ITU стандартизировало конец Интернета (или сказ про DPI)

Пока во всем мире обсуждали и готовились к "концу света по календарю майя", в Дубае, где проходила Всемирная конференция по международной электросвязи 2012 года (WCIT-12), похоже, также постарались если не привести к гибели человечества, то по крайней мере усложнить жизнь той его части, которая "живет" в интернете.

Предупреждение: я решил более-менее полно, но без углублений "пройтись" по этой теме и поэтому не стал экономить на графических иллюстрациях.

Российская международная сверхактивность в 2012 году

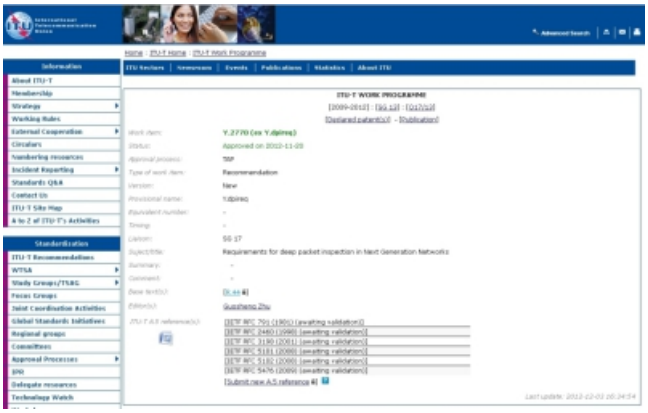
Российское государство давно всем известное, как страна с огромной территорией, ядерным оружием и с большими запасами нефти и газа, в 2012 году, кроме, пока не особо успешных, претензий на роль ещё одного межгосударственного финансового центра, решило обозначить адекватное своим размерам и потенции место и в международном регулировании информационно-компьютерной сферы.

Решили начать с малого. Российские чиновники обнаружили, что в документах международного органа - ITU, до сих пор нет основных определений базовых понятий и предложили сначала хотя бы определить, что же такое "Интернет". Предложенный вариант звучал так: "*Internet: An international conglomeration of interconnected telecommunication networks which provides for the interaction of connected information systems and their users, by carrying their traffic using a single system of numbering, naming, addressing, identification, protocols and procedures that is defined by Internet Standards.*" Инициатива может быть и хорошая, но ...

Ещё были планы ~~"реорганизовать Рабкрин"~~ изменить организационную структуру управления Интернетом, вынеся управление отдельными сегментами на национальный уровень. И хотя у России нашлись и были единомышленники по этому вопросу, ничего не удалось поменять - США стояли как скала. Попытка разобраться с базовыми понятиями также оказалась безрезультатной. Всё мимо.

Закулисные дела

На фоне всей этой активности России и в том числе на конференции, на ней происходили и другие события, череда которых началась ещё раньше и они завершились более удачно. Дело в том, что в эти дни "за закрытыми дверьми" были утверждены "Требования к DPI в сетях NG" ("Requirements for Deep Packet Inspection in Next Generation Networks").



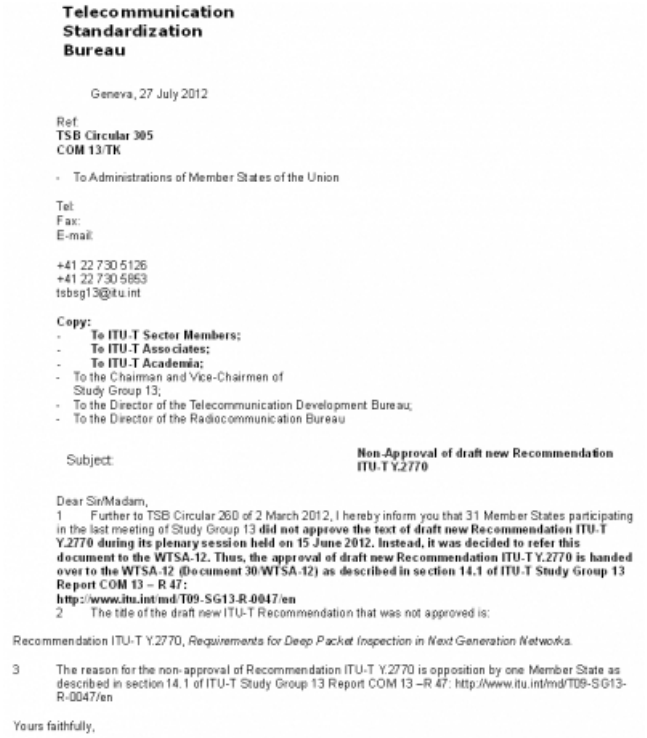
Вот он - Y.2770 со статусом "approved"

