DPI — хранитель сети ШПД или окончание эры свободного Интернета?

Н.В. ДУБЧУК, менеджер по маркетингу ООО "НТЦ ПРОТЕЙ"

Лавинообразный рост объема передаваемых данных в IP-сетях определяет основную тенденцию времени — возможность интеллектуального контроля трафика для операторов фиксированного и мобильного ШПД, в том числе операторов LTE. Центром внимания телекоммуникационной отрасли по всему миру сейчас является технология DPI — Deep Packet Inspection (глубокий анализ пакетов), и решения на ее основе.

Чтобы разобраться в принципе работы DPI, предположим, что IP-пакет — это письмо, а заголовок пакета — адрес на конверте. Простейшие устройства контроля трафика в сети оператора — коммутаторы, маршрутизаторы и межсетевые экраны — обрабатывают информацию аналогично классической схеме работы почтовой службы: адресная строка определяет получателя и путь отправления.

Разница заключается в том, что работник при отправке может взвесить конверт и определить стоимость пропорционально весу, а поставщик услуг широкополосного доступа — нет. Так, например, большая доля Интернет-активности приходится на "тяжелый" трафик файлообменных сетей P2P (Peer-to-Peer) и потокового видео OTT (видео, доступное для просмотра online с таких сайтов, как YouTube). Приходится постоянно расширять сеть и увеличивать скорость доступа для подписчиков. Более того, неконтролируемость тех или иных сетевых приложений ведет к тому, что страдает уровень обслуживания других услуг, и возникает опасность перегрузки.

В системе почтовой корреспонденции отправитель может сам определить приоритет своему письму, назначив ему статус заказного или письма с объявленной ценностью. Очевидно, что в IP-сети правила обработки пакета должны определяться сторонними силами, контроль над которыми осуществляет поставщик услуг ШПД.

На первый план выходит возможность точно идентифицировать данные и определить их принадлежность к тому или иному приложению. Разнообразие организации IP-связи таково, что для решения этой задачи недостаточно разбирать заголовки пакетов: адрес на конверте не дает полной информации о том, какие документы в него вложены.

Платформа DPI имеет в своем арсенале множество методов, часть из которых, например, основана на статистическом и поведенческом характере потока данных. Один из основных — поверка сигнатур протоколов и приложений. Под сигнатурой понимается шаблон описания данных, своеобразная "визитная карточка", которая однозначно соответствует приложению/протоколу. Каждая DPI-платформа хранит библиотеку сигнатур, которая пополняется при появлении новых версий или приложений. Другим, часто используемым методом является анализ сетевых транзакций, заключающийся в исследовании специфичных операций обработки данных, в частности, количества и размеров пакетов в ответ на запрос.

Очевидно, что анализ и извлечение всей необходимой информации требуют значительных вычислительных ресурсов, а одно из основных требований к DPI-платформе — выполнять сканирование пакетов на скорости канала передачи данных. Еще одним обязательным требованием является гибкость применения системы, т. е. добавление новых возможностей и сценариев обработки трафика. Последнее поколение DPI-продуктов успешно справляется с этими задачами, так как базируется на специализированных аппаратных средствах, что позволяет обеспечивать необходимую скорость анализа данных и добавлять новую функциональность, используя только обновление программного обеспечения.

DPI — Diligent Parasite Incinerator (Прилежный уничтожитель паразитов)

Важным моментом является то, что правила, на основании которых DPI-платформа выполняет действия над трафиком, могут быть заданы посредством двух основных базисов — "per-service" или "per-subscriber" ("по сервису" или "по подписчику/группе подписчиков").

Как уже упоминалось, существуют данные, которые занимают ресурсы сети в ущерб другим приложениям. Поэтому задачей поставщика услуг является выявление таких своеобразных "паразитов", блокировка либо разумное ограничение выделяемой для них полосы.

DPI-платформа идентифицирует и фильтрует:

нелегальный контент, передача которого прекращается, если адрес ресурса занесен в черный список;

самый распространенный сетевой "паразит" — спам. Часто абоненты, от которых идет рассылка, являются жертвами почтовых вирусов. В этом случае система автоматически выявляет зараженное устройство и перенаправляет его владельца на страницу, содержащую детальные инструкции по решению проблемы и удалению вируса. Поставщик услуг получает возможность в дальнейшем не вкладывать средства в дополнительные решения по фильтрации спама;

любой вид DDoS-атаки (преднамеренной или нет отправки большого количества информации на вычислительную систему с целью вывести ее из строя).

Таким образом, одна из главных задач, решаемых за счет фильтрации трафика на основе правил "per-service", — обеспечение клиентов безопасной Интернет-средой.

Благодаря второй группе правил — "per-subscriber", поставщик услуг

получает в свое распоряжение мощный маркетинговый инструмент, позволяющий создать широкую линейку тарифов с учетом предпочитаемого абонентом вида контента: работы в социальных сетях, on-line игр или просмотра потокового видео. Важным моментом является то, что интеграция DPI с биллинговой системой позволяет тарифицировать данную услугу и отобразить в счете абонента детальную стоимость.

