

# ЭФФЕКТИВНЫЕ РЕШЕНИЯ УПРАВЛЕНИЯ ТРАФИКОМ

АНАТОЛИЙ ШАВЛОВСКИЙ

**В**настоящий момент телекоммуникационная отрасль находится на этапе конвергенции новых сервисов. Широкополосный доступ в интернет приводит к возникновению новых услуг, которые, в свою очередь, предъявляют повышенные требования к каналам передачи данных. В такой ситуации операторы сталкиваются с новыми проблемами, основной из которых является возможность контролировать растущий трафик в своей сети.

## Есть ли необходимость управлять трафиком?

По прогнозам Cisco (рис. 1) темпы роста сетевого трафика составляют 150% каждый год, при этом видео и P2P являются самыми быстро растущими сегментами. Причем по структуре самым объемным является P2P, то есть, трафик файлообменных сетей.

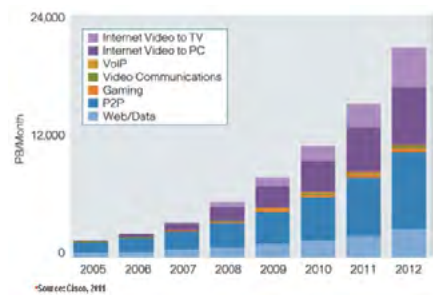


Рис. 1 Структура мирового трафика

Известно, что P2P не приносит дохода поставщикам услуг, но занимает немалую долю (30-40%) ресурсов сети. Особую опасность P2P представляет из-за неконтролируемых всплесков объемов передачи данных, что приводит к перегрузке сети. Это, в свою очередь, ведет к снижению качества предоставления других сервисов, приносящих доход, например, голоса и видео, и к финансовым потерям.

Операторам представляется неэффективным реагировать на рост сетевого трафика простым наращиванием емкости каналов и ресурсов коммутирующего и маршрутизирующего оборудования. Ведь приходится вкладывать значительные инвестиции в сеть уже сегодня, хотя трафик достигнет необходимого уровня только через один-два года. Таким образом, существует разрыв в несколько лет между стартом модернизации сети и моментом получения дохода от обслуживания абонентов, использующих построенную сеть по максимуму. Но это не все: средний доход от абонента

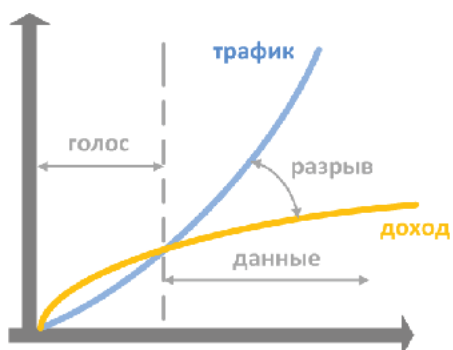


Рис. 2 Зависимость роста сетевого трафика и дохода от абонента

(ARPU) постоянно падает, следовательно, срок возврата инвестиций (ROI) в развитие инфраструктуры постоянно увеличивается (см. рис. 2).

Если бы кривая «доход» на рис. 2 возросла наравне с кривой «трафик», то проблемы не было бы: инвестиции в развитие сетевой инфраструктуры, соответствующей росту сетевого трафика, будут окупаться. Но сегодня возникает «разрыв», который особенно ярко выражен для стремительно падающих в цене сервисов передачи данных.

Вышеописанное ведет к тому, что эффективно предоставлять услуги пере-

дачи данных, организуя для клиента просто «трубу», становится все сложнее. В эпоху YouTube, онлайн-радио, пиринговых сетей и других «тяжелых» сетевых приложений, приходится говорить о политике использования пропускной способности каналов связи, о том, какие принципы распределения «полосы» помогут устранить возникающие проблемы.

