Системы, сети и устройства телекоммуникаций

УДК 004.7

МЕТОДИКА БОРЬБЫ С ПЕРЕГРУЗКАМИ В КОРПОРАТИВНЫХ СЕТЯХ

Васин Николай Николаевич
доктор технических наук, профессор, заведующий кафедрой систем связи
ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики».
E-mail: vasin@psati.ru.

Иванова Елена Александровна
магистрант, инженер кафедры систем связи
ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики».

Мясоедов Вадим Александрович
бакалавр ФГБОУ ВО «Поволжский государственный
университет телекоммуникаций и информатики».
E-mail: maznik@spaces.ru.
Адрес: 443010, г. Самара, ул, Л.Толстого, д. 23.

Аннотация: Данная статья посвящена борьбе с перегрузками в сетях. Для изучения и исследования перегрузок в сетях был создан программно-аппаратный комплекс. Комплекс включает в себя оборудование лаборатории «Технологии пакетной коммутации» (6 коммутаторов, 6 маршрутизаторов), а также персональный компьютер с установленной программой Graphical Network Simulator (GNS3) и пятью сетевыми картами, что позволило смоделировать маршрутизатор. Предложен новый метод, суть которого заключается в перенаправлении простаивающих в очереди пакетов на резервные пути. Была разработана математическая модель данного метода. Метод предусматривает два способа перенаправления трафика. Первый способ - это справедливое распределение, т.е. поровну по всем существующим маршрутам. Второй способ - это распределение нагрузки до порогового значения очередного резервного маршрутизатора, т.е. основной маршрут нагружается по максимуму, а остатки трафика распределяются по резервным маршрутам. При проведении исследований был сформирован трафик, создавший перегрузку маршрутизатора, при этом часть трафика удалось перебросить на резервный путь, и тем самым предотвратить сброс пакетов. Для реализации данного метода будет использоваться маршрутизатор с открытым исходным кодом.

Ключевые слова: перегрузка, самоподобный трафик, OSPF, учебно-исследовательский комплекс, GNS3, маршрутизаторы, коммутаторы.

Введение

Буферизация пакетов на входных и выходных интерфейсах сетевых элементов (коммутаторов и маршрутизаторов) современных мультисервисных сетей позволяет в некоторой мере снизить влияние пульсации нагрузки на пропускную способность сети и обеспечить требуемое качество обслуживания (QoS) передаваемого трафика [1]. Пульсирующий самоподобный (фрактальный) трафик, характерный для корпоративных сетей, приводит к перегрузке буферных устройств, вследствие чего вариация задержек пакетов может превысить допустимые значения, а пакеты с низким приоритетом теряются [2]. Для обеспечения требуемой надёжности потерянные пакеты передаются повторно, в результате чего очереди на обслуживание сетевыми элементами ещё больше возрастают, а QoS снижается [3].

Механизмы управления очередями обработки пакетов обеспечивают снижение влияния перегрузки, но в полной мере решить эту проблему не могут [4]. Поэтому сети работают

в недогруженном режиме, что экономически не выгодно.

Однако в телекоммуникационной сети с коммутацией пакетов обычно существуют альтернативные пути к адресату назначения. Поэтому при перегрузке маршрутизатора часть трафика можно перенаправить по резервным маршрутам, где сетевые элементы в данный момент не догружены. При этом перераспределение (балансировка) нагрузки должно производиться в режиме реального времени.

Программно-аппаратный исследовательский комплекс

Для изучения и отработки методов борьбы с перегрузками на кафедре систем связи ПГУТИ на базе оборудования лаборатории «Технологии пакетной коммутации» был создан программно-аппаратный комплекс по изучению и исследованию возможностей технологий пакетной коммутации [5, 6].

Оборудование лаборатории «Технологии пакетной коммутации» включает 6 маршрутизаторов 2800 фирмы Cisco, 6 коммутаторов 2960 фирмы Catalyst, размещённых в двух телекоммуникационных шкафах (рис. 1).

Кроме того, в комплекс входит персональный компьютер с установленной программой Graphical Network Simulator (GNS3) [7] и пятью сетевыми картами, что позволяет моделировать маршрутизатор в разветвлённой сети.

Дополнительно оборудование включает 12 компьютеров, 6 из которых используются для подключения к консольным портам с целью конфигурирования маршрутизаторов, а 6 – подключены к коммутаторам для создания сети.