Как видите доступ к этому документу (с международным статусом) могут иметь только члены International Telecommunication Union (ITU) (там недвусмысленный "замок"). Но название "рекомендаций" (особенно в первоначальном виде - "Y.dpireq") ясно дает нам понять, что там за "секретные материалы" спрятаны.

А в "открытом эфире", в различных СМИ, в те же дни, когда утверждались "рекомендации Y.2770.dpireq", можно было прочитать, что "Генеральный секретарь ООН Пан Ги Мун призвал участников открывшейся Всемирной конференции по международной электросвязи ВКМЭ-2012 **принять согласованные совместные решения, которые сделают интернет безграничным и доступным для пользователей во всем мире**". "Призываю принять решения, предусматривающие обеспечение доступа к интернету "без границ" во всем мире по приемлемым ценам, учитывая, что электросвязь играет в наши дни основную роль в обеспечении свободы выражать свое мнение и получать информацию", - сказал генсек ООН. Здорово, да?

Предыстория

Летом 2012 года членам ITU-T предстояло рассмотреть и согласовать текст проекта этих рекомендаций. И хотя идея DPI возникла, как говорится, "не вчера", получить сразу всеобщее одобрение не получилось.



Telecommunication Standardization Bureau

Geneva, 27 July 2012

Ref:
TSB Circular 305
COM 13/TK

- To Administrations of Member States of the Union

Tel:
Fax:
E-mail:

+41 22 730 5126
+41 22 730 5853
tsbsg13@itu.int

Copy:
- **To ITU-T Sector Members;**
- **To ITU-T Associates;**
- **To ITU-T Academia;**
- To the Chairman and Vice-Chairmen of Study Group 13;
- To the Director of the Telecommunication Development Bureau;
- To the Director of the Radiocommunication Bureau

Subject: **Non-Approval of draft new Recommendation ITU-T Y.2770**

Dear Sir/Madam,

1 Further to TSB Circular 260 of 2 March 2012, I hereby inform you that 31 Member States participating in the last meeting of Study Group 13 **did not approve the text of draft new Recommendation ITU-T Y.2770 during its plenary session held on 15 June 2012. Instead, it was decided to refer this document to the WTSA-12. Thus, the approval of draft new Recommendation ITU-T Y.2770 is handed over to the WTSA-12 (Document 30/WTSA-12) as described in section 14.1 of ITU-T Study Group 13 Report COM 13 – R 47: http://www.itu.int/md/T09-SG13-R-0047/en**

2 The title of the draft new ITU-T Recommendation that was not approved is:

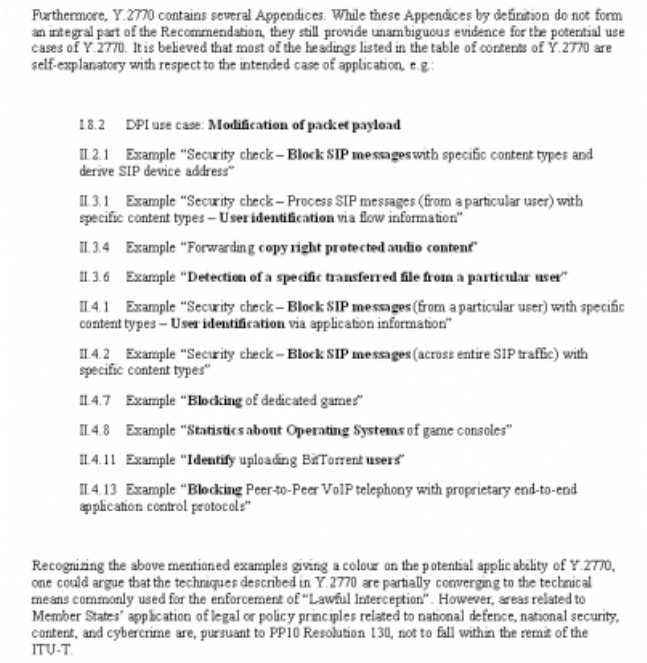
Recommendation ITU-T Y.2770, *Requirements for Deep Packet Inspection in Next Generation Networks.*