Пример тарифного плана — подписка на среднюю скорость доступа в Интернет с ежемесячным лимитом общего трафика, но при этом с неограниченной работой в социальных сетях, бесплатными "Счастливыми часами" и приоритетом для голосового трафика, который получает гарантированную полосу даже во время часа пик.

Возможность точно оценить стоимость услуг и создать персонализированное предложение для пользователя, во-первых, способствует более справедливому распределению абонентской платы, во-вторых, определяет рост дохода провайдера пропорционально возросшему потреблению ресурсов сети.

Внедрение DPI-платформы решает и проблему контроля клиентами своих роуминговых расходов. Благодаря интеграции с биллинговой платформой, тарификация услуг осуществляется в режиме реального времени. Пользователи перед установлением соединения оповещаются о ценах на услуги.

Так, например, если система идентифицирует факт пребывания за границей, то на устройстве клиента открывается меню со следующими опциями: временная блокировка доступа в Интернет, выбор специального тарифа с льготными условиями, либо использование текущего тарифа с дополнительными издержками.

Решение такого широкого спектра задач в тандеме с уже упомянутым обеспечением безопасной Интернет-среды и новой линейки тарифных планов повышает лояльность клиентов, способствует росту ARPU и позволяет оптимизировать использование ресурсов сети. А есть ли у этой технологии спорные или отрицательные стороны?

DPI — Dead of Paradise is Inevitable? (Падение рая неизбежно?)

Внимательный читатель не мог не заметить, что DPI-платформа дает возможность накладывать на пользователя Интернет-ресурсов существенное количество ограничений, например, задавать определенный лимит трафика либо уменьшать скорость для клиента, чрезвычайно активно пользующегося файлообменными сетями. Ведет ли это в конечном итоге к окончанию "райской" эры свободного Интернета в будущем?

Конечно, со стороны пользователя такие меры оцениваются как нежелательные, но естественные законы развития систем подсказывают, что никакие ресурсы не могут существовать в неограниченном количестве. Поэтому перед провайдером встает выбор: либо постоянно расширять свою сеть, либо внедрить DPI-платформу, оценить структуру трафика и сделать последующие расширения более предсказуемыми.

В последнее время на первый план часто выходит такое понятие, как качество восприятия услуг широкополосного доступа пользователем — QoE (Quality of Experience). QoE — более субъективная оценка, чем QoS (Quality of Service). Именно качество восприятия — это стимул, который влияет на лояльность клиентов по отношению к поставщикам услуг.

Так, например, согласно исследованиям независимой компании Vanson Bourne в 2011 г. среди 2 тыс. пользователей услугами мобильного широкополосного доступа в Великобритании, Франции, Германии и США три пользователя из пяти в настоящее время готовы платить за более высокое качество восприятия (QoE):

74 % респондентов заявили о готовности заплатить большую сумму за высокую скорость загрузки при оказании услуг мобильного широкополосного доступа;

61 % высказались за то, чтобы их операторы связи предлагали персонализированные услуги и тарифные планы;

четверо из пяти заявили о том, что они предпочитают иметь один счет или тарифный план на услуги передачи данных, которые охватывают все их потребности в услугах широкополосного доступа.

По России такой статистики пока нет, но, тем не менее, исследование компании "Яндекс", обнародованное в марте 2012 г., показало, что аудитория мобильного Интернета в стране растет гораздо быстрее аудитории Интернета в целом.

Популярность DPI-решений обуславливается еще одним фактором: интересом к проблеме справедливого распределения сетевых ресурсов, актуальной сейчас для провайдеров всех стран. Так, например, в США активно обсуждается вопрос сетевого нейтралитета (принципа, согласно которому провайдеры телекоммуникационных услуг не отдают предпочтения одному целевому предназначению, или одним классам приложений перед другими).

Инициативы сетевого нейтралитета поддерживаются группами защиты прав потребителей и крупными поставщиками Интернет-контента (например, Google, Yahoo и eBay), заинтересованными в свободной доставке контента.

Критиками выступают крупные телекоммуникационные компании и производители сетевого оборудования, главным аргументом которых является то, что оператор вынужден вкладывать средства в расширение сети, вместо обновления существующего оборудования и запуска услуг следующего поколения.

В США активно обсуждается запрет на управление трафиком законных/легальных приложений в отсутствии перегрузок. Но в то же время, отсутствует четкое определение "законности". Логично, что незаконным может быть контент, а не приложение, например, детская порнография явно относится к незаконному контенту, но протоколы HTTP и BitTorrent, посредством которых можно осуществлять его передачу, — вполне легальны.

В России на данный момент ограничений на внедрение DPI-решений не существует, поэтому пока у поставщиков широкополосного доступа есть на руках все карты для интеллектуального контроля трафика в своей сети.