13. Amosov A. A., Kolpakov V. V. Skaljarno-matrichnoe differencirovanie i ego prilozhenie k konstruktivnym zadacham teorii svjazi [Scalar-matrix differentiation and its application ti conatraction communication theory tasks]. *Problemy peredachi informacii*, 1972. vol. VIII, no. 1, pp. 3-15.
14. Cioffi John M., eds. *Advanced Digital Communications. Classic EE379 Series Courses*. Department of Electrical Engineering, Stanford University. Available at: http://www.stanford.edu/group/cioffi/book/chap4.pdf). (accessed 02.10.2013).
15. Gantmaher F. R. *Teorija matric* [Matrix theory]. Moscow, Nauka Publ., 1966. 576 p.

Received 03.09.2015

ТЕХНОЛОГИИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ

УДК 004.7

СНИЖЕНИЕ РИСКА ПЕРЕГРУЗКИ ВНЕШНЕГО КАНАЛА УПРАВЛЕНИЕМ ТРАФИКОМ КОМПЬЮТЕРНОЙ СЕТИ

Колесников И.В.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: 79277127248@ya.ru

В статье рассматривается решение проблемы перегрузки телекоммуникационной сети на примере предприятия путем анализа и последующего управления потоком трафика при использовании оборудования с операционной системой OpenWRT, выявление непрофильного трафика, снижение приоритета непрофильного трафика, расширение пропускной способности телекоммуникационного канала для профильного трафика. Алгоритм реализован для протоколов: P2P, VoIP, HTTP.

Ключевые слова: сетевые технологии, управление трафиком, анализ трафика, P2P, VoIP, HTTP.

Введение

Приложения, использующие для работы внешний канал связи стремительно, развиваются и выходят на новый уровень качества и обслуживания. Все шире развиваются сетевые Desktop приложения, IP-телефония, клиент-серверные приложения. Эти приложения использую разные сетевые протоколы (иногда собственные), а также отличаются многими параметрами: размер пакетов и т.д. В связи с этим нередко возникает ситуация, когда через одну компьютерную сеть передается трафик разных типов.

Актуальность исследования повышается при ограниченной пропускной способности внешнего канала связи предприятия. В данном случае проблема распределения трафика стоит особенно остро. У системных администраторов возникает необходимость разработки алгоритмов и методов управления трафиком.

Периодические случаи перегрузки компьютерной сети предприятия могут вызвать нарушение её функционирования как на отдельных рабочих станциях, так и во всей сети. Причинами чрезмерной нагрузки на внешние и внутренние каналы телекоммуникационной сети могут являться:

- вредоносное ПО;
- сетевые приложения, создающие непредумышленные dos-атаки;
- пульсирующий трафик.

Чаще всего диагностировать и устранить причину перегрузки сети очень трудно в связи с неизвестностью особенностей протокола передаваемого трафика, например P2P (Peerto Peer). Сегодня существуют десятки компьютерных приложений, способных вызвать перегрузку телекоммуникационной сети, большая их часть работает по протоколу P2P. Доля P2P трафика в компьютерных сетях составляет до 70% [2]. В связи с особенностями этого трафика приложения, использующие данный протокол, вызывают периодическую перегрузку внешнего канала связи.

Такие перегрузки приводят к временному отказу сетевых служб и замедлению работы как на отдельных компьютерах, так и во всей подсети. Примеры: временный отказ локальных DNS, задержки при обращении к корневым DNS.В описанных случаях под угрозой нестабильности находятся все службы прикладного уровня. Решение этой проблемы позволит увеличить надежность и отказоустойчивость сети предприятия [1].

Проблема достаточно серьезная в связи с тем, что сеть Internet повсеместно применяется на всех предприятиях. Нарушение функционирова-

ния телекоммуникационной сети может привести к серьезным последствиям, в связи с этим можно сформировать список мер для защиты сети предприятия:

- ограничение непрофильного трафика;
- распределение пропускной способности внешнего канала согласно требованиям профильных приложений, создающих трафик.

В связи с этим поставлены задачи исследования:

- выявление трафика, в том числе: P2P, VOIP, HTTP;
- ограничение пропускной способности на внешнем канале связи для каждого типа трафика;
- определить возможность создания универсального программного компонента для внешних каналов связи практически с любой пропускной способностью от 512Кбит/сек до 102400 Кбит/с;
- определение рабочей станции, являющейся потребителем непрофильного трафика.

Решение поставленных задач не только защитит сеть предприятия от перегрузки, но и позволит системному администратору определить конкретную рабочую станцию, получающую непрофильный трафик.

Алгоритм поиска трафика в компьютерной сети по протоколу.

1. Анализ пакета.

