Методы инспекции пакетов и анализа трафика

Лекция 3
Возможности и применение DPI

Фицов Вадим Владленович

ст.преп. кафедры ИКС

Содержание лекции:

- Возможности.
- Применение.
- Проблемы

Возможности

Из определения:

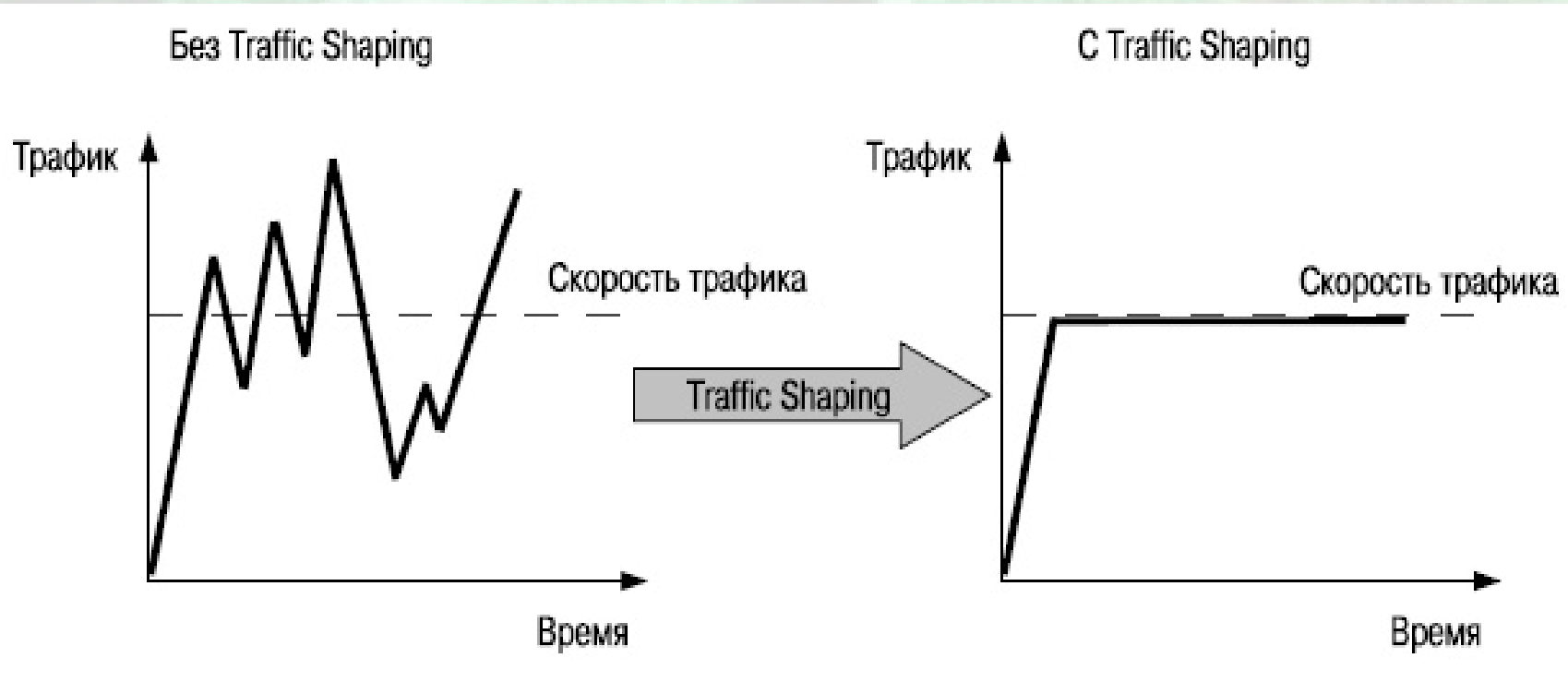
- Накопление
- Анализ
- Классификация
- Контроль
- Модификация
- Маркировка

4

Обеспечения QoS

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


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

Управление трафиком может состоять из следующих компонент:

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

Из определения:

DPI анализирует

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

- Применяются анализ:
  - сигнатурный
  - статистический
  - поведенческий
  - эврестический

8

DPI средства управления трафиком

Многоликий DPI

Современные решения использующие технологию DPI

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.

Сбор статистики:

- по предоставляемым услугам (per-service)
  - (приложениям
  - , протоколам),
- по каждому пользователю (per-subscriber) .

Ограничение передачи:

- к определенным ресурсам (социальные сети, online игры, потоковое видео)

Персонализированные тарифы.

Тарификация по контенту. (доход ~ рост потребления)

Использование аппаратных ресурсов

QoS, SLA.

12

Сетевой нейтралитет или нет?

Дифференциация услуг:

- **тариф для веб-трафика (HTTP)**
- **~~ограничение~~ тариф для P2P приложений**
- **тариф для соц сетей**
- **тариф для развлечений**
- **…**
- **тарификация:**
  - **time-точки**
  - **geo-точки**
  - **empty-точки**
- **тарификация для телефонии и OTT**

14

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

15

Ведение отчетности:

- **h, d, M счетчики для исх. и вх. трафика**
  - **по абонентам**
  - **по протоколам и услугам**
- **сохранение CDR в *.CSV**
  - **по протоколам и услугам**
  - **по каждому абоненту**
  - **выгрузка во внешнюю систему**
- **отчеты (график, гистограмма, таблица)**
- **состояние канала в реальном времени**

16

Контроль потребления трафика:

- **M, d квоты (квоты на услуги)**
- **политика превышения квоты или истечения средств.**

Порядок действий:

- **определяется поток;**
- **определяется политика**
- **политика применяется к потоку.**

Политика:

- **для потока конкретного приложения,**
- **для конкретного абонента.**

17

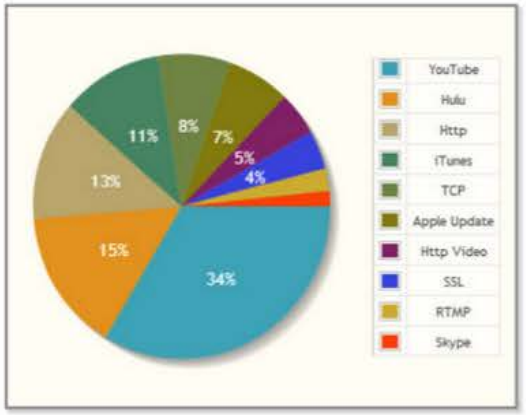
XIRRUS

- Status
  - Array
  - Network
  - RF Monitor
  - Stations
  - Statistics
  - Application Intelligence
    - Stations
  - System Log
  - IDS Event Log
- Configuration
  - Express Setup
  - Network
  - Services
  - VLANs
  - Tunnels
  - Security
  - SSIDs
  - Groups
  - IAPs
  - WDS
  - Filters
  - Clusters
- Tools
  - Help
  - System Tools
  - CLI
  - Options
  - Logout

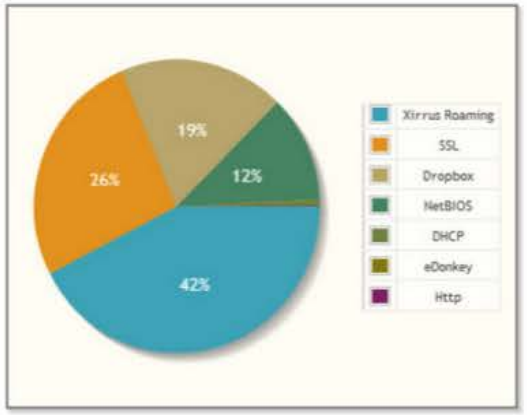
Name: XR402240E1A7E (192.168.0.102) Uptime: 26 days, 20 hours, 8 mins

Display for VLAN all Display for Station all Station Traffic Array Management Traffic By Application By Category Auto Refresh Refresh

