защиты передаваемых данных.

Особенности обработки трафика реального времени

Для передачи трафика реального времени в сетях, не гарантирующих QoS, разработан и применяется протокол H.323, который предоставляет специальную поддержку, необходимую приложениям реального времени. Он состоит из множества спецификаций, определяющих, как мультимедийные приложения взаимодействуют друг с другом по сети, не гарантирующей QoS. Одним из таких протоколов является протокол передачи в реальном масштабе времени (Real-Time Transfer Protocol, RTP), используемый для доставки потокового аудио и видео по сетям с пакетной коммутацией. В качестве транспорта для сервисов реального времени RTP использует UDP и может дополняться протоколом управления трафиком реального времени (Real-Time Control Protocol, RTCP) для мониторинга уровня QoS и передачи сеансовой информации между участниками сеанса. Протокол RTP не способен повлиять на задержку в сети, но он сокращает дрожание изображения и звука при воспроизведении при наличии задержек. Он, в принципе, может установить факт потери пакетов (пакеты нумеруются на передаче), но мер для восстановления потерь не предпринимает, его задача — обеспечить комфортную для получателя транспортировку потока пакетов приложения реального времени.

Один из способов расширения возможностей RTP — использование его совместно с протоколом резервирования ресурсов — RSVP, который поддерживается многими приложениями реального времени [3,4,5].

При сопряжении различных сетей связи существуют определенные проблемы, связанные с обеспечением качества обслуживания при предоставлении услуг связи. Предпосылками для возникновения возможных проблем служат:

- число классов сервиса, используемое для предоставления услуг связи потребителям;
- уровень (канальный и/или сетевой), на котором обеспечивается качество обслуживания;
- используемая политика маркировки трафика при предоставлении различного вида услуг связи;
- политики управления трафиком: ограничения, фильтрация, формирование трафика на сетевых интерфейсах узлов;
- другие — например, использование защитных экранов (Firewall), глубокого анализа пакетов (DPI) в режиме реального времени, криптографических методов шифрования.

Часть проблем в плоскости обеспечения качества услуг при сопряжении может быть решена за счет разработки и применения эффективной схемы отображения (и перемаркировки) классов обслуживания, а также использования принципов иерархического QoS.

Отображение классов обслуживания может выполняться для каждой услуги как в пределах одного уровня (канального или сетевого), так и между уровнями (например, отображение значений приоритетов 802.1q/p или битов MPLS EXP в значения ToS или DSCP).

Контроль качества обслуживания трафика

Качество обслуживания определяется как мера производительности передающей системы, отражающая качество передачи и доступность услуг. Доступность услуг является важнейшим элементом QoS. Для успешного внедрения QoS необходимо обеспечить максимально высокую доступность сетевой инфраструктуры. (Конечной цели высокой доступности соответствует уровень 99,999 процентов, то есть только 5 минут простоя в год). Качество передачи сети определяется следующими факторами [4]:

Доступность — диапазон времени сетевой достижимости между входной и выходной точкой сети — это сетевая доступность.

Доступность сервиса — это диапазон времени, в течение которого этот сервис доступен между определенными входной и выходной точками с параметрами, оговоренными в соглашении об уровне обслуживании (SLA).

Потери — это отношение правильно принятых пакетов к общему количеству пакетов, которые были переданы по сети. Потери выражаются в процентах отброшенных пакетов, которые не были доставлены по назначению. Обычно, потери — это функция от доступности. Если сеть не загружена, то потери (во время отсутствия перегрузок) будут равны нулю. Во время перегрузок действующие механизмы QoS будут определять, какие пакеты могут быть сброшены.

Определяя требования QoS для VoIP трафика, рекомендуется придерживаться следующих правил [5,6]:

Голосовой трафик должен быть промаркирован как DSCP EF, в соответствии с «Базовыми Основами QoS» и RFC 3246.

Сигнализация должна быть промаркирована как CS3, в соответствии с «Базовыми Основами QoS» (во время миграции можно использовать AF31).

