Методы инспекции пакетов и анализа трафика

Лекция 2
Назначение DPI и основные понятия

Фицов Вадим Владленович

ст.преп. кафедры ИКС

Содержание лекции:

- Определение DPI.
- Причины появления.
- Применение.
- Сетевой нейтралитет.
- Законодательство.
- Вендоры.

Определение DPI

Определение DPI и DPP

Deep Packet Inspection (сокр. DPI) — совокупное название технологии, позволяющей проводить накопление, анализ, классификацию, контроль и модификацию сетевых пакетов в зависимости от их содержимого в реальном времени.

Определение DPI и DPP

Иногда употребляют более узкий термин — DPP (Deep Packet Processing), который подразумевает такие действия над пакетами, как модификация, фильтрация или перенаправление.

Сегодня оба термина — DPI и DPP — часто используются как взаимозаменяемые.

Многоликий DPI

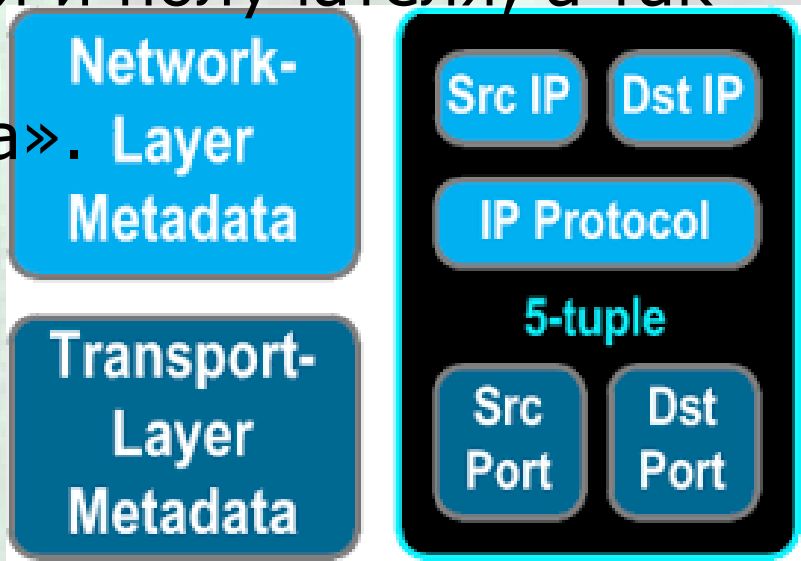
Современные решения использующие технологию DPI

7 tuples (кортеж 7)

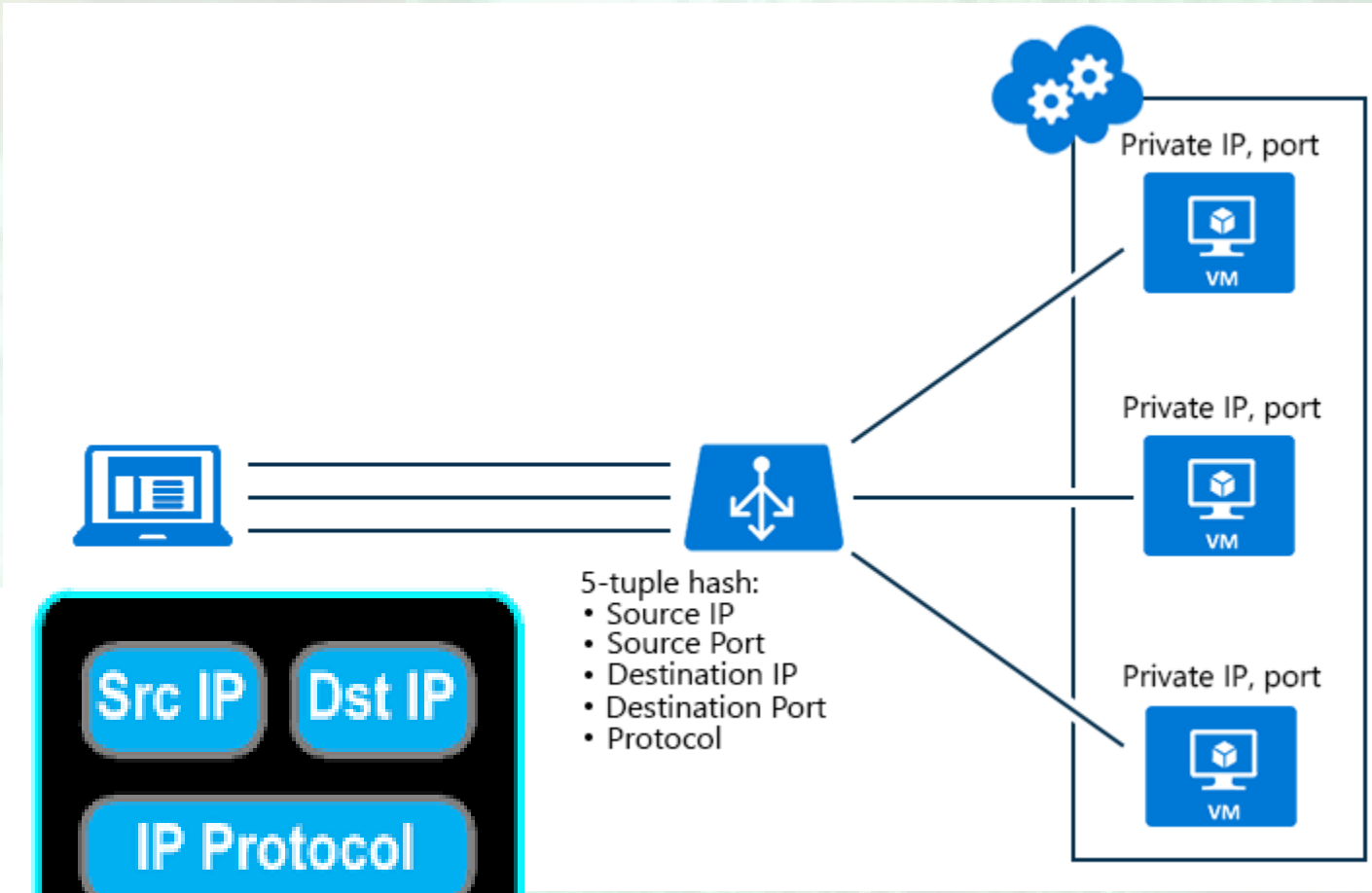
Поток идентифицируется с помощью адресной информации 2–4 уровней.

Критерии, по которым пакет относят к потоку, называют кортежем (tuple).

В кортеж может входить разное число критериев, обычно от 3 до 7: MAC-адреса отправителя и получателя, IP-адреса отправителя и получателя, транспортные порты отправителя и получателя, а так же значение
служебного поля «Тип протокола».

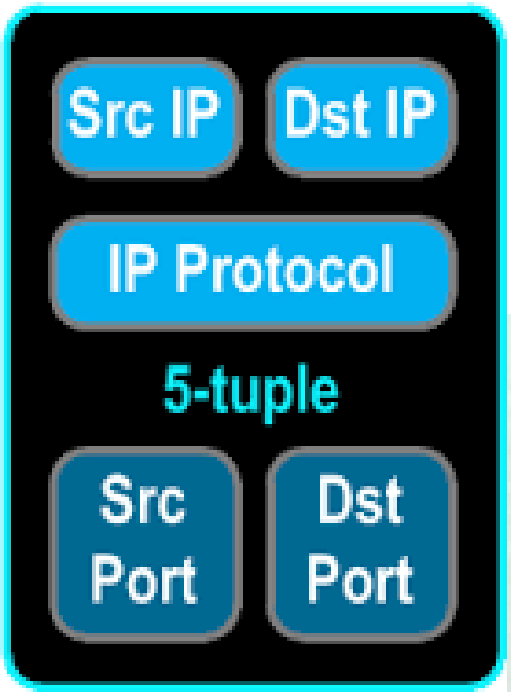


7 tuples (кортеж 7)



Network-Layer Metadata

Transport-Layer Metadata



DPI средства управления трафиком

DPI средства управления трафиком

Инструмент контроля с расширенными политиками

Помимо стандартных инструментов контроля/управления трафиком – ACL и QoS, DPI системы управления трафиком имеют их расширенный функционал – политики. Политики основаны на динамическом изменении правил в зависимости от времени, объемов того или иного трафика, поведения трафика и т.д.

Политики контроля и обработки правил могут создаваться и изменяться как администратором системы, так и быть загруженными от производителя.

Возможно применение политик на географически разобщенный кластер устройств.

В 2012 г. ITU утвердил **Y.2770**

Requirements for deep packet inspection in Next Generation Networks

(Рекомендации для глубокого пакетного анализа в сетях следующего поколения).