Station Traffic by Application



Array Management Traffic by Application



Station Traffic

Application	Transmitted Packets	Transmitted Bytes	Received Packets	Received Bytes
Adobe	3742	2213749	4024	698820
Amazon	51937	56986052	35779	6626277
Apple Update	1701293	2548315581	833784	44717285
Battle.net	9	414	9	486
Bing	19	13583	15	2250
Blackjack	3	138	3	162
Blogger	2732	3200020	1922	346659
CAP	2	92	2	108
CIFS	9474	989785	16567	3781635
Cisco GDP	1	46	1	54
Citrix Jedi	46093	7285054	46068	4162561
Citrix Online	7860	3870551	9753	784069
DHCP	1403	720456	2135	700280

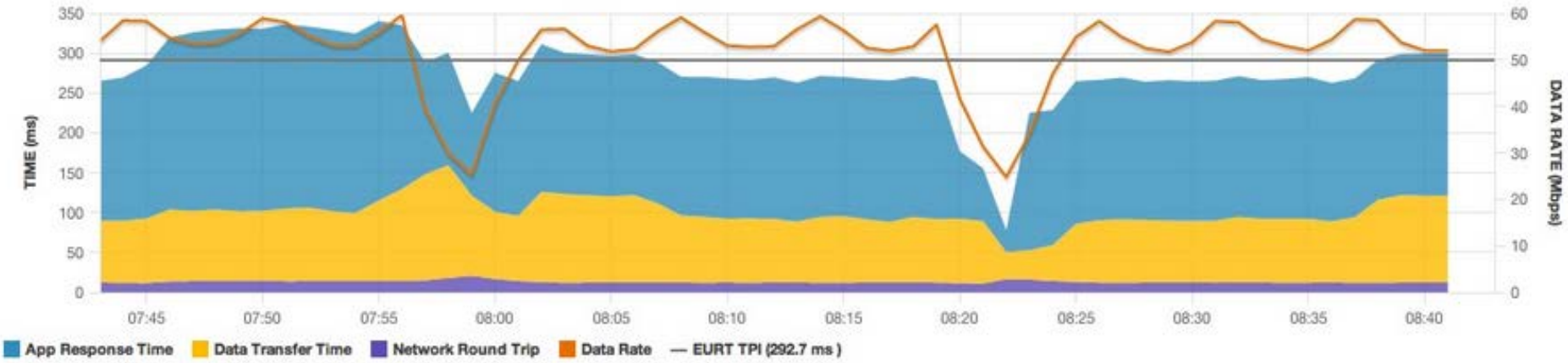
Array Management Traffic

Application	Transmitted Packets	Transmitted Bytes	Received Packets	Received Bytes
DHCP	0	0	400	142728
Dropbox	0	0	31869	4366053
Http	65	9181	77	9070
NetBIOS	0	0	17861	2742850
SSL	6621	5581813	4873	548988
Xirrus Roaming	40229	9896334	0	0
eDonkey	0	0	250	20364

RESPONSE TIME

Show TPI ☑ Overlay Metric: Data Rate

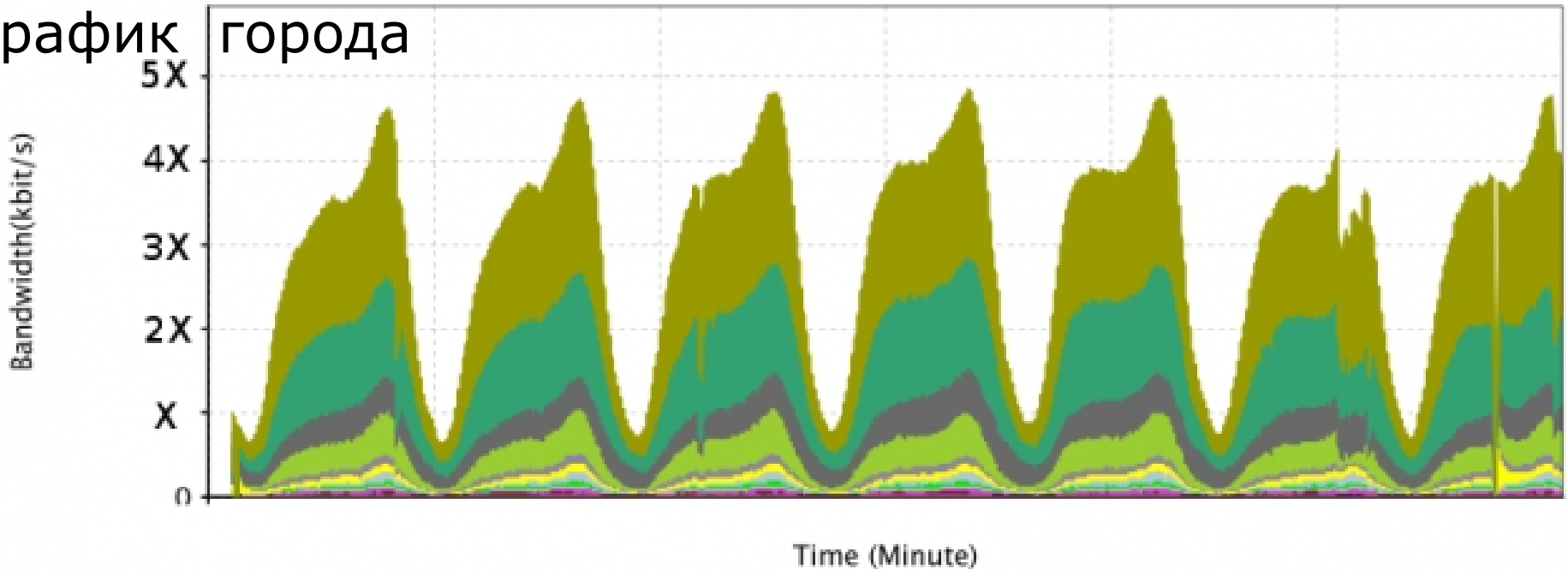
Sep 11, 2012 07:43 - Sep 11, 2012 08:43 EDT **Granularity:** 1 Min
Application: All Applications **Site:** All Sites **Server:** All Servers