3 The reason for the non-approval of Recommendation ITU-T Y.2770 is opposition by one Member State as described in section 14.1 of ITU-T Study Group 13 Report COM 13 –R 47: http://www.itu.int/md/T09-SG13-R-0047/en

Yours faithfully,

Известно, что Германия обозначила свою тревогу и не согласовала проект Y.2770

Я нашел файл с письмом Германии (оно оказалось без "замка"), в котором немцы критиковали многие пункты и обращали внимание на двоякую сторону применения DPI и возможность злоупотреблений как со стороны провайдера, так и, например, по указанию тех или иных государственных органов, в том числе в политических целях. Может получиться так, что слова "управление трафиком", "фильтрация", "цензура" окажутся единым целым.



Furthermore, Y.2770 contains several Appendices. While these Appendices by definition do not form an integral part of the Recommendation, they still provide unambiguous evidence for the potential use cases of Y.2770. It is believed that most of the headings listed in the table of contents of Y.2770 are self-explanatory with respect to the intended case of application, e.g.:

I.8.2 DPI use case: **Modification of packet payload**

II.2.1 Example "Security check – **Block SIP messages** with specific content types and derive SIP device address"

II.3.1 Example "Security check – Process SIP messages (from a particular user) with specific content types – **User identification** via flow information"

II.3.4 Example "Forwarding **copy right protected audio content**"

II.3.6 Example "**Detection of a specific transferred file from a particular user**"

II.4.1 Example "Security check – **Block SIP messages** (from a particular user) with specific content types – **User identification** via application information"

II.4.2 Example "Security check – **Block SIP messages** (across entire SIP traffic) with specific content types"

II.4.7 Example "**Blocking** of dedicated games"

II.4.8 Example "**Statistics about Operating Systems** of game consoles"

II.4.11 Example "**Identify** uploading BitTorrent **users**"

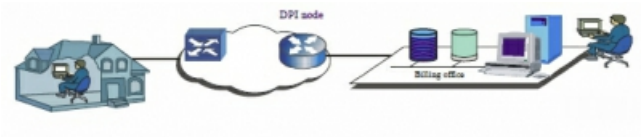
II.4.13 Example "**Blocking** Peer-to-Peer VoIP telephony with proprietary end-to-end application control protocols"

Recognizing the above mentioned examples giving a colour on the potential applicability of Y.2770, one could argue that the techniques described in Y.2770 are partially converging to the technical means commonly used for the enforcement of "Lawful Interception". However, areas related to Member States' application of legal or policy principles related to national defence, national security, content, and cybercrime are, pursuant to PP10 Resolution 130, not to fall within the remit of the ITU-T.

Вот что насторожило представителей Германии и устраивало всех остальных членов ITU

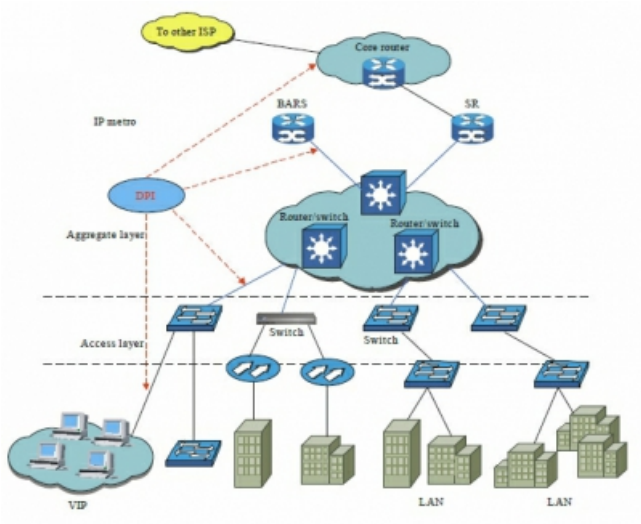
Requirements for Deep Packet Inspection in Next Generation Networks

Всё гениальное просто: встаем на пути трафика и, используя "искусственный разум", решаем задачу оптимизации пропускной способности.