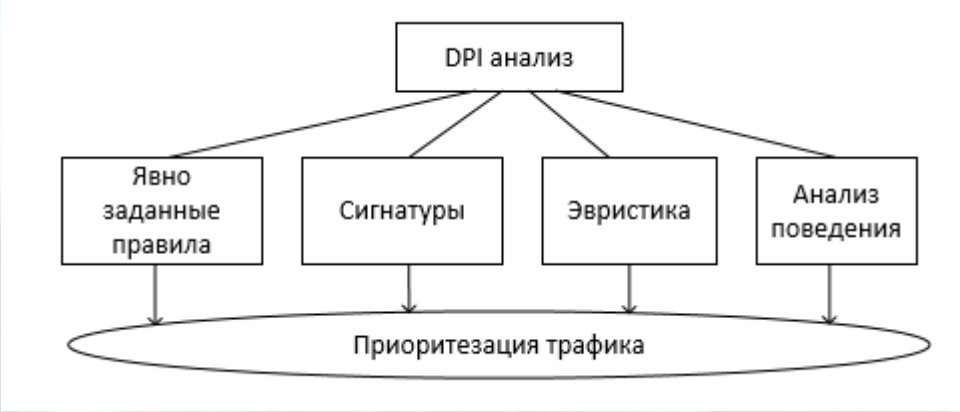
- требования к объектам глубокой инспекции пакетов (DPI)
- идентификация приложений,
- идентификация потоков,
- типы проверяемого трафика,
- управление сигнатурами,
- представление отчетов системе управления сетью (NMS, Network Management System)
- взаимодействие с функциональным объектом принятия решения в соответствии с политикой сети.

11

Что происходит при DPI?

DPI анализирует

- первые пакеты потока трафика
- или все проходящие через нее пакеты.



- Применяются:

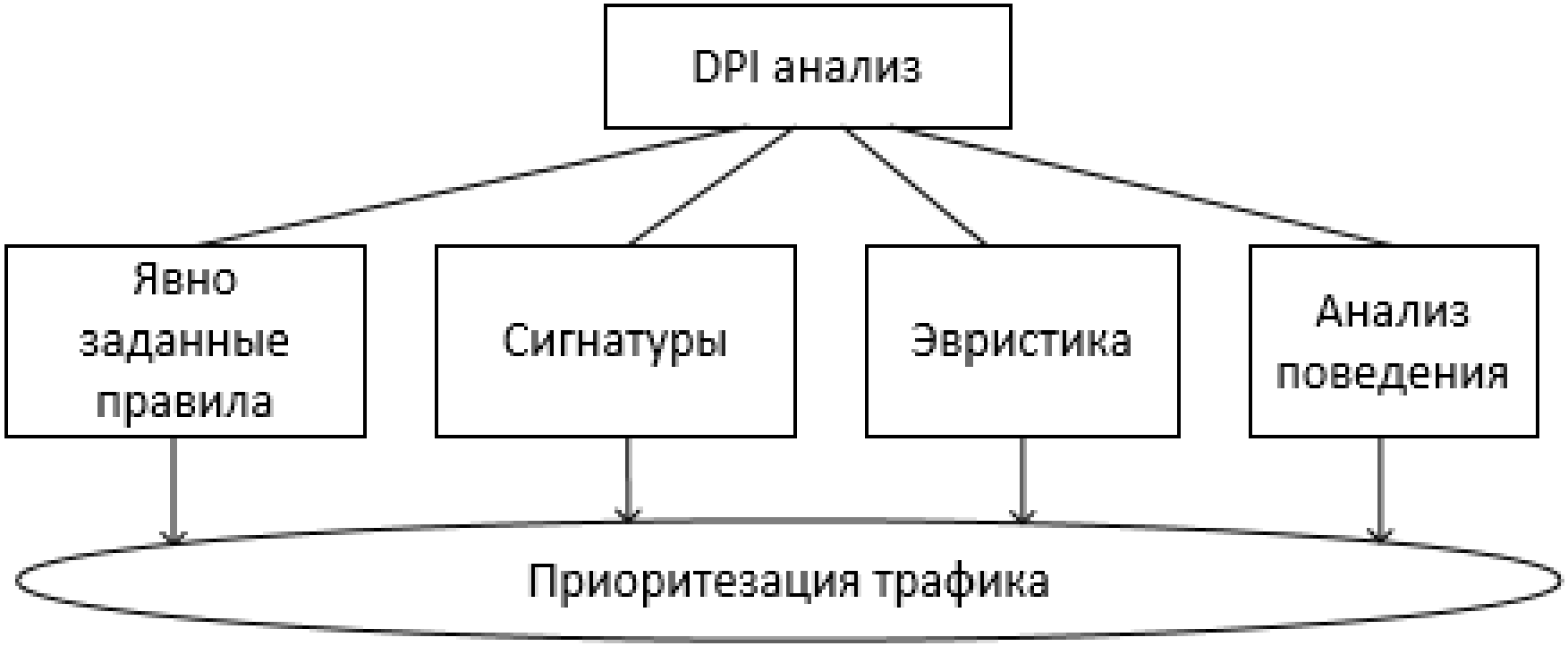
  - сигнатурный анализ,

  - статистические методы слежения за характеристиками пакетов,

  - поведенческий анализ и др.

12

Что происходит при DPI?



13

Идентификация трафика в DPI

Явно заданные правила

Явно заданные правила задаются администратором системы, полностью или частично из предоставленных наборов разработчика системы, путём активирования нужных правил.

Например, вы хотите заблокировать одну из страниц на Facebook.com. Для этого вам нужно выбрать протокол HTTP, выбрать/ввести домен Facebook.com, и ввести дополнительное условие user0165448123.

После проверки возможности блокировки, система заблокирует страницу указанного пользователя.

Что происходит при DPI?

Сигнатурный анализ пакетов:

Сигнатура – это набор байтов в пакете или файле, позволяющий однозначно определить, к какому приложению, протоколу относится трафик, и классифицировать его.

Сигнатуры разрабатываются и распространяются вендором.

Базу сигнатур необходимо обновлять автоматически или вручную.

15

Что происходит при DPI?

Сигнатурный анализ пакетов:

стандартные паттерны (например, HEX),

по которым можно однозначно определить принадлежность пакета определенному приложению.

Например:

- по формату заголовков,
- номерам портов и т. п.

16

Идентификация трафика в DPI

Эвристика

Эвристический алгоритм — это алгоритм решения задачи, правильность которого для всех возможных случаев не доказана, но про который известно, что он даёт достаточно хорошее решение в большинстве случаев.

Эвристический анализ - это технология обнаружения по признакам (без гарантированной точности). Используется, когда невозможно определить трафик с помощью сигнатурного анализа, то есть с помощью поиска и сравнения по базе сигнатур.

Объектам, обнаруженным с помощью эвристического анализа, присваивается вероятность соответствия, к примеру - 85%.

Совместное использование с другими методами анализа позволяет увеличить точность общей идентификации трафика.

Что происходит при DPI?

Поведенческий анализ трафика:

распознает приложения, без заранее известных заголовков и структуры данных.

Например – BitTorrent.

Применяется анализ последовательности пакетов, принадлежащих к одному потоку.

18

Поведенческий анализ трафика

- транспортные порты отправителя и получателя,
- размер пакета,
- частота открытия новых сессий в единицу времени…

Существует множество поведенческих моделей соответствующих протоколов и приложений.

Точность определения различается.

19

DPI выявляет приложения, использующие:

- закрытые проприетарные протоколы
- с гибким выбором транспортных портов
- встроенными механизмами преодоления NAPT (Network Address Port Translation).

Для их определения нельзя ограничиться номером протокола в заголовке IP и номерами портов в заголовке протокола транспортного уровня.

