УДК 621.391:004.9

ПРОГРАММНЫЙ ПАКЕТ ПЛАНИРОВАНИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ НА ОСНОВЕ ТЕОРИИ СЕТЕВОГО ИСЧИСЛЕНИЯ

Лысиков А.А.

ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», Самара, e-mail: lysikov_inc@mail.ru

Рассматриваются проблемы, возникающие на этапе планирования сетей VPN при их совместной реализации в сети оператора с гарантированными характеристиками качества обслуживания QoS и не-VPN соединений с приоритетным трафиком. Рассматриваются достоинства и недостатки теории массового обслуживания для решения задач планирования VPN. Показаны достоинства теории сетевого исчисления при нахождении лучшего маршрута VPN на основе граничных значений характеристик QoS. Рассмотрены особенности применения теории детерминистического и стохастического сетевого анализа для определения строгих и не строгих границ характеристик QoS в VPN. Предложена архитектура и алгоритм пакета прикладных программ для автоматизации операционной деятельности оператора при планировании услуги VPN. Рассмотрены функции каждого блока программного пакета и их взаимодействие между собой.

Ключевые слова: виртуальная частная сеть VPN, характеристики качества обслуживания QoS, планирование услуг VPN, теория сетевого исчисления Network Calculus, пакет прикладных программ

SOFTWARE PACKAGE FOR PLANNING VIRTUAL PRIVATE NETWORKS BASED ON NETWORK CALCULUS THEORY

Lysikov A.A.

Povolzhsky State University of Telecommunications and Informatics, Samara, e-mail: lysikov_inc@mail.ru

Virtual private networks are one of the most popular services in next generation networks. The network operator providing service of virtual private networks must adhere strictly to the service level agreement in such characteristics of quality of service, as packet delay, packet loss, guaranteed bandwidth and others. At the planning stage of virtual private network is necessary to determine the optimal network route, which allows guaranteeing the required quality of service and efficient use of network resources. This paper proposes an algorithm based on Network Calculus models that determines the best network route for virtual private network on the end-to-end least upper delay packet bound. This algorithm can be the basis for a software package, whose architecture is also proposed in this paper. The software package based on the proposed architecture and the algorithm can be useful to network operators at the planning stage of services of virtual private networks for determining optimal network routes.

Keywords: virtual private networks, quality of service, VPN planning, Network Calculus, software package

Виртуальные частные сети (VPN) являются одной из востребованных услуг в современных мультисервисных сетях связи, например, в сетях следующего поколения NGN [1]. При предоставлении услуги VPN провайдером должны быть строго соблюдены установленные в соглашении о гарантированном уровне сервиса SLA характеристики качества обслуживания QoS (например, задержка, потери пакетов и др.). Поэтому на этапе планирования VPN необходимо определить сквозные характеристики QoS. Сеть VPN представляет собой набор фиксированных маршрутов, проходящих через определенные узлы сети с различными характеристиками (размером буфера, дисциплина обслуживания и т.п.) и производительностью, вносящими различную по величине задержку при обслуживании мультисервисного трафика, имеющего «всплесковый» характер. Это делает анализ сквозных характеристик таких маршрутов VPN достаточно сложным. Задача усложняется тем, что через узлы, выбранные для конфигурирования новой VPN, как правило, уже проходят маршруты как ранее сконфигурированных VPN сетей, трафик которых будет использовать часть ресурсов сетевых узлов, и, следовательно, будет являться конкурирующим для трафика новой VPN. Таким образом, оператор на этапе планирования новой VPN сети должен найти оптимальное решение для набора потоков трафика клиента, при котором:

а) оператор сможет предоставить клиенту услугу VPN с запрашиваемым качеством обслуживания и гарантировать его на все время эксплуатации VPN;

б) ввод новой VPN не повлияет на качество обслуживания раннее сконфигурированных VPN сетей и, по возможности, других соединений, передающих приоритетный трафик;

в) ресурсы сети оператора (в первую очередь каналы и узлы сети) используются эффективно, т.е. будут максимально загружены, но не перегружены.

Другими словами, оператору необходимо найти один или несколько оптимальных

маршрутов в своей сети между конечными точками VPN.