Потери пакетов в магистралях, спроектированных для предоставления VoIP сервиса высокого качества, не должны превышать 0.25 процентов.

Задержка — это время, которое требуется пакету для того, чтобы после передачи дойти до пункта назначения. В случае голоса, эта задержка определяется как время прохождения сигнала от говорящего к слушающему.

Колебания задержки (jitter) — это разница между сквозным временем задержки, которая возникает при передаче по сети разных пакетов. Так, например, если для передачи одного пакета по сети требуется 100 мсек, а для передачи следующего пакета — 125 мсек, то колебание задержки составит 25 мсек.

Односторонняя задержка не должна превышать 150ms, в соответствии со International Telecommunication Union (ITU) G.114.

Колебания задержки (jitter) должны быть менее 10 мсек. Максимальный jitter должен быть менее чем бюджет по задержке в сети минус минимальная сетевая задержка. Это типовое значение колебания задержки для VoIP обусловлено бюджетом по задержке, так называемым mouth-to-ear, в 100 мсек. (Это достаточно консервативный бюджет по сравнению с G.114, в котором рекомендуется jitter менее 150 мсек). Из этого значения мы вычитаем время распространения по магистрали (30 мсек) и задержку кодека (35 мсек), что дает нам бюджет для jitter в 35 мсек. Эти 35 мсек разбиваются на 30 мсек на доступе (15 мсек вход/выход) и 5 мсек на магистрали: то есть в худшем варианте, для адаптивных jitter-буферов, колебания задержки должны быть менее 10 мсек.

Для каждого разговора (в зависимости от частоты квантирования, кодека и заголовка второго уровня) требуется 21–106 kbps гарантированной приоритетной полосы пропускания.

Для трафика сигнализации требуется 150 bps (плюс заголовок второго уровня) гарантированной полосы пропускания.

На качество голосовой связи напрямую влияют три фактора качества QoS: потери пакетов, задержка и вариации задержки.

Потери пакетов вызывают кратковременные пробелы в разговоре. Потери двух и более последовательных 20 мсек сэмплов приведут к заметной деградации качества голоса. Предположив случайное распределение сбросов пакетов в одном речевом потоке, сброс 1-го процента в голосовом потоке привела бы в среднем к потере, которую нельзя было бы восстановить каждые 3 минуты. Аналогично, уровень сброса 0,25 процента привел бы в среднем к потере, которую нельзя было бы восстановить каждые 53 минуты.

Задержка более 200 мсек может вызвать деградацию качества голосовой связи. Если общая задержка в канале становится слишком большой, разговор по телефону начинает напоминать переговоры по спутниковому каналу связи или по симплексному радиоканалу. В стандарте Международного Союза Электросвязи для технологии VoIP (G.114) говорится, что задержка величиной в 150 мсек в одном направлении является приемлемой для качество голосовой связи. Было продемонстрировано, что разница в каче-

стве голоса между сетями с задержкой в 150 мсек и 200 мсек является незначительной и практически незаметной для пользователя. В [5,6] предлагается ориентироваться на ITU стандарт 150 мсек, но если существуют ограничения не позволяющие добиться такого бюджета, то размер задержки может быть увеличен до 200 мсек без значительной деградации качества связи.

Для выравнивания вариации задержки в IP-телефонии используются адаптивные джиттер-буферы. Они частично решают проблему, однако могут компенсировать отклонение задержки лишь в пределах от 20 до 50 мсек.