Таким образом, созданный программно-аппаратный комплекс является симбиозом реальной сети лаборатории «Технологии пакетной коммутации» с виртуальной сетью, построенной на базе GNS3. Пакет GNS3 обеспечивает максимальную гибкость при реализации проектов за счёт сочетания моделей аппаратных устройств, которые работают на основе реального программного обеспечения.

GNS3 представляет собой кроссплатформенный графический сетевой симулятор, который может работать с операционными системами Windows, OS X, и Linux.

В отличие от аналогичных приложений, GNS3 не просто имитирует программные обеспечения, команды или функции, а запускает на компьютере фактически файл образа программного обеспечения сетевого элемента. Таким образом, доступны любые функции и протоколы, которые поддерживает данная версия программного обеспечения. Интеграция с программными продуктами VirtualBox или VMWare расширяет возможность подключения к различным сетевым устройствам. Наличие программного продукта Wireshark позволяет проводить мониторинг трафика внутри проектируемой топологии. При работе с большими сложными сетями, можно запускать сер-

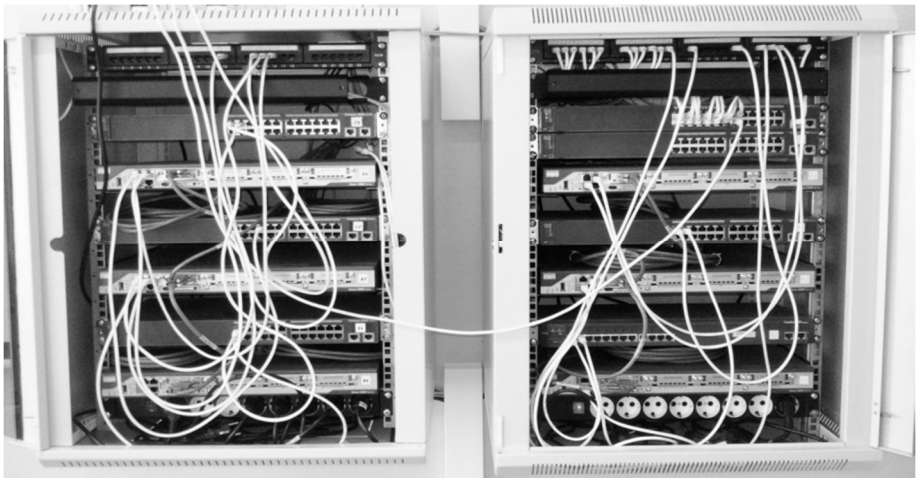

Рис. 1. Оборудование лаборатории «Технологии пакетной коммутации»

вер GNS3 [8].

Используя облако, возможно установить соединение с реальным оборудованием по внешним линиям, а также осуществить настройку подключения к Интернету для GNS3 устройств. Это преимущество дает GNS3 широкие сетевые возможности.

Борьба с перегрузками

На разработанном программно-аппаратном комплексе было проведено исследование методики борьбы с перегрузками сетевых элементов. Методика основана на перенаправлении простаивающих в очереди пакетов на резервные пути. Она позволяет уменьшить очереди и исключить сброс пакетов.

Маршрутизаторы с открытым исходным кодом свободно доступны для скачивания, компиляции и исполнения, а также позволяют модифицировать программу в соответствии с желаниями и потребностями. Набор функций таких маршрутизаторов сопоставим по объёму со стандартами, принятыми у известных производителей [9 - 11]. Поэтому для реализации данной методики использовался маршрутизатор с открытым исходным кодом, реализованный на персональном компьютере.

Алгоритм работы в соответствии с предложенной методикой борьбы с перегрузками представлен на рис 2.

Проверка методики производилась с использованием как математической, так и физической моделей сети.

Математическая модель была реализована в среде MathCAD. Для оптимизации процесса маршрутизации в условиях высокой нагрузки и вероятности перегрузки канала вводится параметр допустимой предельной нагрузки Ns_t, при превышении которого срабатывает механизм защиты от перегрузки.

$$Ns_t := 0{,}95. \qquad (1)$$

Данный параметр лежит в пределах от 0,8 до 1 отношения скорости передачи к пропускной способности, что обеспечивает отсутствие переполнения буфера: в примере расчёта было выбрано значение предельной перегрузки 0,95.