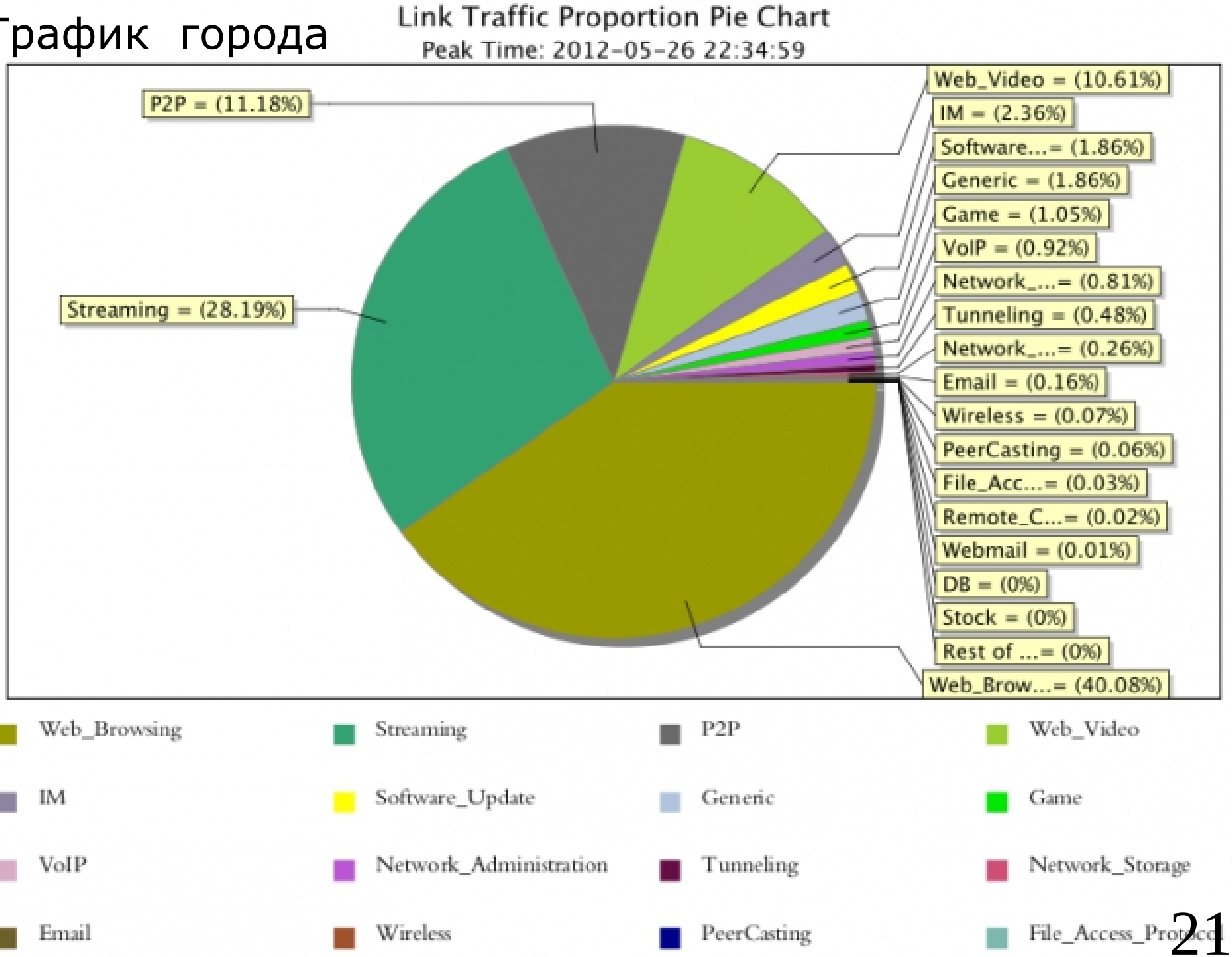
	TIME	EURT (ms)	ART (ms)	DTT (ms)	SERVER DTT (ms)	CLIENT DTT (ms)	NRT (ms)	TRANSACTIONS	DATA RATE (bps)
1	Sep 11, 2012 07:43	265.3	175.1	77.9	49.9	28.0	12.4	259.69 k	54.03 Mbps
2	Sep 11, 2012 07:44	269.6	179.8	77.8	48.2	29.6	11.9	258.54 k	58.48 Mbps
3	Sep 11, 2012 07:45	284.7	191.9	81.1	54.6	26.6	11.7	263.43 k	58.34 Mbps
4	Sep 11, 2012 07:46	319.9	215.9	90.2	60.9	29.3	13.7	263.86 k	54.73 Mbps
5	Sep 11, 2012 07:47	326.2	224.1	88.0	59.5	28.6	14.0	266.17 k	53.49 Mbps
6	Sep 11, 2012 07:48	329.8	225.7	89.9	61.4	28.5	14.2	265.71 k	53.63 Mbps
7	Sep 11, 2012 07:49	331.4	229.6	87.6	59.3	28.3	14.2	263.10 k	55.58 Mbps
8	Sep 11, 2012 07:50	330.8	228.6	87.6	59.7	27.9	14.6	257.92 k	58.93 Mbps
9	Sep 11, 2012 07:51	336.5	231.3	91.2	60.9	30.3	13.9	264.69 k	58.10 Mbps
10	Sep 11, 2012 07:52	333.4	227.0	92.4	62.1	30.2	14.0	267.27 k	55.10 Mbps
11	Sep 11, 2012 07:53	329.5	227.5	87.6	58.8	28.7	14.4	262.61 k	53.11 Mbps
12	Sep 11, 2012 07:54	324.7	225.0	85.4	59.6	25.8	14.3	261.70 k	53.05 Mbps
13	Sep 11, 2012 07:55	340.6	225.2	101.3	72.2	29.1	14.1	263.20 k	55.93 Mbps
14	Sep 11, 2012 07:56	335.1	205.2	115.6	85.8	29.8	14.3	260.84 k	59.65 Mbps
15	Sep 11, 2012 07:57	288.9	140.7	133.1	97.2	35.9	15.1	212.57 k	39.43 Mbps