При передаче трафика интерактивного видео также есть особенности. Так как видео конференция включает аудио кодек G.711 для речи, то у нее и соответствующие голосовому трафику требования к потерям, задержке и колебаниям задержки. Однако трафик видео конференции радикально отличается от трафика голоса. Например, трафик видео конференций использует переменные размеры пакетов и переменные скорости передачи пакетов. Скорость видео конференции — это скорость сэмплирования видео потока, но не реальная полоса пропускания, которую требует видео вызов. Иными словами, полезная нагрузка пакетов видео конференции заполняется 384 kbps потока видео сэмплов. IP, UDP и RTP заголовки (40 байт на пакет) должны быть дополнительно включены в требования по полосе пропускания (так же как и заголовки второго уровня). Так как используются переменные размеры пакетов и скорости генерации пакетов, то достаточно трудно точно подсчитать абсолютное значение накладных расходов. Тестирование, однако, показало, что для расчета можно использовать скорость видео конференции плюс 20 процентов

Оценка качества обслуживания трафика реального времени (TPB) должна давать реальную картину происходящих процессов, поэтому при создании сценария для интервалов оценки обслуживания TPB необходимо учитывать следующие требования [5]:

- интервал оценки должен быть достаточно длительным, чтобы содержать необходимое количество пакетов нужного потока;
- интервал оценки должен быть достаточно длительным, чтобы был отражен период характерного использования (время существования потока) или оценка пользователя;
- интервал оценки должен быть достаточно коротким для обеспечения баланса применяемых рабочих характеристик на протяжении каждого интервала (интервалы плохих рабочих характеристик не должны быть скрыты в слишком длинном оценочном интервале, они должны быть идентифицированы);
- интервал оценки должен быть достаточно коротким для обращения к фактическим аспектам измерения.

Для выполнения оценок, связанных с TPB, минимальный интервал должен быть порядка 10–20 секунд с характерной скоростью передачи пакетов (от 50 до 100 пакетов в секунду), также интервал должен иметь верхнее ограничение в пределах нескольких минут.

Эффективным решением может являться организация взаимодействия системы управления сетью и подсистемы мониторинга показателей QoS. При таком взаимодействии система управления сетью, получая информацию о деградации системы связи, информирует оператора, который может запросить подробную информацию с сервер-менеджера и принять решение о реконфигурации сети для эффективного распределения ресурсов.

Точки контроля могут располагаться как на интерфейсе UNI, так и на местах сопряжения различных сетей, т. е. можно контролировать как end-to-end QoS, так и Segment QoS [7]. Пример расположения точек контроля показан на рис. 1 [9].