Текущая нагрузка Nd_t представлена четырьмя значениями: 0,75; 1,2; 1,5 и 0,8 на интервале времени 0 – 1200 сек, т.е. это модель динамического трафика, включающая 4 режима работы: небольшая нагрузка (значения 0,75 и 0,8) и перегрузка (значения 1,2 и 1,5):

$$Nd_t := \begin{cases} 0{,}75\ if\ (t > 0 \wedge t\ 300); \\ 1{,}2\ if\ (t > 300 \wedge t\ 600); \\ 1{,}5\ if\ (t > 600 \wedge t\ 900); \\ 0{,}8\ if\ (t > 900 \wedge t\ 1200). \end{cases} \qquad (2)$$

Параметр перегрузки Kd_t определяется как отношение текущей нагрузки Nd_t (2) на параметр допустимой предельной нагрузки Ns_t канала связи:

$$Kd_t := ceil\left(\frac{Nd_t}{Ns_t}\right), \qquad (3)$$

где $ceil$ – операция округления результата в большую сторону.

В режиме динамической нагрузки при Kd_t больше единицы, включается режим перераспределения нагрузки. При этом поток разбивается на части (в каждую единицу времени поток трафика разбивается на N частей с округлением в большую сторону). Далее с помощью счётчика hello пакетов от разных источников определяется количество маршрутизаторов, примыкающих к анализируемому маршрутизатору.

Затем трафик распределяется в соответствии с одним из двух вариантов: справедливое распределение и распределение нагрузки до порогового значения очередного резервного маршрутизатора [12, 13].

1. Справедливое распределение – производится равномерно по всем доступным маршрутам:

$$Ed_{t,x} := \begin{cases} if\ Kd_t = 1; \\ \begin{cases} Td_t\ if\ x = M; \\ 0\ otherwise; \end{cases} \\ ceil\left[\frac{Td_t - \sum_{i=0}^{x-1} Ed_{t,i}}{(KOL - x + 1)}\right]\ if\ Kd_t > 1, \end{cases} \qquad (4)$$

где $Td_t = Nd_t \cdot 10^8$ – поток трафика (нагрузка), значение в байтах, KOL – количество маршру-

тов примыкающих к маршрутизатору, $Ed_{t,x}$ - распределение по пути, где x - номер пути.

При параметре перегрузки Kd равном единице, трафик будет направляться по магистральному пути $x = M$, где x – порядковый номер маршрута, M – магистральный маршрут (маршрут с наименьшей метрикой). Это соответствует блоку 7 блок-схемы алгоритма (рис. 2). При возникновении перегрузок, Kd больше единицы, производится перераспределение согласно алгоритму справедливого распределения по маршрутам. Это соответствует блоку 11 блок-схемы алгоритма. Распределения трафика представлены на рис 3, где BS - порог пропускания кабеля, $Ns_t * BS$ - пороговое значение перегрузки. На рис 2. показано:

а) Распределение по первому пути;

б) Распределение по второму пути;

в) Распределение по третьему (магистральному) пути.

Из графиков, представленных на рис. 3 видно, что трафик равномерно распределяется по всем маршрутам.

2. Распределение до порогового значения одного из маршрутов. При этом определяются «основные» и «запасные» пути, заполнение которых происходит до порога «предельной нагрузки»:

$$Ed2_{t,x} := \begin{cases} if\ Kd_t = 1; \\ \begin{cases} Td_t\ if\ x = M; \\ 0\ otherwise; \end{cases} \\ if\ Kd_t > 1; \\ BS * Ns_t\ if\ x = M; \\ ceil\left(\dfrac{Td_t - BS * Ns_t}{(KOL - 1)}\right)\ if\ x \neq M. \end{cases} \quad (5)$$