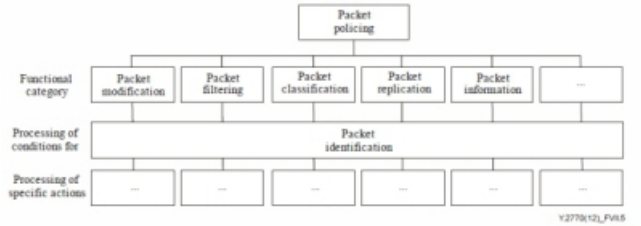


Автоматический "регулировщик" трафика в работе (единичный клиент)

Масштабируя "картинку" с клиентом до "полной" сети, получим примерно такую схему работы (для пакетной сети):

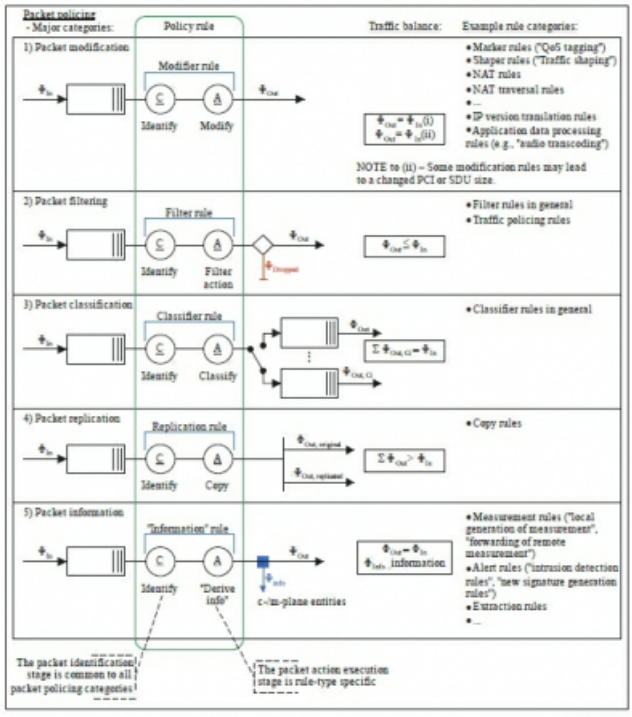


Работа в "большой" сети: присутствие на уровне доступа, на уровне агрегации и стыков



С IP-пакетами можно делать что угодно (есть даже "запасные" прямоугольники)

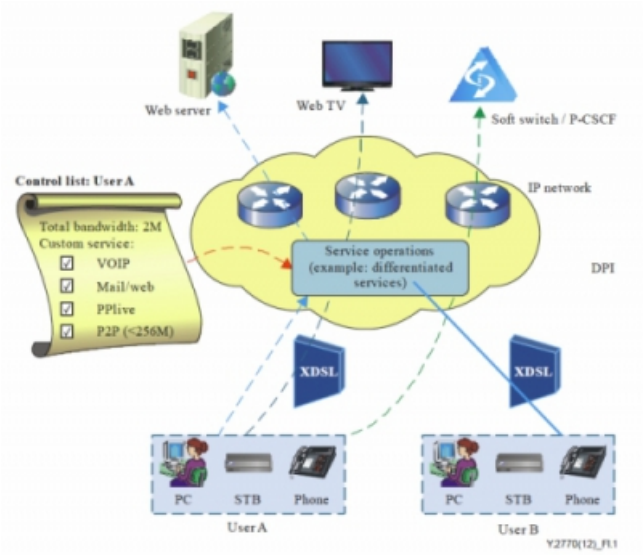
В более "заумном" виде это выглядит так:



Обратите внимание, что объемы трафика "на входе" и "на выходе" в зависимости от поставленных целей и применяемой политики управления трафиком могут не только примерно совпадать, но и быть меньше или больше.

