

ПРОГРАММНЫЙ ПАКЕТ VPN DESIGNER NC

*Росляков А.В., Лысиков А.А.**Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ**E-mail: lysikov_inc@mail.ru*

В статье рассматривается программный пакет анализа и планирования виртуальных частных сетей, который позволяет определять оптимальную топологию маршрутов для планируемой VPN с учетом маршрутов и характеристик кросс-потоков других сетей, таких как берстность и интенсивность поступления пакетов трафика. Рассматриваются проблемы, возникающие на этапе планирования VPN при их совместной реализации в сети оператора связи. Показаны различия между моделями VPN на базе детерминистического и стохастического сетевых исчислений. Рассмотрены методы определения детерминистических и вероятностных границ сквозных задержек для потоков между конечными точками VPN. Описан базовый функционал программного пакета. Приводятся результаты исследования влияния маршрутов кросс-потоков на границу сквозной задержки потока планируемой VPN, полученные с использованием разных моделей.

Ключевые слова: виртуальные частные сети, планирование оптимальной топологии, задержка передачи трафика из конца в конец, детерминированное сетевое исчисление, стохастическое сетевое исчисление, программный пакет

Введение

В настоящее время большую популярность приобрела идея виртуализации в сетях связи (технологии SDN и NFV, XaaS, slicing в 5G и др.). Поддержка виртуализации ресурсов будет являться одной из базовых технологий в сетях будущего (Future Networks) [1]. Первоначальной технологией виртуализации является технология виртуальных частных сетей VPN (Virtual Private Network), позволяющая обеспечивать такие характеристики, как безопасность и гарантированное качество обслуживания QoS (Quality of Service) для потоков трафика клиента в пакетных сетях операторского класса, таких как сети следующего поколения NGN (Next Generation Networks). VPN является одной из наиболее востребованных услуг в сетях NGN [2].

VPN является виртуальной сетью, состоящей из набора физических ресурсов операторской сети (таких как каналы и сетевые узлы), которые логически объединены в одну сеть, предоставляющую услуги корпоративным клиентам. Маршруты VPN между конечными точками клиента в сети оператора являются фиксированными. Технологии виртуализации позволяют реализовать множество VPN на общих физических сетевых ресурсах. В современных крупных сетях оператор реализует сотни и тысячи VPN.

Для каждой VPN оператором должны строго соблюдаться установленные в соглашении о гарантированном уровне сервиса SLA (Service Level Agreement) характеристики QoS. Маршруты разных VPN между точками подключения

клиентов часто пересекаются, что приводит к конфликту за общие физические ресурсы сети. Поэтому оператор должен спланировать оптимальную топологию, то есть определить набор оптимальных маршрутов, для каждой новой VPN, чтобы обеспечить максимальный объем реализованных услуг и эффективное распределение сетевых ресурсов с учетом требуемого качества обслуживания для всех реализованных VPN.

Важнейшим параметром QoS является сетевая задержка между каждой парой конечных точек VPN. При определении оптимальных маршрутов для VPN оператор должен знать задержку для всех вариантов пар конечных точек подключения клиентов. Для этого ему нужны советующие модели и методы анализа и инструменты исследования на их основе.

Большая часть сетевых исследований основана на использовании классической теории массового обслуживания (ТМО), которая описывает потоки трафика и дисциплины обслуживания узлов простыми марковскими процессами и законами распределения с короткими «хвостами» и позволяет определять, в основном, только средние значения задержек. В то же время измерения в современных мультисервисных пакетных сетях NGN/IMS/4G показали, что потоки в них часто самоподобные и описываются распределениями с длинными «хвостами», дисциплины обслуживания потоков в узлах сложные и зависят от трафика и др. Классическая ТМО во многом не приспособлена для исследования таких потоков и систем массового обслуживания.