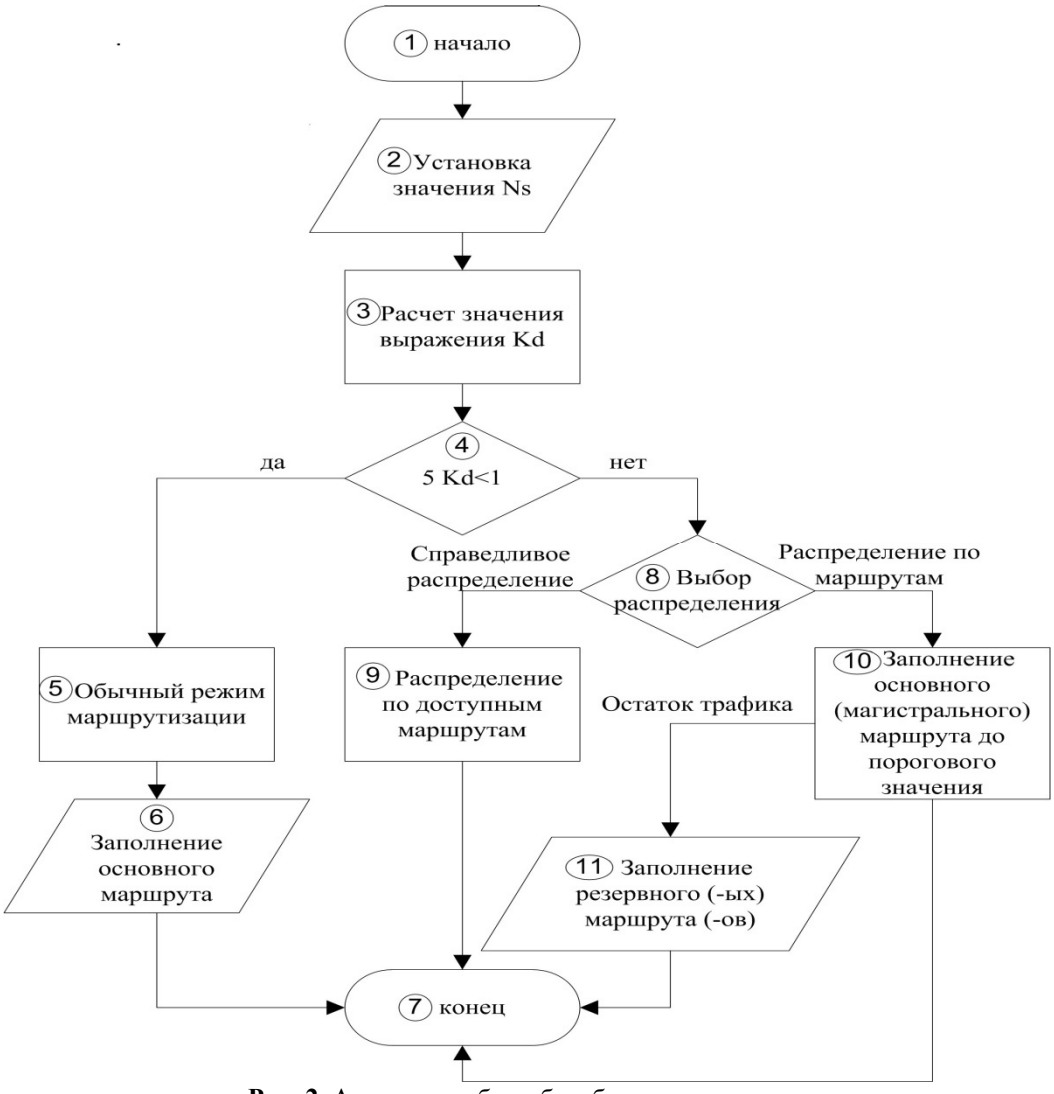

Рис. 2. Алгоритм работы борьбы с перегрузками

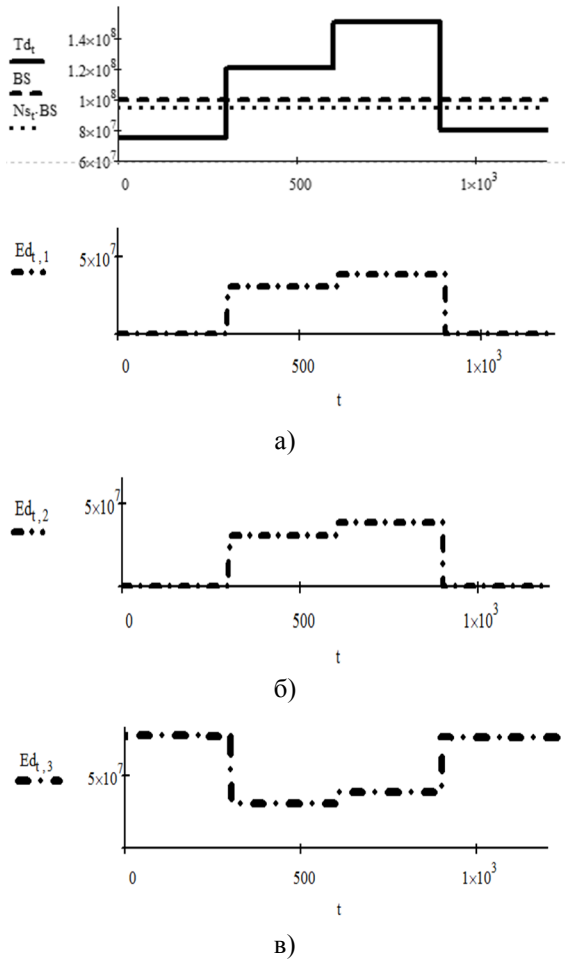

Рис. 3. Справедливое распределение по трем маршрутам

При параметре перегрузки Kd равном единице, трафик будет направляться по магистральному пути $x = M$, где x – порядковый номер маршрута, M – магистральный маршрут (маршрут с наименьшей метрикой). Это соответствует блоку 7 блок-схемы алгоритма (рис. 2). Если параметр перегрузки Kd больше единицы, то трафик перераспределяется на основной маршрут до полного его заполнения, где $BS \cdot Ns_t$ – пороговое значение перегрузки. Это соответствует блоку 12 блок-схемы алгоритма. Оставшаяся часть трафика перераспределяется на резервные маршруты, что соответствует блоку 13 блок-схемы алгоритма. Распределения трафика представлены на рис. 4, на котором изображены:

а) распределение по первому пути;

б) распределение по второму пути;

в) распределение по третьему (магистральному) пути.

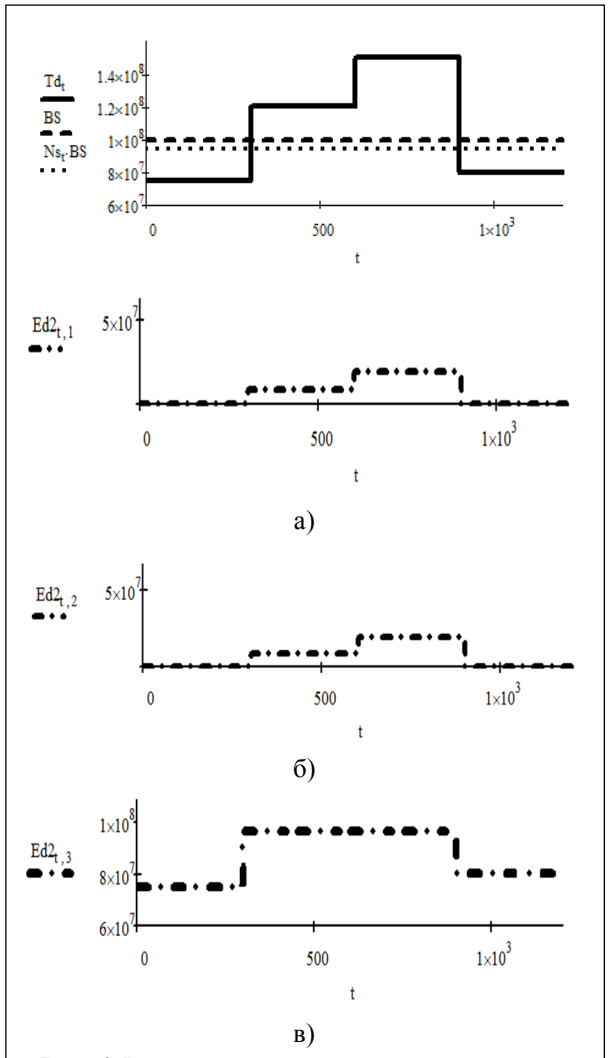

Рис. 4. Распределение нагрузки до порогового значения очередного резервного маршрутизатора

По графикам видно, что большая часть трафика перенаправляется на основной путь (рис. 4в), а оставшаяся часть распределяется по всем резервным маршрутам.

Анализируя графики, полученные в ходе исследований, можно сделать вывод о том, что оба метода повышают эффективность работы сети [14]. Причём, в первом случае трафик разбивается на равные части и передаётся по всем доступным маршрутам, тогда как во втором случае нагружается магистральный маршрут, а остатки трафика в равных частях передаются по резервным путям. Оба метода