1.1. Анализ по номерам портов и известным сигнатурам пакетов.

1.2. Анализ на основе содержимого полезной нагрузки пакета.

2. Анализ методом определения особенностей поведения сетевых приложений.

3. Оценка принадлежности трафика к тому или иному семейству протоколов.

4. Завершение анализа.

Поставленные задачи реализуются на маршрутизаторах под управлением операционной системы OpenWRT.

OpenWRT – это чрезвычайно гибкий дистрибутив GNU/Linux для встраиваемых систем. В отличие от многих других дистрибутивов для роутеров, OpenWRT была создана с нуля и на данный момент является полностью функциональной, легко изменяемой операционной системой для роутера. На практике это означает, что можно создать систему для решения конкретных задач без ненужных приложений, при этом используя новейшее ядро Linux, которое еще не успело появиться в большинстве других дистрибутивов [3]. Для решения поставленных задач и проведения исследования будет применена утилита IPTables – утилита командной строки, является стандартным интерфейсом управления работой межсетевого экрана (брандмауэра) netfilter для ядер Linux [4].

```
$IPTABLES -t mangle -A PREROUTING -j
CONNMARK --restore-mark
$IPTABLES -t mangle -A PREROUTING -m
ipp2p --kazaa --bit -j MARK --set-mark 95
$IPTABLES -t mangle -A PREROUTING -m
mark --mark 95 -j CONNMARK --save-mark
$iptables -t mangle -A POSTROUTING -m
ndpi --bittorrent -j CLASSIFY --set-class 1:10
$iptables -t mangle -A POSTROUTING -m
ndpi --edonkey -j CLASSIFY --set-class 1:10
```

Рис. 1. Фрагмент реализации алгоритма определения трафика

Был разработан программный компонент для межсетевого экрана OpenWRT. На рис. 1 приведен фрагмент реализации алгоритма на основе известных сигнатур передаваемых пакетов.

Практическое применение полученных результатов

Эксперимент проводился на оборудовании диспетчерской компании. Перечень аппаратного обеспечения при проведении эксперимента:

- роутер TP-LinkTL-842ND с операционной системой «OpenWRTBarrierBreakerr39096»;
- 4 компьютера – подключение к внешнему каналу связи по стандарту Ethernet;
- 2 ноутбука. Подключение к внешнему каналу связи по беспроводной сети Wi-Fi;
- 1 IP телефон;
- внешний канал связи – заявленная максимальная пропускная способность 6144 Кбит/с.

Основным инструментом для проведения эксперимента является маршрутизатор под управлением ОС OpenWRT. По умолчанию на оборудовании TP-LinkTL-842ND установлена заводская операционная система Tp-Link. На момент проведения эксперимента на данную модель роутера не было готового OpenWRT решения. Поэтому операционная система для данного роутера была сконфигурирована самостоятельно через Linux консоль:

```
sudo apt-get install g++ ncurses-dev zlib1g-dev
gawk flex git-core
sudo apt-get install subversion
svn co svn://svn.openwrt.org/openwrt/trunk/
./scripts/feeds update -a
./scripts/feeds install -a
makeprereq
makeprereq&& make tools/install && make tool-
chain/install
makemenuconfig
```

Установленные модули OpenWRT:
- kmod-usb-core;
- kmod-usb-ohci;
- kmod-usb-storage;
- kmod-usb2;
- kmod-fs-ext4;
- block-mount;
- relayd;
- luci-proto-relay;
- luci;
- zram-swap;
- swaponoff.

После установки операционной системы был сконфигурирован интерфейс LuCIi для управления операционной системой через браузер. LuCI (Lua Configuration Interface) – это веб-ориентированный интерфейс конфигурирования, написанный на языке программирования Lua. Загрузка внешнего канала связи обусловлена:

- удаленные рабочие столы: 4, использует протокол RDP;
- IP-телефония, использует протокол SIP;
- Skype, использует закрытый протокол на основе механизма Peer-To-Peer (P2P);
- браузерное приложение для ведения бухгалтерии, использует протокол HTTP;
- 1 Приложение uTorrent, использует протокол P2P;
- цифровое телевидение, было включено для полноты эксперимента, использует IP протокол.

Реализация системы контроля пропускной способности выполняется на маршрутизаторе организации TP-Link TL-842ND с операционной системой OpenWRT. Одной из задач исследования является определение суммарного использования канала связи компании по каждому из типов трафика.