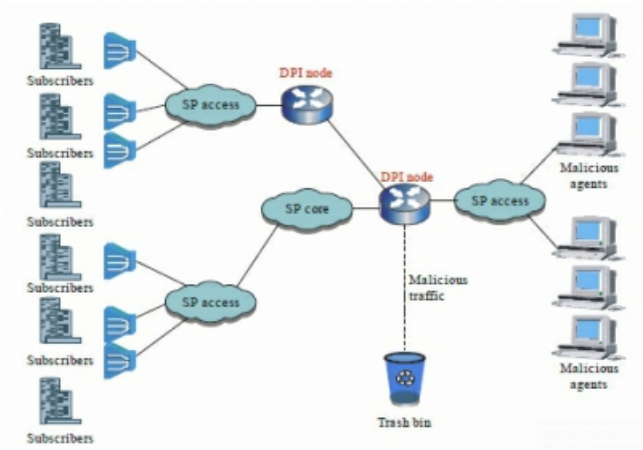
Основная функция оборудования DPI "опознать" трафик (или приложение) на основе тех или иных признаков ("сигнатур"), которые в свою очередь базируются на предварительном анализе IP-пакетов. Область работы "deep": 4-7 уровень OSI.

Известно, что в зависимости от того, что нам требуется от канала связи, будут и разные требования к его работе: нам нужен ("мы ожидаем", "мы так привыкли") непрерывный поток данных в случае голосового общения или при просмотре "живой" онлайн-трансляции. Также важно для нас слушать "непрерывно", например, интернет-радио или смотреть видеоролик (правда, в этих случаях спасёт буферизация). Неискушенному интернет-пользователю может быть непонятно почему у него тарифный план и "100 Мб/с", а при пользовании всем и сразу что-то начинает "лагать", "дергаться", "зависать". И тут как супермен приходит на помощь провайдер с DPI (или с шейп-решениями чуть попроще) и начинает "регулировать".

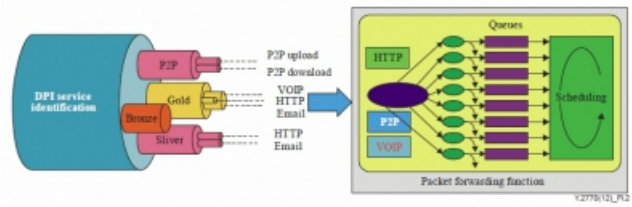


DPI помогает управлять "спросом на трафик" со стороны различных абонентских приложений

Всё более важной и более сложной становится задача защиты клиентов (и своей сети) от нежелательного или опасного трафика. И тут пусть "пашет" DPI и заполняет "мусорную корзиночку".



Самое интересное (для оператора) - это возможность, применяя DPI, не только выступить в роли "сотрудника ДПС, находящимся в ~~не~~нужном месте и в ~~не~~нужное время на дороге", но и получить дополнительный заработок. Деньги лишними не бывают.



Разделение трафика позволяет одинаковым в общем-то IP-пакетам присвоить дополнительную стоимость

Во-первых, у нас есть теперь "стоп-кран", во-вторых, мы делаем хорошее дело, но понесли затраты и вроде бы разумно, что хотим не только облегчить себе жизнь при пропуске трафика (нам этого мало),

но и впрямую окупить сделанные инвестиции и текущие расходы. В-третьих, принято, что гарантии и качество "стоят денег". Обеспечивая QoS, помогая абоненту беспроблемно смотреть кино "про котиков", мы фактически реализуем и предлагаем новую услугу, которая может иметь свой "ценник". Конечно, надо ещё объяснить и продать наше "новое качество связи" (и "нашу доброту").

Резюме: спасайся?

Разнообразие видов приложений или потоков данных, использующих протокол TCP/IP, велико. Но, по мнению ратующих за применение DPI, этот инструмент весьма универсален и позволяет "рулить" (в прямом и переносном смысле) трафиком как угодно и кому угодно. Ниже перечень ситуаций (и целей), которые в качестве примера перечислены в "Рекомендациях ...".

Вчитайтесь и оцените конечный результат, который может быть получен в зависимости от намерений владельца решений DPI. Надеюсь без перевода вполне понятно.