В силу сложности объекта исследования очевидным является отказ от моделей, позволяющих определять точные и средние значения задержек, в пользу моделей, оперирующих с их граничными значениями. Данный подход используется в рекомендациях международных организаций по стандартизации в области телекоммуникаций, таких как МСЭ-Т, IETF, 3GPP и др. Так, согласно рекомендации МСЭ-Т G.1010 задержка при двухсторонней голосовой связи в норме не должна превышать 150 мс, а максимальная задержка не более 400 мс [3].

Последние два десятилетия развивается перспективная теория сетевого исчисления Network Calculus (NC) [4-5], позволяющая проводить анализ сложных сетевых моделей и получать граничные оценки характеристик качества их функционирования. Базовые модели NC подробно рассмотрены в [6]. В [7] разработан алгоритм и архитектура программной системы, позволяющей планировать оптимальную топологию VPN на основе оценки границ задержек. Однако в настоящее время в России и за рубежом отсутствуют подобные программные средства, поэтому создание такой системы является актуальной задачей.

Детерминистическая модель VPN

Теория NC развивается по двум направлениям: детерминистическое DNC (Deterministic Network Calculus) [8-9] и стохастическое SNC (Stochastic Network Calculus) [10]. В [6] модель на основе DNC использована для получения строгих границ задержки в VPN.

Кумулятивный поток трафика $A(t)$ в DNC моделируется кривой поступления $\alpha(t)$ при условии, что для некоторого наблюдаемого периода времени $[0, t]$ выполняется следующее неравенство:

$$A(t) - A(\tau) \leq \alpha(t - \tau), \quad 0 \leq \tau \leq t.$$

Сетевой узел моделируется кривой обслуживания $\beta(t)$ при условии, что для некоторого наблюдаемого периода времени $[0; t]$ число пакетов в выходном потоке $D(t)$ в момент времени t удовлетворяет неравенству:

$$D(t) \geq \inf [A(t - \tau) + \beta(\tau)], \quad 0 \leq \tau \leq t.$$

Верхняя граница задержки для потока $A(t)$ определяется как

$$d(A, D) := \sup_{t \geq 0} \left(\inf \left[d \in \mathbb{R}^+, D(t + \tau) \geq A(t) \right] \right),$$

где $\mathbb{R}^+$ – множество неотрицательных чисел.

В [5] предложен метод оценки граничных задержек в VPN на основе DNC. Согласно данному методу поток планируемой VPN и кросс-потоки других сетей до обслуживания в узле формируются по классическому алгоритму «дырявое ведро», позволяющему настраивать политику обслуживания с учетом интенсивности и берстности входящих в узел потоков трафика.

Кривая поступления $\alpha(t)$ потока трафика VPN и кросс-потоков при этом задается функцией $\gamma_{\sigma, \rho}(t) = \sigma + \rho t$, где σ – максимальная берстность потока (размер «ведра»), ρ – постоянная интенсивность потока (размер отверстия в «ведре») при условии, что $t \geq 0$.

Кривая обслуживания сетевого узла $\beta(t)$ задается функцией $\beta_{T, R}(t) = R[t - T]^+$, где R – постоянная скорость обслуживания в узле, T – фиксированная задержка обработки пакетов в узле при условии, что $R \geq 0$ и $T \geq 0$.

Кривая обслуживания $\beta_{T, R}(t)$ описывает известный алгоритм работы идеального планировщика пакетов GPS (и его модификаций WFQ и DRR), обеспечивающего справедливое распределение ресурсов узла между всеми потоками трафика на интервале времени $[0, t]$.

Граница задержки из конца в конец для VPN, проходящей через цепочку из N узлов с учетом n кросс-потоков в каждом узле, определяется как [6]:

$$d_{(1, N)} = \min \left\{ \sum_{i=1}^N T + \max_{1 \leq k \leq n} \left[\frac{\left(\sigma_{(1, N)} - \sigma_x \right)}{\rho_x} \right]^+ \right\},$$

где $\sigma_{(1, N)}$ – суммарная берстность всех потоков в цепочке узлов, k – номер узла, x – номер потока, $[\cdot]^+$ – обозначает выбор максимального значения из множества значений в скобках.

