УДК 621.391

ДИНАМИЧЕСКАЯ МОДЕЛЬ СИНТЕЗА ОДНОРАНГОВОЙ ВИРТУАЛЬНОЙ ЧАСТНОЙ СЕТИ

В.Л. СТЕРИН, А.С. ЕРЕМЕНКО, ТАРИКИ НАДИЯ
Харьковский национальный университет радиоэлектроники

Abstract *– Analysis of design principles of virtual private networks is conducted. Classification of VPNs is made and the main requirements to such solutions from the viewpoint of their design and QoS provision are formulated. It is confirmed that the restricting factor in increasing VPN networks performance and providing quality of service in them is inefficient allocation of resources of a network service provider among virtual private networks being created. It is shown that the solution for the situation is seen in transfer to dynamic models of structural and functional synthesis of VPN. We propose a dynamic model for synthesis of peer-to-peer private networks, the novelty of which is in the fact that it is presented both as a system of linear difference equations to describe the process of bandwidth reallocation for links of service provider network among different virtual private networks; and by nonlinear algebraic equations to describe processes of flow routing and overload control. Using the model allows to provide more effective resource management in service provider network when designing peer-to-peer virtual private networks through better accounting of the dynamics of information exchange processes occurring in it. The proposed solutions are adapted for both pipe-model and hose-model supported in solutions that are based on MPLS-technology. Realization of state forecasting property in VPN-networks management allows to reallocate resources of service provider network among created virtual private networks more flexibly.*

Анотація *– Запропоновано динамічну модель синтезу одноранговихвіртуальних приватних мереж, новизна якої полягає в тому, що вона представлена як системою лінійних різницевих рівнянь для опису процесу перерозподілу пропускних здатностей трактів передачі мережі сервіс-провайдера між різними віртуальними приватними мережами, так і нелінійними алгебраїчними рівняннями для опису процесів маршрутизації потоків та управління перевантаженням. Використання моделі дозволяє забезпечити більш ефективне управління ресурсами мережі провайдера при створенні одноранговихвіртуальних приватних мереж за рахунок більш повного врахування динаміки процесів інформаційного обміну, що протікають в ній. Запропоновані рішення адаптовані як під модель ізольованого каналу (pipe-модель), так і під розподілену модель (hose-модель), які підтримуються в рішеннях, заснованих на MPLS-технології. Реалізація властивості прогнозування стану при управлінні VPN-мережами дозволяє більш гнучко перерозподіляти ресурси мережі сервіс-провайдера між створюваними віртуальними приватними мережами.*

Аннотация *– Предложена динамическая модель синтеза одноранговых виртуальных частных сетей, новизна которой заключается в том, что она представлена как системой линейных разностных уравнений для описания процесса перераспределения пропускных способностей трактов передачи сети сервис-провайдера между различными виртуальными частными сетями, так и нелинейными алгебраическими уравнениями для описания процессов маршрутизации потоков и управления перегрузкой. Использование модели позволяет обеспечить более эффективное управление ресурсами сети провайдера при создании одноранговых виртуальных частных сетей за счет более полного учета динамики процессов информационного обмена, протекающих в ней. Предложенные решения адаптированы как под модель изолированного канала (pipe-модель), так и под распределенную модель (hose-модель), которые поддерживаются в решениях, основанных на MPLS-технологии. Реализация свойства прогнозирования состояния при управлении VPN-сетями позволяет более гибко перераспределять ресурсы сети сервис-провайдера между создаваемыми виртуальными частными сетями.*

Введение

Задачи синтеза систем телекоммуникаций, функционирующих в рамках парадигмы NGN (Next Generation Network) в интересах тех или иных пользователей, не ограничиваются лишь проектированием новых телекоммуникационных сетей (ТКС). В ряде важных случаев, все больше находящих свое применение на практике, требуется создание сети в интересах различных организаций, предприятий и компаний, их удаленных офисов и других распределенных на некоторой территории отдельных подразделений на базе уже существующей телекоммуникационной инфраструкту-

ры (оборудования и сетевых решений). Все больше проявляются преимущества от заключения субдоговоров на предоставление инфокоммуникационных услуг с внешними провайдерами (outsourcing). Речь идет о создании так называемых виртуальных частных сетей (Virtual Private Network, VPN) [1-3], охватывающих ключевые функциональные подсистемы NGN как доступа, так и транспорта, с широкими возможностями относительно поддержки функций качества обслуживания, безопасности, доступности и надежности конечных решений.

I. Особенности построения виртуальных частных сетей

Прежде чем перейти к обзору вариантов построения и классификации виртуальных частных сетей, остановимся на основных терминах и определениях, касающихся данной предметной области и которые будут использоваться далее.

В состав рассматриваемой ТКС, определяющей основные функциональные компоненты комплексного решения по VPN, входят [1, 4, 5] (рис. 1):

- сеть поставщика (провайдера) сетевых услуг (Р-сеть), ресурсы которой используются для создания VPN в интересах клиентов;

- сети клиентов (С-сети): часть общей сети заказчика услуг, которая находится под контролем клиента.

Некоторые территориально обособленные фрагменты сети клиента (компании, организации, предприятия), для обеспечения информационного взаимодействия между в которыми и создается виртуальная частная сеть на базе сети сервис-провайдера, именуются «сайтами».

Устройства, которые составляют основу сетей провайдера и клиентов, а также служат для обеспечения их взаимодействия, подлежат следующей декомпозиции:

- маршрутизатор клиентов (Customer router), который связывает сайт клиентов с сетью провайдера, называется приграничный клиентский маршрутизатор (Customer Edge router, CE-router) – CE-маршрутизатор. Традиционно это устройство относится к классу абонентского оборудования (Customer Premises Equipment, CPE);

- приграничные устройства сети сервис-провайдера (Provider Edge, PE), к которым подключаются устройства клиентов (CE);

- устройства сети сервис-провайдера (P), которые обеспечивают передачу данных через данную сеть и связаны с клиентским оборудованием (CE) лишь через приграничные устройства (PE).

Для обслуживания клиентов разных VPN на PE-устройстве создается несколько виртуальных объектов (по числу поддерживаемых VPN), которые называются VPN Routing and Forwarding (VRF) и образуются:

- отдельной таблицей IP-маршрутизации, использующейся для маршрутизации пакетов VPN (далее VRF-таблица);
- множеством интерфейсов PE-устройства, к которым подключены устройства CE, принадлежащие одной VPN.

