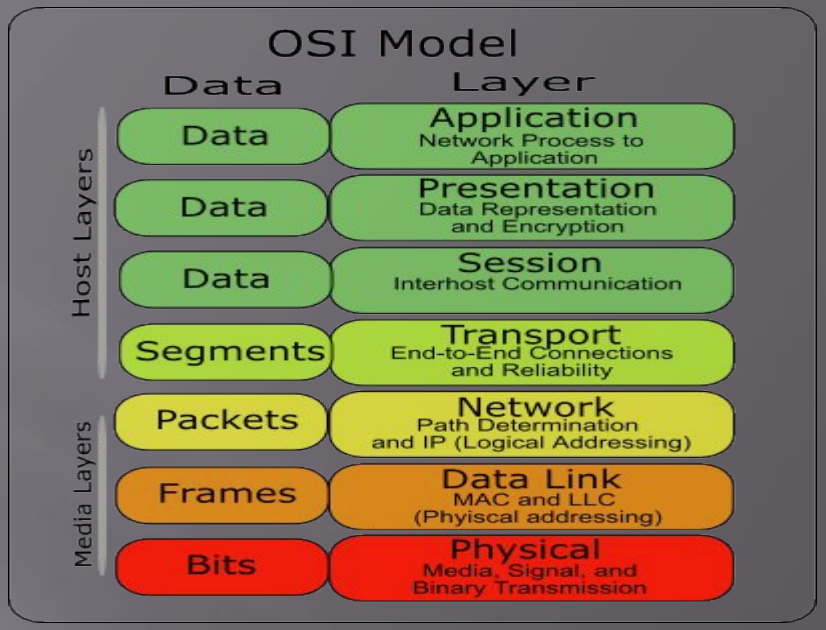
DEEP PACKET INSPECTION

Тябин Алексей
ОТЗИ 20501.10

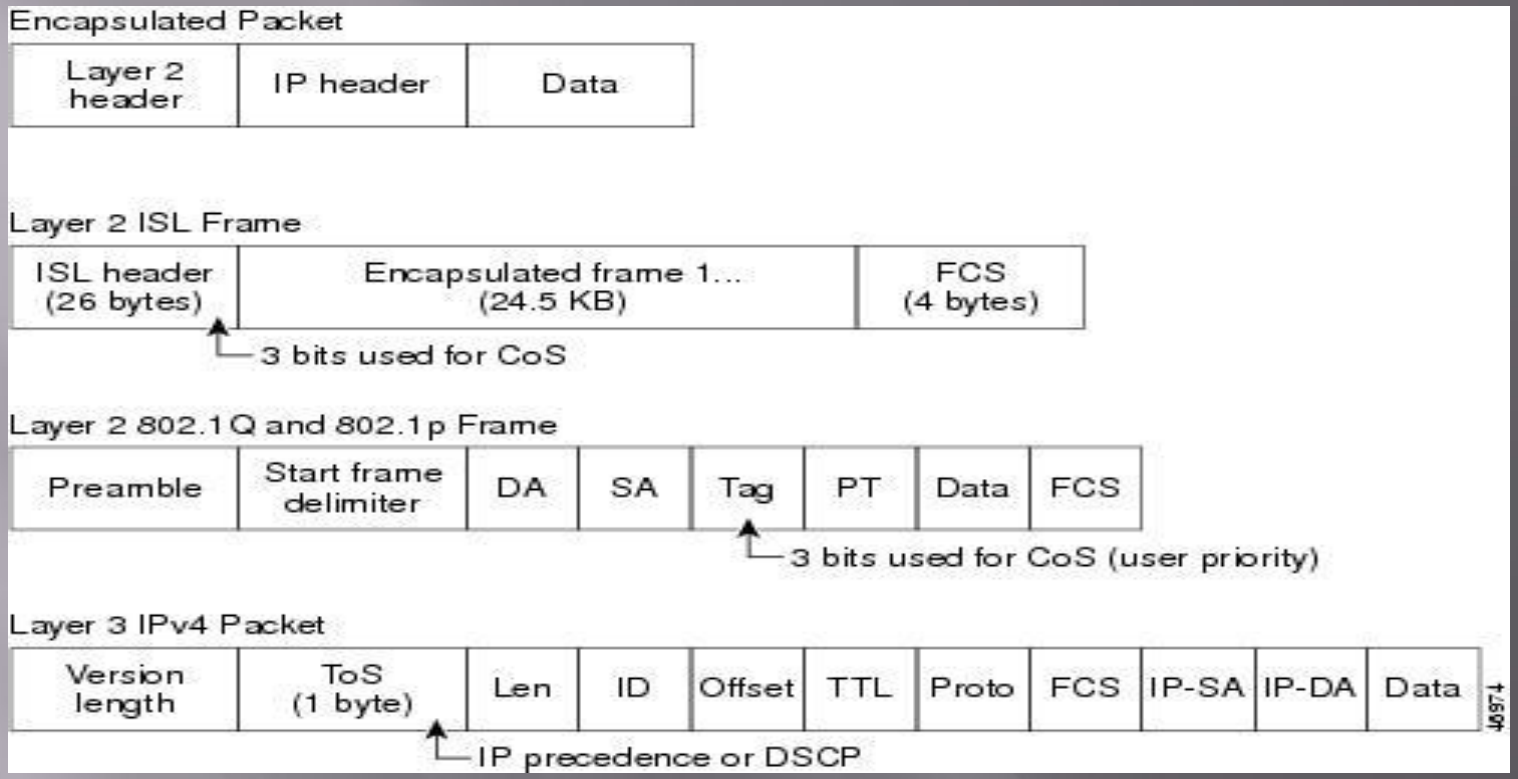


Deep Packet Inspection - технология накопления статистических данных, проверки и фильтрации сетевых пакетов по их содержимому. В отличие от брандмауэров, Deep Packet Inspection анализирует не только заголовки пакетов, но и полное содержимое трафика на уровнях модели OSI со второго и выше. Deep Packet Inspection способно обнаруживать и блокировать вирусы, фильтровать информацию, не удовлетворяющую заданным критериям.

Deep Packet Inspection может принимать решение не только по содержимому пакетов, но и по косвенным признакам, присущим каким-то определённым сетевым программам и протоколам. Для этого может