Cisco Expo 2011

Service Control Engine. DPI решение для анализа и управления трафиком

Сергей Великанов

Системный инженер компании Cisco Systems

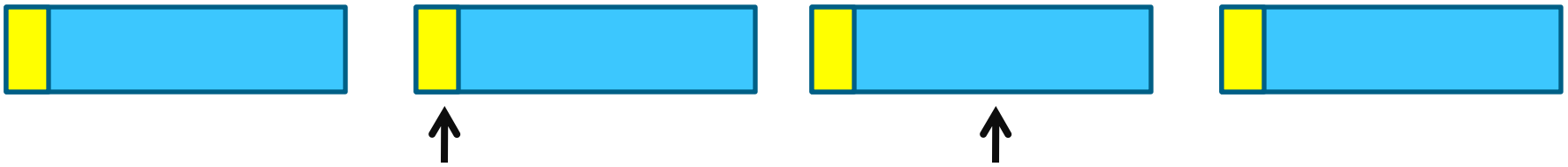
О чем пойдет речь

- Что такое Deep Packet Inspection?
- Service Control Engine – решение DPI от Cisco Systems
- Сервисы DPI в сети передачи данных
- Экосистема Service Control Engine
- Система мониторинга и отчетов
- Вопросы и ответы

Что такое DPI?

Как передаётся информация

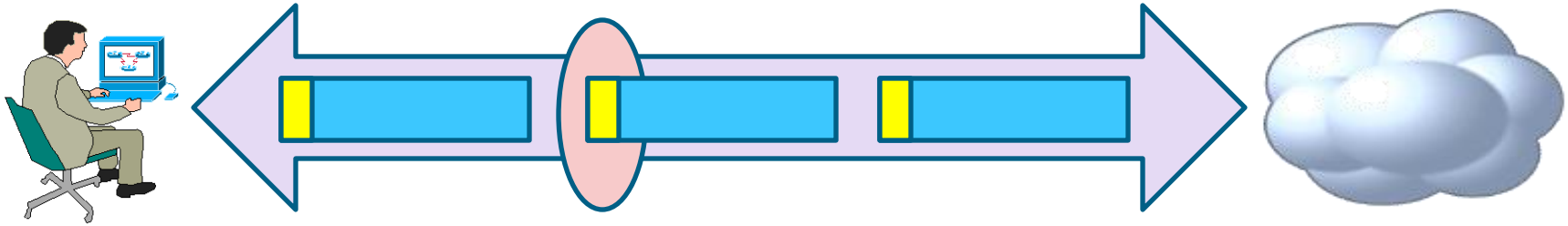
- Информация от пользователя в интернет (и обратно) передается в виде пакетов небольшого размера



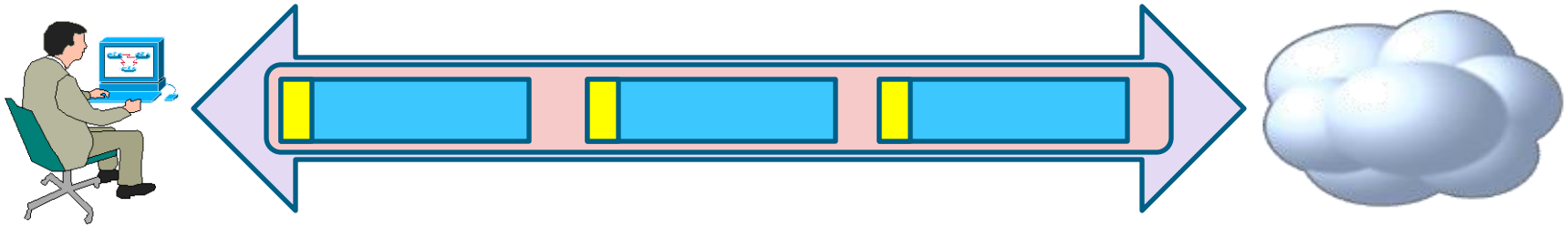
- В каждом пакете есть заголовок и передаваемая информация

Что такое DPI

- Пакетный фильтр (Firewall) может анализировать только служебный заголовок пакета



- Решения DPI (Deep Packet Inspection – глубокий анализ пакетов) могут анализировать весь пакет целиком, а также устанавливать взаимосвязь между несколькими пакетами, для более полного выявления типа и характера передаваемой информации