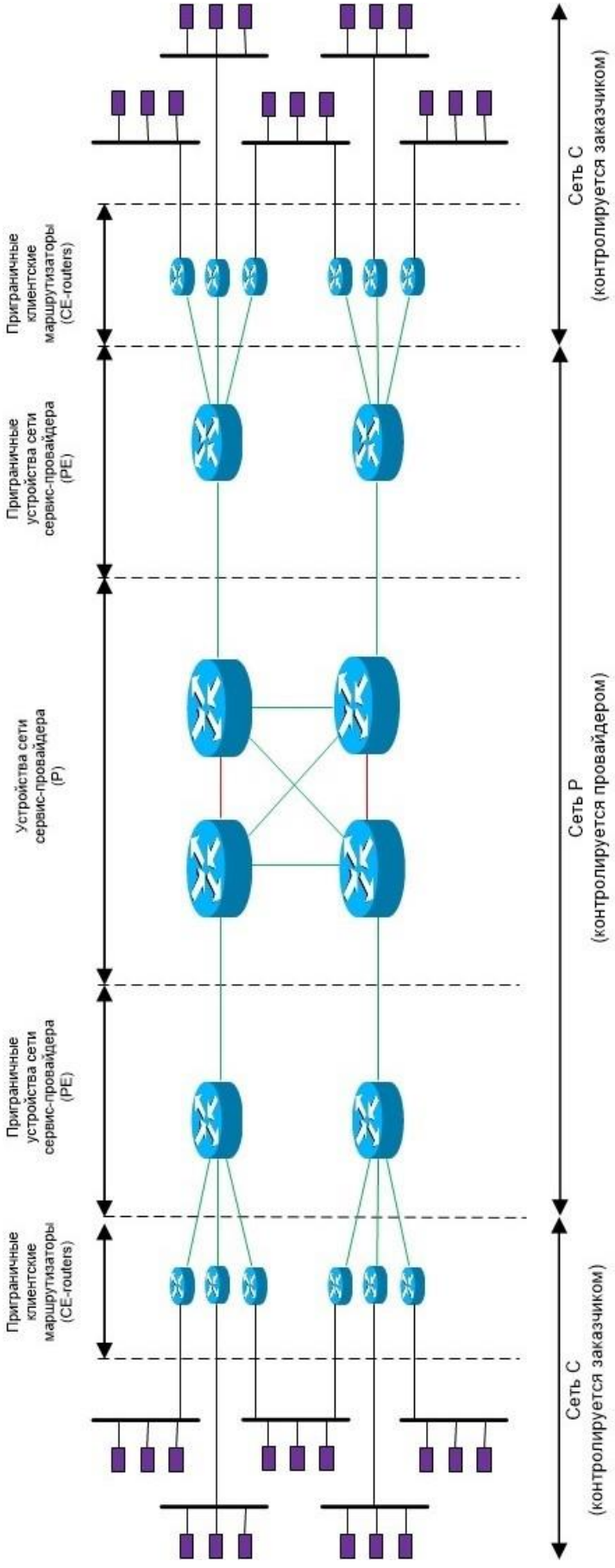


Рис. 1. Вариант комплексного решения по VPN

II. Классификация виртуальных частных сетей

Широкое использование VPN-решений позволило классифицировать их по ряду основных признаков (рис. 2) [1-3].

В зависимости от того, средствами какого уровня эталонной модели взаимодействия открытых систем (ЭМВОС, OSI) организуется работа виртуальных частных сетей, их разделяют на VPN канального, сетевого и сеансового уровней. Средства VPN канального уровня OSI (L2VPN) обеспечивают построение виртуальных туннелей типа «точка-точка», инкапсулируя различные виды трафика третьего и более высоких уровней. К этой классификационной группе относятся VPN-решения, которые используют протоколы L2F (Layer 2Forwarding), PPTP (Point-to-Point Tunneling Protocol) и стандарт L2TP (Layer 2 TunnelingProtocol).

При использовании средств сетевого (L3VPN) уровня при создании VPN чаще других используют протоколы GRE (Generic Routing Encapsulation) и IPSEC (IPSecurity), которые предназначены для организации туннелирования, шифрования и аутентификации IP-пакетов. На сеансовом уровне иногда используется подход под названием circuit proxy (посредники каналов) для ретрансляции трафика из защищенной сети в общедоступную сеть.

На практике VPN-сети могут находить своё применение в зависимости от способа технической реализации в виде как программного решения, так и интегрированного программно-аппаратного обеспечения. В первом случае сеть настраивается программно, как правило – удаленно, на основе распределения ресурсов IP/MPLS-сети за счет настройки сетевого оборудования и конфигурирования основных механизмов и протоколов управления, в т.ч. туннелирования трафика. При использовании интегрированных решений наряду с программными средствами могут использоваться и специализированные аппаратные платформы, что приводит к некоторому удорожанию процесса создания и поддержки VPN-сети, но способствует повышению ее эффективности как по производительности ТКС, так и по безопасности.

В соответствии с их непосредственным функциональным назначением виртуальные частные сети классифицируются на VPN с удаленным доступом (Remote Access), внутрикорпоративные (Intranet-VPN) и межкорпоративные сети (Extranet-VPN), Internet VPN и клиент-серверные VPN. VPN с удаленным доступом, как правило, предназначены для обеспечения защищенного удаленного доступа к ресурсам ТКС сотрудникам компании. Внутрикорпоративные VPN-сети могут использоваться для объединения в единую защищённую сеть нескольких распределённых филиалов одной организации, обменивающихся данными по открытым каналам связи. Межкорпоративные VPN-решения предназначены для подключения внешних пользователей, уровень доверия которых ниже, чем у сотрудников компании, что связано с дифференциацией применяемых политик обеспечения сетевой безопасности. Internet VPN в основном используется для предоставления услуг интернет-доступа, а клиент-серверные VPN-решения – для защиты передаваемых данных между двумя узлами (сайтами) корпоративной сети, в интересах которой и создается VPN.