20

DPI средства управления трафиком

Суммарное использование различных методов анализа позволяет значительно увеличить точность идентификации трафика

DPI
Анализ

Явно заданные правила

Сигнатуры

Эвристика

Анализ поведения

Классификация трафика

Причины появления DPI

Классические методы маркировки

DS5	DS4	DS3	DS2	DS1	DS0	ECN	ECN

Код DSCP — 6 бит (DS5-DS0)

ECN – явн. увед. о пер.(2 бита)

Рис.5 Структура поля DiffServ

Метка	EXP	S	TTL
20	3	1	8

Метка

EXP – поле эксп. битов

S – ср. подд. Иер. Стр. ст. меток

TTL – время жизни

Рис.6 Заголовок метки MPLS

TPID	Priority	CFI	VID
16	3	1	12

TPID – ид. пр. маркировки

Priority – приоритет

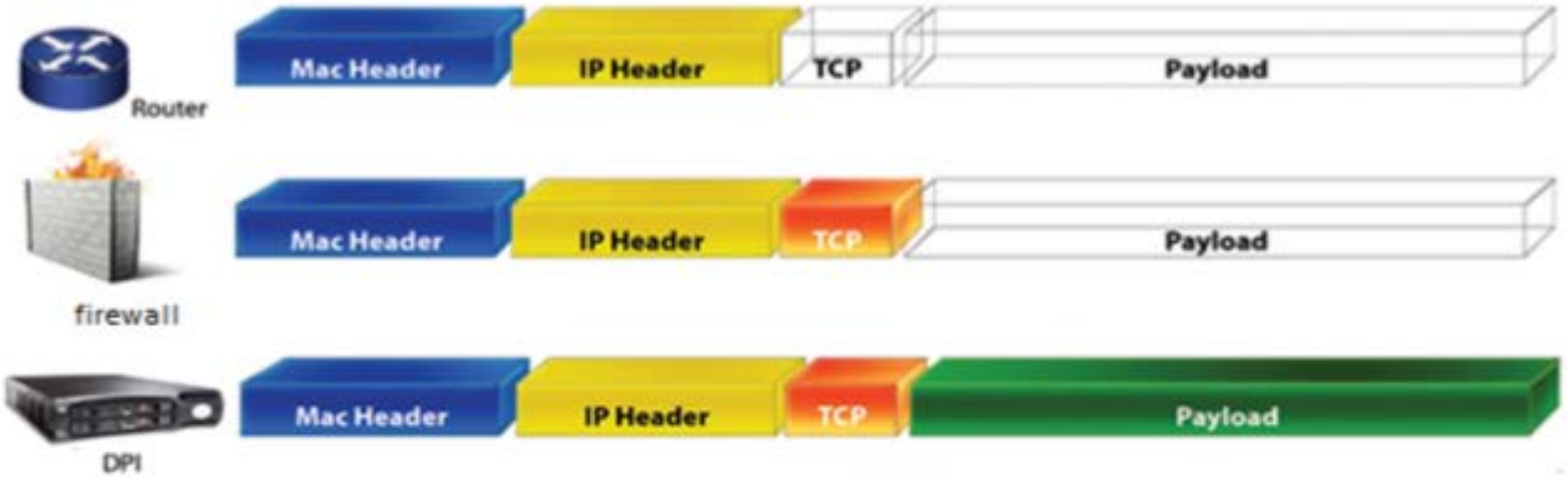
CFI – инд. канон. формата

VID – идент. виртуальной сети

Рис.7 Структура метки VLAN

Обеспечения QoS

- Классификация трафика
- Маркирование трафика
- Управление очередями
- Резервирование и профилирование

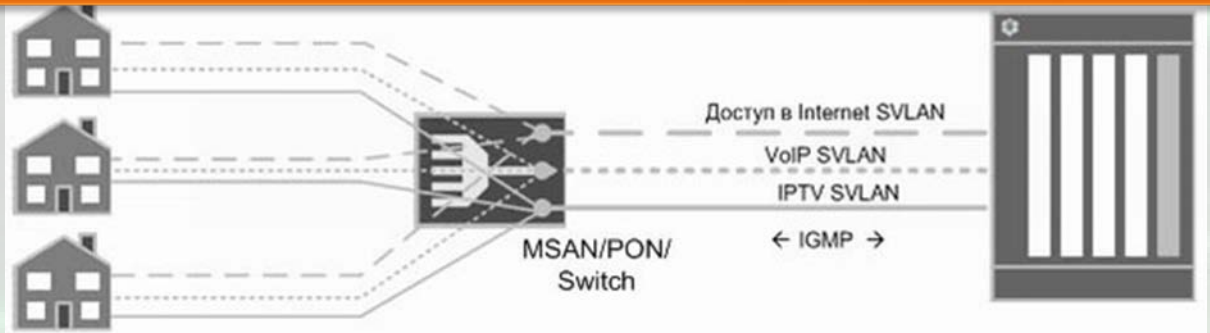

Router
Mac Header
IP Header
TCP
Payload
firewall
Mac Header
IP Header
TCP
Payload
DPI
Mac Header
IP Header
TCP
Payload

- DiffServ
- SPI
- Port-based
- URL-filter
- MPI
- Lightweight Packet Inspection
- Deep Packet Inspection
- Data Mining

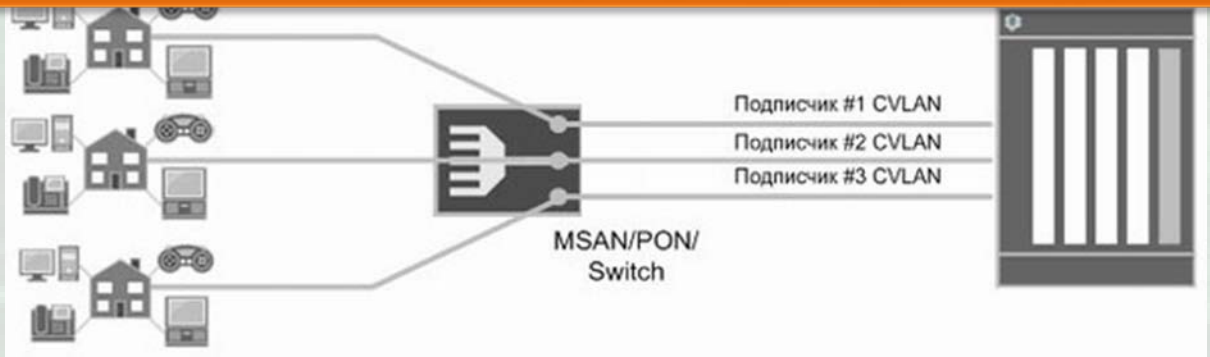
26

РАЗЛИЧНЫЕ МОДЕЛИ VLAN

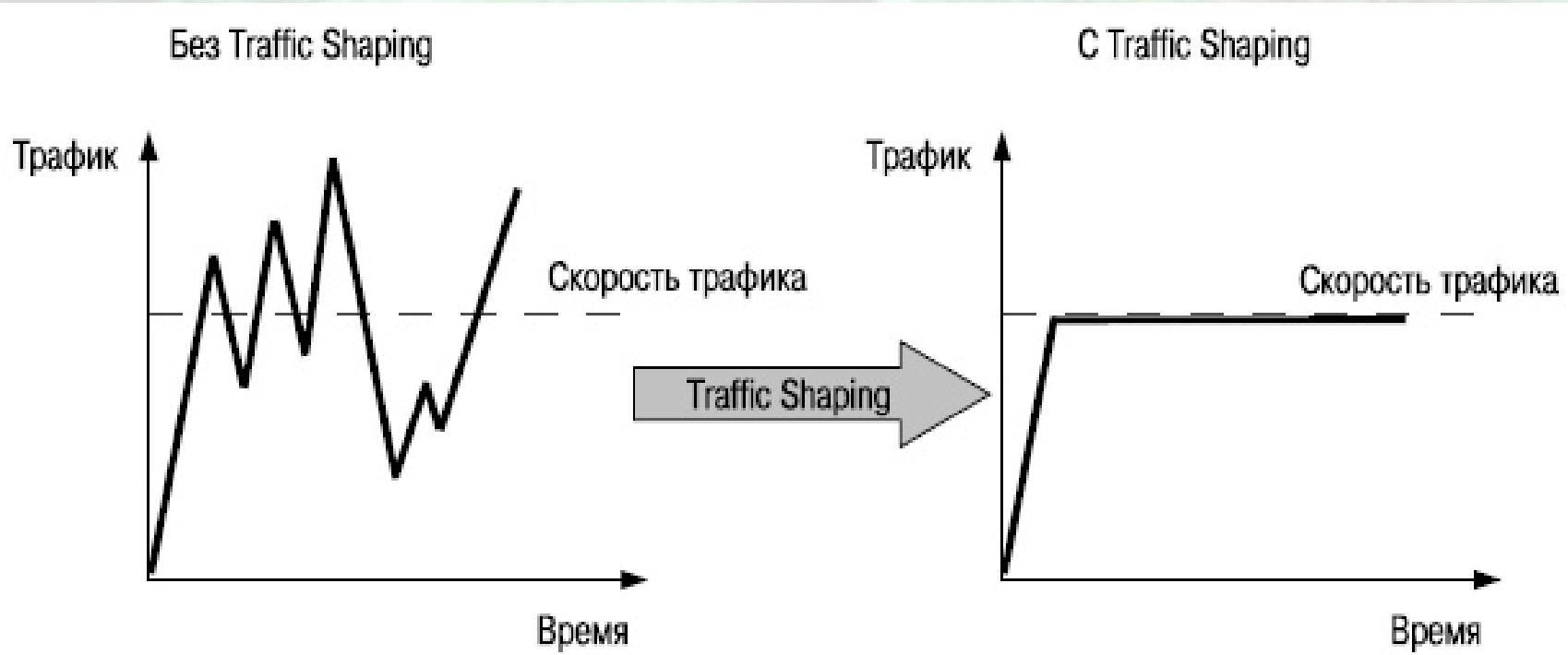
Сервисный VLAN (S-VLAN) - каждая услуга находится в своем VLAN