Базовые протоколы маршрутизации, используемые в современных пакетных сетях (например, дистанционно-векторные, такие, как RIP), определяют для трафика кратчайший маршрут согласно некоторой метрики и выбирают один маршрут при наличии нескольких альтернативных, не учитывая текущую загрузка узлов сети. Поэтому если кратчайший маршрут уже перегружен, то пакеты все равно будут пересылаться по нему. Выбранный маршрут может быть более оптимальным, если анализируется сквозная задержка всех возможных маршрутов между конечными точками, вносимая трафиком конкурирующих VPN с учетом использования ими сетевых ресурсов. Очевидно, что необходимы иные модели и алгоритмы на их основе, позволяющие определять сквозные характеристики QoS на этапе планирования новой VPN.

Теория массового обслуживания (ТМО), широко используемая для анализа характеристик QoS в мультисервисных сетях связи (МСС), позволяет определять средние значения характеристик качества обслуживания (например, среднее число пакетов в очереди и др.). Математические модели ТМО хорошо развиты и применялись для решения задач анализа МСС в большом количестве работ отечественных и зарубежных авторов. Однако, ТМО имеет ряд существенных недостатков. Во-первых, в моделях ТМО входящие и исходящие потоки и дисциплины обслуживания узлов описываются ограниченным числом распределений (например, пуассоновский процесс). Однако в современных МСС трафик в редких случаях может быть пуассоновским, т.к. часто проявляет изменчивость в широком диапазоне масштабов времени. Дисциплины обслуживания в сетевых узлах МСС часто характеризуются сложными функциями, зависящими от различных механизмов обеспечения QoS (таких как дисциплины постановки пакетов в очередь, различные формирователи и ограничители трафика, алгоритмы борьбы с перегрузками), а также алгоритмов маршрутизации. Учитывая нормы QoS, приведенные в рекомендациях ведущих международных организаций по стандартизации в области телекоммуникаций, таких, как МСЭ-Т (например, рекомендация G.1010) можно говорить о том, что в современных сложных пакетных сетях важнее определить не точные, а граничные значения характеристик QoS. ТМО не позволяет этого сделать. В 1990–х годах Р. Крузом была разработана теория, позволяющая определять границы характеристик QoS таких, как задержки передачи пакетов и загрузки сетевых узлов, названая теорией сетевого анализа Network Calculus (NC) [2].

Базовые принципы теории сетевого исчисления Network Calculus

Теория NC развивалась по двум направлениям: детерминистическое (Deterministic Network Calculus, DNC) [3] и стохастическое (Stochastic Network Calculus, SNC) [4]. Теория DNC позволяет определять детерминистические границы, гарантирующие, что реальные параметры QoS в сети оператора (такие, как границы задержки, загрузки, потери пакетов, эффективная полоса пропускания) будут не хуже запрашиваемых пользователем параметров или будут в некоторых нормированных пределах. Таким образом, теория DNC подходит в случае, если требуются строгие оценки граничных характеристик QoS. Тем не менее, анализ с использованием DNC будет всегда давать только пессимистичные оценки, что может привести к необходимости резервирования излишних сетевых ресурсов. Теория SNC позволяет определять стохастические границы, гарантирующие, что реальные параметры QoS с некоторой допустимой вероятностью *e* будут не хуже запрашиваемых пользователем параметров. Таким образом, теория SNC подходит в случае, если не требуются строгие оценки граничных характеристик QoS и допустимы некоторые нарушения нормируемых параметров QoS, однако, при этом сетевые ресурсы используются более рационально. Теория NC была использована в рекомендации ITU-T Y.1315 [5] для моделирования входящего потока и работы узла VPN. На основе этого подхода в [6] было предложено использовать теорию NC также для решения задач оптимального планирования VPN. Модели сети VPN на основе DNC и SNC могут быть совместно использованы для определения границ сквозных характеристик QoS при определении оператором оптимального маршрута на этапе планирования VPN. DNC можно использовать в случае, если клиенту необходимы строгие гарантии QoS и нарушение их очень критично (например, в корпоративных сетях банков, сетях связи спецслужб). При этом оператору необходимо обеспечить дополнительное резервирование сетевых ресурсов, что естественно приведет к увеличению стоимости предоставляемой услуги. SNC подойдет в случае, если клиенту не критичны нарушения гарантий QoS (например, если клиент планирует использовать VPN сеть для передачи некритичных данных, для выхода в сеть Интернет и т.п.). Алгоритмы опреде-

ления границ сквозных характеристик QoS на основе моделей сети VPN, построенные с использованием теорий DNC и SNC, могут быть реализованы в пакете прикладных программ, который позволит автоматизировать процесс планирования услуг VPN.