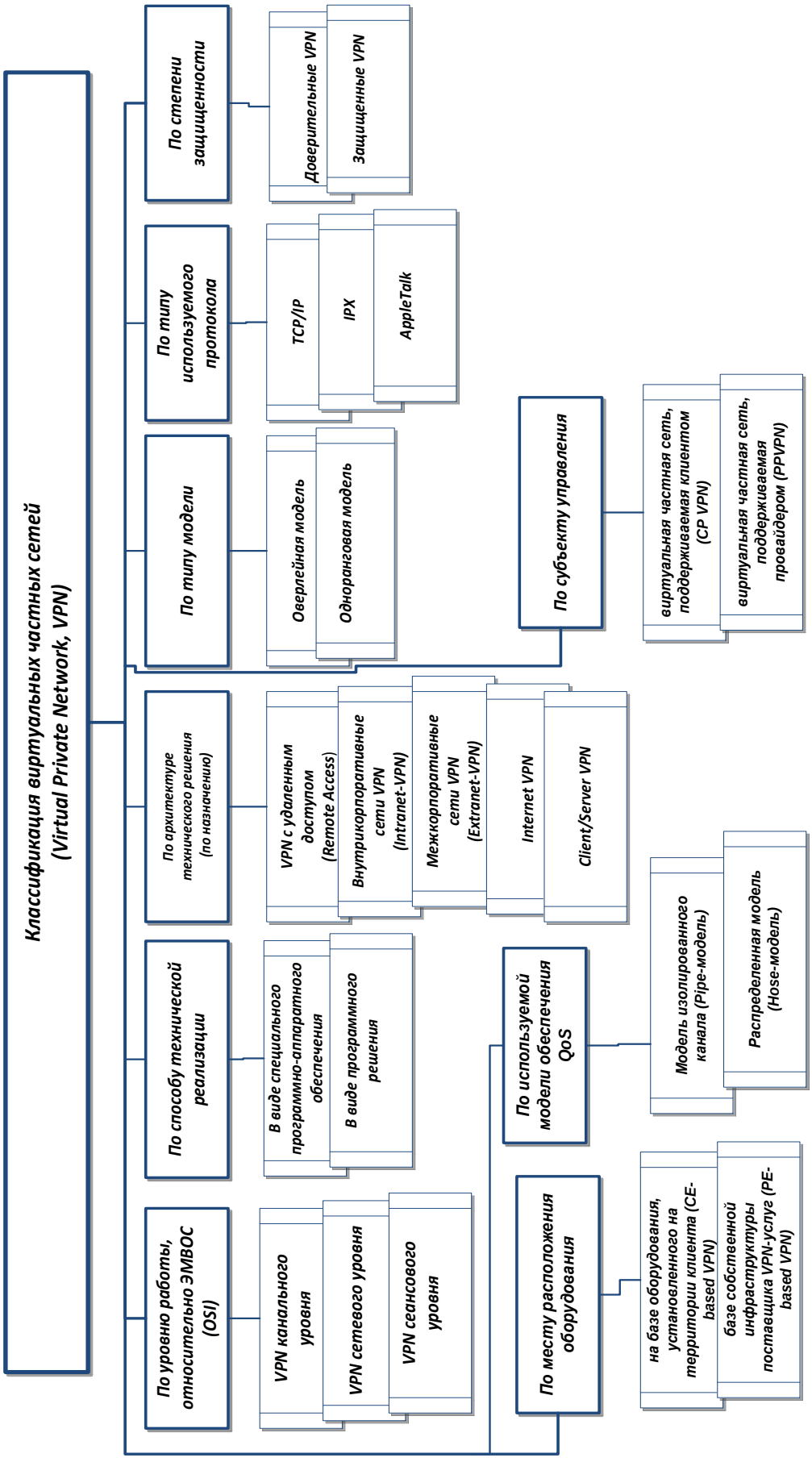


Рис. 2. Классификация виртуальных частных сетей

По типу используемого протокола VPN-сети подразделяются на сети с поддержкой протоколов TCP/IP, AppleTalk и IPX, среди которых наибольшее распространение получил первый стек протоколов (TCP/IP).

По степени защищенности виртуальные частные сети делятся на доверительные (незащищенные) и защищенные VPN. Доверительные VPN ввиду простоты их реализации используются в случае невысоких требований к уровню безопасности. В противном случае с использованием IPSec, OpenVPN и PPTP строятся защищенные VPN.

В зависимости от того, кто поддерживает VPN-сеть и управляет ею (по субъекту управления), виртуальные частные сети подразделяются на два основных вида. В случае использования виртуальной частной сети, поддерживаемой клиентом (Customer Provided Virtual Private Network, CP VPN), практически все задачи по поддержке VPN-сети возлагаются на оборудование (на сторону) клиента. Поставщик VPN-услуги (сервис-провайдер) предоставляет только традиционные услуги по объединению сайтов клиента в единую сеть, а настройкой и конфигурированием средств VPN занимаются сетевые администраторы со стороны клиента

В случае реализации виртуальной частной сети, поддерживаемой провайдером (Provider Provisioned Virtual Private Network, PPVPN), поставщик услуг (провайдер) на основе собственной сети настраивает виртуальную частную сеть для каждого своего клиента в соответствии с выдвигаемыми требованиями относительно уровня качества обслуживания и безопасности (защищенности). Именно этот способ наиболее перспективный. Т.к. работа по созданию и управлению VPN достаточно сложна и специфична большинство клиентов (компаний, предприятий и фирм) предпочитают переложить ее на оборудование провайдера. Кроме того, важно отметить, что реализация VPN-услуг позволяет провайдеру предоставлять и ряд дополнительных услуг, включая контроль за состоянием клиентской сети, веб-хостинг и хостинг почтовых служб, хостинг специализированных приложений клиентов и др.

Кроме того, в зависимости от места расположения оборудования, выполняющего функции VPN, виртуальная частная сеть может строиться как на базе оборудования, установленного на территории клиента (Customer Premises Equipment based VPN, CPE-based VPN или Customer Edge based VPN, CE-based VPN), так и на базе собственной инфраструктуры поставщика VPN-услуг (Network-based VPN или Provider Edge based VPN, PE-based VPN).

По типу поддерживаемой модели построения VPN разделяют на оверлейные и одноранговые (peer-to-peer, P2P). Для оверлейной модели характерно то, что сервис-провайдер предоставляет корпоративному заказчику (компании, предприятию), для которого и строится VPN, частную сетевую магистраль (Private Network Backbone). Маршрутизаторы VPN-сети, в свою очередь, могут поддерживать виртуальные соединения «точка–точка» с помощью средств туннелирования трафика (GRE). При этом функции маршрутизации, как правило, возлагаются на клиентское оборудование (маршрутизаторы). Для организации оверлейных VPN обычно используют технологии X.25 Frame Relay, ATM (Layer 2 VPN), а также GRE и IPSec (Layer 3 VPN).

В отличие от оверлейных решений, обладающих хорошей наглядностью, но плохой масштабируемостью, при использовании архитектуры одноранговой сети функции маршрутизации возлагаются на сервис-провайдера, что несколько упрощает работу клиентского оборудования. Стандарт MPLS VPN иногда позиционируется как одноранговое решение [1, 4, 5], но все чаще [1] этот стандарт рассматривается как вариант, сочетающий преимущества оверлейных и одноранговых сетей. При этом PE-маршрутизатор со стороны провайдера (MPLS-домена), к которому подключаются устройства CE, выполняет функции маршрутизаторов LER (Label Edge Router, LER), P-маршрутизаторы функционируют как LSR-маршрутизаторы, а роль туннелей выполняют пути коммутации по меткам (Label Switched Path, LSP), которые рассчитываются на LER.

При создании VPN-сетей на основе MPLS-технологии нашли свое применение две основные модели реализации: модель изолированного канала (pipe-модель) и распределенная модель (hose-модель) [3]. При синтезе VPN-сети на основе использования модели изолированного канала провайдер обеспечивает заданные гарантии качества обслуживания для потоков пакетов, которые передаются между соответствующими парами CE-маршрутизаторов виртуальной частной сети. Условно данная модель может быть представлена как логический канал (pipe) между этими двумя маршрутизаторами. Для реализации pipe-модели необходимо знать характеристики передаваемых потоков и их QoS-требования для последующего планирования создаваемого канала (туннеля). Данная модель во многом аналогична архитектурной модели IntServ/IP. С ее помощью можно обеспечить гарантии качества обслуживания, в особенности, если это касается гарантий по пропускной способности маршрутов между двумя PE-маршрутизаторами.

В ходе использования распределенной модели обеспечения QoS в VPN-сетях со стороны провайдера для каждого CE-маршрутизатора определяются согласованная входная скорость (Ingress Committed Rate, ICR) и согласованная выходная скорость (Egress Committed Rate, ECR). Величина ICR задает скорость, с которой CE-маршрутизаторы создаваемой VPN-сети могут принимать пакеты от рассматриваемого CE-маршрутизатора. Параметр ECR используется для определения скорости, с которой другие CE-маршрутизаторы могут отправлять пакеты на заданный CE-маршрутизатор. Как правило, численные значения ICR и ECR могут разниться. Распределенная модель в целом реализует функционал архитектурной модели DiffServ на основе нескольких классов обслуживания.