Клиентский VLAN (C-VLAN) - каждый абонент находится в своем VLAN




Без Traffic Policing
Трафик
Скорость трафика
Время
Traffic Policing
С Traffic Policing
Трафик
Скорость трафика
Время


Без Traffic Shaping
Трафик
Скорость трафика
Время
Traffic Shaping
С Traffic Shaping
Трафик
Скорость трафика
Время

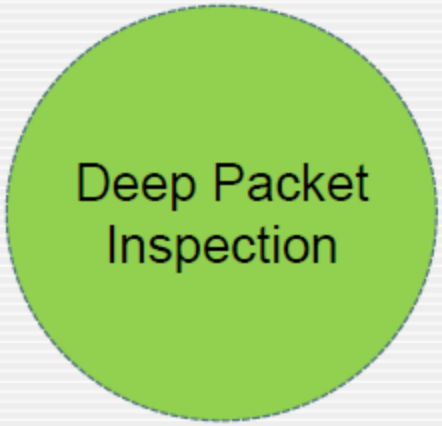
Анализ результатов исследования алгоритма PortLoad

	Точность опр-я **приложения**	Точность опр-я **категории** приложения
Port-based	19,57%	15,95%
PortLoad	74,24%	73,88%

PortLoad - анализ первых неск. байт данных

История развития DPI

Глубокий анализ пакетов



Технология DPI возникла из-за необходимости анализировать, контролировать и управлять передаваемым трафиком. Технология DPI получила развитие, прежде всего, из-за стремительного роста вычислительных способностей чипов (процессоров), их быстродействия.

Внедрение DPI

Три основных причины внедрения DPI

Применение DPI

Внедрение DPI

Основные направления применения DPI систем управления трафиком

Внедрение DPI

Сейчас большинство операторов не блокируют конкурирующие сервисы VoIP, IPTV и теряют на этом как минимум сумму равную стоимости утилизации своих каналов связи. Таким образом, пропуская бесплатно ЁМКИЙ риал-тайм трафик внешних сервисов, оператор связи наносит себе экономический ущерб, из-за необходимости практически гарантированно на длительное время выделять необходимую полосу.

Оператор должен зарабатывать на своих сервисах!

DPI системы управления трафика позволяют не только ограничивать подобный трафик, но и управлять им помогая реализовать его как дополнительные сервисы.

DPI-решения управления трафиком в большинстве случаев позволяют снизить нагрузку на сеть от 25 до 50 %.

За счет управления, ограничения и оптимизации трафика P2P приложений, потоковых аудио- и видеосервисов.

Для мобильных операторов системы DPI позволяют контролировать загруженность каждой базовой станции путем распределения ресурсов базовых станций

35

С помощью DPI-систем управления трафиком возможно отслеживание и блокирование источников того или иного контента в сети.

Маркировка цифрового контента позволяет устанавливать источники утечки и распространения нелегальной цифровой продукции.

Технологии цифровой маркировки информации широко используется правообладателями и распространяющими компаниями

36

Системы DPI могут использоваться как инструмент для статистического анализа и проверки маркетинговых проектов, которые осуществляют операторы или их клиенты.

Маркетологам исследование трафика позволяет выстраивать политику продаж, повышать эффективность тарифных планов и, как следствие, планировать доходы и расходы.

Большую популярность набирает вставка персонализированной рекламы на основе выявленных предпочтений пользователя.

37

Управление трафиком может состоять из следующих компонент:

- управление полосой пропускания,
- управление перегрузками,
- фильтрация трафика,
- переадресация,
- перенаправление трафика,
- блокировка атак,
- СОРМ.

38

Перенаправление трафика:

- переадресовывать HTTP-трафик на рекламные порталы для перехода к частичной или полной «рекламной» модели: абонент за некоторую скидку просматривает на портале рекламу партнерских компаний/участвует в социологических опросах и т. п.
- при попытке доступа к запрещенному URL или при окончании средств;

подменяется содержимое страниц при попытке получить нелегальный контент и/или переадресовывать на партнерские порталы распространения аналогичного легального контента.

39

Внедрение DPI

Для кого?

DPI система, установленная у оператора связи, имеет прямое или косвенное влияние на всех участников единой сети передачи данных, так как оптимизированный/ освобожденный ресурс сети может быть распределён между другими типами абонентов.

Сетевой нейтралитет

41

выявление ***P2P*** трафика

Сетевой нейтралитет

Возможность приоритизации одних и блокировки других потоков трафика (или трафика к конкретным услугам) может ущемлять права абонентов.

А компании, предоставляющие контент, не хотели бы отдельно оплачивать высокоскоростной доступ пользователей к их серверам.

Такое решение обусловлено технологиями мультисервисных сетей. Сетевой нейтралитет вредит качеству предоставляемых услуг. Технически оператор связи не может применить сетевую нейтральность к такой услуге, как HD IPTV.

Сетевой нейтралитет

- В **США** директива Федеральной комиссии по связи (FCC) о сетевом нейтралитете, действующая с 2010 г., была отменена в январе 2014 г. Но уже в феврале 2015 г. был подготовлен коммуникационный акт № 1934 (раздел II), предполагающий компромиссный подход к сетевому нейтралитету. Его правила вступили в действие в июне 2015 г. В частности, операторам связи запрещается предлагать приоритетный доступ за дополнительную плату.
- В 2017г FCC отменила сетевой нейтралитет в США.
- В 2018г Калифорния ввела сетевой нейтралитет.

Сетевой нейтралитет

- **Европарламент** в апреле 2014 г., наоборот, принял пакет законов о реформе телекоммуникационной отрасли.
- В нем, в том числе, был сформулирован принцип сетевой нейтральности, а также указана необходимость его выполнения (поправки 234 — 236).
- Однако Совет Европейского Союза в мае 2015 г. исключает это понятие полностью из итогового документа, утвержденного 6 июля 2015 г.

Сетевой нейтралитет

- В РФ в 2009 г. МегаФон и ТТК инициировали разбирательство ФАС относительно принципов сетевой нейтральности.
- Антимонопольный комитет считает, что операторы имеют право управлять трафиком, но публично и без дискриминации других участников рынка.
- Билайн самостоятельно прекратил применять ограничения по типу трафика и использует DPI для прогнозирования уровня загрузки каналов и повышения качества услуг.
- Важен п.27 Постановления 575 от 2007 (2008) гг

Конфиденциальность

Существует техническая возможность DPI систем анализировать передаваемую информацию (например текст письма электронной почты)

в режиме реального времени, что может восприниматься как потенциальное нарушение тайны переписки.

(см. Конституцию РФ и ФЗ-126 гл.9 ст.63)

Конфиденциальность

Технология поведенческого таргетинга

BT (Behavioral Targeting) на основе анализа взаимодействия между сайтами сети Интернет.

Путем применения переменных в ссылках на другие сайты или javascript-указаний, либо посредством запросов данных, хранящихся в веб-браузере (cookies), собирается информация о посещенных страницах.

Все эти данные собираются в профиль интересов пользователя, могут продаваться и использоваться для таргетированной рекламы.

Конфиденциальность

Технология поведенческого таргетинга

BT (Behavioral Targeting)

Средства DPI позволяют сделать поведенческий таргетинг более точным и всеобъемлющим.

Провайдеры, применяющие DPI, могут не только собирать информацию, но и внедрять в проходящий трафик рекламу.

Законодательство

Правовая часть DPI

Правомерность использования DPI систем в РФ

Упрощенная структура правовой системы РФ

Правовая часть DPI

Конституция РФ

Конституция Российской федерации – высший нормативный правовой акт РФ.

Глава 2. Права и свободы человека и гражданина

Статья 23

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.
2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Статья 24

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.
2. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 29

1. Каждому гарантируется свобода мысли и слова.
2. Не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненавист и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства.
3. Никто не может быть принужден к выражению своих мнений и убеждений или отказу от них.
4. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законны способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом.
5. Гарантируется свобода массовой информации. Цензура запрещается.

Правовая часть DPI

Федеральные законы

N 126-ФЗ
Глава 9. ЗАЩИТА ПРАВ ПОЛЬЗОВАТЕЛЕЙ УСЛУГАМИ СВЯЗИ
Статья 63. Тайна связи

1. На территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи.