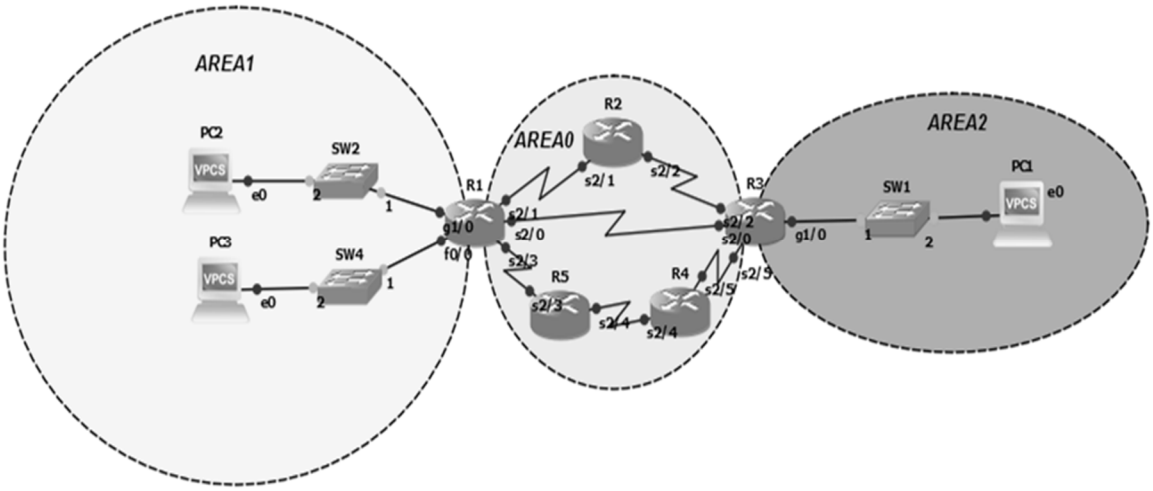

Рис. 5. Схема физической модели сети

предотвращают сброс пакетов при перегрузках.

Физическое моделирование

Для проверки математической модели методики борьбы с перегрузками сетевых элементов была создана физическая модель сети, схема которой приведена на рис 5.

При исследовании физической модели анализировался самоподобный трафик [15], генераторами трафика выступали PC1 и PC2.

Передача трафика осуществлялась с использованием программного продукта utorent, в котором задействован специальный протокол, предназначенный для обмена файлами между пользователями [16]. В качестве трафика передавался медиаконтент [17]. Мониторинг сети проводился с помощью программного продукта WireShark. В качестве маршрутизатора R1, на котором моделировалась борьба с перегрузками, использовался персональный компьютер с пятью сетевыми платами, что обеспечивало пути для достижения пункта назначения.

Была исследована двухсторонняя передача данных между компьютерами PC1 и PC2.

На персональном компьютере PC1 в программе GNS3 создается требуемая топология виртуальной проектируемой сети [18]. Затем на PC1 настраивается подключение к реальному маршрутизатору R3. Таким образом, обеспечивается доступ виртуальной проектируемой сети к реальному оборудованию лаборатории «Технологии пакетной коммутации». Далее запускается процесс передачи данных между PC1 и PC2. В процессе эксперимента были получены графики рис. 6 - 7.

На рис. 6 показан трафик сети, полученный в программном продукте utorent. На графике видно, что в момент перегрузки (падения) сети на участке 2 включился режим перераспределения, что привело к увеличению пропускной способности сети, которая возросла практически вдвое на участке 3. Работоспособность се-

Рис. 6. Перегрузка сети

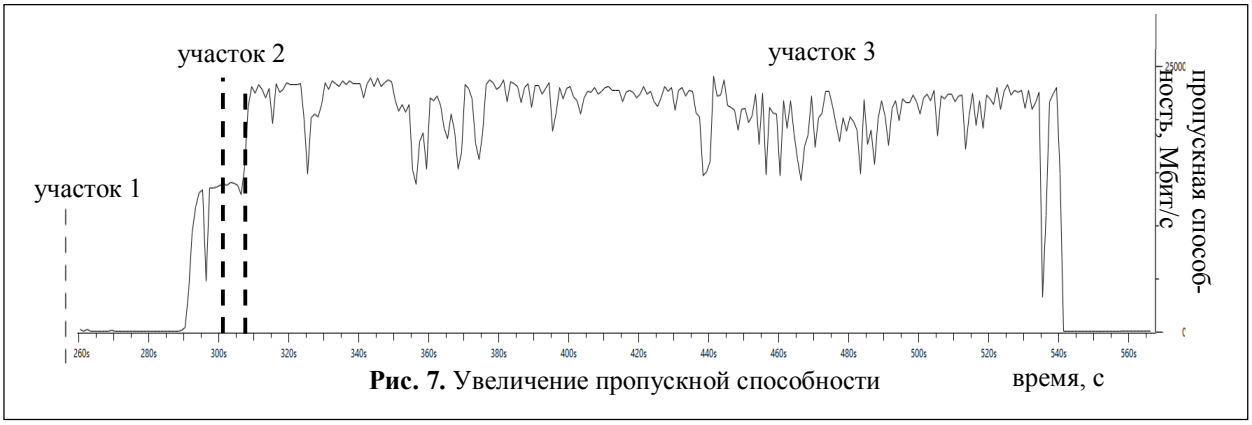

Рис. 7. Увеличение пропускной способности

ти была восстановлена.