- Example "Security check - Block SIP messages with specific content types and derive SIP device address";
- Example "Detection of Malware";
- Example "Detection of specific video format" (H.264 as example);
- Example "Detection of File Transfer in general";
- Example "Security check - Process SIP messages (from a particular user) with specific content types - User identification via flow information";
- Example "Application-specific traffic policing" ;
- Example "Business Card (vCard) application - Correlate Employee with Organization" ;
- Example "Forwarding copy right protected audio content" (by checking on embedded digital watermarks in MP3 data) ;
- Example "Measurement-based traffic control" ;
- Example "Detection of a specific transferred file from a particular user" ;
- Example "Security check - Block SIP messages (from a particular user) with specific content types - User identification via application information" ;
- Example "Checking resource locators in SIP messages" ;
- Example "Deletion of a particular audio channel in a multi-channel media application" ;
- Example "Identify particular host by evaluating all RTCP SDES packets" ;
- Example "Measure spanish Jabber traffic" (counting Jabber messages with spanish text) ;
- Example "Blocking of dedicated games" ;
- Example "Statistics about Operating Systems of game consoles" ;
- Example "Measure abnormal traffic with respect to packet sizes" ;
- Example "Detect abnormal MIME attachments in multiple application protocols" ;
- Example "Identify uploading BitTorrent users" ;
- Example "Detection of BitTorrent traffic" ;
- Example "Measure BitTorrent traffic" ;
- Example "Blocking Peer-to-Peer VoIP telephony with proprietary end-to-end application control protocols" ;
- Example "Specific handling of old IP packets" ;
- Example "Security check - SIP Register flood attack (using a SNORT rule)" ;
- Example "Detection of eDonkey traffic" ;
- Example "Detecting a specific Peer-to-Peer VoIP telephony with proprietary end-toend application control protocols" ;
- Example "Detection of Remote Telnet"

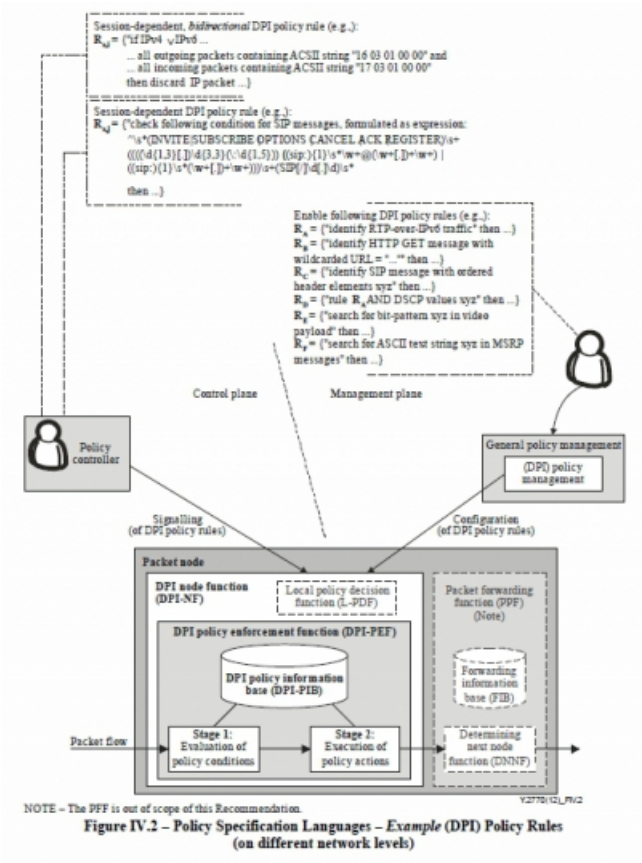
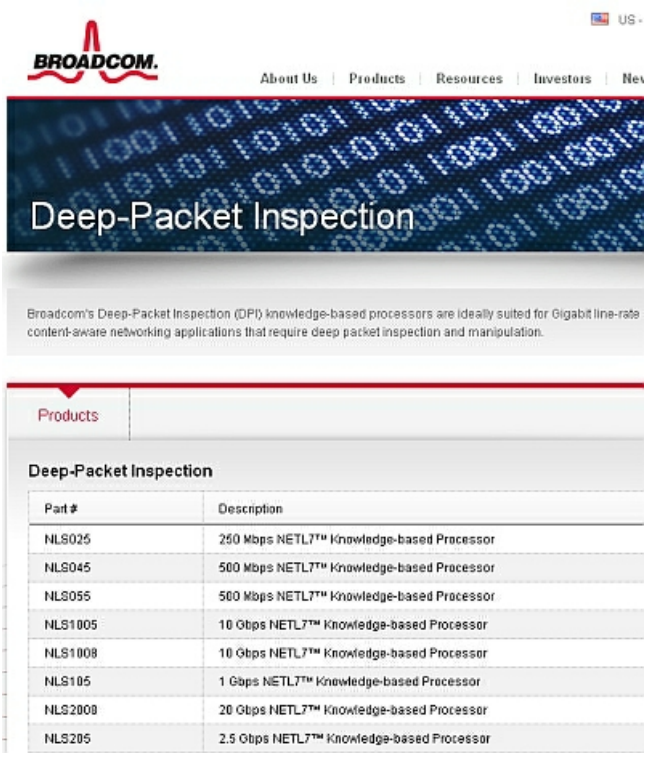