Ограничение права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных федеральными законами.

2. Операторы связи обязаны обеспечить соблюдение тайны связи.

3. Осмотр почтовых отправлений лицами, не являющимися уполномоченными работниками оператора связи, вскрытие почтовых отправлений, осмотр вложений, ознакомление с информацией и документальной корреспонденцией, передаваемыми по сетям электросвязи и сетям почтовой связи, осуществляются только на основании решения суда, за исключением случаев, установленных федеральными законами.

4. Сведения о передаваемых по сетям электросвязи и сетям почтовой связи сообщениях, о почтовых отправлениях и почтовых переводах денежных средств, а также сами эти сообщения, почтовые отправления и переводимые денежные средства могут выдаваться только отправителям и получателям или их уполномоченным представителям, если иное не предусмотрено федеральными законами.

ФЗ-139 от 2012г

Одним из факторов применения средств анализа HTTP-протокола стал

139 Федеральный Закон от 2012 г., вносящий изменения в Закон «О защите детей от информации, причиняющей вред их здоровью и развитию» **(«белый» список**).

Также имеется **поправка** к **ФЗ-149** (2006г)«Об информации, информационных технологиях и о защите информации»,

«черного» списка сайтов,

направленного на «борьбу с противоправным контентом в Интернете» и защиту детей.

В единую базу должны вноситься веб-ресурсы с запрещенным содержанием, а именно – пропагандой наркотических, психотропных веществ, детской порнографией, призывами к самоубийству.

Правовая часть DPI

Федеральные законы

Федеральный закон от 28.07.2012 N 139-ФЗ
"О внесении изменений в Федеральный закон
"О защите детей от информации, причиняющей вред их здоровью и развитию"
и отдельные законодательные акты Российской Федерации"

(Статьи 2 и 3 настоящего Федерального закона вступают в силу с 1 ноября 2012 года.)

Статья 2

Статью 46 Федерального закона от 7 июля 2003 года N 126-ФЗ "О связи" (Собрание законодательства Российской Федерации, 2003, N 28, ст. 2895; 2007, N 7, ст. 835; 2010, N 7, ст. 705; N 31, ст. 4190) дополнить пунктом 5 следующего содержания:

5. Оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", обязан осуществлять ограничение и возобновление доступа к информации, распространяемой посредством информационно-телекоммуникационной сети "Интернет", в порядке, установленном Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации"

Правовая часть DPI

Федеральные законы

Статья 3

10. В течение суток с момента включения в реестр сетевого адреса, позволяющего идентифицировать сайт в сети "Интернет", содержащий информацию, распространение которой в Российской Федерации запрещено, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", обязан ограничить доступ к такому сайту в сети "Интернет".

Примечание: Текст пункта 11 приведен в соответствие с публикацией в "Собрании законодательства РФ", 30.07.2012, N 31, ст. 4328 и на Официальном интернет-портале правовой информации http://www.pravo.gov.ru, 30.07.2012.

В "Российской газете", N 172, 30.07.2012 фрагмент текста пункта 11 после слов "...либо на основании вступившего в законную силу решения суда об отмене решения..." опубликован в следующей редакции:

"...уполномоченного Правительством Российской Федерации федерального органа исполнительной власти о включении в реестр доменного имени, указателя страницы сайта в сети "Интернет" или сетевого адреса, позволяющего идентифицировать сайт в сети "Интернет".

Постановление Пр-ва РФ 575 от 2007г (2008г)

П.27 Осуществлять ограничение отдельных действий … пользователя, если такие действия создают угрозу для нормального функционирования сети связи.

Правовая часть DPI

Отраслевые постановления и акты

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОСТАНОВЛЕНИЕ
от 10 сентября 2007 г. N 575
ОБ УТВЕРЖДЕНИИ ПРАВИЛ
ОКАЗАНИЯ ТЕЛЕМАТИЧЕСКИХ УСЛУГ СВЯЗИ
(в ред. Постановления Правительства РФ от 16.02.2008 N 93)
В действии с 1 января 2008 г.

26. Оператор связи обязан:

и) исключить возможность доступа к информационным системам, сетевые адреса или унифицированные указатели которых абонент сообщает оператору связи в предусмотренном договором виде.

27. Оператор связи вправе:

приостанавливать оказание телематических услуг связи абоненту и (или) пользователю в случае нарушения абонентом и (или) пользователем требований, предусмотренных договором, а также в случаях, установленных законодательством Российской Федерации;

осуществлять ограничение отдельных действий абонента и (или) пользователя, если такие действия создают угрозу для нормального функционирования сети связи.

Правовая часть DPI

Международные акты и соглашения

После обсуждения за закрытыми дверьми эксперты Международного союза электросвязи (МСЭ), в который входит и Россия, утвердили стандарт (рекомендации) Y.2770 на применение технологий Deep Packet Inspection.

Представители России и некоторых других стран предлагают сделать этот стандарт обязательным для интернет-провайдеров.

В текущей редакции документа, технические спецификации Y.2770 не предусматривают инспекции зашифрованного трафика, но предусматривают обязательную инспекцию незашифрованных фрагментов такого трафика.

Несмотря на то, что 6 декабря 2012 года на блоге МСЭ было опубликовано сообщение, что ситуация взята под контроль и утвержденный стандарт Y.2770 не разрешает доступ к личной информации пользователей, вероятность того, что DPI не будет применяться для обработки личной информации, исключить нельзя.

Нужно учитывать, что указанный стандарт теперь является официально разрешенным на территории стран-участниц МСЭ, что дает властям право использовать его.

Вендоры

DPI в РФ

Внедрение систем DPI в России - 2004 г.

компания RGRCom

(дистрибьютор DPI Allot, PeerApp и OverSi)

впервые поставила систему DPI для ТТК.

61

DPI в РФ

Широкое распространение DPI началось в конце 2000-х годов.

Силами Inline Telecom, Allot, Cisco, Procera, Juniper, Huawei и отечественных Traffica и НТЦ Протей

системы DPI были внедрены в сетях “большой тройки”, Ростелекома и др.

К этому времени объем трафика, приходящегося на **P2P** протоколы (например, Skype и bit-torrent), в том числе для аудио- и видеофайлообмена,

достигал уже порядка **80 % от всего трафика**.

62

DPI в РФ

Установка DPI решений в сетях подвижной связи и Ростелекома - 2012 г.

- бурное распространение USB-модемов,
- ФЗ-139.

63

DPI в РФ

кипрская компания iMarker с 2010 г. предлагает интернет-провайдерам бесплатную установку систем DPI (Gigamon, Xterica) с последующей таргетированной рекламой.

Система поведенческого таргетинга (BT) получает информацию обо всех сайтах, посещаемых пользователями, и на основе этого может предложить им персонализированную рекламу.

Она применяется у 11 операторов, включая филиалы Ростелекома.

64

DPI в РФ

Технология DPI используется в решениях СОРМ

в Китае и странах Ближнего Востока (Cisco, Verint, Narus, НТЦ Протей, Verso Technologies),

а также в России (НТЦ Протей, Малвин, МФИ-Софт)

65

DPI в РФ

- Летом 2014 г. МГТС внедрила DPI от Procera Networks (PL10024), предоставив абонентам услуги по детализации трафика и персональному черному списку web-страниц.

- Yota внедряет комплекс динамического управления трафиком на основе DPI (Procera)

с целью не допустить критических перегрузок на сети путем превентивных мер по оптимизации трафика

в С.-Петербурге, Москве, Сочи, Самаре, Краснодаре, Владивостоке и Новосибирске.

На сети соблюдался принцип приоритета интерактивных услуг и обеспечения стабильности работы остальных приложений при любых изменениях интенсивности трафика.