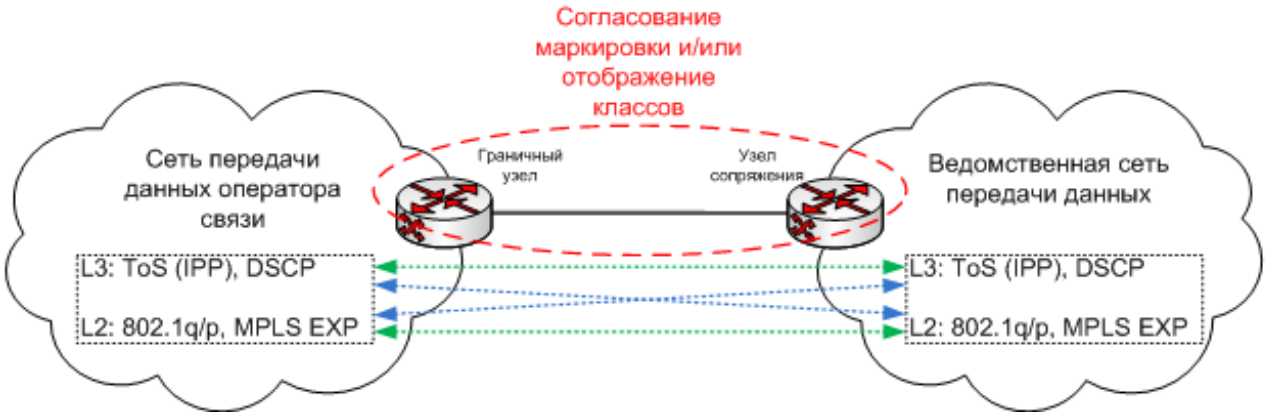

Рис 1. Расположение точек контроля

Существует более простой способ контроля показателей качества обслуживания в сетях, который зачастую используется операторами связи. Многие операторы и пользователи телекоммуникационных услуг используют для контроля показателей QoS простые методы, например ICMP PING или трассировка. При использовании данных методов можно измерить только задержку при передаче сигнала в IP-сети в прямом и обратном направлениях (IPRTD), а задержка при передаче сигнала в одном направлении для пакетной сети, конечно же, не равна точно половине IPRTD. Существуют также другие проблемы, связанные с PING: 1 — на маршрутизаторах PING иногда отключается для уменьшения вероятности проникновения хакера и воздействий, вызывающих отказ в обслуживании законных пользователей; 2 — PING имеет наименьший приоритет при обработке пакетов на маршрутизаторе. Следовательно, задержка, измеренная при помощи PING, не является точной мерой задержки трафика пользователя [6].

Другим важным аспектом контроля качества сетевых параметров является управление пропускной способностью. Для этого следует применять методы управления трафиком, такие как Traffic Engineering (TE). Эти методы позволяют контролировать и приоритезировать различные типы трафика в сети, что позволяет гарантировать необходимое качество обслуживания для приложений в режиме реального времени.

Для обнаружения и устранения возможных проблем с качеством обслуживания также полезно использовать системы мониторинга сетевого трафика, такие как сетевые анализаторы или системы пакетного анализа. Эти системы позволяют анализировать сетевой трафик и идентифицировать возможные проблемы.

В целом, контроль качества сетевых параметров трафика в мультисервисных сетях специального назначения требует применения различных методов и инструментов. Он должен быть основан на комбинации протоколов уровня приложения, управления трафиком и систем мониторинга, чтобы обеспечить стабильное и надежное функционирование сети.

Заключение

В современных мультисервисных сетях широкое применение получило туннелирование трафика. Туннелирование трафика обеспечивает управление потоками данных за счёт построения сети на 2(3) уровне модели OSI, позволяет связывать удаленные узлы в единую сеть с общими ресурсами, упрощает администрирование сети за счёт разделения на уровень инфраструктуры и уровень пользователей и обеспечивает построение единых сетей на базе различных сетевых технологий.

Туннелирование трафика ориентировано на построение сети и обеспечение надежной передачи данных, в то же время, вопросы обеспечения качества обслуживания при транспортировке инкапсулированного трафика требуют дополнительного рассмотрения.

Контроль качества предоставления услуг и контроль качества обслуживания трафика в сети передачи данных являются важными составляющими процесса эксплуатации сети. Поскольку существенная доля сетевой инфраструктуры мультисервисной сети специального назначения являются арендованными ресурсами доверенного оператора, важную роль в обеспечении требуемого качества обслуживания трафика играет соглашение между оператором и заказчиком.

На сегодняшний день самый распространенный способ согласования требований заказчика и возможностей оператора — заключение соглашений об уровне сервиса (Service Level Agreement, SLA), т. е. контрактов, где четко указано, какого уровня доступность, сервисы и цены ожидает получить заказчик. В таком соглашении доверенный оператор должен гарантировать срок бессбойной работы и длительность задержки в конкретное время суток для конкретных видов приложений. Соглашение также может содержать информацию о доступности пользовательского соединения [8,9].

Кроме того, должно быть определено, какие сервисы и гарантии обслуживания предлагаются для каждого класса трафика, пропускная способность (скорость, с которой пакеты передаются по сети), задержка (время между отправкой и приемом пакетов на конечных станциях), процент потерянных пакетов (максимально возможное число удаленных при передаче пакетов) и вариация задержки (разницу во времени доставки пакетов из одного потока).

Поскольку, как правило, в сети оператора существует собственная политика в области QoS, важной проблемой является обеспечение единого понимания механизмов дифференциации трафика в сетях заказчика и доверенного оператора [10].