Figure IV.2 – Policy Specification Languages – *Example* (DPI) Policy Rules (on different network levels)

Пример "описания" различного рода политик/правил

Есть спрос, есть предложения. И наоборот

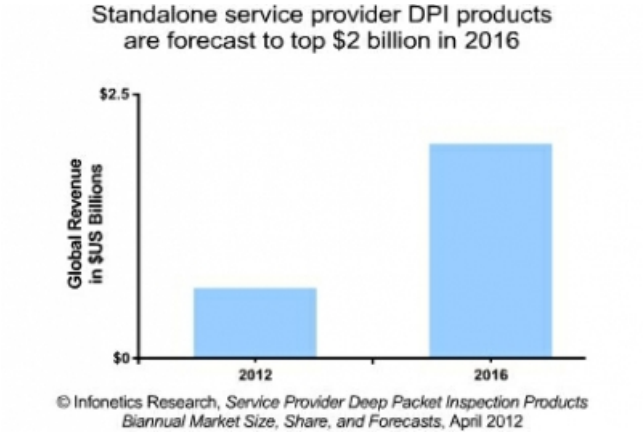
Операторы будут использовать всё больше и чаще решения DPI, так как жизнь заставляет: трафик самого разного происхождения растет лавинообразно, маржинальность снижается. Тем более теперь есть "добро" на международном уровне. Особо чувствительны к бешеному возрастанию трафика данных операторы мобильной связи, а абоненты требуют и ожидают высоких скоростей и дома и в дороге. При этом понятие "широкополосное соединение" для "проводного" провайдера и для какой-либо сотовой компании могут в реальности в цифровом виде отличаться в разы.



Вот и Broadcom решил "урвать" свой "кусочек" на рынке DPI

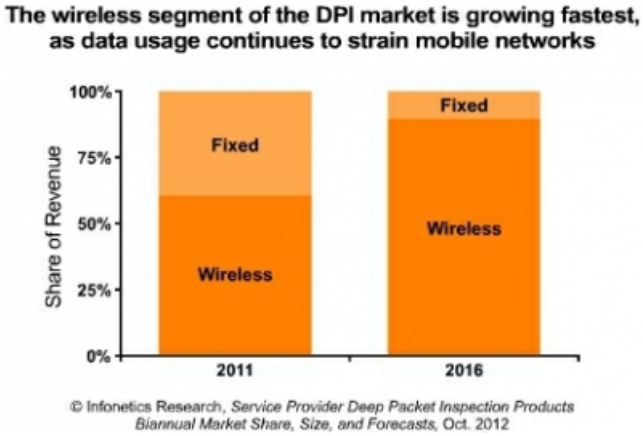
На рынке DPI много игроков: какие-то компании свои усилия направляют на совершенствование программных приложений, кто-то занят разработкой и производством аппаратной поддержки

(серверы и т.д.), кто-то может предложить специализированные чипы, кто-то внедряет и т.д.