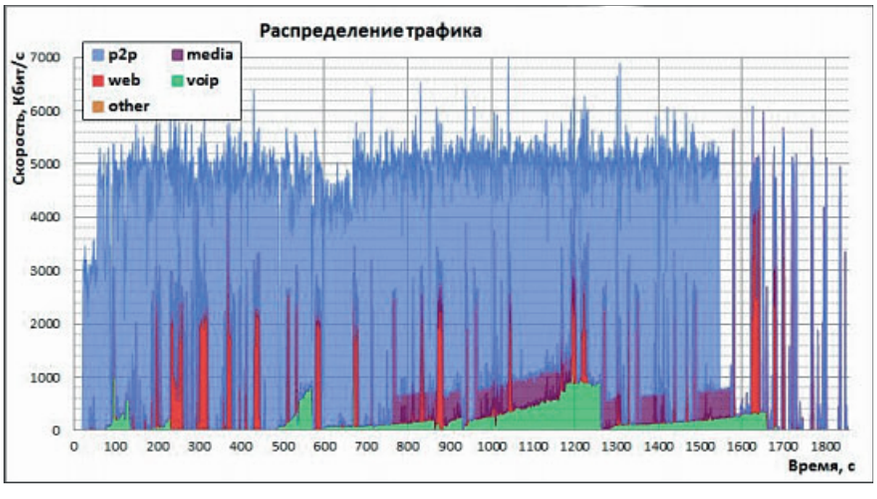

Рис. 2. Распределение трафика на внешнем канале связи
без применения алгоритма управления трафиком

Рис. 3. Распределение трафика на внешнем канале связи
с применением алгоритма управления трафиком

Эксперимент проводился следующим образом. В одинаковых условиях при 100% загрузке внешнего канала связи анализировался трафик, проходящий по нему в течение одного часа с использованием алгоритма управления трафиком и без него. Без применения алгоритма управления трафиком (см. рис. 2) возникают перегрузки при одновременном использовании всех приложений сети. Возникают разрывы связи при использовании IP-телефонии, Skype, существенно замедляется работа по протоколу HTTP. Экспериментальное внедрение компонента на роутере под управлением ОС OpenWRT показало эффективность применения разработанного алгоритма, трафик не перекрывает доступность других протоколов связи и, в свою очередь, используется вся пропускная способность внешнего канала связи (см. рис. 3).

Заключение

Экспериментально подтверждается эффективность работы алгоритма управления трафиком. Это показывает сравнение результатов, представленных на рис. 2 (распределение трафика без применения алгоритма) и рис. 3 (распределение трафика с применением алгоритма).

Внешний канал связи компьютерной сети-компании использовался полностью, без перегрузки отдельными типами трафика. Трафик, создаваемый сетевыми приложениями по различным протоколам (HTTP, VoIP, P2P, media), равномерно распределяется в канале связи.

Дальнейшее направление исследования – возможность создания универсального модуля Linux, содержащего программное обеспечение для защиты сети от перегрузки. Данный модуль управления трафиком в перспективе может быть задействован в домашних сетях, в сетях общественного пользования и в сетях предприятий и организаций.

Литература

1. Оливер Ибе. Сети и удаленный доступ. Протоколы, проблемы, решения. М.: ДМК Пресс, 2002. – 81 с.
2. Олифер В.Г., Олифер Н.А., Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2006. – 958 с.
3. Ronald Cohn, Jesse Russell. OpenWRT, VSD, 2012. – 46 с.
4. Iptables // help.ubuntu.ru/wiki/iptables (дата обращения 18.03.2015)
5. Пиринговые (P2P) сети // URL://www. visti. net/dwl/art/P2P/P2P-end.pdf (дата обращения 18.03.2015)
6. Kim H.C., Claffy K.C., Fomenkov M, Barman D., Faloutsos M., Lee K.Y. Internet Traffic Classification Demystified: Myths, Caveats and the Best Practices // ACM CONEXT, 2008. – 5p.
7. Won Y.J., Park B.C., Ju H.T., Kim M.S., Hong J.W. A hybrid approach for accurate application traffic identification // IEEE/IFIP E2EMON, 2006. – 7 p.

Получено 25.05.2015

Колесников Иван Владимирович, аспирант Кафедры информатики и вычислительной техники Поволжского государственного университета телекоммуникаций и информатики. Тел. (8-846) 922-72-48. E-mail: 79277127248@ya.ru

REDUCING OF RISK FOR EXTERNAL CHANNEL OVERLOAD BY COMPUTER NETWORK TRAFFIC MANAGEMENT

Kolesnikov I.V.
Povolzhskiy State University of Telecommunication and Informatics, 23 L.Tolstoy str., Samara 443010, Russian Federation
E-mail: 79277127248@ya.ru

This work is concerned with solution of the problem of telecommunication network overload in the context of enterprise network by analysis and following management of traffic flow under using of router with installed operating system Open WRT. We developed algorithm for uniform traffic distribution over computer network. Software unit determines protocol packet and then defines band-width assigned to particular network protocol and realized it for P2P, VoIP, and HTTP protocols. Proposed algorithm was successfully used for computer network of dispatcher company. We associate further researches with development of universal unit for operational system with Open WRT protocol for bandwidth management of particular protocol traffic: P2P, VoIP, and HTTP.