Архитектура программного пакета планирования услуг VPN

Рассмотрим архитектуру программного пакета планирования услуг VPN, представленную на рис. 1.

База данных. Служит для хранения информации об услугах VPN, информации о сети оператора, результатов вычислений блока вычислений NC. Для повышения управляемости, производительности и доступности база данных может быть секционирована на 3 раздела: база данных клиента, база данных оператора и база данных результатов вычислений.

Блок вычислений Network Calculus. Служит для вычисления сквозных границ характеристик QoS, таких как загрузка, задержка,

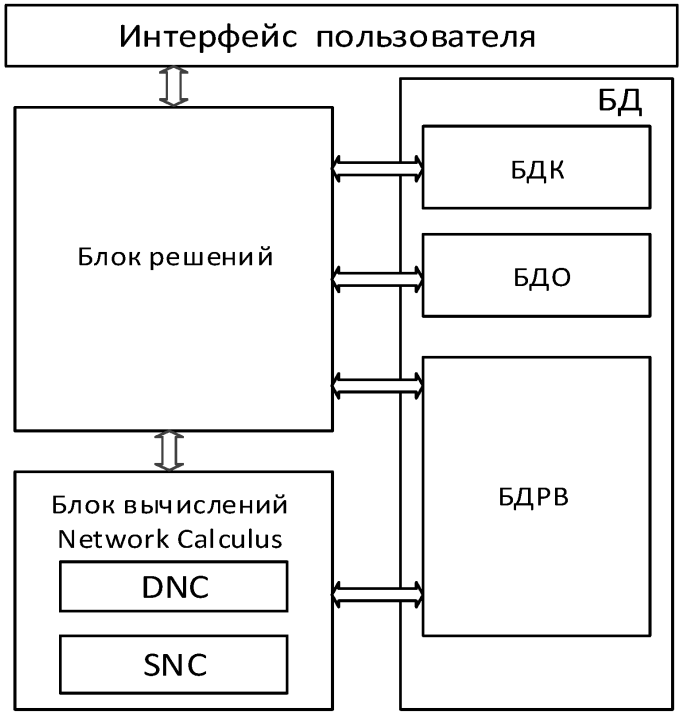

Рис. 1. Архитектура программного пакета планирования услуг VPN

Интерфейс пользователя. Интерфейс пользователя выполняет следующие функции:

1. Ввод информации об услуге VPN: указывается класс обслуживания QoS, прописанный в договоре SLA между клиентом и оператором, уровень гарантий (строгие или не строгие), указываются географические точки подключения конечных точек VPN к соответствующим узлам сети оператора.

2. Ввод информации о сети оператора: указывается число возможных маршрутов между точками подключения офисов клиентов; число узлов каждого маршрута и число конкурирующих потоков в каждом узле; для каждого конкурирующего потока указывается узел входа и выхода.

3. Вывод результатов расчетов из блока решений.

потери пакетов. В зависимости от того, какие необходимы гарантии QoS (строгие или не строгие), блок может вычислять соответственно детерминистические и стохастические границы характеристик QoS.

Детерминистические границы вычисляются в блоке DNC. Алгоритм вычислений может быть основан на методологии LUDB (Least Upper Delay Bound) [7], применение которой для решения задач планирования VPN рассматривалось в [10, 11]. Методология LUDB основана на математическом аппарате теории DNC и позволяет вычислять наименьшую верхнюю границу задержки передачи пакетов. Стохастические границы вычисляются в блоке SNC. Алгоритм вычислений может быть реализован на основе моделей теории SNC [8].