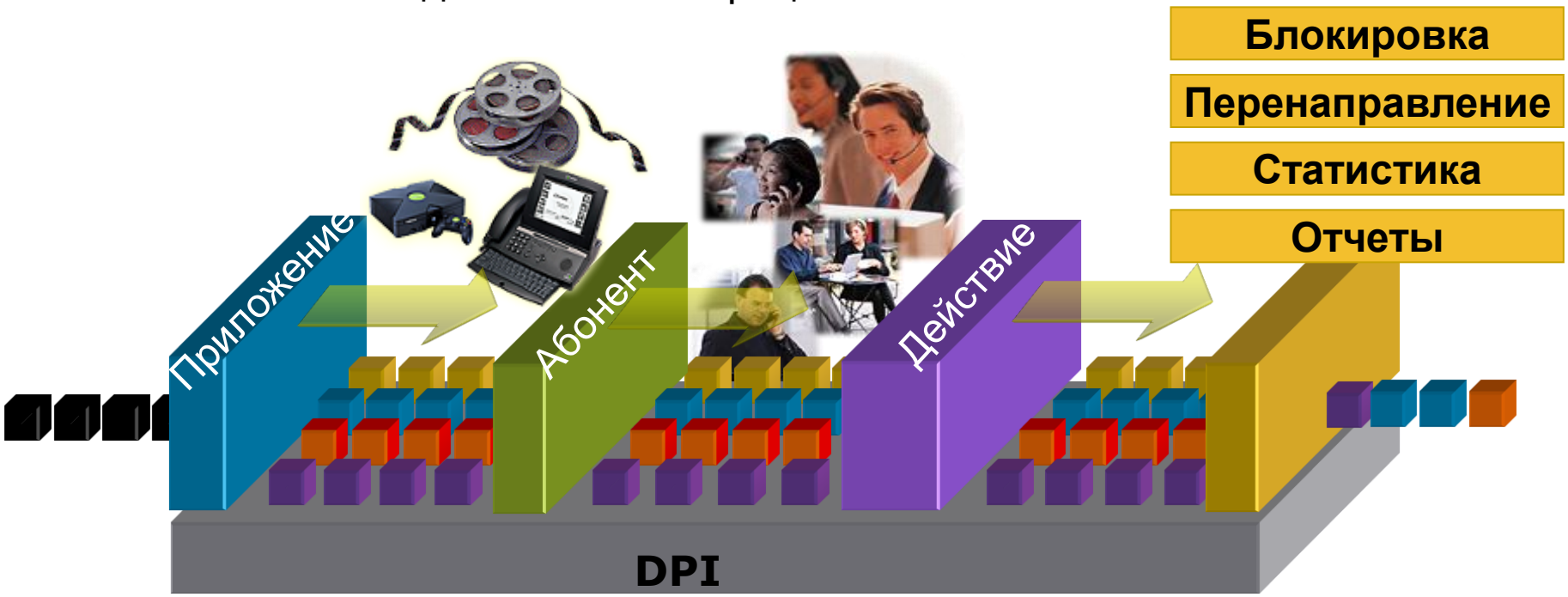


Текущее состояние и проблемы в сетях передачи данных

- Новые Over-The-Top (OTT) протоколы и приложения – файловый обмен P2P, VoIP, HTTP-видео, он-лайн игры…
- Неконтролируемые требовательные к полосе приложения могут повлиять на общее впечатление абонента от качества предоставляемых услуг.
- Интерактивные и требовательные к задержкам видео и голосовые приложения требуют поддержания постоянного впечатления от качества сервиса.
- Протоколы и приложения постоянно видоизменяются.
- Сетевой трафик некоторых специфических приложений тяжело поддается анализу и классификации (например P2P), вредоносный трафик (напр. «черви») и т.д

Концепция Deep Packet Inspection

- Интеллектуальный анализ и управление IP трафиком
- Классификация по приложениям;
- Привязка к индивидуальному абоненту, политике и состоянию
- Выбор действия в зависимости от условий – время суток, наличие перегрузки, потребленный объем и др
- Выполнение действия и генерация отчетов



Service Control Engine – решение DPI от Cisco Systems

Service Control Engine

- Более 750 Компаний используют SCE

  Все типы широкополосного доступа: xDSL, FTTx, Cable, Mobile 3G, Fixed-Wireless

- Самое большое внедрение DPI в мире – обслуживается более 100 миллионов абонентов

Что же такое Service Control Engine?