Стохастическая модель VPN

Основным недостатком DNC является то, что оно позволяет получить детерминированные границы качества обслуживания, которые основываются на наихудшем случае. Однако в большинстве случаев входные потоки трафика и обслуживающие устройства характеризуются некоторыми стохастическими процессами и использование для них детерминированных моделей приводит к слишком завышенным требованиям к сетевым ресурсам для обеспечения гарантий QoS.

Кривая поступления $\gamma_{\sigma,\rho}(t)$ предполагает, что любые «всплески» (берстность) трафика повышают требования к пропускной способности независимо от вероятности их появления, что приводит к неэффективному использованию сетевых ресурсов при передаче мультимедийного трафика. Кроме того, линейная зависимость кривой поступления от количества потоков препятствует реализации статистического мультиплексирования, что особенно сильно сказывается на эффективности использования ресурсов многоканальных транспортных сетей.

SNC позволяет получить оценки того, что реальные значения параметров QoS не будут превышать граничные величины с некоторой вероятностью, меньшей единицы:

$$P\{\text{Реальное QoS} \geq \text{Требуемое QoS}\} \leq \varepsilon,$$

где ε – допустимая вероятность, с которой реальное качество обслуживания QoS нарушает гарантированные границы. Основой SNC являются стохастические кривые поступления и обслуживания. Поток трафика имеет стохастическую кривую поступления α , учитывающую объем трафика, с граничной функцией f , если для всех $0 \leq \tau \leq t$ и всех $x \geq 0$ имеет место неравенство [10]:

$$P\{A(\tau, t) - \alpha(t - \tau) > x\} \leq f(x).$$

Сетевой узел имеет стохастическую кривую обслуживания β с граничной функцией g , если для всех $t \geq 0$ и $x \geq 0$ имеет место неравенство [10]:

$$P\left\{\sup_{0 \leq \tau \leq t} [A \otimes \beta(t) - D(t)] > x\right\} \leq g_t(x),$$

где $\otimes$ – символ (min,+)-свертки; индекс t у граничной функции указывает ее зависимость от времени. Задержка потока $d(t)$ будет иметь следующую вероятностную границу

$$P\{d(t) > H\} \leq f \otimes g_t(x),$$

где $H = h(\alpha + x, \beta)$ – максимальное горизонтальное расстояние между функциями $\alpha(t) + x$ и $\beta(t)$ для $x \geq 0$.

В [6] модели на основе SNC предлагается использовать для получения нестрогих границ задержки в VPN. Стохастическая модель VPN основана на методе, представленном в [11]. Согласно данному методу время разбивается на фиксированные интервалы, а объем трафика моделируется непрерывной (жидкостной) моделью.

Определение 1. Пусть $(\alpha_i)_{i \in N}$ является последовательностью неотрицательных действительных случайных величин. Тогда поток $A(t)$, входящий в узел, будет характеризоваться кумулятивным числом пакетов, поступивших в узел до момента времени t :

$$A(t) = \sum_{i=1}^t a_i.$$

Для описания «хвостов» функций распределения кривых поступления и обслуживания в SNC наиболее часто используется производящая функция моментов (ПФМ), которая ограничена сверху.

Определение 2. ПФМ для функции распределения некоторого входящего потока $A(t)$ со свободным параметром θ определяется как

$$\phi_{A(t)}(\theta) = E(e^{\theta A(t)}),$$

где E – математическое ожидание случайной величины.

ПФМ для хвоста функции входящего потока $A(t)$ с моделью $\gamma_{\sigma,\rho}$ и параметром $\theta > 0$ существует, при условии что:

$$\phi_{A(\tau, t)}(\theta) \leq e^{\theta \rho(\theta)(t - \tau) + \theta \sigma(\theta)}, \quad \tau \leq t, \quad (1)$$

где $\sigma(\theta)$ и $\rho(\theta)$ – параметры ПФМ, характеризующие, соответственно, берстность и интенсивность потока трафика $A(t)$.