использоваться статистический анализ (например статистический анализ частоты встречи определённых символов, длины пакета и т. д.)

Deep Packet Inspection часто используются провайдерами для контроля трафика, а иногда и для блокировки некоторых приложений, таких как BitTorrent. С помощью Deep Packet Inspection можно определить, какое приложение сгенерировало или получает данные, и на основании этого предпринять какое-либо действие.

Помимо блокирования, Deep Packet Inspection может собирать подробную статистику соединения каждого пользователя по отдельности.



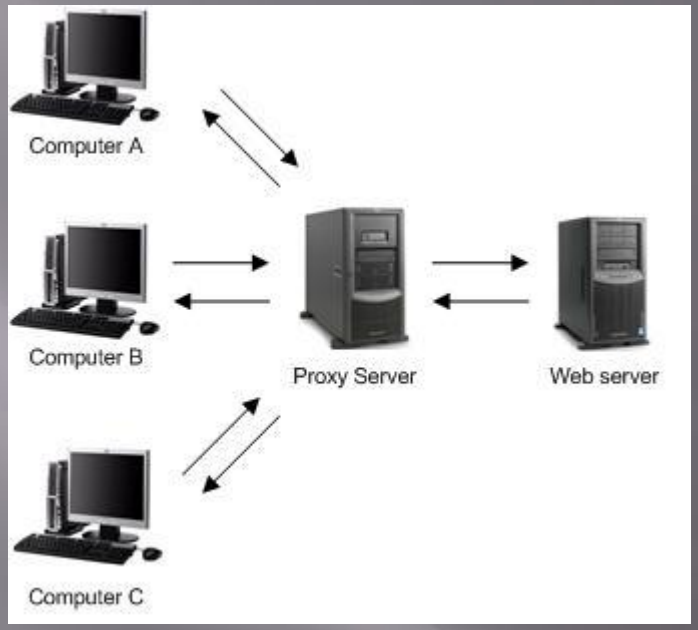
Также, при помощи quality of service Deep Packet Inspection может управлять скоростью передачи отдельных пакетов, подняв её или, напротив, уменьшив.