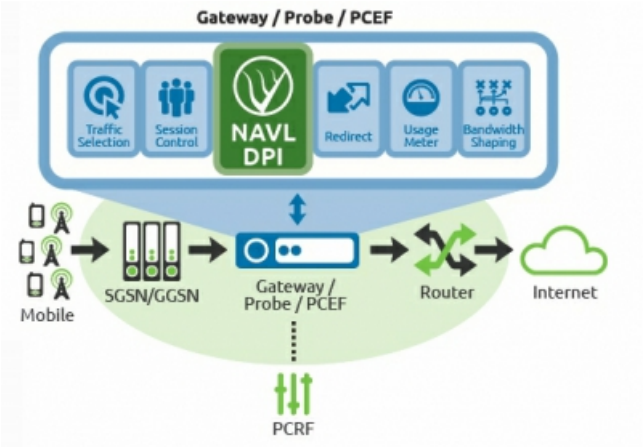
Рынок deep packet inspection (DPI) к 2016 году вырастет до 2 миллиардов долларов, по прогнозу Infonetics Research

Infonetics Research в своем отчете "Service Provider Deep Packet Inspection Products", вышедшем осенью 2012 года, пишет, что управление трафиком - это, конечно, основное "занятие" для DPI. Но наблюдается повышенный интерес к другим прикладным возможностям, таким как video optimization, content caching, usage-based billing.



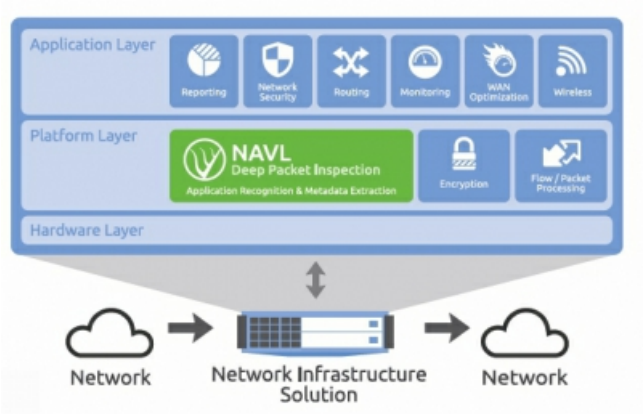
Вот так заметно изменится рынок DPI

DPI уже имеет историю, есть и прогнозы на ближайшие годы. По оценкам компании Infonetics Research рынок решений DPI в период с 2011 по 2016 год будет расти в среднегодовом темпе 34%, причем в большей степени увеличение будет касаться участников, работающих на рынке беспроводных услуг связи. Операторы мобильной связи развертывают решения на базе DPI для управления трафиком, используют при предоставлении VAS (value-added services), а также для приложений, связанных с ограничением трафика. В 2012 году компании, работающие на рынке DPI, получат доходы не менее 600 миллионов долларов.



Рынок DPI-услуг и решений - "живой" и хорошо растущий. Характерным дополнительным свидетельством, кроме вышеописанных прогнозов, является то, что там происходят изменения и среди "игроков" - сделки M&A в разных формах. Самое свежее, датируется январем этого года, когда появилось сообщение о том, что известная фирма Procera Networks "поглощает" компанию Vineyard Networks Inc, лидера на сегменте "Enterprise OEM DPI". Поглощаемая компания небольшая (34 чел),

при этом за Vineyard Networks заплатят 28 миллионов канадских долларов, частично деньгами, частично акциями. По ожиданиям Procera Networks эффект от приобретения уже будет в этом году: в виде добавки к общей выручке дополнительно ещё от 4 до 5 миллионов долларов. В своём пресс-релизе Procera Networks оценивает сегмент рынка "Enterprise OEM DPI" в 2013 году - около 300 миллионов долларов.



Из презентации Vineyard Networks

Трендами на этом сегменте будут: SDN (Software Defined Networking), "облачные" сервисы (услуги и хранение) и такое явление как "Bring Your Own Device" (BYOD). Всё большее усложнение корпоративных сетей, тесное взаимодействие с обслуживающими их операторами, новые тренды, внимание к оптимизации ИТ-затрат и различного рода ИТ-угрозы увеличивают степень интереса к DPI-решениям и в больших компаниях, не обязательно являющихся операторами.

Закончить хочу весьма красноречивой иллюстрацией из Wired:



Ближайшие годы покажут, что же всё-таки победит в Интернете: когда-то заявленная технологическая справедливость и равноправие (нельзя устраивать дискриминацию по виду трафика) или "бабло" (делаем то, что нам выгодно. "OTT к ноге"). Без свободы нет динамичного развития, но и без денег - трудно.