Зададим модель трафика VPN. Предположим, что за интервал времени t передано $a(t)$ пакетов трафика VPN, которые являются стохастически независимыми и распределены экспоненциально с параметром интенсивности λ . Плотность экспоненциального распределения определяется как:

$$f(x) = \lambda e^{-\lambda x}, \quad x \geq 0, \quad (2)$$

где $f(x) = 0$ при $x < 0$. Учитывая (2) ПФМ для единичного приращения функции, $a(t)$ может быть определена как $\phi_{a(t)}(\theta) = \lambda / (\lambda - \theta)$. Вследствие стохастической независимости приращений функции $A(t)$ имеем

$$\phi_{A(\tau, t)}(\theta) = \prod_{r=\tau+1}^t \phi_{a(r)}(\theta) = \left(\frac{\lambda}{\lambda - \theta} \right)^{t - \tau}. \quad (3)$$

Таким образом, исходя из (3) параметры интенсивности и берстности для (1) можно определить как:

$$\rho(\theta)=1/\theta \log\left(\frac{\lambda}{\lambda-\theta}\right), \sigma(\theta)=0. \quad (4)$$

Определение 3. Двухпараметрический стохастический процесс S с суммарным числом обслуженных пакетов $S(\tau, t) \geq 0$ и $S(\tau, t) \leq S(\tau, t')$ для всех $0 \leq \tau \leq t \leq t'$ называется динамическим S -сервером, характеризующим дисциплину обслуживания в узле, если для любого поступающего в узел потока $A(t)$ и всех $t \geq 0$ выполняется следующее условие:

$$D(t) \geq A \otimes S(0, t) = \min_{0 \leq \tau \leq t} \{A(0, \tau) + S(\tau, t)\},$$

где $D(t)$ описывает поток обслуженных пакетов на выходе узла.

ПФМ для «хвоста» распределения функции обслуживания $S(t)$ с $\theta > 0$ существует, при условии что

$$\phi_{S(\tau, t)}(-\theta) \leq e^{\theta \rho(\theta)(t-\tau) + \theta \sigma(\theta)}, \quad \tau \leq t, \quad (5)$$

где знак « $\rightarrow$ » обозначает то, что дисциплина обслуживания ограничена снизу.

Зададим модель обслуживания потока в узле VPN. Предположим, что узел обслуживает поток трафика VPN без задержки с постоянной скоростью R , то есть $S(\tau, t) = R(t - \tau)$. Тогда ПФМ для «хвоста» распределения $S(\tau, t)$ данного узла можно определить как

$$\phi_{S(\tau, t)}(-\theta) = e^{-R(t-\tau)}. \quad (6)$$

Таким образом, исходя из (6) параметры интенсивности и берстности в (5) есть

$$\rho(\theta) = -R, \quad \sigma(\theta) = 0. \quad (7)$$

Для определения стохастической границы задержки потока трафика, проходящего через сетевой узел, используем теорему [11].

Теорема. Пусть функция входящего потока $A(\tau, t)$ и функция обслуживания узла $S(\tau, t)$ ограничены производящими функциями моментов соответственно:

$$\phi_{A(\tau, t)}(\theta) \leq e^{\theta \rho_A(\theta)(t-\tau) + \theta \sigma_A(\theta)};$$

$$\phi_{S(\tau, t)}(-\theta) \leq e^{\theta \rho_S(\theta)(t-\tau) + \theta \sigma_S(\theta)},$$

где σ_A и ρ_A – параметры ПФМ, характеризующие, соответственно, берстность и интенсивность входящего потока, а σ_S и ρ_S – функции обслуживания узла. Если $A(\tau, t)$ и $S(\tau, t)$ стохастически независимы, то вероятность превыше-

ния границы задержки для потока $A(\tau, t)$ в узле можно определить как

$$P(d(t) > H) \leq \frac{e^{\theta \rho_S(\theta)T} e^{\theta \sigma_A(\theta) + \theta \sigma_S(\theta)}}{1 - e^{\theta(\rho_A(\theta) + \rho_S(\theta))}}.$$