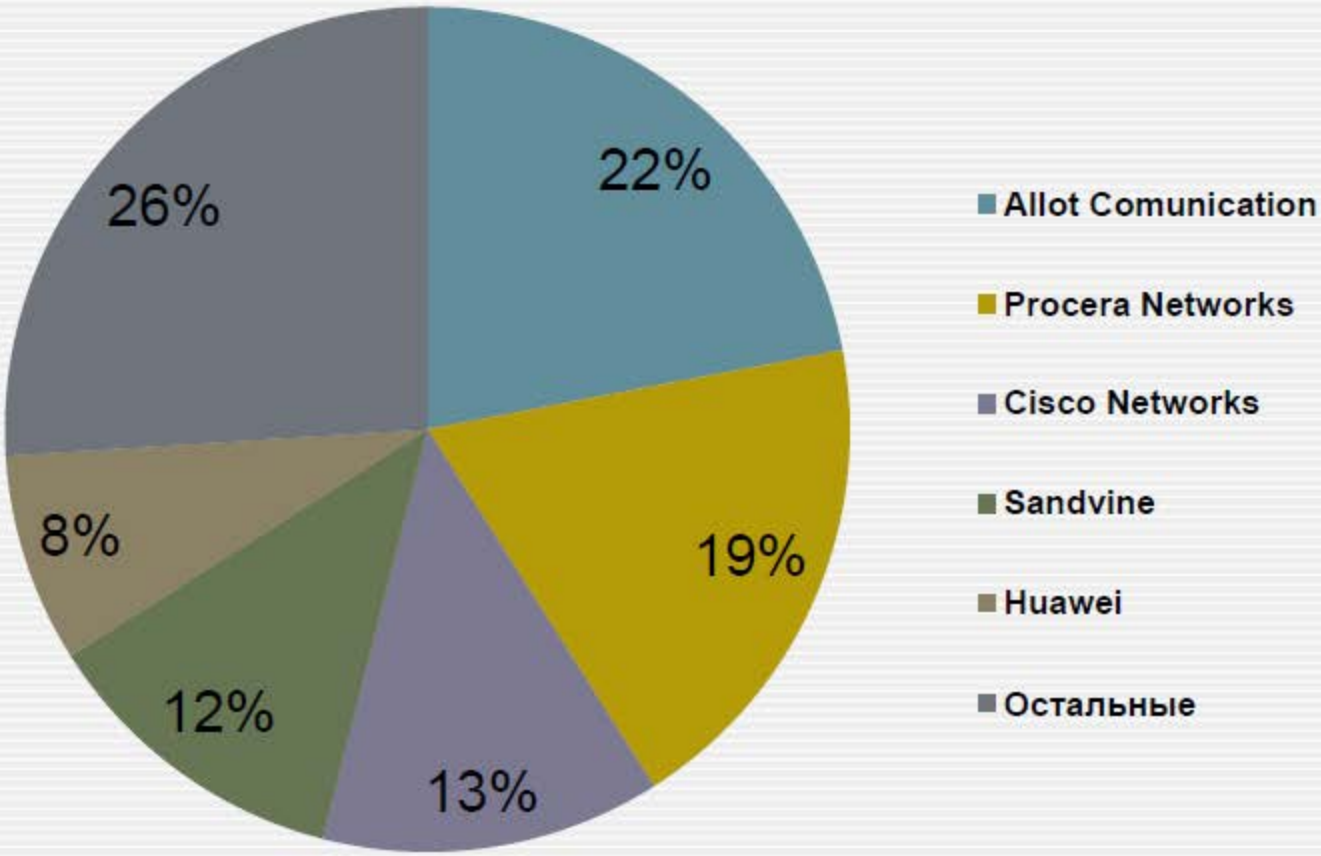
В результате удалось отказаться от постоянного расширения внешних каналов связи, повысить емкость сети и снизить капитальные затраты.

66

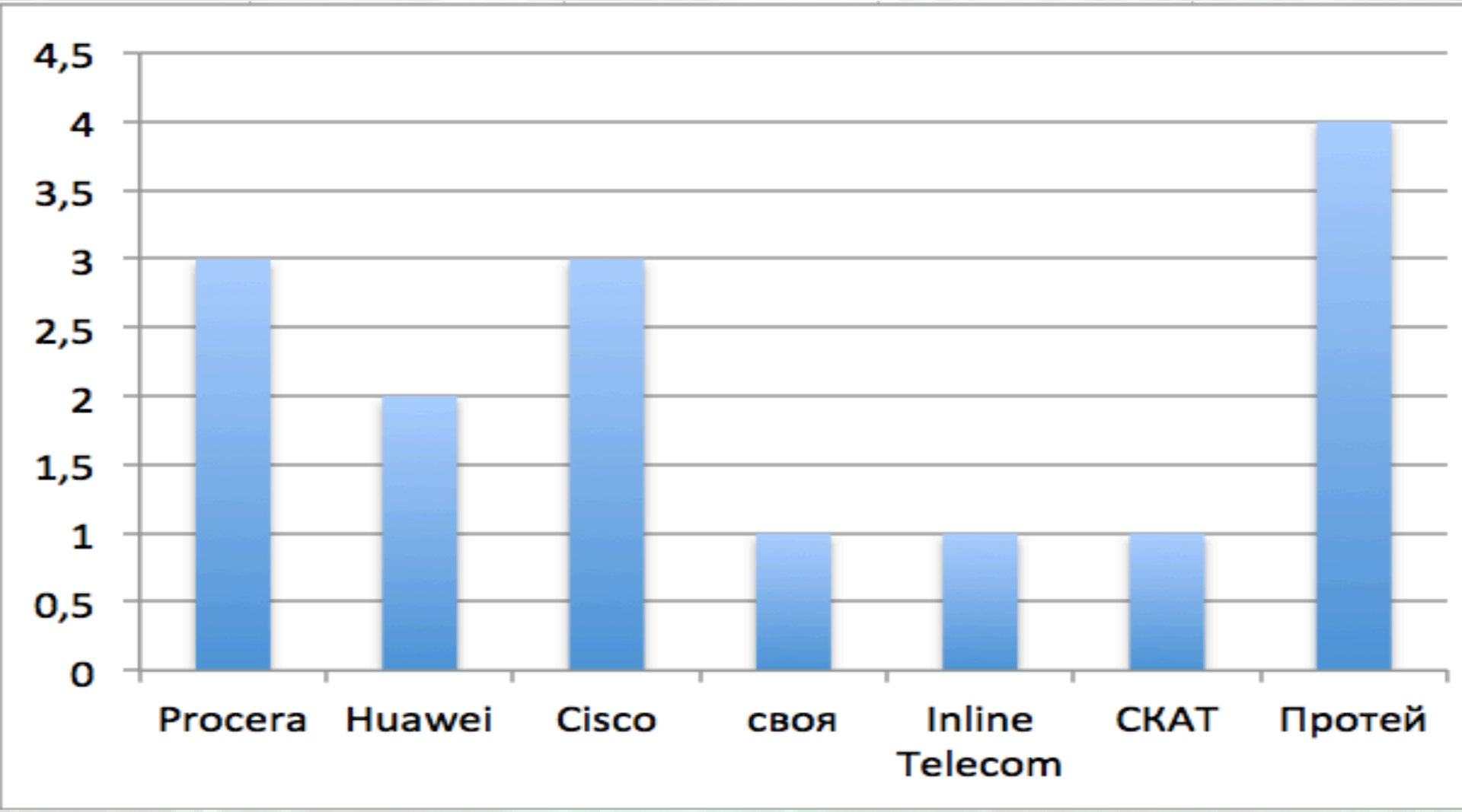
Основные производители DPI систем

Диаграмма:

Основные производители DPI систем управления трафиком и их доли на рынке



Гистограмма количества упоминаний вендоров по производителям



DPI решения основных производителей

Производитель	Головной офис компании (Hi Support)	Наименовании линейки оборудования	Серии	Модельный ряд (актуальные модели)
Allot Comunication	Израиль	NetEnforcer, SG Sigma, SG Sigma E	AC, Sigma E	AC-500, AC-1400, AC-3000, AC-5000, AC-10000, Sigma E14, Sigma E6
Procera Networks	Канада	PacketLogic™	EDGE, ACCESS, CORE	EDGE - PL7810, ACCESS - PL8720, PL8820, PL8920, PL8960, CORE - PL10024, PL20000
Cisco Networks	США/Китай	SCE (Service Control Engine)	SCE 8000	SCE 8000
Sandvine	Канада	PTS (Policy Traffic Switch)	PTS 22000, PTS 24000	PTS 22050, PTS 22100, PTS 22600,PTS 22000 Cluster, PTS 24500, PTS 24700, PTS 24000 Cluster
Huawei	Китай	SIG (Service Inspection Gateway)	SIG9800	SIG9810, SIG9820

69

Вендор	Система	Страна	Дистрибьютер
Sandvine	(PTS XXXXX)	Канада	Inline Telecom
Allot	NetEnforcer, SG Sigma (AC-XXXX, Sigma EXX)	Израиль	RGRCom, Inline Telecom, NVision Group
Cisco	Service Control Engine (SCE-XXXX)	США	Inline Telecom, NVision Group, Микротест
Procera	PacketLogic (PL-XXXX)	США	Web Control
Juniper	(VXAXXXX)	США	Микротест
Huawei	Service Inspection Gateway (SIGXXXX)	Китай	NVision Group
НТЦ Протей	DPI	Россия	–
Arbor (Ellacoya)	eSeries EXXX	США	NVision Group, Микротест
VAS Experts	СКАТ	Россия	ИТ-ГРАД
Traffica	Monitorium	Россия	–
Palo Alto Networks	Palo Alto (PA-XXXX)	США	AXXTEL

Обзор оборудования

Производитель	Количество обрабатываемых протокол/приложений	Сигнатурный анализ	Эвристический анализ	Поведенческий анализ	VAS
Allot Comunication	Более 1500	Да	Да	Да	Да
Procera Networks	Более 1500	Да	Да	Да	Да
Cisco Networks	Около 1500	Да	Да	Частично	Частично
Sandvine	Более 1000	Да	Да	Да	Да
Huawei	Около 1000	Да	Да	Частично	Да

СПО (OpenDPI)

- Надстройки для межсетевого экрана: L7-filter и IPP2P.