На втором графике (рис. 7), полученном при анализе распечаток из программного продукта WireShark, на участке 1 пропускная способность составляла 10 Мбит/с. Затем в условиях созданной перегрузки на участке 2 часть трафика была перенаправлена на второй путь. При этом наблюдается рост трафика. На участке 3 пропускная способность выросла в два раза до 20 Мбит/с, что говорит о том, что для передачи трафика задействовано два маршрута.

Таким образом, оба программных продукта (utorent и WireShark) дают практически одинаковые результаты, подтверждающие достоверность проведённых исследований.

Вывод

Предложенная методика борьбы с перегрузками позволяет эффективно использовать пропускную способность сети и не допускать сброс пакетов.

Литература

1. Фомин В. В. Исследование и разработка методов анализа качества обслуживания сетевого трафика при использовании протокола управления очередями. Дис. канд. техн. наук. - Самара, 2010. 146 с.

2. Шелухин О.И., Осин А.В., Смольский С.М. Самоподобие и фракталы. - М.: ФИЗМАТЛИТ, 2008. - 368 с.

3. Задорожный В. Н., Кутузов О. И. Методы моделирования очередей в условиях фрактального трафика в сетях с коммутацией пакетов. - Омск: ОмГТУ, 2013. - 104 с.

4. Тимошина М.М. Разработка и исследование метода повышения скорости передачи данных в мультисервисных сетях на основе протоколов TCP/IP. Дис. канд. техн. наук. - Самара, 2013. 133 с.

5. Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство. - М.: Издательский дом «Вильямс», 2005. - 1168 с.

6. Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство. - М.: Издательский дом «Вильямс», 2006. - 1000 с.

7. Документация по GNS3 [Электронный ресурс]: сайт фирмы GNS3 Technologies Inc., 2016. URL: https://www.gns3.com/support/docs/quick-start-guide-for-windows-us.

8. Jason C. Neumann. The Book of GNS3. - No Starch Press, Inc., 2015, - 272 s.

9. Руководство по маршрутизаторам с открытым исходным кодом [Электронный ресурс]. URL: http://www.coo.ru/rukovodstvo-po-marshrutizatoram-s-otkrytym/.

10. VyOS [Электронный ресурс]. URL: https://vyos.io/.

11. Маршрутизатор XORP Inc. [Электронный ресурс]: сайт фирмы XORP URL: http://www.xorp.org/.

12. Справедливое разделение канала [Электронный ресурс]. URL: https://habrahabr.ru/post/133244/.

13. Справедливое деление трафика [Электронный ресурс]. URL: http://liferama.blogspot.ru /2013/11/ pcq-mikrotik.html.

14. Лихтциндер Б.Я. Интервальный метод анализа трафика мультисервисных сетей доступа. - Самара: ИУНЛ ПГУТИ, 2015. - 121 с.

15. Карташевский В.Г. Основы теории массового обслуживания. – М.: Горячая линия - Телеком, 2013. – 130 с.

16. µTorrent [Электронный ресурс]: сайт фирмы BitTorrent, Inc., 2016. URL: http://www.utorrent.com/intl/ru/.

17. Буранова М. А. Исследование влияния статистических свойств мультимедийного IP-трафика на характеристики качества обслуживания. Дис. канд. техн. наук. - Самара, 2013. 137 с.

18. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. - СПб.: Питер, 2014. - 944 с.

Поступила 28 сентября 2016 г.

English

Protection techniques against overload in corporate networks

Nikolay Nikolaevich Vasin – Doctor of Engineering, Professor Head of Communication Systems Department Povolzhskiy State University of Telecommunications and Informatics. *E-mail*: vasin@psati.ru.

Elena Aleksandrovna Ivanova – Master student, engineer of Communications Systems Department Povolzhskiy State University of Telecommunications and Informatics.