Из теоремы [11] следует, что вероятность превышения границы задержки $d_N(t)$ для потока трафика, проходящего через цепочку из N сетевых узлов есть

$$P\left(d_N(t) > H\right) \leq e^{-\theta \rho_A(\theta)H} \frac{e^{\theta \sigma_A(\theta) + \sum_{j=1}^N \theta \sigma_j(\theta)}}{\prod_{j=1}^N 1 - e^{\theta(\rho_j(\theta) + \rho_A(\theta))}}, \quad (8)$$

где ρ_j и σ_j – параметры ПФМ для «хвоста» функции обслуживания j -го узла.

Учитывая (4) и (7)-(8), вероятность превышения границы задержки $d_N(t)$ для потока VPN будет определяться как

$$P\left(d_N(t) > H\right) \leq e^{-\theta \left(1/\theta \log\left(\frac{\lambda}{\lambda-\theta}\right)\right)H} \frac{1}{\prod_{j=1}^N 1 - e^{\theta \left(-R_j + 1/\theta \log\left(\frac{\lambda}{\lambda-\theta}\right)\right)}}$$

VPN Designer NC

Программный пакет VPN Designer NC реализован на языке Delphi на основе архитектуры, представленной в [6]. Пакет имеет удобный графический пользовательский интерфейс. Главное окно пакета показано на рисунке 1.

Ввод узлов физической сети и конечных точек (офисов) VPN осуществляется путем добавления в главное окно объектов двух типов, соответственно, «узел» и «офис». Связность узлов физической сети и офисов VPN осуществляется путем соединения объектов направленными стрелками, которые представляют каналы связи. Физическим узлам можно задать два параметра: максимальная задержка передачи трафика через узел и минимально гарантированная скорость обслуживания трафика. Для конечных точек VPN можно задать два параметра: максимальную берстность трафика и максимальную интенсивность трафика.

Параметры узлов и офисов задаются путем ввода числовых значений в специальных меню. Объединение офисов в одну VPN осуществляется путем ввода числовых значений в специальном меню параметров физических каналов связи и в меню офисов VPN. Для удобства ввода и редактирования физической сети и VPN предусмотрены функции создания объектов через общее