- Эти механизмы легли в основу проекта OpenDPI, распространяемый по лицензии LGPLv3, построенного на коде коммерческого продукта PACE, который разрабатывался компанией Ipoque.
- OpenDPI был модулем для iptables и умел фильтровать большое количество различных типов пакетов. Проект прекратил свое существование в 2011 году.
- Компания Ntop, на базе исходников OpenDPI, создала nDPI.
- Из исходников nDPI, создали модуль для iptables, таким образом, восстановив проект OpenDPI

СПО (OpenDPI)

- Проект IPP2P более не поддерживается и, в качестве замены, предлагает использовать именно OpenDPI.
- IPP2P создавался для определения p2p трафика.
- OpenDPI поддерживает идентификацию 170 протоколов/приложений).
- OpenDPI изначально спроектирован для очень низкого уровня ложных положительных срабатываний.
- OpenDPI (в отличие от L7-filter) не требует наложения патчей на iptables и ядро; работает в виде модуля ядра и библиотеки xtables.
- Определение протоколов представляют собой не список регулярных выражений, а модули на C, что повышает быстродействие.

73

СПО (OpenDPI)

Основными недостатками таких продуктов являются:

- Ограниченность производительности (2-5 Гбит/с)
- Низкая надежность
- Отсутствие масштабируемости решений
- Отсутствие кластеризации и общих политик управления
- Отсутствие обновления сигнатур и политик
- Отсутствие тех. поддержки

74

Allot


Allot NetEnforcer
Allot Service Gateway
Speed
160G
60G
16G
8G
2G
400M
Cost Effective
10G Links
SG-Sigma
SG-Sigma E
AC-6000
AC-3000
AC-1400
AC-500
Common Allot Operating System and Feature Set

Allot

Распознавание пользователей:

DART может определять пользователей, которые генерируют трафик.

Например, оператор может определить, что определенный пользователь пользуется сервисом YouTube, со своего ноутбука,

в то время, как другой пользователь совершает звонок с помощью Skype со своего мобильного телефона.

Масштабирование сетевой производительности DART – это технология интегрированная в платформы NetEnforcer и SigmaE, которые масштабируются по производительности от 10Mbps до 160Gbps

76

Allot

Функционал решений NetEnforcer и Sigma E:

- Allot VideoClass – интеллектуальная оптимизация передачи видеоконтента
- Allot MediaSwift – кэширование данных и акселерация трафика
- Allot ServiceProtector – детектирование и блокирование аномального трафика
- Allot WebSafe – URL фильтрация
- Allot Proactive Analytics – многоуровневый анализ веб-трафика и поведения пользователей

Procera


1RU PL7810
11xGE channels
5 Gbps, 4M flows
2RU PL8720
8x10GE / 16xGE channels
15 Gbps, 8M flows
EDGE
ACCESS
CORE
14RU PL20000
Up to 36x10GE, 2x100GE
320 Gbps, 120M flows
2RU PL8820
8x10GE / 16xGE channels
30 Gbps, 20M flows
2RU PL8920
12x10GE / 24xGE channels
50 Gbps, 20M flows
2RU PL8960
12x10GE / 24xGE channels
70 Gbps, 20M flows
13/14RU PL10024
6x10GE / 8xGE channels
120 Gbps, 120M flows

78

Sandvine

	PTS 22000				PTS 24000		
	PTS 22050	PTS 22100	PTS 22600	Cluster	PTS 24500	PTS 24700	Cluster
Form Factor / Rack Space	2 RU	2 RU	2 RU	12 RU	4 RU	4 RU	24 RU
Max. Intersection Capacity	10 Gbps	10 Gbps	40 Gbps	240 Gbps	160 Gbps	160 Gbps	480 Gbps
Max. Inspection Throughput	4 Gbps	10 Gbps	40 Gbps	240 Gbps	80 Gbps	160 Gbps	480 Gbps
Max. New Flows per Second	50,000	100,000	200,000	1,200,000	1,500,000	2,000,000	9,000,000
Max. Concurrent Flows	2,000,000	4,000,000	16,000,000	96,000,000	50,000,000	72,000,000	270,000,000
10 GE Ports/RU	11	11	11	11	4	4	4
Max. Intersection/RU	5 Gbps	5 Gbps	20 Gbps	20 Gbps	40 Gbps	40 Gbps	20 Gbps
Max. Inspection/RU	2 Gbps	5 Gbps	20 Gbps	20 Gbps	20 Gbps	30 Gbps	20 Gbps
Max. New Flows Per Second/RU	25,000	50,000	100,000	100,000	375,000	500,000	375,000
Max. Concurrent Flows/RU	1,000,000	2,000,000	8,000,000	8,000,000	12,500,000	18,000,000	12,500,000

79

Cisco (SCE 2-30Gbps)

NBAR (Network Based Application Recognition) – механизм используемый в сетях передачи данных для распознавания потока данных (dataflow).
NBAR, который позволял классифицировать более 150 приложений, использующих статические порты.
NBAR2 – с методом DPI - более 1500 приложений

Классифицировав приложения, можно применить политики QoS для них, например, ограничить полосу пропускания для трафика bittorrent или перемаркировать поля DSCP для youtube.

80

Cisco (SCE 2-30Gbps)

Политики QoS позволяют обеспечить контроль полосы пропускания для классифицированных приложений.

При помощи технологии PfR (Performance Routing) также можно реализовать контроль маршрутов приложений с учётом информации о состоянии и метриках производительности каналов связи (потери пакетов, загрузка канала, задержки и jitter) в режиме реального времени.

81

Huawei

SIG9810

SIG9820

82

VAS-Experts СКАТ (в Бонче)

- Детектирует более 6000 протоколов,
- управляет абонентами с динамическим IP
- поддерживает несколько видов Netflow.
- сбор и анализ статистики,
- фильтрация запрещенных сайтов,
- оптимизация uplinks,
- приоритизация трафика,
- уведомление абонентов и др.

83

Протей-DPI

- Поддержка более 2700 протоколов и более 6000 параметров протоколов.

- Детектирование трафика уровня приложений на основе сигнатурного и статистического анализа, включая приложения P2P, IM, Voice/Video поверх IP, потоковое видео, игровой трафик, шифрованные данные.

- Фильтрация трафика по черным и белым спискам сайтов и категорий сайтов.

- Детектирование Tethering, обнаружение и предотвращение мошенничества.

84

”Трафика”

- Специализированные DPI решений для корпоративного сектора
- Пример: Российская компания «Трафика» и её DPI продукт «Monitorium»
- Monitorium - это система для комплексной защиты данных предприятия от несанкционированных утечек и разглашения.
- Задача системы: контроль входящего/исходящего трафика и автоматическое выявление нарушений пред настроенных правил/политик

85

URL-фильтрация

- Периметр-Ф от МФИ-Софт решает проблему блокировки сайтов и материалов по URL-адресу.
- Усовершенствованный межсетевой экран компании Palo Alto Networks.
- Программное решение Monitorium по стоимости 14 тыс. руб.