Кроме того, Deep Packet Inspection способно обнаруживать среди общего потока трафика кусочки, соответствующие компьютерным вирусам и блокировать их, повышая, таким образом, безопасность сети.

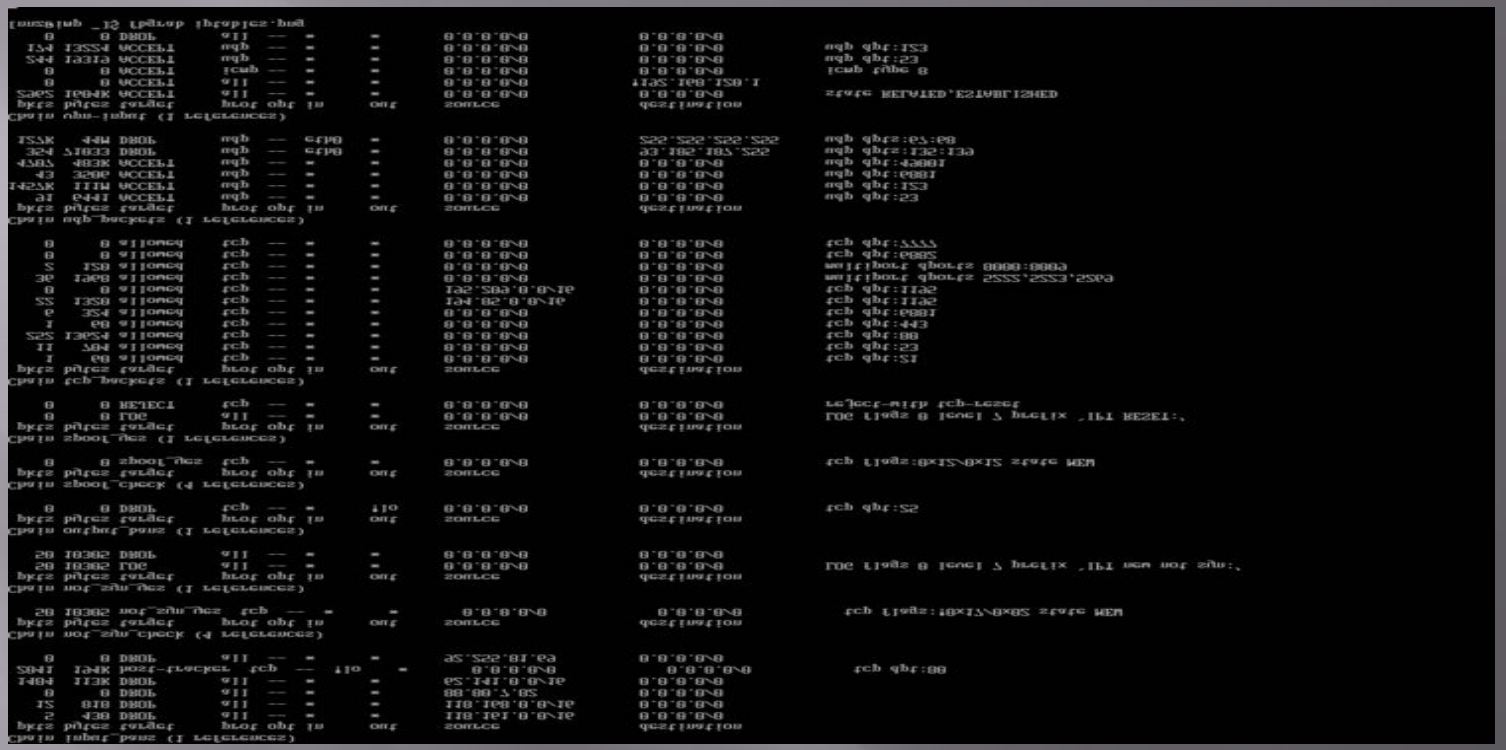
- Иногда Deep Packet Inspection используется в больших корпорациях для предотвращения случайных утечек данных, а также для защиты от отправки по e-mail внутренних защищённых файлов.