Доверенный оператор использует атрибуты маркирования третьего уровня (IPP или DSCP) для определения какому операторскому классу сервиса следует назначить этот пакет. Следовательно, заказчики для достижения соответствующего уровня сервиса должны маркировать/перемаркировать трафик в соответствии политикой операторской сети. Дополнительно, оператор

может перемаркировать трафик вне контракта в пределах своего облака, что может повлиять на пользовательский трафик и требует последовательной политики сквозной маркировки. Следующие вопросы должны быть учтены при определении стратегии маркировки/перемаркировки на границе клиент-оператор.

Общее правило маркировки в корпоративных сетях заключается в маркировке трафика и установке границ доверия как можно ближе к источнику, насколько это возможно административно и технически. В [10] рекомендуется не доверять маркировке, установленной на хостах пользователей (так как здесь возможны злоупотребления). Определенные типы трафика, возможно, нужно перемаркировывать еще до передачи на пограничные устройства оператора для получения доступа к определенному классу. Если требуется такая перемаркировка, то рекомендуется производить ее на граничном маршрутизаторе узла. Это связано с тем, что набор предлагаемых оператором сервисов может измениться или расшириться со временем, а производить перенастройку проще, если она производится только на границе пользовательской сети. Могут существовать классы, где множество типов трафика требуется пометить одинаковыми значениями для получения доступа к определенным очередям. Например, на высокоскоростных каналах может потребоваться передавать голос, интерактивное видео и сигнализацию в операторском классе реального времени. Если в операторский класс реального времени направляются только пакеты, промаркированные DSCP EF и CS5, то это означает, что три этих приложения должны использовать один и тот же код приоритета DSCP. Однако, полосу пропускания, выделенную для EF, следует ограничивать, чтобы другие классы трафика могли быть обработаны, поскольку возможна ситуация, что всю полосу пропускания займет трафик EF. В то же время, очередь, выделенная для EF должна иметь наивысший приоритет, чтобы предназначенный для нее трафик проходил быстро и не вызывал значительных задержек.

Качество обслуживания трафика реального времени обычно контролируется процедурами без обратной связи, основанными на понятии SLA — соглашении между пользователем услуг и администрацией сети относительно параметров передаваемого трафика и качества его обслуживания.

При организации межсетевого взаимодействия в этом случае критичными аспектами являются:

- разграничение зон ответственности служб технической эксплуатации;
- выбор размещения точек контроля показателей качества функционирования сети и качества предоставления услуг связи.

Контроль показателей QoS с использованием рассмотренных в работе способов может эффективно использоваться в процессе эксплуатации сетей, в том числе для контроля SLA, что позволит существенно повысить качество предоставляемых телекоммуникационных услуг.

Литература

1. Ясинский С.А., Репин Б.Г., Григорчук А.Н., Аникеев А.И. О моделировании трафика в мультисервисной сети специального назначения // Труды ЦНИИС. Санкт-Петербургский филиал. 2022. Т. 1. № 13. С. 96–105.
2. Ясинский С.А., Одоевский С.М., Рафальская М.И. Анализ сложности решения обратных оптимизационных задач при обосновании сетевых механизмов обеспечения качества обслуживания мультимедийного трафика // Информация и космос. 2023. №2., с.54-63.
3. Елисеев Д.И., Никитин И.С., Оранский С.В., Репин Б.Г. Управление механизмами QoS с помощью политик. //В сборнике: Современное состояние и перспективы развития инфокоммуникационных сетей связи специального назначения. Материалы научно-практической конференции. Санкт-Петербург, 2024. С. 104–108.
4. Аникеев А.И., Григорчук А.Н., Оранский С.В., Репин Б.Г. Исследование свойств туннелированного голосового трафика в VPN сети специального назначения. //В сборнике: Современное состояние и перспективы развития инфокоммуникационных сетей связи специального назначения. Сборник материалов научно-практической конференции. Санкт-Петербург, 2023. С. 105–112.
5. Григорчук А.Н., Оранский С.В., Репин Б.Г. Проблема использования маркировки при туннелировании маркированного трафика. Труды ЦНИИС. Санкт-Петербургский филиал. 2022. Т. 1. № 13. С. 146–160.
6. Аникеев А.И., Григорчук А.Н., Оранский С.В., Репин Б.Г. Особенности передачи мультимедийного трафика в мультисервисной сети специального назначения. //В сборнике: Современное состояние и перспективы развития инфокоммуникационных сетей связи специального назначения. Сборник материалов научно-практической конференции. Санкт-Петербург, 2023. С. 113–118.
7. Оранский С.В., Репин Б.Г., Селезнев А.В., Ясинский С.А. О влиянии туннелирования на величину задержки пакетов в мультисервисной сети специального назначения. //В сборнике: Современные тенденции инженерного образования. Сборник материалов Научно-практической конференции. Санкт-Петербург, 2023. С. 258–263.