III. Анализ требований, выдвигаемых к виртуальным частным сетям

Таким образом, в ходе классификации VPN-решений установлено, что эффективность работы виртуальных частных сетей во многом определяется качеством решения задач по их созданию и управлению. В этой связи к числу *основных требований*, которые выдвигаются к виртуальным частным сетям, следует отнести [1-4]:

- масштабируемость, под которой понимается возможность наращивания VPN-сети без существенных технологических и временных затрат по настройке и реконфигурации сети провайдера и клиента;

- безопасность, т.е. способность обеспечить надежную защиту передаваемых данных;

- гарантированная производительность, подразумевающая удовлетворение QoS-требований клиентских потоков по скорости, средней задержке, уровню потерь пакетов и джиттеру в соответствии с содержанием соглашения об уровне обслуживания (SLA);

- совместимость, т.е. создаваемая VPN должна быть совместима с сетевыми протоколами и технологиями, используемыми в клиентских С-сетях.

Поэтому, несмотря на наличие в настоящее время достаточно большого числа вариантов построения подобного рода сетей, с разной степенью эффективности нашедших свое применение на практике, наибольший интерес представляют подходы, связанные с созданием VPN средствами сетевого уровня, базирующиеся на технологиях IP/MPLS и комбинирующие преимущества оверлейных (наложенных) и одноранговых решений.

При этом в данной статье объектом исследования являются процессы обеспечения высокой (заданной) производительности создаваемых VPN-сетей, что может быть реализовано лишь на основе оптимизации во времени процесса управления (перераспределения) топологическим, канальным и буферным ресурсом сети сервис-провайдера (Р-сети) в интересах множества создаваемых на ее основе виртуальных частных сетей. К сожалению, ввиду непроработанности этих задач производительность VPN-сетей всегда оставляет желать лучшего, особенно в условиях высокой динамики числа и характеристик клиентских потоков и связанных с ними QoS-требований. Ввиду того, что современные ТКС по определению мультисервисные, при синтезе VPN-сетей необходимо предусмотреть комбинированную реализацию моделей изолированного канала и hose-модели.

Учитывая высокую динамику состояния IP/MPLS-сетей, на базе которых, как правило, и создаются VPN, математические модели, описывающие процессы создания и управления ресурсами виртуальных частных сетей, должны относиться к классу динамических. Поэтому предложенные в работах [6-9] математические модели, представленные разностными уравнениями состояния, будут в настоящей статье адаптированы под новые цели исследования, предметную область и терминологию.

IV. Структурное описание сети провайдера и виртуальных частных сетей в виде графа

Пусть структура сети провайдера (рис. 3) описывается с помощью графа (рис. 4)

$$G = (R, L),$$

где $R = \{R_i, i = \overline{1,m}\}$ – множество маршрутизаторов сети провайдера, $L = \{L_{i,j}, i, j = \overline{1,m}, i \neq j\}$ – множество трактов передачи между маршрутизаторами той же Р-сети.

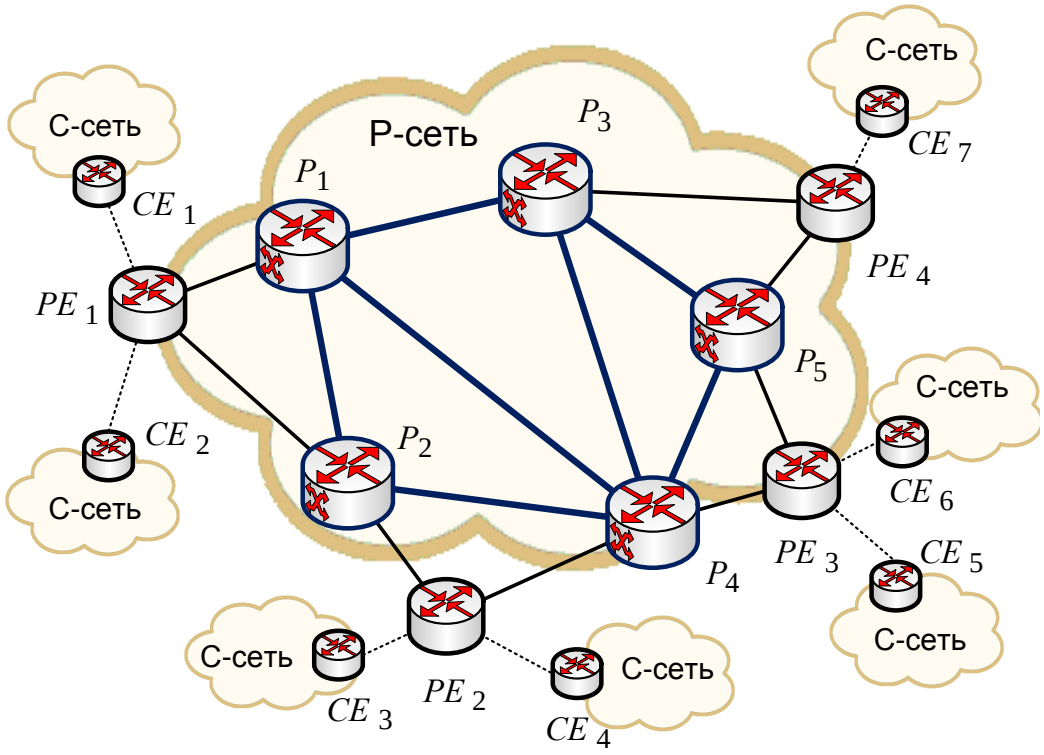


Рис. 3. Пример структуры сети провайдера (Р-сети) и расположения клиентских сайтов (С-сетей)

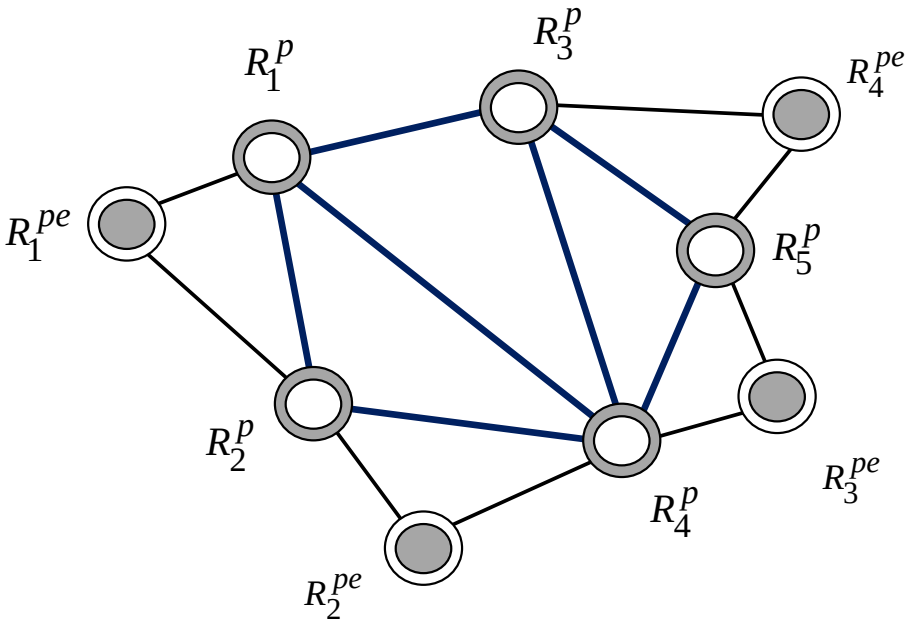


Рис. 4. Структурная модель ТКС провайдера, представленная графом $G = (R, L)$

Мощность множества $|R| = m$ определяет общее число маршрутизаторов в Р-сети, а $|L| = n$ – число трактов передачи в ней же. Все множество маршрутизаторов (устройств) сети провайдера в соответствии с принципами построения сети VPN-сетей можно разбить на два подмножества: $R^{pe} = \{R_i^{pe}, i = \overline{1, m_{pe}}\}$ – подмножество приграничных устройств (маршрутизаторов) сети сервис-провайдера (PE); $R^{p} = \{R_j^{p}, j = \overline{1, m_{p}}\}$ – подмножество устройств (маршрутизаторов) сети сервис-провайдера (P).