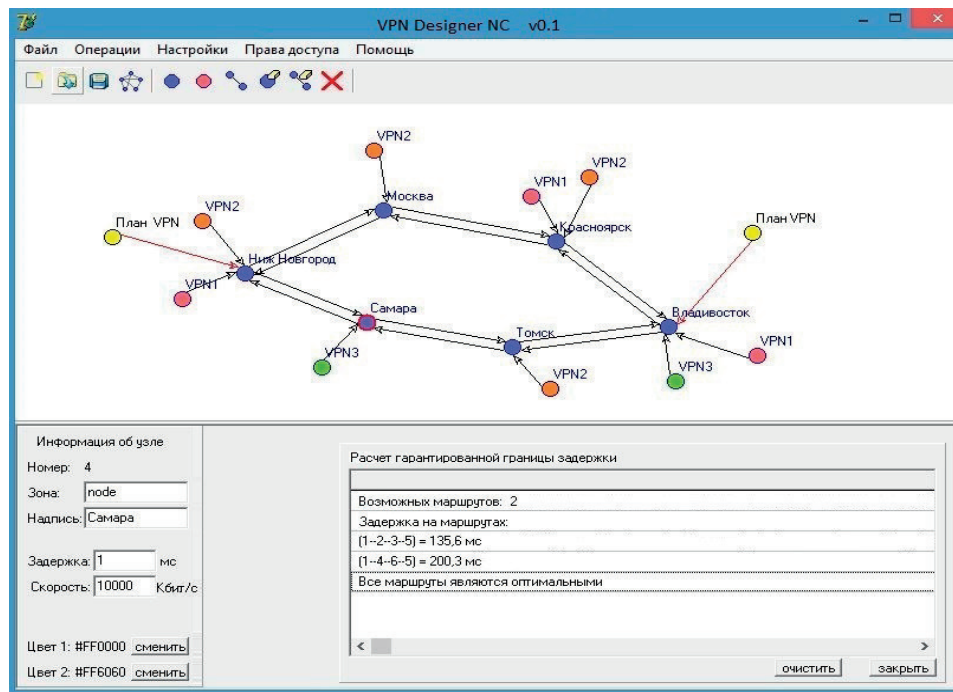


Рисунок 1. Главное окно пакета VPN Designer NC

меню или непосредственно из панели инструментов.

VPN Designer NC для заданной конфигурации сети позволяет определять набор оптимальных маршрутов между двумя любыми физическими сетевыми узлами, к которым планируется подключение офисов новой VPN с заданными характеристиками берстности и интенсивности трафика, а также с требуемой границей сквозной задержки, которая вводится в пакет ранее. Данная операция выполняется при выборе пользователем специальной команды в главном меню пакета.

Пакет на основе введенной пользователем конфигурации сети определяет возможные маршруты между двумя заданными физическими узлами и кросс-поток других VPN, которые будут пересекаться с потоками планируемой VPN, а затем вычисляет для каждого маршрута границу сквозной задержки по моделям, рассмотренным выше. После вычисления задержек для всех возможных маршрутов пакет сравнивает их с требуемой задержкой для планируемой VPN и выводит в главное окно решение о наличии или отсутствии оптимальных маршрутов.

Пользователь имеет возможность задать режим для определения детерминистической или стохастической границ задержки. При отсутствии оптимальных маршрутов пакет предлагает возможные варианты решения данной проблемы. Так, если в результате расчета детерминистиче-

ских границ задержки оптимальных маршрутов нет, то одним из возможных вариантов пакет предложит пользователю рассчитать стохастические границы задержки для возможных маршрутов. Пакет имеет модульную структуру, что позволяет в дальнейшем добавлять другие модули.

Исследование влияния маршрутов кросс-поток на границу задержки VPN

С использованием VPN Designer NC было проведено экспериментальное исследование влияния маршрутов кросс-поток на детерминистическую и стохастическую границы сквозной задержки планируемой VPN. Для анализа использовались два варианта сценариев маршрутов: длинный маршрут кросс-потока $\alpha_{\sigma 2, \rho 2}$ (см. рисунок 2а) и короткие маршруты кросс-поток $\alpha_{\sigma 2, \rho 2}, \alpha_{\sigma 3, \rho 3}$ и $\alpha_{\sigma 4, \rho 4}$ (см. рисунок 2б).

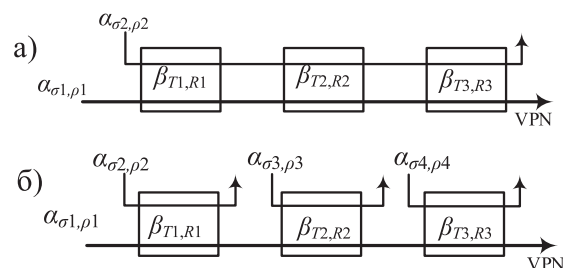


Рисунок 2. Схемы исследования

Исследование детерминистической модели NC подтвердило важное свойство DNC, что при про-

хождении через узлы трафик за счет формирова-
телей выравнивается и наибольшая задержка будет
проявляться в первом узле. В англоязычной ли-
тературе по NC такая закономерность называется
PBOO (Pay Burstiness Only One) и дословно пере-
водится как «плати за берстность один раз». По-
этому при длинном маршруте кросс-потока (рис.
3а) задержка будет значительно ниже, чем в случае
с короткими кросс-потоками (см. рисунок 3б).

При исследовании стохастической модели
VPN влияние маршрутов кросс-потоков на гра-
ницу задержки планируемой VPN не выявлено.
Это можно объяснить тем, что в данной модели
VPN не учитывается берстность трафика.