## Пути решения

Чтобы справиться с быстрорастущими объемами данных, операторы рассматривают или уже опробовали несколько методик. Ряд компаний (в том числе украинских) ограничивали месячный объем общего используемого трафика абонента, но такой подход снижает привлекательность услуг и не пользуется популярностью у клиентов. Другие провайдеры ограничивают полосу пропускания всего трафика абонента, что также нельзя назвать оптимальным вариантом: резкое лимитирование не удовлетворяет потребности пользователей, а незначительное — не решает проблемы с ростом трафика.

Как показывает опыт ведущих поставщиков услуг, наиболее оптимальным решением данной задачи является управление трафиком клиентов на уровне приложений. В основе методики лежит технология глубокой инспекции пакетов (Deep Packet Inspection, DPI), которая позволяет с помощью эвристического или сигнатурного анализа определять трафик различных приложения. Такой подход позволяет маркировать, применять ли политики QoS или ограничивать разные типы приложений. Эти инструменты позволяют создать прозрачный для управления поток данных, рост которого становится контролируемым.



Рис. 3 Грануляция потока данных с помощью DPI

Как видно на рис. 3, DPI позволяет выделить из общего потока данных нужные приложения: P2P, VoIP, видео и другие, которыми можно управлять. Например, ограничить torrent-поток или сделать высокоприоритетным Skype. И если изначально P2P-трафик загружал сетевые ресурсы непредсказуемо и почти не приносил прибыль, то теперь его можно ограничить, или же внедрить для такого типа трафика новые тарифные пакеты.

## Специфика технологии глубокой инспекции пакетов

Всем хорошо известно, что сетевой трафик можно контролировать, т.е. применять к нему различные политики на 3-м и 4-м уровне модели OSI.

Обычно сетевое оборудование не имеет возможности работать с верхними уровнями модели OSI — уровнем Приложений, поскольку в заголовке IP пакета нет никаких данных о его содержимом.

С развитием технологий сетевой безопасности произошел значительный прогресс в сигнатурном анализе трафика, то есть в определении типа трафика, атаки или вируса по определенным последовательностям прохождения пакетов в момент установления соединения или работы приложения. Именно развитие сигнатурного анализа стало началом развития технологии DPI, которая, ко всему прочему, использует еще и эвристический анализ, подразумевающий анализ поведения трафика в режиме реального времени. В целом, решение DPI — это анализ заголовка и данных пакета, корреляция данной информации и эвристический анализ для идентификации приложения.

## Как использовать DPI?

Если есть технология, которая позволяет определить различные приложения в общей структуре трафика, значит, появляется возможность управлять трафиком таких приложений — ограничивать, квотировать, назначать приоритеты, а также считать.

Подобные возможности дают в руки операторам услуг инструмент не только по контролю трафиком приложений и оптимизации полосы пропускания, но и управлению абонентами, дифференциации услуг, внедрению новых сервисов и визуализации сети. Такие инструменты позволяют решать технологические задачи, например, ограничить «паразитирующий» трафик, и увеличить доходность бизнеса и лояльность абонентов.

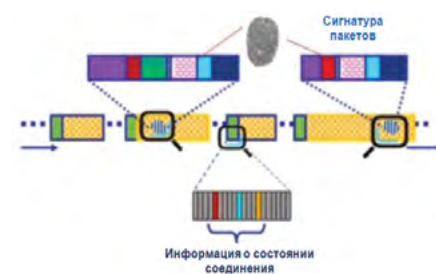


Рис. 4 Механизм работы технологии DPI

Среди задач, которые позволяют решить технология DPI, можно выделить следующие:

### Контроль приложений

- Назначение политик для трафика приложения
- Оптимизация полосы пропускания
- Предоставление новых услуг
- Родительский контроль
- Защита от DDoS атак
- Анти-спам
- Веб-фильтрация
- Антивирусная защита
- «Турбо-кнопка»

### Управление абонентами

- Управление квотами
- Уменьшение P2P и пр.
- Оптимизация видео потоков и http

### Визуализация сети

- Динамический просмотр загрузки сетевых ресурсов и построение отчетов по приложениям, абонентам, базовым станциям и т.д.