История

Первые брандмауэры могли быть реализованы двумя способами.



В первом способе прокси-сервер защищал внутреннюю локальную сеть от доступа из внешнего мира. Прокси-сервер проверяет, удовлетворяют ли сетевые пакеты заданным критериям. После этого либо отсеивает их, либо пересылает дальше. Такой способ использовался традиционно, так как он снижает риски, что кто-либо сможет воспользоваться уязвимостями протокола

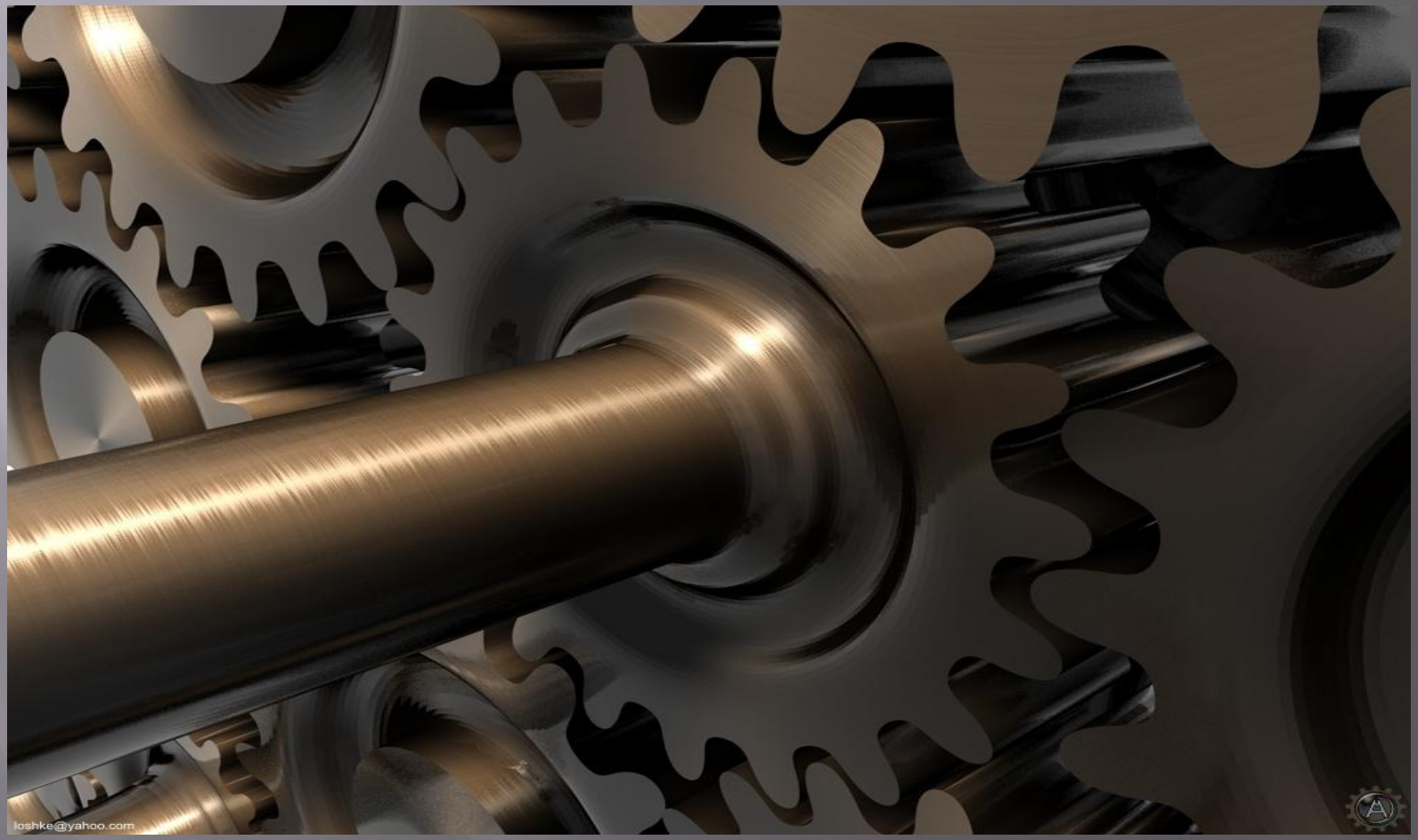


Во втором способе брандмауэром использовалась программа, осуществляющая фильтрацию сетевых пакетов