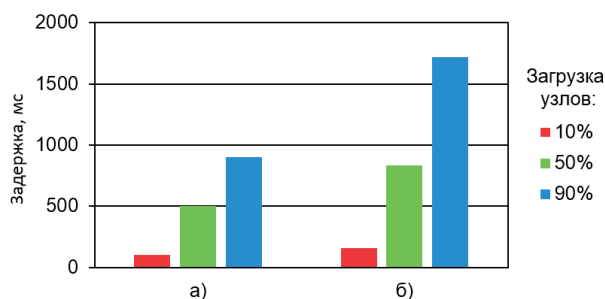


Рисунок 3. Результаты эксперимента

Поэтому на практике желательно выбирать
такие маршруты для потока VPN, где его пересе-
чение с одними и теми же кросс-потоками будут
в большем числе узлов, то есть с длинными мар-
шрутами. Выявленное свойство можно рекомен-
довать на практике при планировании топологии
VPN, что позволит обеспечить лучшее качество
обслуживания клиентов.

Заключение

Пакет VPN Designer NC позволяет плани-
ровать топологию VPN с учетом допустимых
границ задержек из конца в конец. Результаты
планирования VPN, полученные с помощью раз-
работанного пакета, позволят на практике повы-
сить эффективность загрузки ресурсов узлов и
каналов сети связи, а также обеспечить выполне-
ние требуемых параметров SLA и улучшить каче-
ство предоставляемых услуг VPN.

Пакет может быть использован проектными,
эксплуатационными и научно-исследовательски-
ми организациями, а также провайдерами услуг

VPN, при проектировании, разработке и плани-
ровании виртуальных частных сетей.

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

Литература

1. Росляков А.В., Ваняшин С.В. Будущие сети (Future Networks) – Самара: ИУНЛ ПГУТИ, 2015. – 274 с.
2. Росляков А.В. Виртуальные частные сети. Основы построения и применения. – М.: Эко-Трендз, 2006. – 304 с.
3. ITU-T G1010 Series G: Transmission systems and media digital systems and networks. Quality of service and performance. End-user multimedia QoS categories. – 2001. – 18 p.
4. Cruz R.L. A calculus for network delay, part I: Network element in isolation // IEEE Transaction on information theory. – 1991. – Vol.1. – No. 37. PP.114-131. doi: 10.1109/18.61109.
5. Cruz R.L. A calculus for network delay, part II: Network Analysis // IEEE transaction on information theory. – 1991. – Vol.1. – No. 37. –P. 132-141. doi: 10.1109/18.61110.
6. Лысиков А.А. Исследование граничных значе-
ний задержек трафика VPN с учетом конкури-
рующих потоков // Инфокоммуникационные
технологии. – 2017. – Т.15. – № 1. – С. 40-49.
doi: 10.18469/ikt.2017.15.1.06.
7. Лысиков, А.А. Программный пакет планиро-
вания виртуальных частных сетей на основе
теории сетевого исчисления // Междунаро-
дный журнал прикладных и фундаментальных
исследований. – 2016. – № 11-3. – С. 375-379.
8. Le Boudec J.-Y., Thiran P. Network Calculus: A
Theory of Deterministic Queuing Systems for the
Internet. Springer-Verlag, 2012. – 263 p.
9. Chang S.-C. Performance Guarantees in
Communication Networks. Springer-Verlag,
2000. – 401 p.
10. Jiang Y., Yong L. Stochastic Network Calculus.
Springer-Verlag, 2008. – 240 p.
11. Beck M.A., Henningsen S.A. Technical Report
The Stochastic Network Calculator. – CoRR
abs/1707.07739. – 2017.

Получено 01.03.2018

Росляков Александр Владимирович, д.т.н., профессор, заведующий Кафедрой автоматической электросвязи (АЭС) Поволжского государственного университета телекоммуникаций и информатики. Тел. 8 (846) 333-69-25. E-mail: aros1@mail.ru

Лысиков Андрей Александрович, старший преподаватель кафедры АЭС ПУТИ. Тел. 8 (846) 339-11-39.
E-mail: lysikov_inc@mail.ru

VPN DESIGNER NC SOFTWARE

Roslyakov A.V., Lysikov A.A.