Все указанные выше задачи позволяют операторам решить основные задачи:

- Минимизация капитальных (CAPEX) и операционных (OPEX) расходов
- Повышение эффективности инвестиций
- Максимизация прибыли от услуг, повышение ARPU

Ограничения рисков, связанных с атаками на безопасность ИТ-инфраструктуры

Технология DPI позволяет операторам расширить услуги не только на массовом рынке, но также построить взаимовыгодные отношения с бизнес-партнерами. Широкий инструментарий дает возможность обрабатывать трафик облачных сервисов, т.е. применить политики SLA и квотировать трафик популярных ресурсов — Amazon, eBay, Google или Skype (рис. 5).



Рис. 5 Модель взаимодействия операторов с OTT

Используя концепцию «умной трубы», поставщики могут играть ключевую роль в цепочке создания стоимости облачных услуг.

Еще один вид новых дополнительных сервисов (VAS), связанных с внедрением

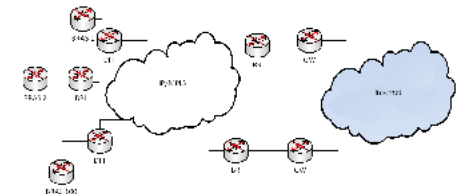


Рис. 6 архитектура включения решения DPI на сети агрегации

решения DPI на сети оператора, касается вставки и изменения содержимого потока приложений. Например, вставка рекламы в видео/http-поток позволяет создавать целевые рекламные показы или проводить маркетинговые исследования. Такой функционал поможет операторам получать дополнительный доход от рекламодателей или проводить кампании самостоятельно.

## Архитектура решения по управлению трафиком

Системы на базе DPI целесообразно размещать в точках концентрации трафика, то есть, там, где должны применяться основные политики управления трафиком и контроля пользователей. Если рассмотреть структуру сети фиксированного доступа, то первой такой точкой является BRAS, в таком случае комплекс DPI размещают в разрыв между BRAS и транспортной сетью оператора. Подобный подход существенно увеличивает совокупную стоимость решения DPI, так как сеть даже небольшого оператора насчитывает множество локальных точек концентрации, но позволяет применять политики в точке возникновения трафика, передавая в сеть уже «обтесанный» трафик.

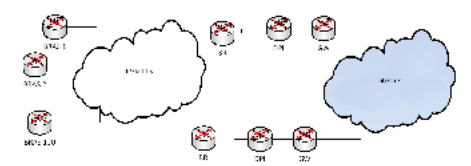


Рис. 7 Архитектура включения решения DPI на соединениях с Internet

Многие операторы размещают DPI в сегменте подключения к Internet (рис. 7). Такой подход способствует уменьшению инвестиций, но требует использования более мощных устройств и исключает возможность контроля внутреннего трафика сети.

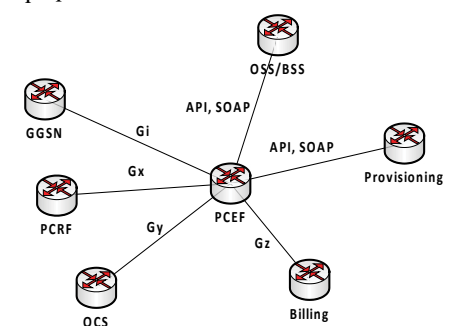


Рис. 8 Архитектура решения DPI на мобильной сети

Любая стратегия размещения устройств DPI в сети может быть эффективна в тех или иных условиях. Выбор топологии применения устройств DPI зависит в первую очередь от тех задач, которые оператор хочет решить внедрением этой технологии и требует обсуждения в каждом случае отдельно.