Тогда имеет место тождество

$$m = m_{pe} + m_p .$$

Каждой дуге $L_{i,j} \in L$ графа, моделирующей соответствующий тракт передачи в Р-сети, ставится в соответствие ее пропускная способность $c_{i,j}^{P}$.

Пусть общее число создаваемых VPN-сетей равно m_c, это же число определяет количество типов клиентских С-сетей, функционирующих в интересах одной и той же компании (предприятия). В связи с этим все множество поступающих в сеть провайдера потоков F можно декомпозицировать на подмножества

$$\{F_g, g = \overline{1, m_c}\},$$

где F_g – множество потоков, циркулирующих в g-й VPN.

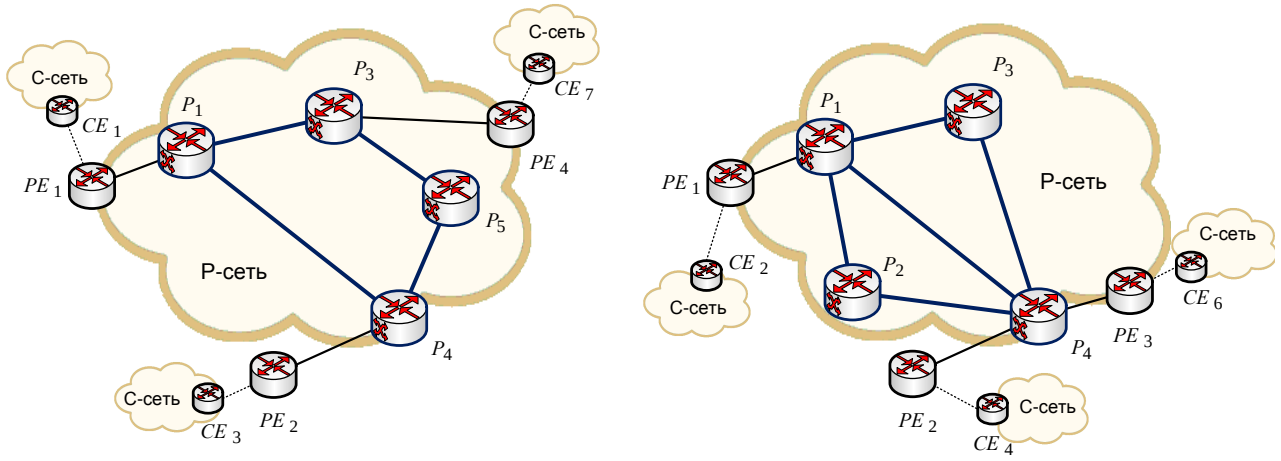
Каждому потоку из множества F_g сопоставляется ряд параметров: R_s^{pe} – s-й PE-маршрутизатор, на который поступает поток пакетов в Р-сеть (узел-источник); R_d^{pe} – d-й PE-маршрутизатор, через который поток пакетов убывает из Р-сети (узел-получатель); $r^{(l,g)}$ – интенсивность l-го потока, циркулирующего в g-й VPN.

В связи с этим произвольную g-ю VPN-сеть, которая наряду с другими создается на основе сети сервис-провайдера, можно представить в виде графа

$$G^{VPN_g} = (R^{VPN_g}, L^{VPN_g}),$$

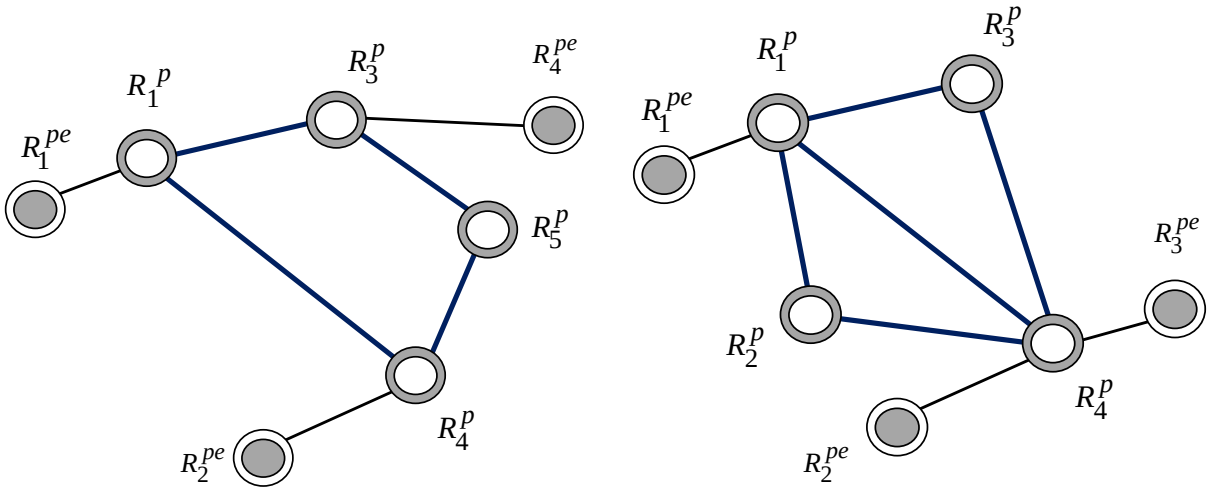
где $R^{VPN_g} \in R$ – подмножество маршрутизаторов Р-сети, которые используются в интересах g-й VPN-сети; $L^{VPN_g} \in L$ – множество трактов передачи Р-сети, часть пропускной способности которых может использоваться для обслуживания потоков g-й VPN-сети.

Например, на рис. 5 показаны варианты топологии создаваемых VPN-сетей, а на рис. 6 соответствующие этим решениям графы.



а) топология 1-й VPN б) топология 2-й VPN

Рис. 5. Варианты топологии создаваемых VPN-сетей



а) граф 1-й VPN б) граф 2-й VPN

Рис. 6. Графы, соответствующие VPN-сетям, представленным на рис. 5

V. Функциональное описание процесса синтеза одноранговых виртуальных частных сетей

При разработке математической модели структурно-функционального синтеза виртуальных частных сетей примем следующие обозначения: $\Delta t = t_{k+1}^{VPN} - t_k^{VPN}$ – время перерасчета управляющих переменных, связанных с созданием и функционированием VPN-сетей, t_k^{VPN} и t_{k+1}^{VPN} – моменты времени начала и окончания k-го временного интервала; K^{VPN} – число временных интервалов, на протяжении которых оптимизируется (моделируется) работа VPN-сетей; $c_{i,j}^g(k)$ – пропускная способность тракта передачи (который представлен дугой $L_{i,j} \in L$), выделенная для соответствующего канала $L_{i,j}^{VPN_g}$ g-й VPN на k-м временном интервале (*бит/с*); $u_{i,j}^g(k)$ – доля

пропускной способности $c_{i,j}^{P}$ тракта передачи, представленного дугой $L_{i,j} \in L$, которая берется со знаком «плюс», если выделяется для наращивания ПС $c_{i,j}^{g}(k)$ g-й VPN, или со знаком «минус» при ее перераспределении в интересах других виртуальных частных сетей на k-м временном интервале.