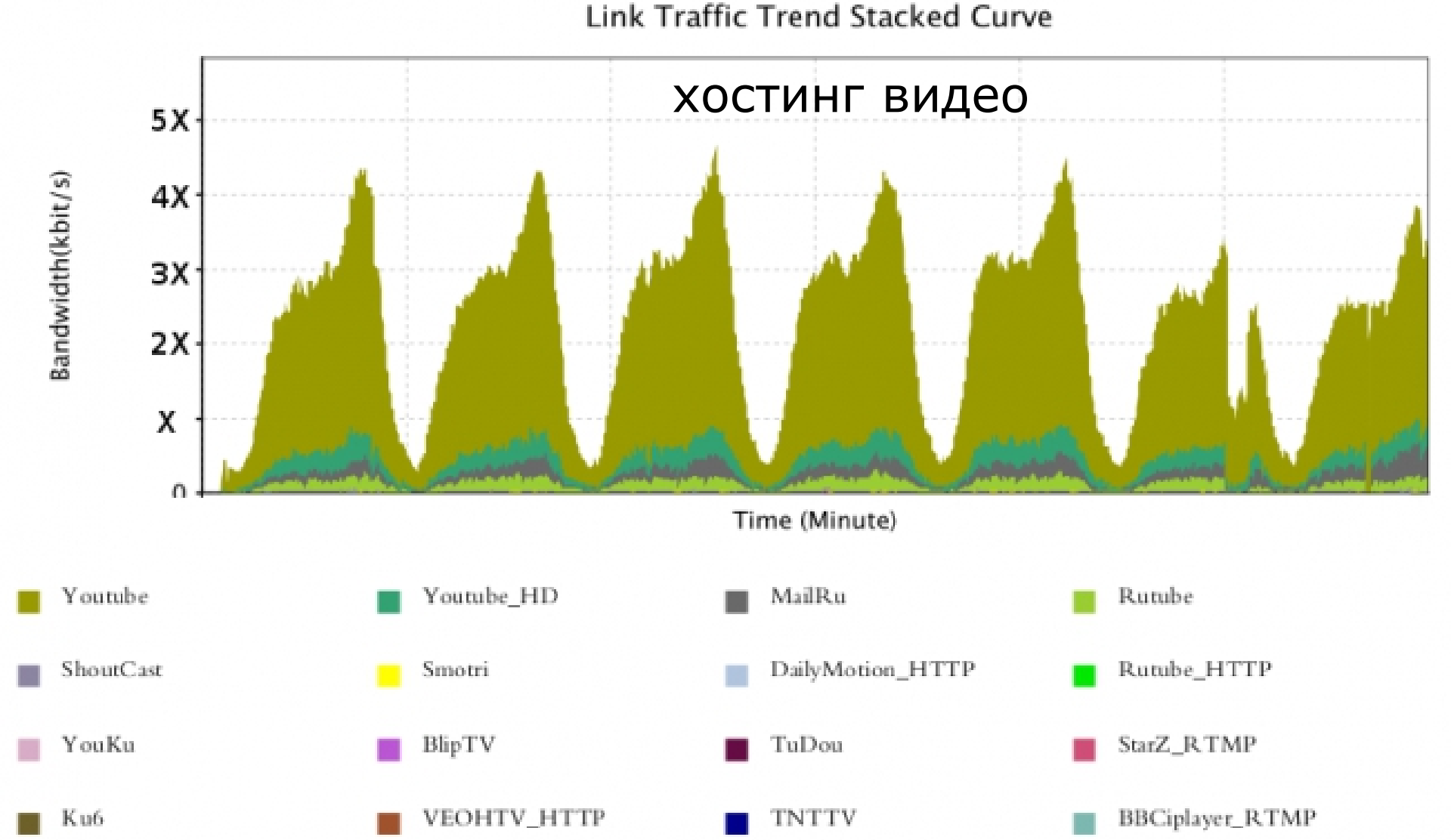
Display 15 Page 1 of 4 60 records

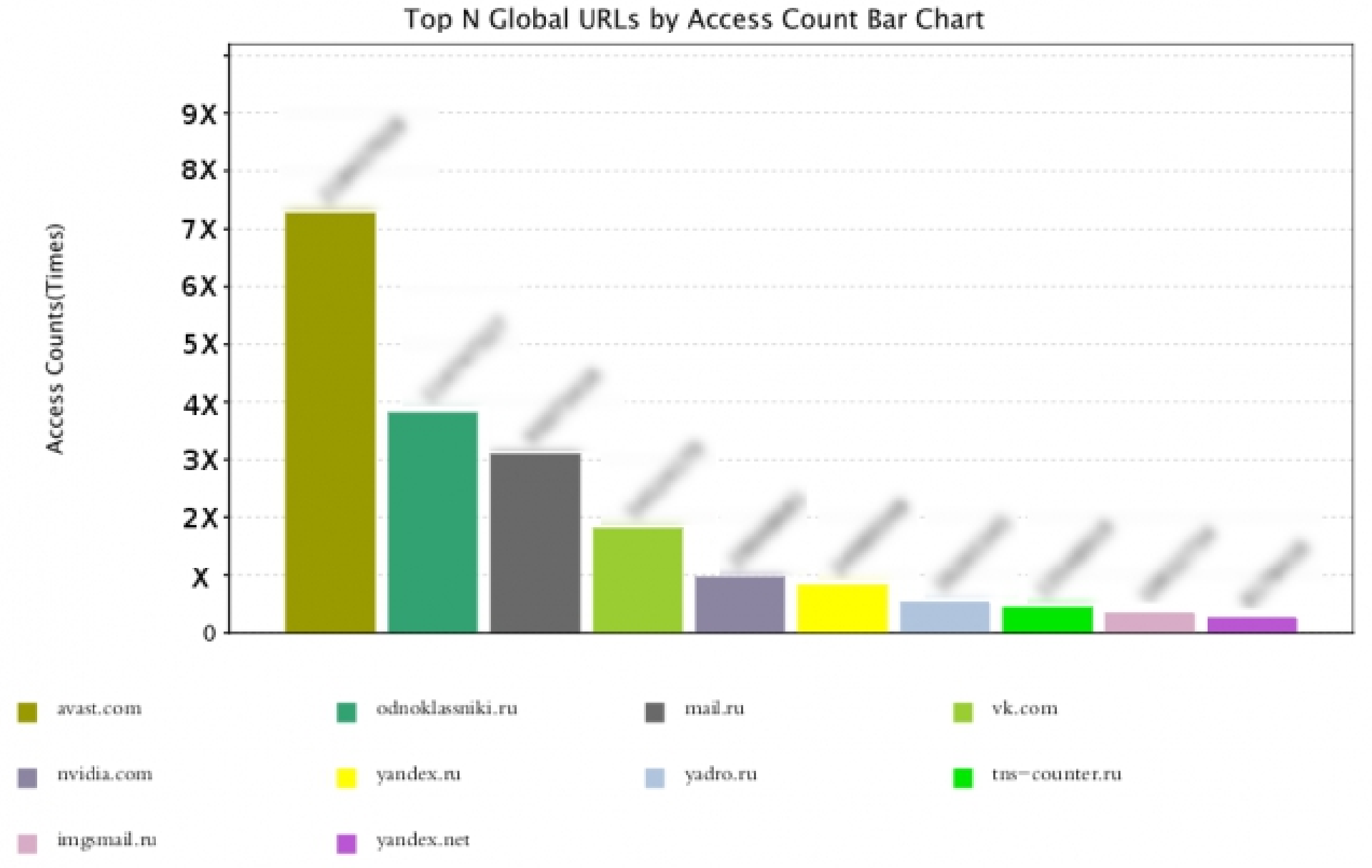
Трафик города



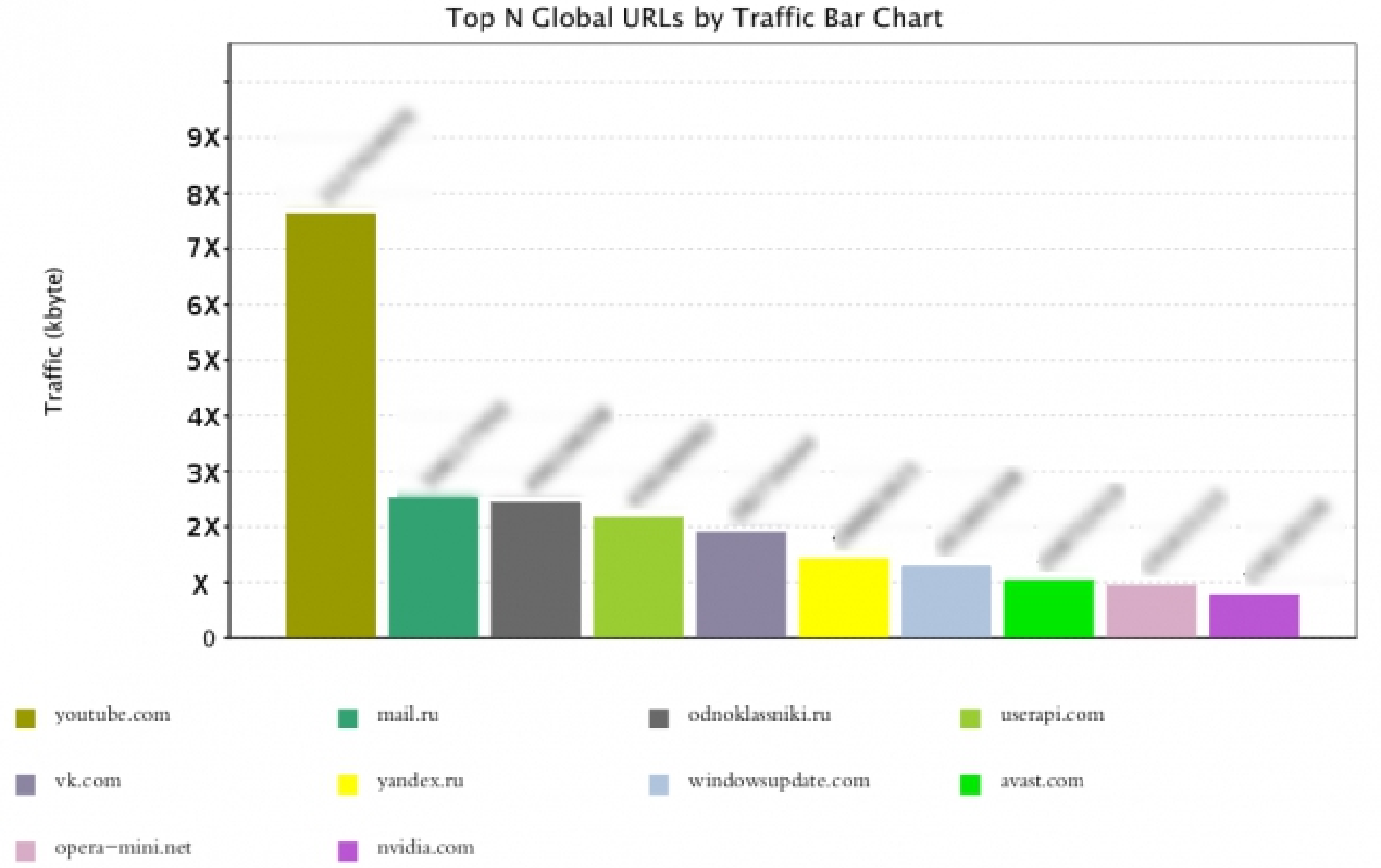
Трафик города



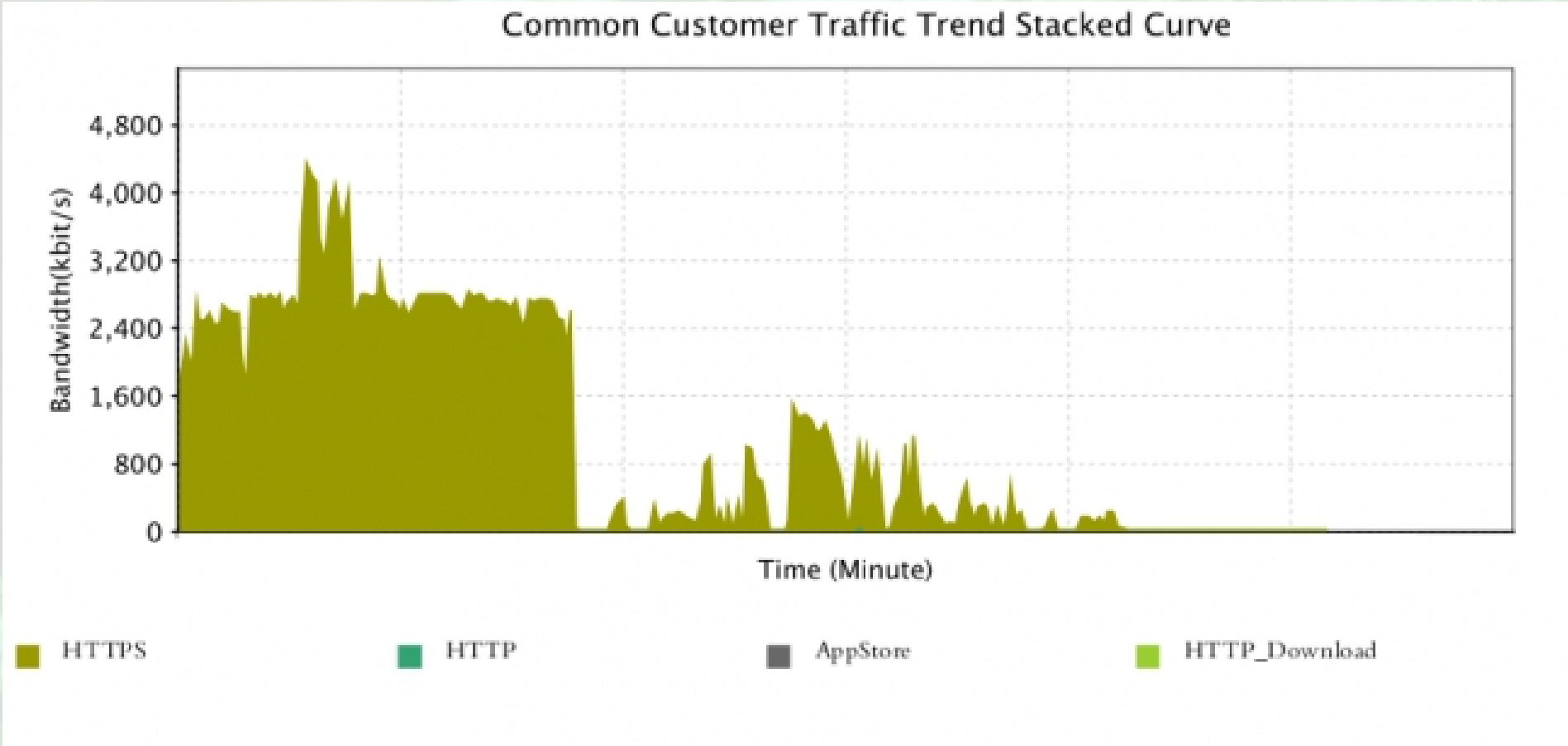

Link Traffic Trend Stacked Curve
хостинг видео
Bandwidth(kbit/s)
5X
4X
3X
2X
X
0
Time (Minute)
Youtube
Youtube_HD
MailRu
Rutube
ShoutCast
Smotri
DailyMotion_HTTP
Rutube_HTTP
YouKu
BlipTV
TuDou
StarZ_RTMP
Ku6
VEOHTV_HTTP
TNTTV
BBCiplayer_RTMP