Надежные механизмы анализа (DPI) : Вместо обработки отдельных пакетов SCE обрабатывает потоки приложений на 7-м уровне.

Программируемость: Быстрая адаптация под новые виды протоколов и приложений.

Операторский класс: Разработано для построения решений операторского класса с высокой производительностью на скоростях Multi-Gigabit и10 Gigabit .
Высокая надежность и доступность с обеспечением резервирования.

Управление полосой на уровне приложений, блокировка, перенаправление (HTTP, RTSP, SIP)

Управление состоянием абонента с индивидуальным контролем полосы, квотами на объем трафика и др.

Платформа Service Control Engine

- Возможности
  - •Глубокий анализ пакетов
  - •Stateful инспекция приложений
  - •Гибкие политики управления
- Устройство операторского класса
  - •Модульность и расширяемость
  - •Защита от сбоев (Bypass)
  - •Специализированный процессор для анализа трафика
  - •Компактный размер

Платформа Service Control Engine

Флагман линейки - SCE8000

- Специализированная архитектура нового поколения 10Гбит/с
  - Использует многолетний опыт Cisco на рынке устройств управления сервисами
  - Новый хорошо расширяемый дизайн
- Потрясающие параметры производительности
  - Производительность на один модуль DPI до15Gbps
    - Увеличение до 30Gbps установкой второго модуля
  - До 1M одновременных абонентских подключений
  - До 16 миллионов однонаправленных потоков (flow) трафика
    - Увеличение до 32 миллионов с установкой второго модуля
- 10Gig и GBE SPA интерфейсные модули
  - Использование существующих на рынке Cisco SPA модулей

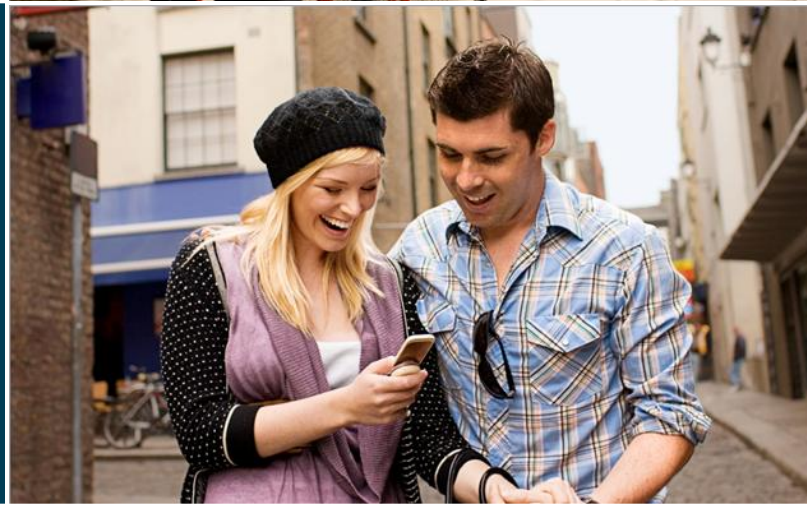
Доступные платформы Service Control Engine

Категория	SCE1000 	SCE2000 	SCE8000 
Интерфейсы	2-GBE (Fiber SX/LX)	4-GBE (Fiber SX/LX)	2-10G 4-10G (Fiber SX/LX/ZX)
Интерфейсы управления	2 x 10/100/1000 Eth	2 x 10/100/1000 Eth	2 x 10/100/1000 Eth
Макс. количество однонаправленных потоков приложений	2M	2M	16M / 32M
Макс. количество абонентов	40,000	200,000	1,000,000
Включение в сеть	Out of Line Inline	Out of Line Inline Clustering	Out of Line Inline Clustering