по наборам правил. Такие программы получили название фильтрующих брандмауэров. Фильтрующий брандмауэр способен блокировать пакеты, не удовлетворяющие некоторым простым правилам, таким как IP источника, IP назначения, порт источника, порт назначения. Такие пакетные фильтры являются наиболее быстро работающим типом брандмауэров, так как делают совсем немного вычислений.

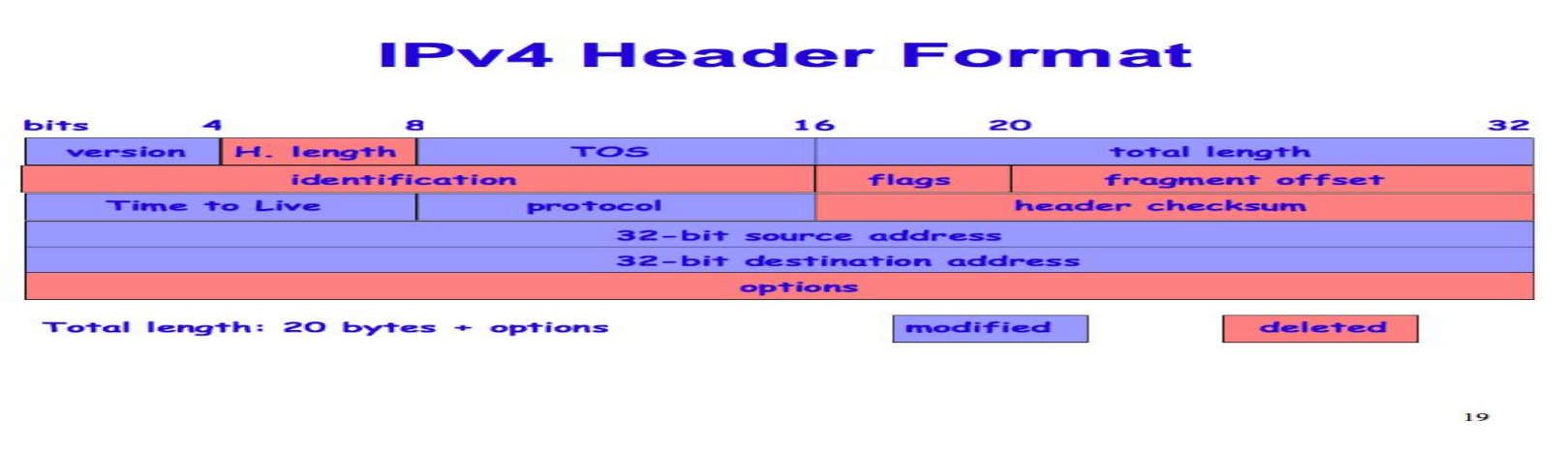
С самого начала прокси-сервера были признаны более безопасными, нежели пакетные фильтры, поскольку они более детально осуществляли проверку пакетов.