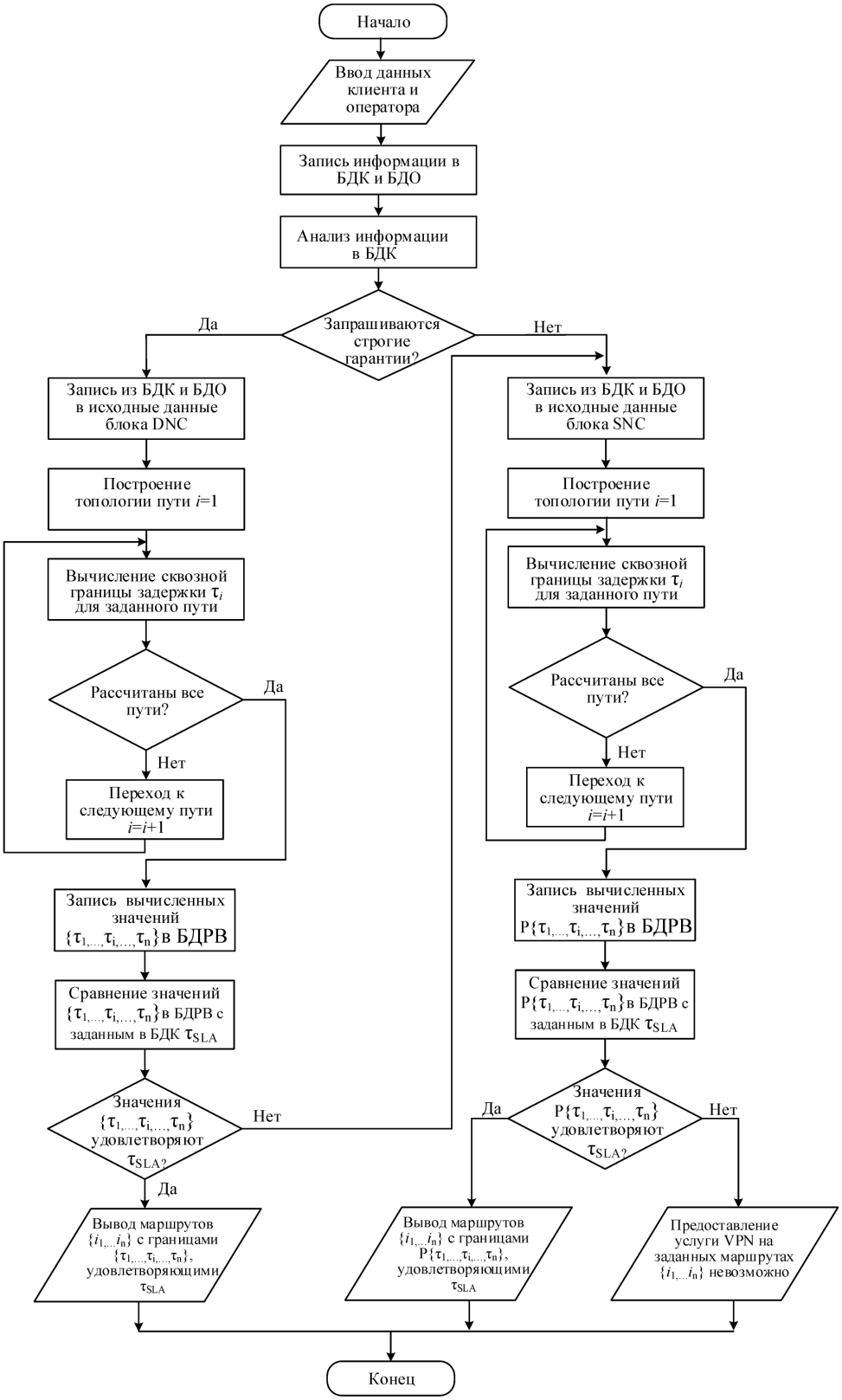

Рис. 2. Алгоритм планирования услуги VPN

Блок решений. Координирует работу всех блоков программного пакета. Производит различные операции над информацией: анализ, сравнение, запись, чтение, удаление. Выводит решения об оптимальных маршрутах, формирует рекомендации по оптимизации сети при наличии перегруженных маршрутов.