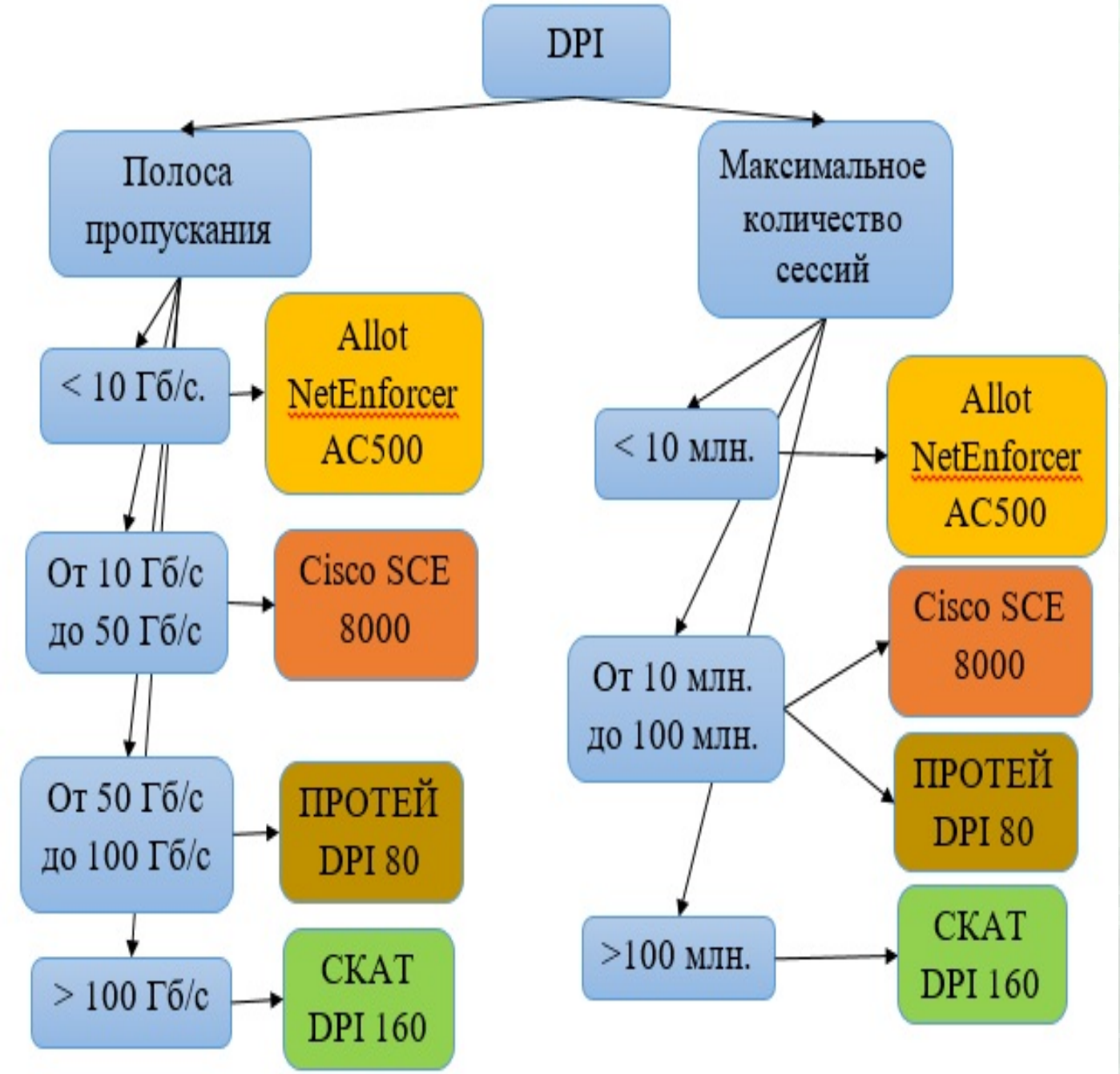
86

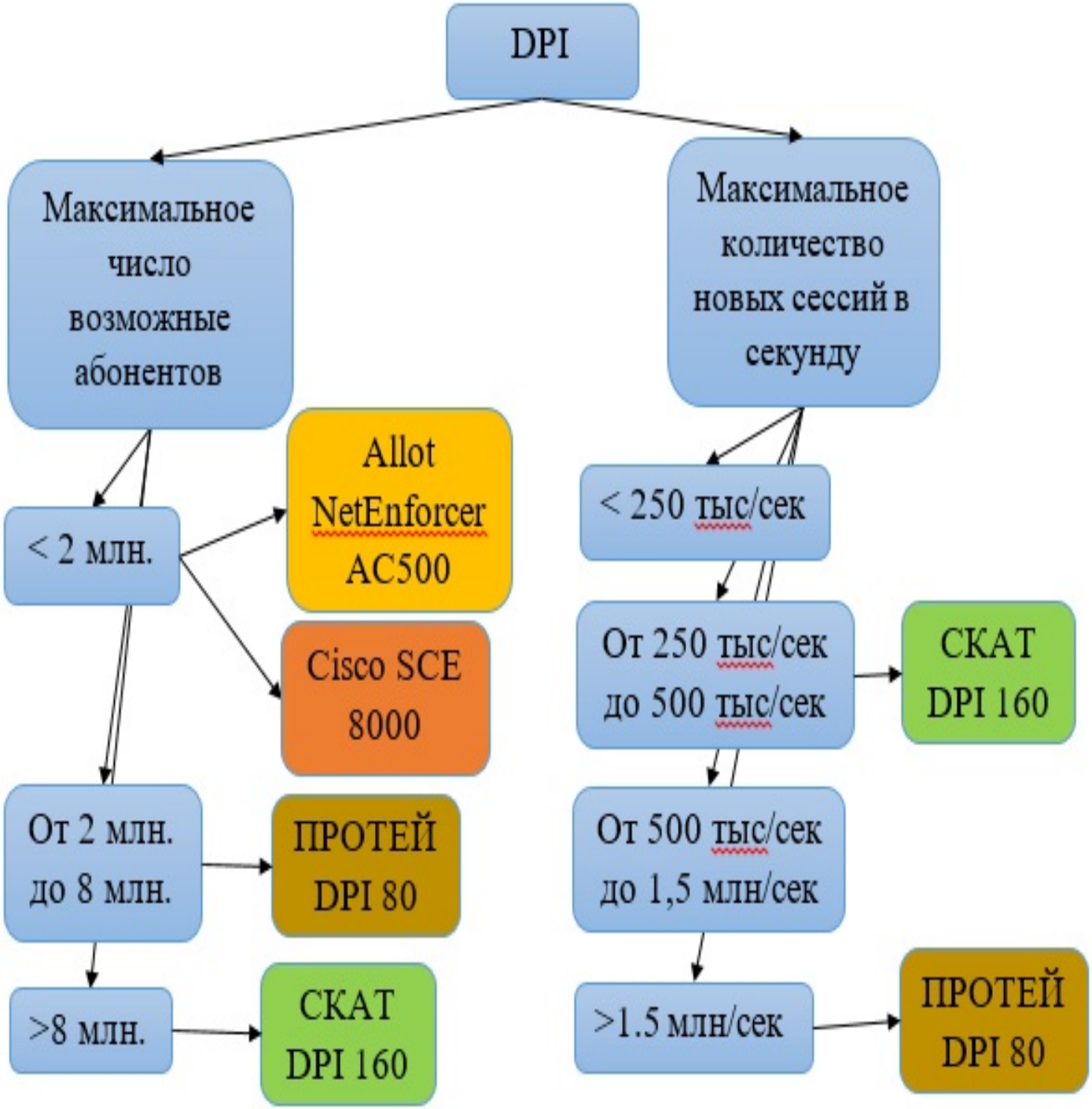
Тестирование DPI

Французский национальный профсоюз звукозаписи SNEP (the Syndicat National de l'Édition Phonographique, an organization that represents the interests of the French music industry) совместно с компанией EANTC (The European Advanced Networking Test Center) провел тестирование DPI решений основных производителей

- На тест были приглашены 28 компаний разрабатывающие DPI решения.
- Участие было бесплатно, все расходы оплатил SNEP
- Продолжительность тестирования составила 6 месяцев
- Для настройки оборудования допускалось использование инженеров от производителя оборудования
- Из 28-ми приглашенных согласились участвовать только 5 компании на условиях – не публикации результатов если им не понравится результат.
- Только два производителя согласились с публикацией результатов Arbor (Ellacoya) и ipoque GmbH.

87


DPI
Полоса пропускания
Максимальное количество сессий
< 10 Гб/с.
Allot NetEnforcer AC500
От 10 Гб/с до 50 Гб/с
Cisco SCE 8000
От 50 Гб/с до 100 Гб/с
ПРОТЕЙ DPI 80
> 100 Гб/с
СКАТ DPI 160
< 10 млн.
Allot NetEnforcer AC500
От 10 млн. до 100 млн.
Cisco SCE 8000
ПРОТЕЙ DPI 80
>100 млн.
СКАТ DPI 160


DPI
Максимальное число возможные абонентов
Максимальное количество новых сессий в секунду
< 2 млн.
Allot NetEnforcer AC500
Cisco SCE 8000
От 2 млн. до 8 млн.
ПРОТЕЙ DPI 80
>8 млн.
СКАТ DPI 160
< 250 тыс/сек
От 250 тыс/сек до 500 тыс/сек
СКАТ DPI 160
От 500 тыс/сек до 1,5 млн/сек
>1.5 млн/сек
ПРОТЕЙ DPI 80

Спасибо за внимание.

Далее: Возможности технологии DPI

Вопросы?

Ст. преп. каф. Инфокоммуникационных систем СПбГУТ,

Фицов Вадим Владленович,