Механизмы классификации Cisco SCE

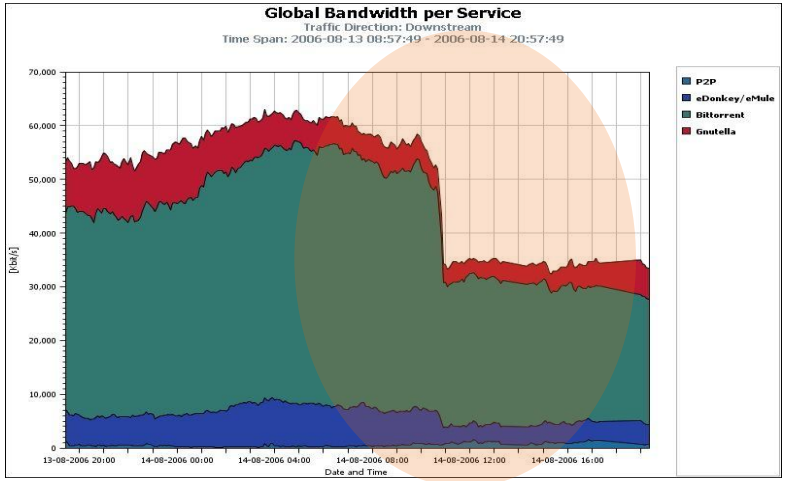
- Обновляемые производителем раз в 3 месяца сигнатуры:
  - Более **1200** сигнатур для классификации **800** приложений
  - Типы приложений: VoIP, Video, P2P, Streaming, Web browsing, Web download, Web video, File-Hosting, Gaming, IM, Enterprise applications, и т.д.
  - Классификация приложений использующих шифрование - Encrypted P2P, Skype, и др.
  - Классификация по портам, когда это применимо.
- Возможность создавать вручную собственные сигнатуры
- Поведенческие механизмы классификации для поддержки новых приложений с нулевого дня.
  - Классифицирует новые приложения VoIP, P2P, File sharing до момента выхода сигнатуры.

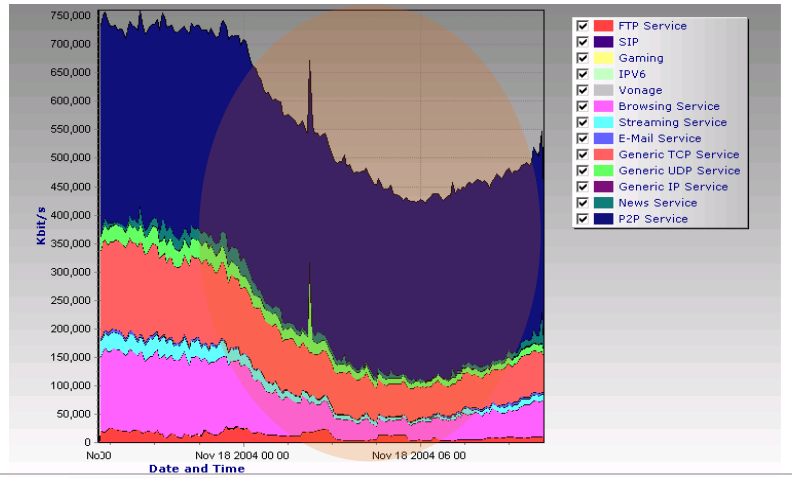
Сервисы DPI в сети оператора связи и предприятия



Управление и оптимизация P2P

- Контроль исходящего P2P
  - По сессиям или полосе
- Временная привязка
  - Политики в ЧНН/ вне ЧНН
- Управление в перегрузках
  - Приоритезация чувствительных приложений при перегрузках
- Справедливость по абонентам
  - Квотирование и лимиты
- Управление по направлениям
  - Различные политики для внутрисетевого и внешнего трафика