Для сети мобильных операторов архитектура решения становится несколько сложнее. В сравнении с фиксированными, мобильные сети имеют не так много точек концентрации трафика, с другой стороны, архитектура усложняется наличием разных биллинговых систем для прицепид- и постпейд-абонентов, систем контроля политик доступа, провижининга и OSS. В таких сетях решение DPI должны полностью соответствовать спецификациям 3GPP и поддерживать протокол Diameter для возможностей интеграции в сеть мобильного оператора.

## ДОСТУПНАЯ ИТ-ИНФРАСТРУКТУРА ОТ KERIO TECHNOLOGIES



**З**адачи ИТ-отделов в сегментах среднего и малого бизнеса требуют качественных, хорошо зарекомендовавшихся себя на рынке решений. Запросы состоят из первоначальных — это покупка программного обеспечения — и на его внедрение в существующую инфраструктуру предприятия, а также последующее администрирование. Ситуация на трудовом рынке Украины такова, что ИТ-специалисты высокой квалификации «стоят» немалых денег и далеко не все предприятия из SMB могут позволить содержать их штат. Продукты Kerio Technologies разработаны для предприятий SMB и имеют многолетнюю историю успеха на рынках США, стран Европы и СНГ, в частности Украины. Главные преимущества продуктов — простота и интуитивность администрирования продуктов, доступная цена по сравнению с аналогами.

Линейка продуктов состоит из таких элементов:

- Kerio Control — UTM-система для защиты трафика и контроля пользователей;
- Kerio Connect — решение для построения корпоративной почтовой системы и коллективного взаимодействия;
- Kerio Operator — VoIP-система.

Бесперебойный и безопасный доступ к сети Интернет — основа эффективной бизнес-коммуникации на любом предприятии, но при этом сеть таит в себе большое количество угроз и ресурсов, снижающих продуктивность персонала. Вопросы управления доступом в

Интернет многие компаний доверили UTM-системе Kerio Control. Она защищает корпоративную сеть от возникающих угроз путем постоянного обновления сигнатур сетевых атак, являясь стабильным, безопасным и простым в управлении продуктом. Гарантия качества связи осуществляется при помощи QoS, имеется защита для сетей IPV6, фильтрация HTTPS и вложенных URL. Решение доступно для Hyper-V, VMware, Parallels. Возможность гибкой настройки политик доступа к сети, а также системы отчетов о ее использовании, позволяют повысить продуктивность работы сотрудников компании.

«Решение приобрести Kerio Control было принято уже после сравнения его с аналогами, а после недельного тестирования сомнений в правильности решения не осталось вовсе, — прокомментировал Олег Шишкин — начальник ИТ-департамента НПФ «Техвагонмаш». — Кроме необходимого функционала — веб-фильтрации, мы получили мощное средство управления резервными каналами, а также высококлассную систему статистической отчетности Kerio Star».

Kerio Connect, пожалуй, лучшая альтернатива Microsoft Exchange для малого и среднего бизнеса, отмеченная многими наградами. Kerio Connect дает компаниям возможность использовать корпоративную почту, совместные календари и списки контактов на большинстве почтовых клиентов, веб-браузеров и мобильных устройств при гораздо меньших затратах денег и ИТ-ресурсов. В этом решении есть все, что нужно для безопасной работы с почтой: интегрированный антивирус, мощный антиспам Kerio Greylisting, встроенная система

архивации, автоматическое резервное копирование и удобный веб-интерфейс администрирования. Kerio Connect имеет настраиваемые политики доступа пользователей. Возможность развертывания на Windows, Linux, Mac OS X, VMware и Parallels, а также в «облаке» позволяют интегрировать его практически в любую ИТ-инфраструктуру.

Kerio Connect дает возможность обеспечить сразу несколько вариантов для удаленного доступа к почте, синхронизацию с мобильными устройствами, надежную антивирусную фильтрацию почтового трафика, блокировку более 90 % нежелательной почты, а также легкость и удобство управления системой электронной почты компании.