8. Ибрагимов Б.Г., Гасанов А.Г. Исследование и оценка эффективности мультисервисных сетей NGN/ IMS при передаче мультимедийных трафиков // T-Comm: Телекоммуникации и транспорт. 2017. Том 11. №2. С. 15–18.
9. Смирнов П.И. Способы оценки показателей качества обслуживания в мультисервисных сетях // НИИ Масштаб — научно-исследовательский институт, разработчик сложных систем и средств телекоммуникаций, защиты информации, автоматизированного управления. https://mashtab.org/company/massmedia/articles/qos/
10. Принципы построения мультисервисной сети ПАО «Ростелеком» С.Л. Гавлиевский, В.Г. Карташевский, Д.В. Проскура, Д.С. Сахарчук, М.Ю. Сподобаев // Горячая линия — Телеком, 2019. 228 с., ил.

QUALITY OF SERVICE OF REAL TRAFFIC TIME IN A MULTI-SERVICE NETWORK SPECIAL PURPOSE

Anikeev A.I.[1], Repin B.G.[2], Seleznev A.V.[3]

Keywords: *packet-switched network, quality of service agreement, network traffic, transmission quality, service availability, traffic prioritization, control points, trusted operator network.*

The purpose of the article is to *develop approaches to the implementation of control mechanisms based on the analysis of the features of ensuring the quality of service of real-time traffic in a special-purpose multiservice network.*

Research method: *the methods of the teletraffic theory were applied.*

Result: *the paper analyzes the mechanisms of marking and processing real-time traffic in a special-purpose multiservice network, which is a composite VPN MPLS network. Approaches to the implementation of quality control mechanisms are proposed. The problem of ensuring the required quality of traffic service is formulated, associated with the features of marking, relabeling and setting up mechanisms for processing real-time traffic when moving it through a composite network, since it is the tunneling of traffic in the IP/MPLS network that generates this problem. A method for correcting the situation based on the mutation of the DSCP field of the packet is determined, in particular, it is proposed to mark traffic with the EF class, which provides a service with low latency and minimizes jitter latency.*

The practical value *lies in the fact that the article proposes the implementation of QoS mechanisms, taking into account the existing practice of marking real-time traffic at end nodes and remarking traffic in the IP/MPLS network of the trusted operator. In particular, it is proposed to use the DSCP class to mark the initial flow of real-time traffic, which ensures the preservation of the original encoding when moving from the IP domain to the MPLS domain. Traffic Processing Processes in the Network of the Trusted Operator are beyond the control of the communication management system of a special-purpose multiservice network, so quality control points are determined in the work, since in cases where it is difficult to measure, the analysis of the current characteristics of the quality of traffic service is relevant.*