Тогда динамику состояния (топологии и изменения пропускных способностей трактов передачи) создаваемых одноранговых VPN-сетей при распределении ресурсов сети сервис-провайдера можно описать следующей системой линейных разностных уравнений:

$$c_{i,j}^{g}(k+1) = c_{i,j}^{g}(k) + u_{i,j}^{g}(k) c_{i,j}^{P}. \quad (1)$$

В уравнениях (1) величины $c_{i,j}^{g}(k)$ трактуются как переменные состояния процесса структурно-функционального синтеза VPN-сетей, а переменные $u_{i,j}^{g}(k)$ выступают в качестве управляющих, описывающих процесс перераспределения пропускной способности трактов передачи сети сервис-провайдера в интересах каналов создаваемых виртуальных частных сетей.

На переменные состояния, исходя из их физической трактовки, накладываются следующие условия-ограничения:

$$0 \le c_{i,j}^{g}(k), \qquad (g = \overline{1, m_c}), \quad (2)$$

$$\sum_{g=1}^{m_c} c_{i,j}^{g}(k) \le c_{i,j}^{P}. \quad (3)$$

Выполнение условия (3) гарантирует то, что в процессе распределения ресурсов сети сервис-провайдера пропускные способности трактов передачи P-сети не будут перегружены.

Согласно физическому смыслу переменных $u_{i,j}^{g}(k)$ в общем случае на них накладываются следующие ограничения:

$$-1 \le u_{i,j}^{g}(k) \le 1. \quad (4)$$

Дополнительной управляющей переменной, вводимой для формализации и решения задач маршрутизации в рамках VPN-сетей, служит величина $x_{i,j}^{(l,g)}$, которая характеризует долю l-го потока, протекающего в канале $L_{i,j}^{VPN_g}$ g-й VPN. В соответствии с физикой решаемой задачи на переменные $x_{i,j}^{(l,g)}$ накладываются следующие ограничения:

$$0 \le x_{i,j}^{(l,g)}(k) \le 1, \quad (5)$$

соблюдение которых ориентирует на реализацию многопутевой стратегии маршрутизации с балансировкой нагрузки, а в терминах MPLS-сети подобные решения согласовываются с концепцией Traffic Engineering [2, 3].

Для предотвращения перегрузки каналов создаваемых виртуальных сетей маршрутизируемыми по ним клиентскими потоками необходимо обеспечить выполнение условий:

$$\sum_{l} r^{(l,g)} x_{i,j}^{(l,g)}(k) \le c_{i,j}^{g}(k), \ (g = \overline{1, m_c}). \tag{6}$$

Для контроля за уровнем потерь пакетов на P-маршрутизаторах, вызванных переполнением очередей на их интерфейсах, необходимо принять к рассмотрению следующие условия сохранения потока [10, 11]:

$$\sum_{j:(i,j)} x_{i,j}^{(l,g)}(k) = 1; \tag{7}$$

$$\sum_{j:(i,j)} x_{i,j}^{(l,g)}(k) - \sum_{j:(j,i)} x_{j,i}^{(l,g)}(k)(1 - p_{j,i}^{(l,g)}(k)) = 0; \tag{8}$$

$$\sum_{j:(i,j)} x_{j,i}^{(l,g)}(k)(1 - p_{j,i}^{(l,g)}(k)) = \varepsilon^{(l,g)}(k), \tag{9}$$

где $p_{i,j}^{(l,g)}$ – вероятность потерь пакетов l-го потока на j-м интерфейсе i-го P-маршрутизатора g-й VPN по причине перегрузки очереди; $\varepsilon^{(l,g)}$ – доля интенсивности l-го потока пакетов, обслуженного g-й VPN.

Условия (7) должны быть справедливы для приграничного PE-маршрутизатора, к которому через CE-маршрутизатор подключена C-сеть-отправитель пакетов, условия (8) – для всех транзитных P-маршрутизаторов, а условия (9) – для приграничного PE-маршрутизатора, к которому через CE-маршрутизатор подключена C-сеть-получатель пакетов. В случае моделирования процесса обслуживания пакета системой массового обслуживания $M/M/1/N$, вероятность потерь пакетов на интерфейсе маршрутизатора (для удобства индексы опущены) может быть рассчитана как [12]

$$p = \frac{(1-\rho)(\rho)^N}{1-(\rho)^{N+1}}, \tag{10}$$

где ρ – коэффициент загруженности канала рассматриваемой VPN; $N = \Theta_{буф} + 1$ – максимальное число пакетов, которое может находиться на интерфейсе, включая буфер ($\Theta_{буф}$) и сам канал.

В ходе расчета маршрутных переменных $x_{i,j}^{(l,g)}$ необходимо, чтобы для l-го потока вероятность потерь пакетов была не больше допустимой ($p_{\text{доп}}^{(l,g)}$), что в рамках выражений (7)-(9) может быть сформулировано как

$$1 - \varepsilon^{(l,g)} \le p_{\text{доп}}^{(l,g)}. \tag{11}$$

Численные значения допустимой вероятности потерь пакетов для того или иного типа потока, для примера, указаны в рекомендации ITU-T Y.1541 [13]. Для каждой конкретной поддерживаемой услуги эти значения могут несколько отличаться.

При реализации распределенной модели обеспечения качества обслуживания в MPLS/VPN-сетях сумма всех интенсивностей $r^{(l,g)}$ потоков, исходящих от одного PE-маршрутизатора, не должна превышать установленное значение согласованной входной скорости ICR. А сумма всех произведений $r^{(l,g)}\varepsilon^{(l,g)}$ для потоков, которые поступают на данный PE-маршрутизатор, не должна превышать значения согласованной выходной скорости ECR.

Критерием оптимальности решений относительно синтеза одноранговых VPN-сетей предлагается использовать минимум следующего функционала

$$J = \sum_{k=1}^{K^{VPN}} \left[\sum_{g=1}^{m_c} \sum_{l} \sum_{L_{i,j} \in L} f_{i,j}^{(l,g)}(k) x_{i,j}^{(l,g)}(k) + \sum_{g=1}^{m_c} \sum_{L_{i,j} \in L} v_{i,j}^{g}(k) c_{i,j}^{g}(k) + \sum_{g=1}^{m_c} \sum_{L_{i,j} \in L} \gamma_{i,j}^{g}(k) u_{i,j}^{g}(k) \right], \qquad (12)$$

в котором $f_{i,j}^{(l,g)}(k)$ – маршрутная метрика канала, представленного дугой $L_{i,j}^{VPN_g}$, для l-го потока на k-м временном интервале; $v_{i,j}^{g}(k)$ – относительная стоимость использования единицы пропускной способности канала, представленного дугой $L_{i,j}^{VPN_g}$, на k-м временном интервале; $\gamma_{i,j}^{g}(k)$ – условная стоимость процесса перераспределения пропускной способности трактов передачи сети сервис-провайдера между каналами создаваемых VPN-сетей на k-м временном интервале.