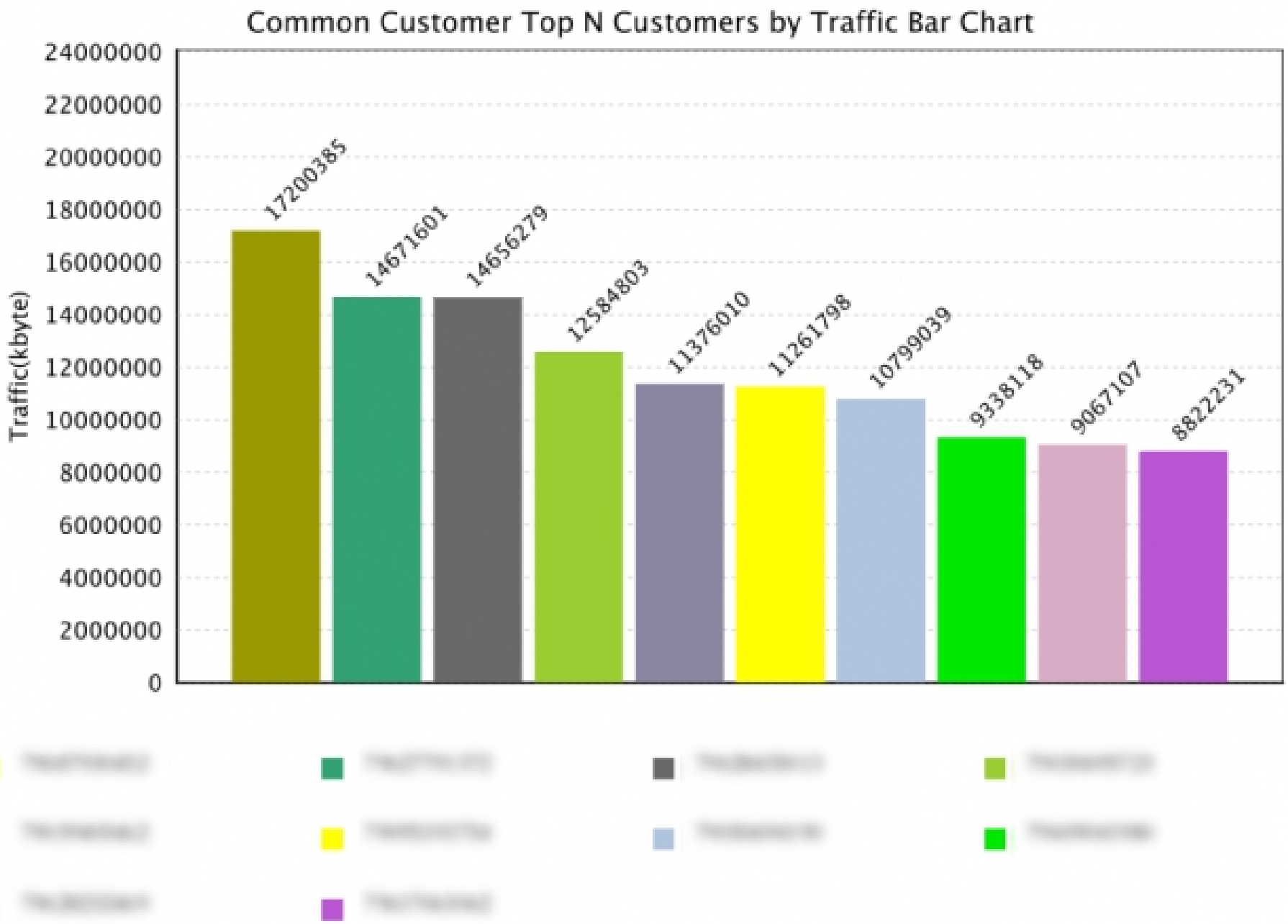
Топ 10 сайтов – по соединениям



Топ 10 сайтов – по трафику



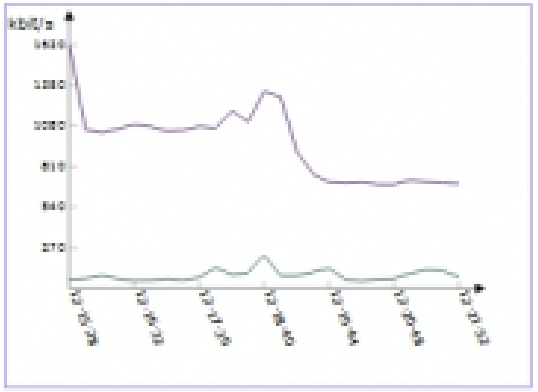
WEB трафик конкретного пользователя

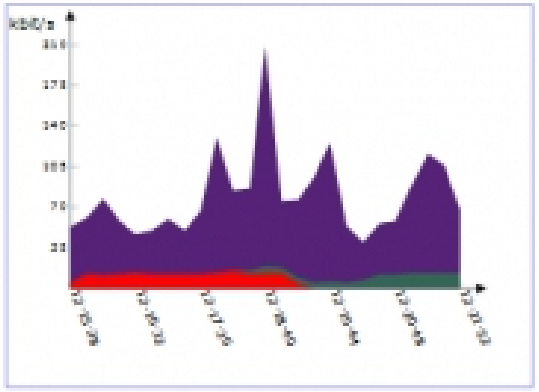


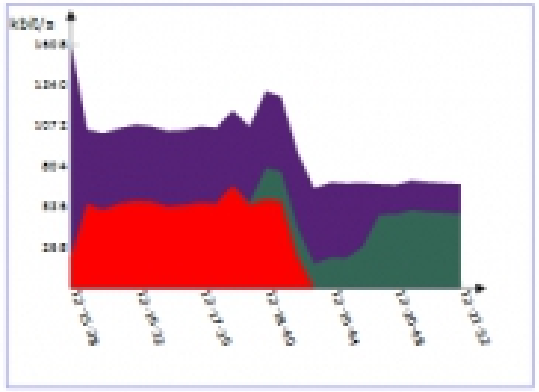
активные пользователи:

	IP Address	Protocol Categ...	Protocol	Time	Upstream Ban...	Downstream B...	Upstream Pack...	Downstream P...	Traffic Rate	Proportion to T...
1	10.30.0.20	Total	----	2012-07-18 12...	76	698	72	75	----	----
2	10.30.0.20	P2P	----	2012-07-18 12...	55	199	35	29	----	32.8165%
3	10.30.0.20	Web_Video	----	2012-07-18 12...	13	492	25	41	----	65.2455%
4	10.30.0.20	Generic	----	2012-07-18 12...	5	1	9	2	----	0.7752%
5	10.30.0.20	Web_Browsing	----	2012-07-18 12...	2	5	1	1	----	0.9044%
6	10.30.0.20	VoIP	----	2012-07-18 12...	1	0	1	0	----	0.1292%
7	10.30.0.20	Network_Ad...	----	2012-07-18 12...	0	1	1	2	----	0.1292%

Real-time Traffic Curves

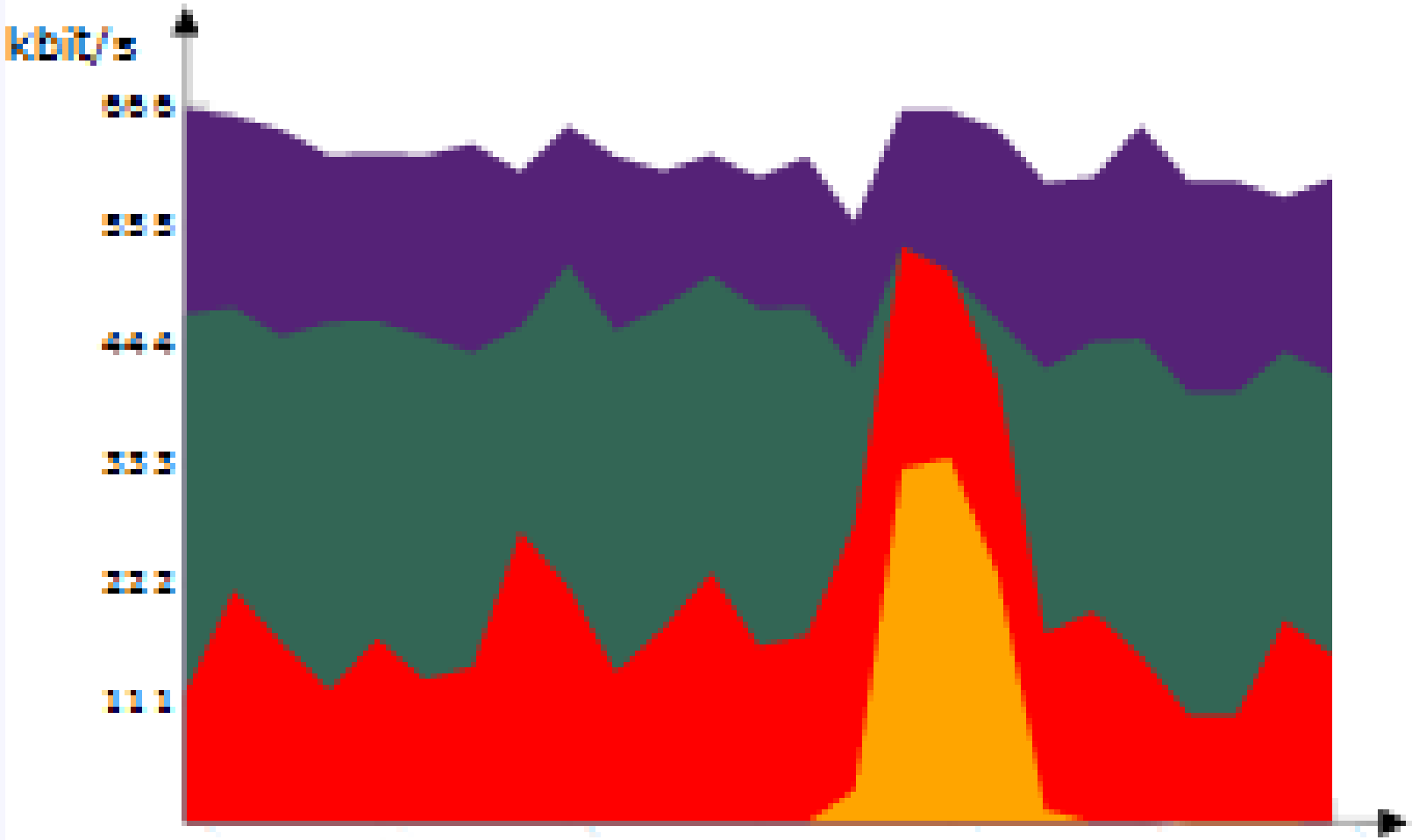






Attention:If your browser can not display the above pictures, please click Download to install the plugin for your browser.

этом приоритет на видео (зелёный),
а для P2P (фиолетовый) гарантировано 200 кб/с.