References

1. Jasinskij S.A., Repin B.G., Grigorchuk A.N., Anikeev A.I. O modelirovanii trafika v mul'tiservisnoj seti special'nogo naznachenija // Trudy CNIIS. Sankt-Peterburgskij filial. 2022. T. 1. № 13. S. 96–105.
2. Jasinskij S.A., Odoevskij S.M., Rafal'skaja M.I. Analiz slozhnosti reshenija obratnyh optimizacionnyh zadach pri obosnovanii setevyh mehanizmov obespechenija kachestva obsluzhivanija mul'timedijnogo trafika // Informacija i kosmos. 2023. №2., s.54-63.
3. Eliseev D.I., Nikitin I.S., Oranskij S.V., Repin B.G. Upravlenie mehanizmami QoS s pomoshh'ju politik. //V sbornike: Sovremennoe sostojanie i perspektivy razvitija infokommunikacionnyh setej svjazi special'nogo naznachenija. Materialy nauchno-prakticheskoj konferencii. Sankt-Peterburg, 2024. S. 104–108.
4. Anikeev A.I., Grigorchuk A.N., Oranskij S.V., Repin B.G. Issledovanie svojstv tunnelirovannogo golosovogo trafika v VPN seti special'nogo naznachenija. //V sbornike: Sovremennoe sostojanie i perspektivy razvitija infokommunikacionnyh setej svjazi special'nogo naznachenija. Sbornik materialov nauchno-prakticheskoj konferencii. Sankt-Peterburg, 2023. S. 105–112.
5. Grigorchuk A.N., Oranskij S.V., Repin B.G. Problema ispol'zovanija markirovki pri tunnelirovanii markirovannogo trafika. Trudy CNIIS. Sankt-Peterburgskij filial. 2022. T. 1. № 13. S. 146–160.

[1]Alexander I. Anikeev, Lecturer, Department of Communication Networks and Switching Systems, Military Academy of Communications, St. Petersburg, Russia. E-mail: aai1956@yandex.ru
[2]Boris G. Repin, Ph.D., Associate Professor, Associate Professor of the Department of Communication Networks and Switching Systems, Military Academy of Communications, St. Petersburg, Russia. E mail: rbg@inbox.ru
[3]Andrey V. Seleznev, Ph.D., Researcher of the Military Academy of Communications, St. Petersburg, Russia. E-.mail: andrsel@mail.ru

6. Anikeev A.I., Grigorchuk A.N., Oranskij S.V., Repin B.G. Osobennosti peredachi mul'timedijnogo trafika v mul'tiservisnoj seti special'nogo naznachenija. //V sbornike: Sovremennoe sostojanie i perspektivy razvitija infokommunikacionnyh setej svjazi special'nogo naznachenija. Sbornik materialov nauchno-prakticheskoj konferencii. Sankt-Peterburg, 2023. S. 113–118.
7. Oranskij S.V., Repin B.G., Seleznev A.V., Jasinskij S.A. O vlijanii tunnelirovanija na velichinu zaderzhki paketov v mul'tiservisnoj seti special'nogo naznachenija. //V sbornike: Sovremennye tendencii inzhenernogo obrazovanija. Sbornik materialov Nauchno-prakticheskoj konferencii. Sankt-Peterburg, 2023. S. 258–263.
8. Ibragimov B.G., Gasanov A.G. Issledovanie i ocenka jeffektivnosti mul'tiservisnyh setej NGN/ IMS pri peredache mul'timedijnyh trafikov // T-Comm: Telekommunikacii i transport. 2017. Tom 11. №2. S. 15–18.
9. Smirnov P.I.. Sposoby ocenki pokazatelej kachestva obsluzhivanija v mul'tiservisnyh setjah // NII Masshtab — nauchno-issledovatel'skij institut, razrabotchik slozhnyh sistem i sredstv telekommunikacij, zashhity informacii, avtomatizirovannogo upravlenija. https://mashtab.org/company/massmedia/articles/qos/
10. Principy postroenija mul'tiservisnoj seti PAO «Rostelekom» S.L. Gavlievskij, V.G. Kartashevskij, D.V. Proskura, D.S. Saharchuk, M.Ju. Spodobaev // Gorjachaja linija — Telekom, 2019. 228 s., il.