Использование критерия (12) позволяет минимизировать условные суммарные затраты на синтез одноранговых VPN-сетей (второе и третье слагаемое) и на их функционирование с точки зрения маршрутизации по ним клиентских потоков (первое слагаемое) на некотором упреждающем временном интервале, который можно трактовать как интервал прогнозирования. Реализация свойства прогнозирования состояния при управлении VPN-сетями ($K_{VPN} > 1$) позволяет более гибко перераспределять ресурсы сети сервис-провайдера, на которые претендуют различные создаваемые виртуальные частные сети.

VI. Анализ предложенных решений по синтезу одноранговых виртуальных частных сетей

В ходе исследования влияния значения периода прогнозирования K_{VPN} на эффективность синтеза VPN-сетей в рамках предложенной модели (1)-(12) численно оценивался следующий показатель:

$$P_{в}^{VPN} = \frac{P_{VPN}(K_{VPN}) - P_{VPN}(1)}{P_{VPN}(1)} 100\%, \qquad (13)$$

который основан на использовании выражения

$$P_{VPN} = \sum_{k=1}^{K_M} \sum_{g=1}^{m_c} \sum_{l} r^{(l,g)}(k) \varepsilon^{(l,g)}(k) \qquad (14)$$

и характеризовал выраженный в процентном отношении выигрыш по производительности создаваемых VPN-сетей в зависимости от $K_{VPN} > 1$ по отношению к решению, не предполагающему прогнозирование состояния сети ($K_{VPN} = 1$).

Выражение (14), в свою очередь, использовалось для оценки эффективности решений, связанных с созданием VPN-сетей, и характеризовало максимальную производительность виртуальных частных сетей с учетом возможных потерь пакетов ввиду перегрузки очередей на маршрутизаторах ТКС, где $K_{м}$ – число временных интервалов $\Delta t = t_{k+1}^{VPN} - t_{k}^{VPN}$, на протяжении которых моделировалась работа VPN-сетей.

Отдельно стоит отметить, что эффективность динамического управления созданием VPN-сетей во многом зависит от качества прогнозирования (точности) параметров трафика (Δr), поступающего в сеть, а именно интенсивности потока r. Для численного расчета точности прогнозирования интенсивности потока будет использоваться выражение

$$\Delta r(k+s) = \left[1 - \frac{\left| r^{ист}(k+s) - r^{пр}(k+s) \right|}{r^{ист}(k+s)}\right] 100\%, \quad s = \overline{1, K-1}, \qquad (15)$$

где $r^{ист}(k+s)$ – истинное значение интенсивности потока на интервале времени $k+s$; $r^{пр}(k+s)$ – прогнозируемое значение интенсивности потока, которое будет на интервале времени $k+s$, при этом прогноз осуществляется в момент времени t_k.

В ходе исследований были выбраны следующие исходные данные:

- период прогнозирования (K_{VPN}) изменялся от 2 до 9;
- число маршрутизаторов в сети сервис-провайдера варьировалось от 20 до 30;
- связность (S) узлов VPN-сети изменялась от 2 до 5;
- точность прогнозирования характеристик потоков (15) дискретно изменялась от 50 до 100%.

Результаты сравнительного анализа по показателю $P_{в}^{VPN}$ (13) подтвердили преимущества управления с прогнозированием состояния сети, что проявилось в росте производительности созданной VPN-сети в среднем от 14-18 до 24-30%. Особенно проявлялся выигрыш по производительности с ростом связности сети и точности прогнозирования интенсивности абонентских потоков (15). Количественно результаты сравнения представлены в табл. 1, а также на рис. 7.

Как свидетельствуют результаты исследования (рис. 7), предпочтительным является ограничение периода прогнозирования значениями $K_{VPN} = 4 \div 5$, т.к. последующее его увеличение, приводя к пропорциональному росту размерности решаемой задачи, не сопровождалось существенным ростом результирующей производительности VPN-сети (до 2-3%).

Таблица 1. Результаты сравнительного анализа по показателю $P_в^{VPN}$ (13)

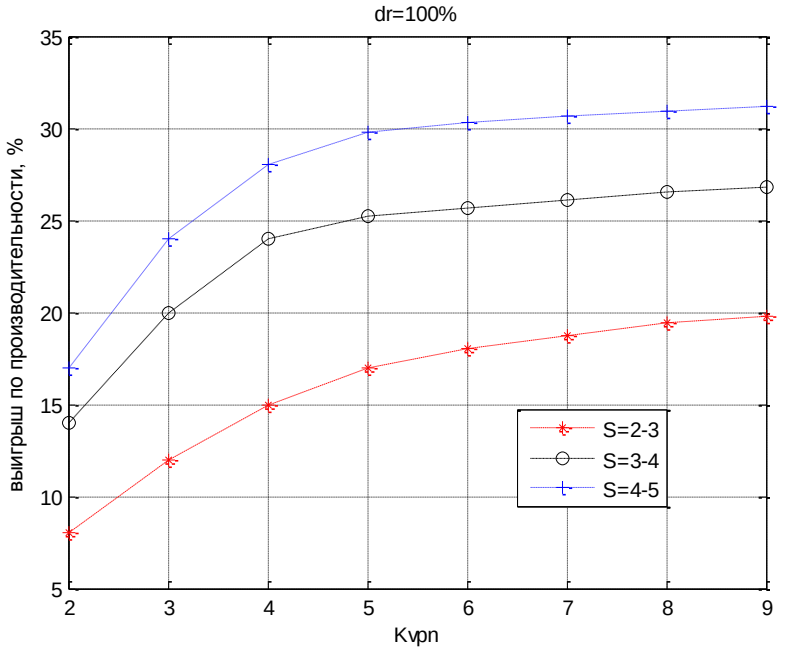
Точность (Δr)	100%			75%			50%		
Связность (S)	2÷3	3÷4	3÷5	2÷3	3÷4	3÷5	2÷3	3÷4	3÷5
$K_{VPN} = 2$	8	14	17	6	8	9	3	5,2	6
$K_{VPN} = 3$	12	20	24	10	13	14,5	5	8	9
$K_{VPN} = 4$	15	24	28	12	16,2	17,4	8	11,1	11,8
$K_{VPN} = 5$	17	25,2	29,8	13	17,2	18,8	9,1	11,4	12,3
$K_{VPN} = 6$	18	25,7	30,3	13,5	17,7	19,3	9,5	11,7	12,6
$K_{VPN} = 7$	18,7	26,1	30,7	13,9	18,1	19,7	9,9	12	12,9
$K_{VPN} = 8$	19,4	26,5	30,9	14,2	18,3	20	10,1	12,2	13,2
$K_{VPN} = 9$	19,8	26,8	31,2	14,3	18,5	20,1	10,2	12,3	13,3