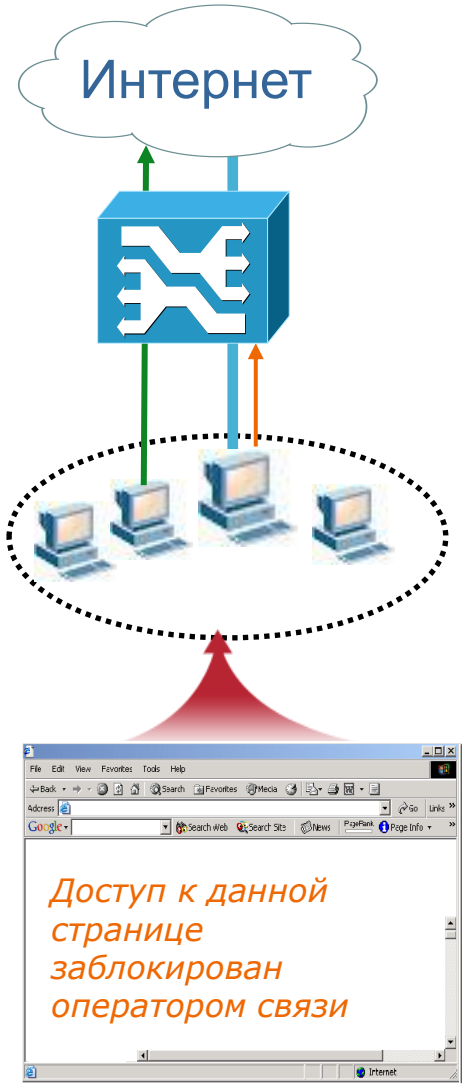


Родительский контроль

- Родители через пользовательский портал могут установить контроль доступа в интернет для своих детей
- Блокировка доступа на некоторые категории сайтов
- Определение временных рамок и ограничение времени пользования Интернетом

Использование черных списков URL на SCE

- Предназначение
  - Родительский контроль
  - Реализация политик компании
  - Пресечение доступа к незаконному контенту и соответствие законодательству
- Возможности
  - Поддерживаются базы – ЦАИР, Websense
  - Блокирование и перенаправление в зависимости от категории URL и политики абонента
  - Встроенные отчеты по категориям посещаемых URL



Сервисы безопасности

Возможность идентифицировать и предотвращать атаки исходящие от собственных абонентов

- Открытый доступ: Провайдер не может ограничить доступ (напр. заблокировать диапазон портов)
- Отсутствие обязательных инструментов безопасности: абонент может не иметь даже элементарных средств защиты
- Абонент как правило не имеет опыта в сетевой безопасности

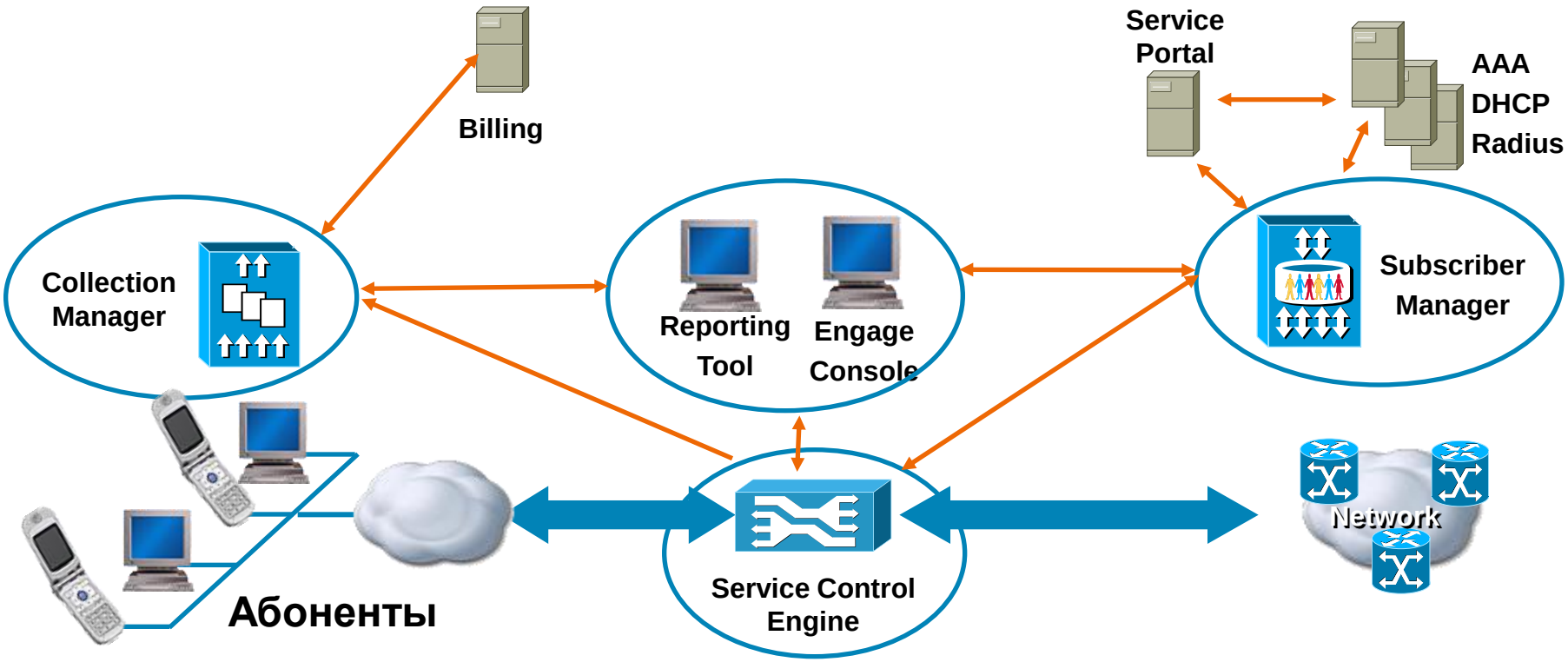
Сервисы безопасности

Возможность идентифицировать и предотвращать атаки исходящие от собственных абонентов