Povolzhskiy State University of Telecommunications and Informatics, Samara, Russia

E-mail: lysikov_inc@mail.ru

The article discusses a software for virtual private network analysis and planning that allows to determine the optimal topology of routes for a virtual private network, taking into account the routes and characteristics of cross-flows of other networks, such as burstiness and the traffic flow rate. The problems arising at the planning stage of VPN networks during their joint implementation in the network of the telecoms operator are considered. Differences between deterministic and stochastic network calculus are shown. The models underlying algorithms for determining the deterministic and probabilistic boundaries for virtual private network flows are studied. The basic functionality of the software is considered. The results of a study of the influence of cross-flow routes of other networks on the VPN delay bound obtained using different models are presented.

Keywords: virtual private networks, optimal topology planning, end-to-end traffic delay, deterministic network calculus, stochastic network calculus, software

DOI: 10.18469/ikt.2018.16.3.05

Roslyakov Alexander Vladimirovich, Povolzhskiy State University of Telecommunications and Informatics, 23 L. Tolstoy str., Samara 443010, Russian Federation, the Head of Department of Automatic Telecommunication, Doctor of Technical Sciences, Professor. Tel. +78463336925. E-mail: arosl@mail.ru

Lysikov Andrey Aleksandrovich, Povolzhskiy State University of Telecommunications and Informatics, 23 L. Tolstoy str., Samara 443010, Russian Federation, Senior Lecturer of the Department of Automatic Telecommunication. Tel. +78463391139. E-mail: lysikov_inc@mail.ru

References

1. Roslyakov A.V., Vanyashin S.V. *Budushchiye seti* [Future Networks]. Samara, PSUTI Publ., 2015. 274 p.
2. Roslyakov A.V. *Virtualnye tyastnye seti. Osnovy postroeniya i primeneniya* [Virtual private networks. Bases of construction and application]. Moscow, Eco-Trends Publ., 2006. 304 p.
3. ITU-T. G1010. Series G: Transmission systems and media digital systems and networks. Quality of service and performance. End-user multimedia QoS categories. 2001. 18 p.
4. Cruz R.L. A calculus for network delay, part I: Network element in isolation. *IEEE Transaction on information theory*, 1991. vol. 1, no. 37, pp. 114-131. doi: 10.1109/18.61109.
5. Cruz R.L. A calculus for network delay, part II: Network Analysis. *IEEE transaction on information theory*, 1991. vol. 1, no. 37, pp. 132-141. doi: 10.1109/18.61110.
6. Lysikov A.A. Issledovanie granitnykh znateniy zaderzek trafika VPN s ytyotom konkuriruysih potokov [Study of boundary values of VPN traffic delays considering cross flows]. *Infokommunikacionnye tehnologii*, 2017, V.15, no.1, pp. 40-49. doi: 10.18469/ikt.2017.15.1.06
7. Lysikov A.A. Programniy paket planirovaniya virtualnih tyastnykh setei na osnove teorii setevogo istisleniya [Software package for planning virtual private networks based on the theory of network calculus]. *Megdunarodnyi zhurnal prikladnykh i fundamentalnykh issledovaniy*, 2016, no. 11-3, pp. 375-379.
8. Le Boudec J.-Y., Thiran P. *Network Calculus: A Theory of Deterministic Queuing Systems for the Internet*. Springer-Verlag, 2012. 263 p.
9. Chang S.C. *Performance Guarantees in Communication Networks*. Springer-Verlag, 2000. 401 p.
10. Jiang, Y., Yong L. *Stochastic Network Calculus*. Springer-Verlag, 2008. 240 p.
11. Beck M.A., Henningsen S.A. *Technical Report The Stochastic Network Calculator*. CoRR abs/1707.07739. 2017.

Received 01.03.2018