Keywords: network technologies, traffic management, traffic analysis, P2P, VoIP, HTTP.

DOI: 10.18469/ikt.2016.14.1.06

Kolesnikov Ivan Vladimirovich, Povolzhsky State University of Telecommunications and Informatics, 23 Lev Tolstoy str., Samara 443010, Russian Federation; PhD Student of the Department of Computer Science and Engineering. Tel. +78469227248. E-mail: 79277127248@ya.ru.

References

1. Oliver Ibe. *Seti i udalenniy dostup. Protocoli, problemi, reshenia* [Network and remote access. Protocols, problems, solutions]. Moscow, DMK-Press Publ., 2002. 81 p.
2. Olifer V.G., Olifer N.A. *Komputernyeseti. Principy, tehnologii, protokoly* [Computer networks. Principles, technologies and protocols]. St.Peterburg, Piter Publ., 2006. 174 p.
3. Ronald Cohn, Jesse Russell. *OpenWRT*. VSD, 2012. 46 p.
4. Iptables. Available at: help.ubuntu.ru/wiki/iptables (accessed 25.03.2015).
5. *Piringovie P2P seti*. Available at: www.visti.net/~dwl/art/P2P/P2P-end.pdf (accessed: 18.03.2015).
6. Kim H.C., Claffy K.C., Fomenkov M, Barman D., Faloutsos M., Lee K.Y. *Internet Traffic Classification Demystified: Myths, Caveats and the Best Practices*. ACM CONEXT, 2008. 5p.
7. Won Y.J., Park B.C., Ju H.T., Kim M.S., Hong J.W. *A hybrid approach for accurate application traffic identification*. IEEE/IFIP E2EMON, 2006. 7 p.

Received 25.05.2015

УДК 621.396.4

ЭКСПЕРИМЕНТАЛЬНЫЙ ВЫБОР СИГНАЛЬНО-КОДОВОЙ КОНСТРУКЦИИ ДЛЯ ЗАБОЙНОЙ ТЕЛЕМЕТРИЧЕСКОЙ СИСТЕМЫ В УСЛОВИЯХ РЕАЛЬНЫХ ПОМЕХ

Суханов Д.В.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: dms_cyx@mail.ru

В статье изложены результаты сравнения ранее полученных теоретических результатов с экспериментом по выбору наилучшей сигнально-кодовой конструкции для забойных телеметрических систем. Показано сравнение предлагаемых вариантов построения забойной телеметрической системы с вариантом, использованным в скважинном приборе производства ООО «ТехГеоБур». В ходе эксперимента подверглись модернизации в передатчике блок «Кодер помехозащищённого кода», а в приемнике блок «Демодулятор-Декодер». Для корректного сравнения обоих вариантов весьма желательно сравнивать показания, закодированные разными кодами, при одном уровне одинаковых по своим вероятностным характеристикам шумов и при одинаковых искажениях канала. Результаты сравнения представлены в таблице, в которой показаны различные значения достоверности телеметрического параметра «Гравитационный отклонитель».

Ключевые слова: телеметрия скважин, горизонтальное бурение, помехоустойчивость приема, электромагнитный канал связи, достоверность данных, цифровой прием, нестационарный шум.

Введение

Наклонно направленное и горизонтальное бурение невозможно без применения забойных телеметрических систем (ЗТС, по зарубежной терминологии MWD и LWD), которые обеспечивают оперативное управление траекторией ствола скважин. По различным средам передачи телеметрических данных телесистемы делятся на следующие типы: с кабельным каналом связи, гидравлическим, акустическим, электромагнитным, комбинированным. При использовании электромагнитных (ЭМ) систем используется канал связи сверхдлинноволнового диапазона [1-10]. Средняя (несущая) частота передаваемого сигнала в таких системах составляет обычно 1-10 Гц (окно прозрачности 0,5-20 Гц). Более высокочастотные сигналы практически полностью поглощаются породой в процессе распространения на практически значимых расстояниях (1-4 км). При подаче электрического напряжения между верхней и нижней частями бурильной колонны (выполняющей роль антенны), разделенных диэлектрической вставкой, возникают токи, текущие в толще земли. Часть этих токов течет по поверхности и образует падение напряжения между устьем скважины и дополнительным электродом, установленным на расстоянии обычно 50-100 м от нее (см. рис. 1).