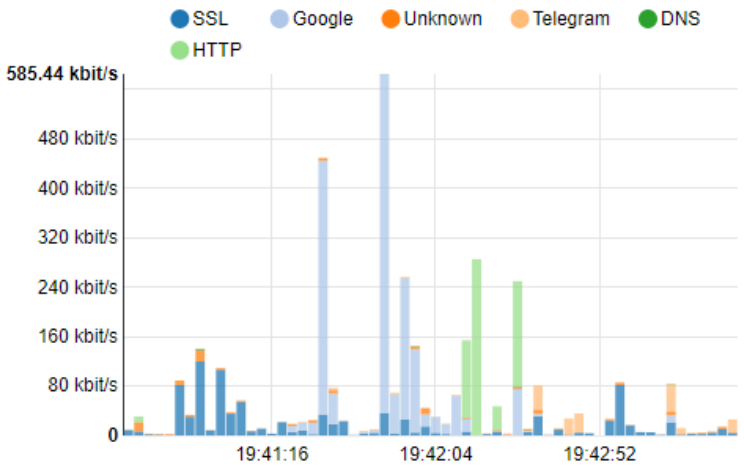


наивысший приоритет у видео (зелёный),
на втором месте FTP (красный)
и на последнем фиолетовый P2P

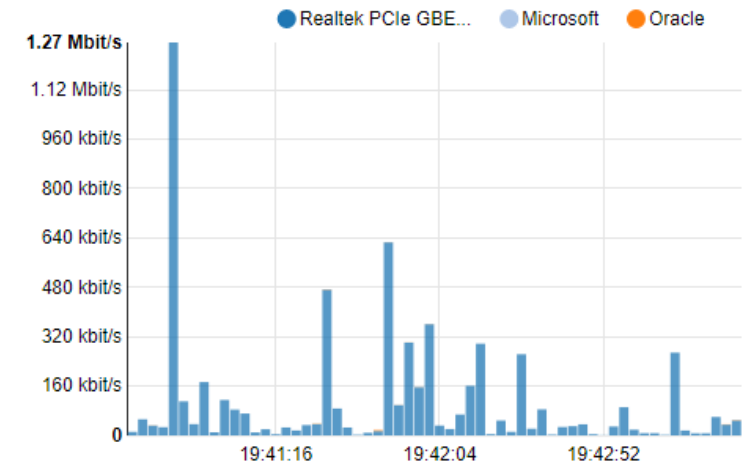
Flows Hosts Devices Interfaces Search Host

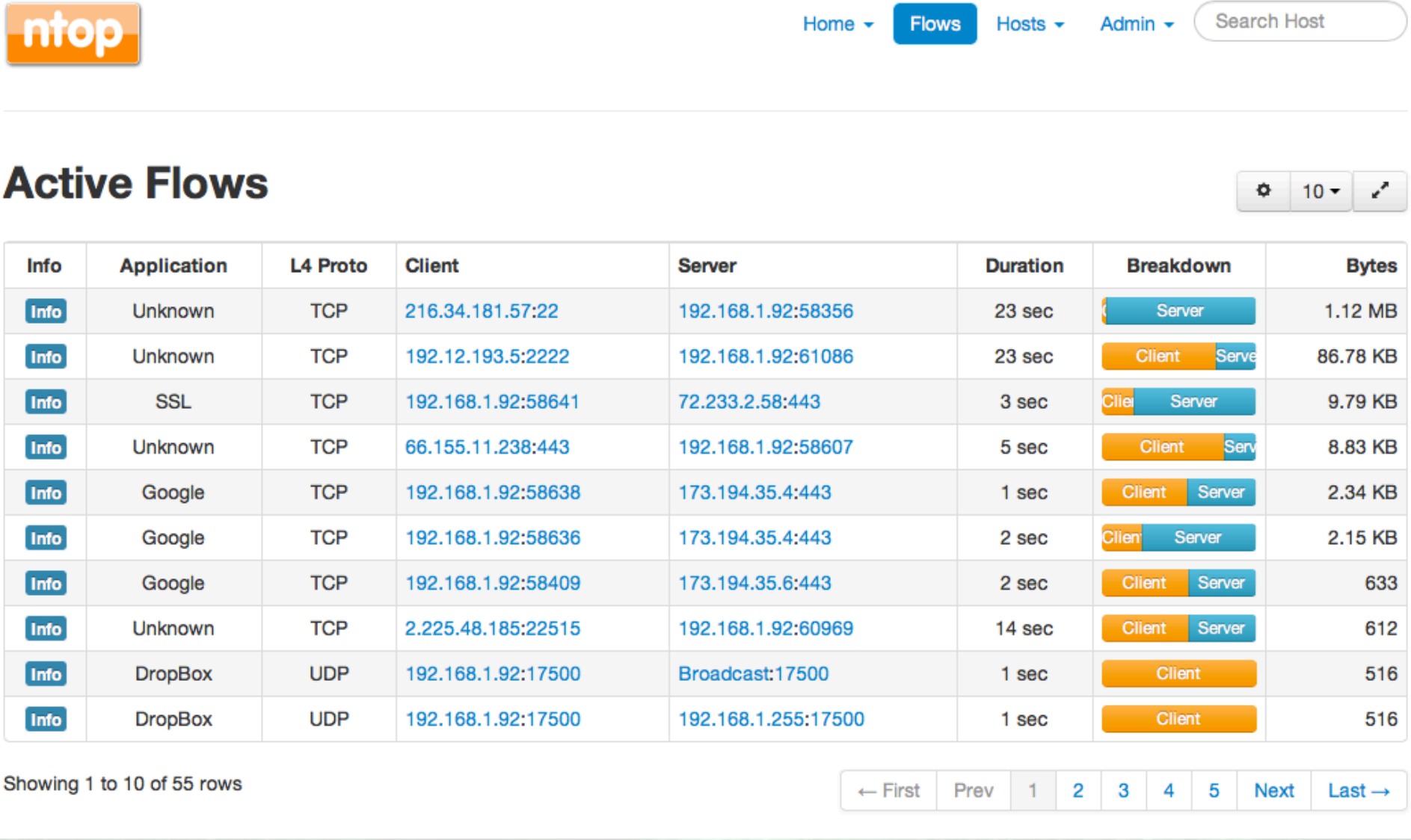
Actual Traffic
35.51 kbit/s ↑
6.32 kbit/s ↑
4.31 kbit/s ↑
358.26 bit/s ↑
238.3 bit/s ↑

Realtek PCIe GBE...: Realtime Top Application Traffic



Network Interfaces: Realtime Traffic




ntop
Home
Flows
Hosts
Admin
Search Host
Active Flows
10
Info Application L4 Proto Client Server Duration Breakdown Bytes
Info Unknown TCP 216.34.181.57:22 192.168.1.92:58356 23 sec Server 1.12 MB
Info Unknown TCP 192.12.193.5:2222 192.168.1.92:61086 23 sec Client Serve 86.78 KB
Info SSL TCP 192.168.1.92:58641 72.233.2.58:443 3 sec Clie Server 9.79 KB
Info Unknown TCP 66.155.11.238:443 192.168.1.92:58607 5 sec Client Serv 8.83 KB
Info Google TCP 192.168.1.92:58638 173.194.35.4:443 1 sec Client Server 2.34 KB
Info Google TCP 192.168.1.92:58636 173.194.35.4:443 2 sec Clien Server 2.15 KB
Info Google TCP 192.168.1.92:58409 173.194.35.6:443 2 sec Client Server 633
Info Unknown TCP 2.225.48.185:22515 192.168.1.92:60969 14 sec Client Server 612
Info DropBox UDP 192.168.1.92:17500 Broadcast:17500 1 sec Client 516
Info DropBox UDP 192.168.1.92:17500 192.168.1.255:17500 1 sec Client 516
Showing 1 to 10 of 55 rows
← First Prev 1 2 3 4 5 Next Last →

Внедрение системы DPI обеспечивает:

-централизованный **контроль сайтов и нелегального контента** (по адресу ресурса внесенному в черный список в БД категорий **URL**);

-**персонализированный доступ** пользователей (“черный” или “белый” списки общие или частные, - персонализация самого понятия безопасность);