Эволюция брандмауэров на основе прокси-серверов привела к появлению первых программ Deep Packet Inspection. Они были созданы в целях устранения сетевых проблем и для блокирования вирусов, а также в целях защиты от DoS-атак. Первоначально компьютеры, на которых был установлен Deep Packet Inspection, не были достаточно мощными, чтобы контролировать весь Интернет-трафик пользователей в режиме реального времени.

Пример работы Deep Packet Inspection



Идентификация протокола транспортного уровня сетевой модели OSI



В структуре пакета протокола IPv4 выделен специальный байт для указания номера протокола транспортного уровня. Им является десятый байт от начала заголовка IPv4 пакета. Например: номер равняется шести — для TCP протокола, номер равняется семнадцати — для UDP протокола.

В структуре пакета IPv6 так же существует специальная область, в которой находится аналогичный идентификатор протокола транспортного уровня. Эта область носит название Next Header.

Идентификация BitTorrent

- Клиенты BitTorrent соединяются с трекером по протоколу TCP. Для того, чтобы обнаружить среди всего трафика TCP такие пакеты, достаточно проверить, что содержимое данных TCP пакета со второго байта совпадает с «BitTorrent protocol»

Идентификация HTTP

- Для идентификации HTTP протокола достаточно проверить, что пакет является TCP, и содержимое этого TCP пакета начинается с одной из следующих команд: «GET», «POST», «HEAD». Кроме того, после команды должен стоять пробел, а также через некоторый промежуток должен встретиться текст «HTTP/». Если всё это выполняется, то этот пакет несёт в себе HTTP запрос

Идентификация RTSP

- Для того, чтобы обнаружить среди всего трафика пакеты RTSP, достаточно убедиться, что пакет является TCP и содержимое этого TCP пакета начинается с одной из следующих команд: «OPTIONS», «DESCRIBE», «ANNOUNCE», «PLAY», «SETUP», «GET_PARAMETER», «SET_PARAMETER», «TEARDOWN». После команды должен стоять пробел. Также, через некоторый промежуток должен встретиться текст «RTSP/»

Для чего применяется DPI?

- - Реализация QoS
- - Subscriber Management

Реализация QoS

- С точки зрения эксплуатации, оператор может контролировать утилизацию подключенных через DPI каналов на уровне приложений. Раньше он решал задачи реализации QoS (Quality of Service) исключительно средствами построения очередей на основании маркировки трафика служебными битами в заголовках IP, 802.1q и MPLS, выделяя наиболее приоритетный трафик (разного рода VPN'ы, IPTV, SIP и т. д.) и гарантируя ему определённую пропускную способность в любой момент времени. Трафик типа Best Effort, к которому относится весь интернет трафик домашних абонентов (HSI — High Speed Internet), оставался фактически без контроля, что давало возможность тому же Bittorrent забрать себе всю свободную полосу, что, в свою очередь, вело к деградации любых других веб-приложений. С использованием DPI у оператора появляется возможность распределить канал между различными приложениями. К примеру, в ночные часы разрешить трафику Bittorrent забирать себе больше полосы, чем днём, в часы-пик, когда в сети ходит большое количество другого веб-трафика. Другая популярная мера у многих мобильных операторов — блокировка Skype-трафика, а также любых видов SIP-телефонии. Вместо полной блокировки оператор может разрешать работу данных протоколов, но на очень низкой скорости с соответствующей деградацией качества предоставления сервиса у конкретного приложения, чтобы вынудить пользователя платить за услуги традиционной телефонии, либо за специальный пакет услуг, разрешающий доступ к VoIP-сервисам.