Выводы

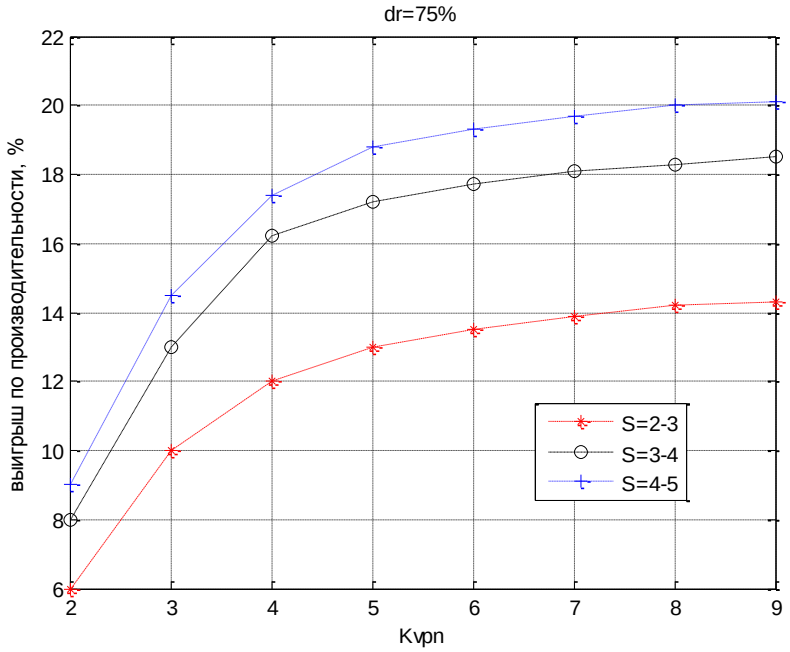
1. Проведен анализ принципов построения виртуальных частных сетей, приведена классификация VPN и сформулированы основные требования, которые предъявляются к подобного рода решениям с точки зрения их создания и обеспечения QoS. Установлено, что сдерживающим фактором в повышении производительности VPN-сетей и обеспечения в них качества обслуживания является неэффективное распределение между создаваемыми виртуальными частными сетями ресурсов (топологических, канальных и буферных) сети сервис-провайдера. Показано, что выход из сложившейся ситуации видится в переходе к динамическим моделям структурного и функционального синтеза VPN.

2. Предложена динамическая модель синтеза одноранговых частных сетей (1)-(12), новизна которой заключается в том, что она представлена как системой линейных разностных уравнений для описания процесса перераспределения пропускных способностей трактов передачи сети сервис провайдера между различными виртуальными частными сетями, так и нелинейными алгебраическими уравнениями для описания процессов маршрутизации потоков и управления перегрузкой. Использование модели позволяет обеспечить более эффективное управление ресурсами сети провайдера при создании одноранговых виртуальных частных сетей за счет более полного учета динамики процессов информационного обмена, протекающих в ней.

3. Предложенные решения адаптированы под различные модели обеспечения гарантированного и (или) дифференцированного качества обслуживания в создаваемых VPN-сетях как под модель изолированного канала (pipe-модель), так и под распределенную модель (hose-модель), которые поддерживаются в решениях, основанных на MPLS-технологии.



а) Δr=100%



б) Δr=75%

Рис. 7. Результаты сравнительного анализа по показателю (13)

4. В рамках модели задача синтеза одноранговой VPN-сети сформулирована как оптимизационная. В этой связи обоснован к применению критерий оптимальности (12), выполнение которого позволяет минимизировать суммарные затраты на структурный синтез VPN-сетей и на их функционирование с точки зрения маршрутизации по ним клиентских потоков с поддержкой качества обслуживания на некотором упреждающем временном интервале, который можно трактовать как интервал про-

гнозирования. Реализация свойства прогнозирования состояния при управлении VPN-сетями позволяет более гибко перераспределять ресурсы сети сервис-провайдера между создаваемыми виртуальными частными сетями. Как показали результаты исследований предпочтительным является ограничение периода прогнозирования значениями $K_{VPN} = 4 \div 5$, т.к. последующее его увеличение, приводя к пропорциональному росту размерности решаемой задачи, не сопровождалось существенным ростом результирующей производительности VPN-сети.

Список литературы:

1. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е издание. – СПб.: Питер, 2006. – 958 с.
2. *Гольдштейн А.Б., Гольдштейн Б.С.* Технология и протоколы MPLS. – М.: Эко-Трендз, 2005. – 304 с.
3. *Олвейн В.* Структура и реализация современной технологии MPLS: Пер. с англ. – М.: Издательский дом «Вильямс», 2004. – 480 с.
4. *Браун С.* Виртуальные частные сети. – Издательство «Лори», 2001. – 503 с.
5. *Álvarez S.* QoS for IP/MPLS networks. – Cisco Press, 2006. – 299 p.
6. *Лемешко А.В., Стерин В.Л.* Динамическая модель структурно-функционального синтеза транспортной ТКС [Электронный ресурс] // Проблеми телекомунікацій. – 2011. – № 3 (5). – С. 8 – 17. – Режим доступа к журн.: http://pt.journal.kh.ua/2011/3/1/113_lemeshko_synthesis.pdf.
7. *Лемешко А.В., Стерин В.Л.* Оптимизация структурного и функционального синтеза транспортной телекоммуникационной сети // Системи обробки інформації. – 2012. – Вип. 9 (107). – С. 186-190.
8. *Lemeshko O., Sterin V.* Design and structural-functional optimization transport telecommunication network // XIIth International Conference «The experience of designing and application of CAD systems in microelectronics», Polyana-Svalyava-(Zakarpattya), UKRAINE 19-23 February 2013: Publishing House of Lviv Polytechnic, 2013. – P. 208-210.
9. *Поповский В.В., Лемешко А.В., Евсеева О.Ю.* Математические модели телекоммуникационных систем. Часть 1. Математические модели функциональных свойств телекоммуникационных систем [Електронний ресурс] // Проблеми телекомунікацій. – 2011. – № 2 (4). – С. 3 – 41. – Режим доступу до журн.: http://pt.journal.kh.ua/2011/2/1/112_popovsky_functional.pdf.
10. *Лемешко А.В., Евсеева О.Ю., Гаркуша С.В.* Потоковая модель маршрутизации с учетом потерь пакетов на узлах телекоммуникационной сети // Радиотехнические и телекоммуникационные системы. – 2013. - № 2. – С. 52-60.
11. *Лемешко А.В., Евсеева О.Ю.* Тензорная модель многопутевой маршрутизации с гарантиями качества обслуживания одновременно по множеству разнородных показателей [Электронный ресурс] // Проблеми телекомунікацій. – 2012. – № 4 (9). – С. 16 - 31. – Режим доступа: http://pt.journal.kh.ua/2012/4/1/124_lemeshko_tensor.pdf.
12. *Агеев Д.В., Игнатенко А.А., Копылев А.Н.* Методика определения параметров потоков на разных участках мультисервисной телекоммуникационной сети с учетом эффекта самоподобия [Електронний ресурс] // Проблеми телекомунікацій. – 2011. – № 3 (5). – С. 18 – 37. – Режим доступу до журн.: http://pt.journal.kh.ua/2011/3/1/ 113_ageyev_method.pdf .
13. ITU-T Recommendation Y.1541 Network performance objectives for IP-based services.