Kerio Operator позволяет получить современную систему IP-телефонии, не затрачивая при этом большие ресурсы. С помощью VoIP в ней реализованы передовые функции телефонии, обычно присущие корпоративным телефонным системам, в том числе: конференц-связь, интеграция с CRM, переадресация вызовов, парковка вызова, запись звонков, группы обработки вызовов, пересылка сообщений голосовой почты на электронную почту, автоматическое голосовое меню и очереди звонков. Приложение Kerio Operator Softphone для мобильных устройств под управлением Apple iOS и Android позволяет пользователям всегда иметь при себе офисный телефон. Данный продукт был разработан не так давно, но уже успел завоевать довольно обширный круг пользователей.

«Мы искали решения для организации системы IP-телефонии и корпоративной электронной почты. Помимо высокой

степени надежности и защищенности, одним из основных критериев выбора было получение требуемого результата при сопоставимых затратах на развертывание и сопровождение. Поэтому особое внимание уделялось оценке решений с точки зрения удобства развертывания и простоты администрирования. Кроме того, были требования, продиктованные ИТ-инфраструктурой, — наличие интеграции решений со службой каталога ActiveDirectory и возможность работы в виртуализированной среде. Исходя из результатов тестирования и успешной эксплуатации, мы можем уверенно заявить, что решения Kerio оказались удачным выбором», — Артем Каушан, начальник управления ИТ, «Банк «Софийский».

Как видно, компании различных секторов экономики доверяют построение своей ИТ-инфраструктуры продуктам Kerio. Стоит отметить, что компания Kerio Technologies находится на острие ИТ-рынка, постоянное развитие с учетом мировых тенденций позволяет ей завоевывать доверие новых пользователей. Ни для кого не секрет, что SaaS — это тренд. Kerio Connect и Kerio Operator доступны на территории Украины как услуга через хостинг партнеров официального дистрибутора Kerio Technologies Группы компаний БАКОТЕК®.



Тел./факс: +38044 273-3333  
E-mail: Kerio@bakotech.com  
www.bakotech.ua

В мобильных сетях решение DPI называют PCEF (Policy and Charging Enforcement Function), так как DPI дополняет функции политик доступа PCRF.

В общем случае, решение DPI — это программное обеспечение, которое можно установить на сервер или разработанный программно-аппаратный комплекс. Как правило, для обработки большого количества трафика более 100 Гб/с применяют блейд-решения, которые также называют ATCA (Advanced Telecommunications Computing Architecture). Для обработки небольшого трафика до 30 Гб/с используют аппаратные системы. Отличительной особенностью любого решения DPI является его включение в разрыв прохождения сетевого трафика. Это предьявляет ряд

дополнительных требований по надежности, поэтому любой комплекс DPI должен содержать пассивный байпас (медный или оптический), который обеспечивает непрерывное прохождение трафика в случае выхода DPI из строя.

#### Заключение

В настоящее время растет число операторов, применяющих решение DPI для управления трафиком. Это позволяет снизить затраты на развитие сетевой инфраструктуры на фоне растущего трафика популярных сервисов. Также такие решения способствуют увеличению дохода за счет предоставления новых услуг, дифференциации тарифных планов, улучшения безопасности

доступа и т. д. По оценкам аналитических агентств, рынок систем управления трафиком (DPI) уже достиг 1 млрд. долл. и продолжает расти (по оценкам Infonetics Research — до 2 млрд. долл в течении 3 лет).

### Преимуществом наших решений является поддержка высоких скоростей передачи данных

Компания S&T Ukraine предлагает решения по управлению трафиком для операторов как фиксированных, так и

мобильных услуг, а также корпоративному сектору. Наши решения подойдут не только крупным операторам с большой нагрузкой сетевого трафика, но и средним компаниям, которые желают увеличить перечень предоставляемых услуг. Преимуществом наших решений является поддержка высоких скоростей передачи данных (более 1Тб/с), гибкость интеграции, что особенно важно мобильным операторам, быстрая масштабируемость, широкие возможности по внедрению новых сервисов.