Subscriber Management

- Важным моментом является то, что правила, на основании которых выполняется шейпинг/блокировка, могут быть заданы посредством двух основных базисов — per-service или per-subscriber. В первом случае простейшим образом оговаривается, что конкретному приложению позволяется утилизировать определённую полосу. Во втором привязка приложения к полосе осуществляется для каждого подписчика или группы подписчиков независимо от других, что производится через интеграцию DPI с существующими OSS/BSS системами оператора. То есть можно настроить систему таким образом, что подписчик Вася, который за неделю накачал торрентов на 100 гигабайт, до конца месяца будет ограничен по скорости скачивания этих же торрентов на уровне 70 % от купленного им тарифа. А у подписчика Пети, который купил дополнительную услугу под названием «Skype без проблем», трафик приложения Skype не будет блокироваться ни при каких условиях, но любой другой — легко. Можно сделать привязку к User-Agent и разрешить браузинг только при помощи рекомендуемых браузеров, можно делать хитрые редиректы в зависимости от типа браузера или ОС. Иными словами, гибкость тарифных планов и опций ограничена лишь здравым смыслом. Если же речь идёт о трафике мобильных операторов, то DPI позволяет контролировать загрузку каждой базовой станции в отдельности, справедливо распределяя ресурсы БС таким образом, чтобы все пользователи остались довольны качеством сервиса. Большинство производителей пакетного ядра EPC (Evolved Packet Core) для LTE интегрирует в свой PDN-GW функционал DPI, приспособленный для решения задач мобильных операторов.

Программное обеспечение

- Hippie (Hi-Performance Protocol Identification Engine) — реализация Deep Packet Inspection для Linux с открытым исходным кодом на C.
- L7-filter — ещё одна реализация Deep Packet Inspection для Linux с открытым исходным кодом на C, ориентированная на классификацию данных седьмого уровня модели OSI.
- SPID (Statistical Protocol IDentification) — реализация Deep Packet Inspection для Windows с открытым исходным кодом на C#. Идентифицирует протокол седьмого уровня модели OSI с помощью статистического анализа трафика.

Использование Deep Packet Inspection в России и мире

США

- Deep Packet Inspection способно изменять данные в пакетах. В Соединённых Штатах Америки и Великобритании Deep Packet Inspection часто используется для генерации рекламы, основанной на поведении абонентов. Таким образом реализуется так называемый целевой маркетинг.

Россия

- Основные сотовые операторы России внедрили DPI в 2009 (Мегафон, оборудование Huawei), 2010 (МТС, Cisco) и 2011 (Билайн, Procera) годах. Они могут использовать DPI в том числе для подавления peer-to-peer и VoIP сервисов. Ростелеком планирует внедрить DPI для мобильного интернета в 2014 году.

- В России тенденции к внедрению Deep Packet Inspection у интернет-провайдеров также связаны с федеральным законом № 139 о внесении изменений в закон «О защите детей от информации, причиняющей вред их здоровью и развитию» (вступил в силу 1 ноября 2012 года). Большинство интернет-провайдеров обеспечивают блокирование сайтов, занесённых в чёрный список, основываясь только на IP адресах этих сайтов. Но некоторые провайдеры могут блокировать выборочные URL-адреса, если у них используется Deep Packet Inspection для анализа HTTP-запросовK шифрованным соединениям (HTTPS) применение техники DPI затруднено.

- Одним из препятствий обязательного применения DPI-технологий российскими провайдерами для блокировки запрещенных сайтов стала дороговизна подобных решений, а также наличие более дешевых альтернатив для фильтрации по URL-адресу с целью исполнения закона.

Вопросы

- 1) Что такое DPI ?
- 2) Для чего используется DPI ?
- 3) Приведите пример идентификации HTTP запроса в DPI.

Используемые источники

- http://www.ranum.com/security/computer_security/editorials/deepinspect/
- http://it-giki.com/post/95.html
- http://www.freepress.net/sites/default/files/fp-legacy/Deep_Packet_Inspection_The_End_of_the_Internet_As_We_Know_It.pdf