Vadim Aleksandrovich Myasoyedov – Bachelor Povolzhskiy State University of Telecommunications and Informatics. *E-mail*: e.ivanova@psuti.ru. *Address:* 34, 443010, Samara, L. Tolstoy, 23.

Abstract: Self-similar (fractal) bursty traffic is specific for corporate networks that often causes an overload of buffer devices. Therefore, packet delay variation can exceed admissible values and low priority packets are lost. All this leads to queues and reducing QoS as the lost packets are transferred repeatedly for the purpose to ensure required reliability. Control mechanisms of packet processing queues do not fully ensure overload reduction effect. That is why networks operate in the underloaded mode and that it is not cost-efficient economically. However, there are usually alternate paths to the network destinations in the telecommunication packet switched network. Therefore, when the router is overloaded then the traffic partly can be redirected via the redundant paths where the network elements are underloaded for the time being. Thus, the load reallocation (balancing) has to be performed in real time. Hardware and software system was designed for research of overloads in networks. This system includes the equipment of Technologies of Package Switching laboratory (6 switches, 6 Cisco routers), and also the personal computer with five network interface cards that enabled to simulate a router. The new method was suggested which implies the redirection of the queued packets into redundant paths. The mathematical model of this method was developed. The method provides two ways of the traffic redirection. The first way consists in equitable distribution, i.e. equally along all existing paths. The second way implies the load distribution to threshold value of the next redundant router, i.e. the main path is loaded to the maximum, and the remaining traffic is reallocated along the redundant paths. When carrying out research the traffic was formed to make the router's overload and partly the traffic was transferred into the redundant path and thus to prevent packets discard. To implement this method the router with the open initial will be used. The suggested methods of protection against overloads will enable to prevent packet discards as well as to use effectively network transmission capacity.

Key words: overload, self-similar traffic, OSPF, educational and research complex, GNS3, routers, switches.

References

1. Fomin V. V. Research and development of analysis methods of network traffic service quality using queue control protocol. Thesis, Cand. Of Tech. Sci. - Samara, 2010. 146 p.

2. Shelukhin O. I., Osin A. V., Smolskiy S. M. Self-similarity and fractals. - M.: FIZMATLIT, 2008. - 368 p.

3. Zadorozhny V. N., Kutuzov O. I. Queue implementation methods within fractal traffic in the packet switched networks. - Omsk: OmSTTU, 2013.- 104 p.

4. Timoshina M. M. Development and research of data transmission speed method in TCP/IP protocol multiservice networks. Thesis, Cand. Of Tech.Sci. - Samara, 2013. 133 p.

5. CCNA 1-2 program of Cisco network academy. Reference manual. M.: Williams publishing house, 2005. - 1168 p.

6. CCNA 3-4 program of Cisco network academy. Reference manual. M.: Williams publishing house, 2006. – 1000 p.

7. GNS3 documentation [electronic resource]: GNS3 Technologies Inc website., 2016. URL: https://www .gns3.com/support/docs/quick-start-guide-for-windows-us

8. Jason C. Neumann. The Book of GNS3. - No Starch Press, Inc., 2015, - 272 p.

9. Guide to routers with open source code [Electronic resource]. URL: http://www.coo.ru/rukovodstvo-po-marshrutizatoram-s-otkrytym/. 10. VyOS [electronic resource]. URL: https://vyos.io/.

11. XORP Inc router. [Electronic resource]: XORP Co. website o URL: <http://www.xorp.org/>.

12. Fair channel division [electronic resource]. URL: https://habrahabr.ru/post/133244.

13. Fair traffic division [electronic resource]. URL: <http://liferama.blogspot.ru/2013/11/> pcq-mikrotik.html

14. Likhttsinder B. Ya. Interval method of the traffic analysis in multiservice access networks. - Samara: PHARL PSUTI, 2015. - 121 p.

15. Kartashevsky V. G. Queuing theory fundamentals. M.: Goryachaya liniya - Telecom, 2013. - 130 p.

16. µTorrent [Electronic resource]: BitTorrent, Inc website 2016. URL: http://www.utorrent.com/intl/ru/

17. Buranova M. A. Research of statistical properties effect of multimedia IP traffic on service quality features. Thesis, Cand. Of Tech.Sci. - Samara, 2013. 137 p.

18. Olifer V.G., Olifer N. A. Computer networks. Principles, technologies, protocols. - SPb.: St. Piter, 2014. - 944 p.