Автор статьи: ведущий консультант отдела разработки системных решений компании «ЭС ЭНД ТИ УКРАИНА».

## НОВОСТИ

### СИСТЕМЫ ХРАНЕНИЯ ДАННЫХ Netgear выпускает настольную ReadyData

Netgear расширила свою линейку унифицированных систем хранения ReadyData, которая до сих пор состояла только из стоечной двухюнитовой модели на двенадцать дисков ReadyData 5200. Новая ReadyData 516 выполнена в настольном формате и, как утверждает производитель, впервые позволяет применять технологии хранения корпоративного класса в офисах небольших компаний и филиалах корпораций, у которых нет своего собственного ЦОДа.

ReadyData 516 рассчитана на установку шести заменяемых в горячем режиме 3,5-дюймовых жестких дисков SATA суммарной емкостью до 24 Тб и как опция поддерживает использование 100-Гб SSD, причем в одной системе можно комбинировать жесткие диски и SSD. В стандартной конфигурации нового продукта применяются такие

технологии систем хранения корпоративного класса, как динамическое выделение емкости (thin provisioning), сжатие и дедупликация данных как на уровне блоков (при использовании системы в составе сети хранения SAN), так и на уровне файлов (если система выполняет функции устройства NAS), поддержка виртуальных частных сетей (VPN). Также для обеспечения целостности данных ReadyData 516, как и ReadyData 5200, поддерживает создание неограниченного числа «мгновенных снимков» для записанных на ее дисках данных и их удаленную репликацию на другую ReadyData 516/5200 или в публичное облако (на базе инфраструктуры Amazon S3), в том числе с применением 128-разрядного шифрования SSL.

ReadyData 516 может также работать как хранилище резервных копий, поскольку она совместима с известными пакетами ПО резервного копирования Symantec, Acronis, CommVault и Veeam, или обслуживать инфраструктуру виртуальных серверов, развернутых на базе технологий VMware, Microsoft и Citrix.

Система оборудована процессором Intel Core i3 (Ivy Bridge) 3,3 ГГц, оперативной памятью ECC объемом 16 Гб, двумя сетевыми портами Gigabit Ethernet с подержкой агрегирования каналов и переключения трафика между портами при сбое, одним портом USB 2.0, двумя портами USB 3.0 и тремя портами eSATA.

### КОМПЬЮТЕРНЫЕ КОМПОНЕНТЫ Seagate представила полноценную линейку SSD-накопителей

Компания Seagate Technology анонсировала новый портфель решений на основе технологии флэш-памяти. Среди них: первый твердотельный накопитель (SSD) для клиентских устройств и следующее поколение SSD корпоративного уровня. Новая линейка накопителей, включающая Seagate 600 SSD, Seagate 600 Pro SSD и Seagate 1200 SSD, была создана для обеспечения высочайшей скорости

передачи данных и их целостности. В качестве дополнения к новому портфелю компания Seagate также представила решение Seagate X8 Accelerator для СХД, являющееся картой памяти PCIe. Карта ускорения основана на технологии компании Virident и предлагает возможность работы со всеми ключевыми интерфейсами, включая SATA и SAS.

«Появление новых моделей SSD в дополнение к нашим жестким и гибридным дискам позволяет предложить клиентам самый обширный в отрасли на данный момент портфель продуктов для хранения информации — теперь наши покупатели и партнеры могут приобрести полный спектр решений у единого поставщика. И это только начало. Компания Seagate стремится стать ведущим поставщиком как SSD-накопителей, так и устройств хранения данных на основе твердотельной памяти», — заявил Гэри Джентри (Gary Gentry), старший вице-президент и генеральный менеджер подразделения твердотельных накопителей компании Seagate.