-**уведомление о посещении** потенциально опасных ресурсов, с проверкой трафика на наличие вирусов;

- **контроль трафика файлообменных сетей** на основе политик (ограничение/выделение минимальной гарантированной/блокировка общей скорости передачи, скорости по типу трафика (web, video, P2P, IM и пр.), **указание приоритета** для каждого типа);

Внедрение системы DPI обеспечивает:

-**контроль почтового спама** (по количеству рассылок). При этом зараженный пользователь перенаправляется на страницу с инструкциями по удалению вируса;

-**обнаружение DoS/DDoS атак** (по большой нагрузке на вычислительную систему);

- **обнаружение сканирования** сети;

Внедрение системы DPI обеспечивает:

- **сбор статистики** (используемая полоса пропускания по каждому типу трафика, по каждому интернет серверу или **пользователю**, их процентное соотношение, количество соединений или обьем трафика к интернет серверам);

-**фильтрация** по адресам, портам, доменным именам и протоколам (например, P2P или Skype);

-применение **динамических индивидуальных политик** для фиксированных и мобильных абонентов (APN, телефонный номер, тип доступа (2G, 3G, 4G));

- **блокировка или ограничение** скорости **при** опасности **перегрузки** или высокой загруженности в соте (для сетей подвижной связи).

Применение

Внедрение DPI

Три основных причины внедрения DPI

Внедрение DPI

Основные направления применения DPI систем управления трафиком

Централизация обеспечения безопасности доступа в Интернет на основе DPI-платформы в сети оператора связи, сокращает издержки клиентов (организаций) на обеспечение безопасности.

Например, это позволит **сократить** использование **антивирусов и фаерволов на каждом оконечном** устройстве, и контроль на прокси-сервере.

Однако это **не спасет от угрозы внутри сети**.

37

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

38

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.

39

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.

40

URL-фильтрация:

Анализируя трафик на уровне приложений DPI позволяет точечно заблокировать запрещенный ресурс по URL-адресу,

без полной блокировки сервера компании хостинга.

Такой подход удовлетворяет требованию по блокировке трафика на основе доменного имени или сочетанию IP-адреса и адреса ведущего к запрещенному контенту.

41

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.

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.

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.

Применение Оператором

- анализ работы пользователей
- анализ работы приложений
- управление существующим у оператора ресурсом
- контроль разрешенного уровня потребления трафика
- биллинг.

Корпоративное применение

Управление информационной безопасностью:

- Контроль передачи конфиденциальных документов (целиком или любой части текста документа, в том числе и в заархивированном виде)

(ч/з email, site, ftp …)

- Предотвращение утечки конфиденциальной информации
- Выявление нарушителей
- Защита персональных данных

Корпоративное применение

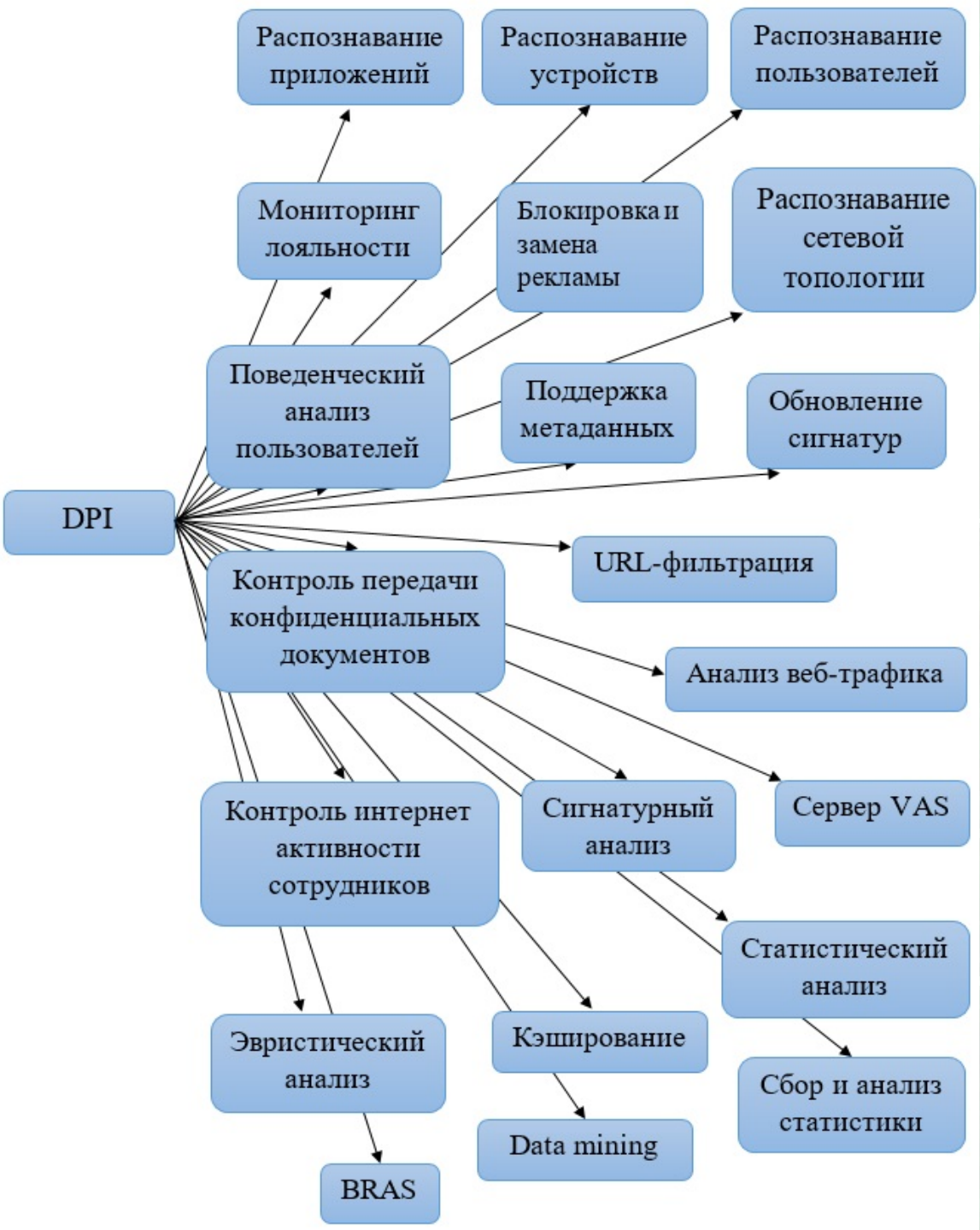
Управление сетью:

- Контроль интернет активности сотрудников
- Ограничение доступа пользователей корпоративной сети к Интернет ресурсам.
- Мониторинг лояльности сотрудников (сайты о работе и т.д.)

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.


Распознавание приложений
Распознавание устройств
Распознавание пользователей
Мониторинг лояльности
Блокировка и замена рекламы
Распознавание сетевой топологии
Поведенческий анализ пользователей
Поддержка метаданных
Обновление сигнатур
DPI
URL-фильтрация
Контроль передачи конфиденциальных документов
Анализ веб-трафика
Контроль интернет активности сотрудников
Сигнатурный анализ
Сервер VAS
Статистический анализ
Эвристический анализ
Кэширование
Сбор и анализ статистики
Data mining
BRAS

Применение

Проблема шифрования

Шифрование

- DPI-системы не способны расшифровать данные
- проанализировав, идентифицировать и классифицировать эти данные, основываясь на эвристической информации или поведенческом анализе
- DPI находит зашифрованный трафик BitTorrent,

но не определить, какой именно файл

Обработка ***неизвестностного*** трафика

выявление ***P2P*** трафика

Спасибо за внимание.

Далее: СОРМ … и DPI

Вопросы?

Ст. преп. каф. Инфокоммуникационных систем СПбГУТ,

Фицов Вадим Владленович,