Алгоритм планирования услуги VPN

Рассмотрим алгоритм планирования услуги VPN, на основе которого работает блок решений программного пакета планирования услуг VPN (рис. 2). Входные данные об услуге VPN и сети блок решений записывает в соответствующие разделы базы данных: базу данных клиента (БДК) и базу данных оператора (БДО). Затем блок решений, проанализировав информацию в БДК, принимает решение в какой блок вычислений направить информацию из БДК и БДО. Если требуются строгие гарантии QoS, то в блоке DNC на основе методологии LUDB определяется топология возможных маршрутов передачи трафика VPN и для каждого маршрута вычисляется сквозная наименьшая верхняя граница задержки. После вычисления границ задержки для всех маршрутов результаты записываются в базу данных результатов вычислений (БДРВ). Блок решений сравнивает полученные границы задержки для маршрутов с информацией из БДК. На основе сравнения блок решений выбирает маршруты с границей задержки, меньшей либо равной значению задержки заданного класса обслуживания QoS. Если один или несколько маршрутов удовлетворяют заданному классу обслуживания QoS, то информация о них выводится в окно интерфейса пользователя как окончательное решение. Если маршруты не удовлетворяют заданному классу, блок решений перенаправляет исходные данные в блок SNC, где рассчитываются вероятностные границы задержки для каждого маршрута. Аналогично, они сравниваются в блоке решений с заданными значениями задержки в классе качества QoS в БДК, и, если они удовлетворяют им (но уже с некоторой допустимой вероятностью), то результаты выводятся через интерфейс пользователю. При этом блок решений указывает, что точные значения границ задержки не могут быть гарантированы на возможных маршрутах, однако услуга VPN может быть предоставлена клиенту с вероятностными гарантиями границ задержки по более дешевому тарифу. Если вычисленные границы задержки, как точные, так и вероятностные, не удовлетворяют заданным в БДК, то блок решений выводит информацию о том, что услуга VPN не может быть предоставлена клиенту в данном сетевом сегменте. Помимо этого, блок решений выдает рекомендации о том, что возможно необходимо пересмотреть конфигурацию маршрутов, ранее сконфигурированных VPN. Если клиенту изначально не требуются строгие гарантии, то блок решений записывает информацию из БДК и БДО в блок SNC. Процесс вычисления и вывода решения происходит по алгоритму, описанному выше, но при этом вычисляются вероятностные границы задержки.

Заключение

Предлагаемый алгоритм вычисления сквозных границ задержки передачи пакетов в сети VPN, основанных на методологии LUDB, может служить основой для разработки специализированного программного пакета планирования услуг VPN, который позволит провайдерам услуг VPN эффективно использовать имеющиеся сетевые ресурсы и обеспечить гарантированное качество обслуживания. Детерминистические и стохастические модели VPN на основе теории сетевого исчисления требуют экспериментального исследования, результаты которого будут представлены в следующих статьях.

Исследование выполняется при финансовой поддержке РФФИ в рамках научного проекта № 16–37–00363 мол_а.

Список литературы

1. Росляков А. В. Виртуальные частные сети. Основы построения и применения. – М.: Эко-Трендз, 2006. – 304 с.

2. Cruz R. L. A calculus for network delay/ Part I, II // IEEE Trans. Information Theory. 1991. Vol. 37. №1. P.114–141.

3. Le Boudec J.-Y., Thiran P. Network Calculus. A Theory of Deterministic Queuing Systems for the Internet. – Berlin, Heidelberg: Springer-Verlag, 2012. – 263 p.

4. Jiang, Y., Yong L. Stochastic Network Calculus. – London: Springer-Verlag, 2008. – 240 p.

5. ITU-T Recommendation Y.1315. QoS support for VPN services – Framework and characteristics. [Электронный ресурс] – Режим доступа: https://www.itu.int/rec/T-REC-Y.1315–200609–I/en.html (дата обращения 30.10.16).

6. Росляков А.В., Лысиков А.А. Применение теории стохастических сетевых исчислений к анализу характеристик VPN // T-Comm. Телекоммуникации и транспорт. – 2013. – №7. – С. 106–108.

7. Lenzini L., Mingozzi E., Stea G. A Methodology for Computing End-to-end Delay Bounds in FIFO-multiplexing Tandems // Elsevier Performance Evaluation. – 2008. – V. 65.– P. 922–943.

8. Лысиков А.А. Использование LUDB-методологии для определения сквозной функции обслуживания виртуальной частной сети // VI-Международная молодежная научно-практическая конференция СКФ МТУСИ «ИНФОКОМ-2013». – Ростов-на-Дону, 2013. – С. 133–136.