- Спам-боты – выявление на основе анализа SMTP:
  - Чрезмерно большое число SMTP-соединений с одного адреса
- DDoS-атака – выявление по аномалиям трафика
  - Аномальное число соединений от одного внутреннего адреса один внешний адрес
- Сканирование/Распространение – выявление по аномалиям трафика
  - Аномальное число соединений от одного хоста на один или несколько других хостов:
  - Сканирование: Несколько портов, один адресат
  - Распространение червя: Один порт, несколько адресатов.

Экосистема Service Control Engine

Как выглядит решение с SCE в целом?



1. Устройство SCE для разбора и управления трафиком

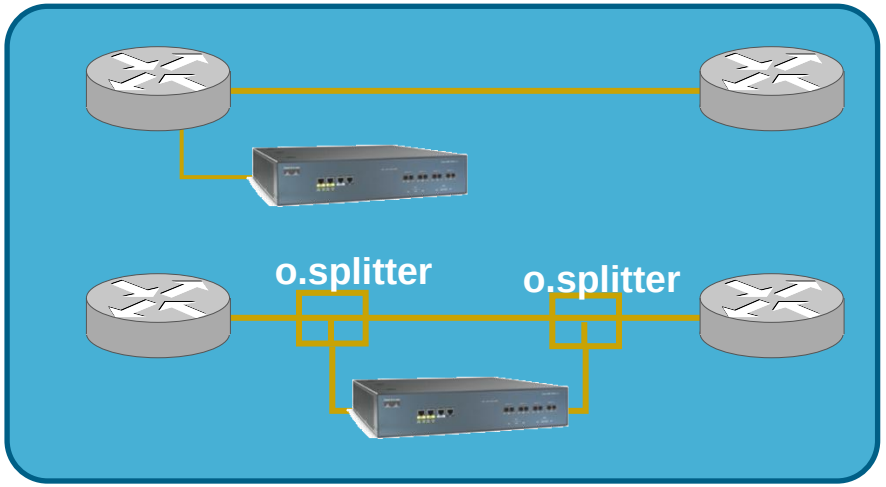
2. Subscriber Manager для координации информации об абоненте с сетевым адресом и политиками обслуживания

3. Collection Manager для сбора статистики для отчетов и биллинга

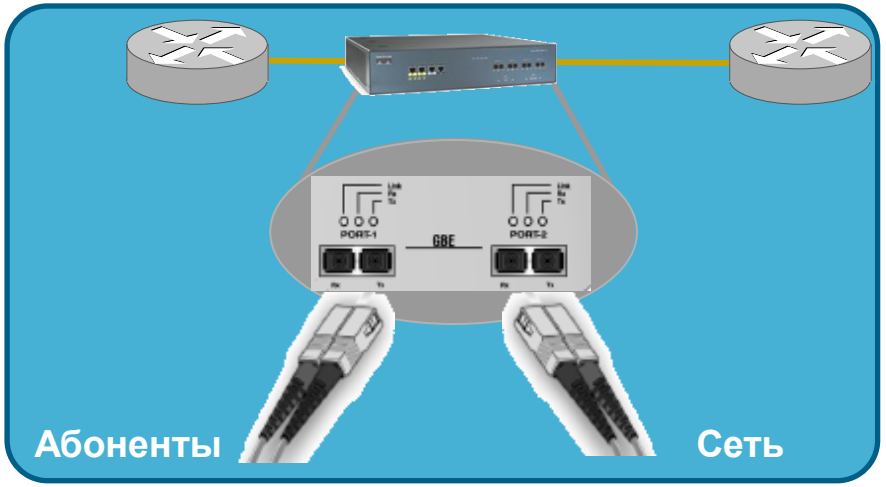
4. SCA-BB & Cisco Insight Предоставление статистики и отчетов

Схема установки SCE

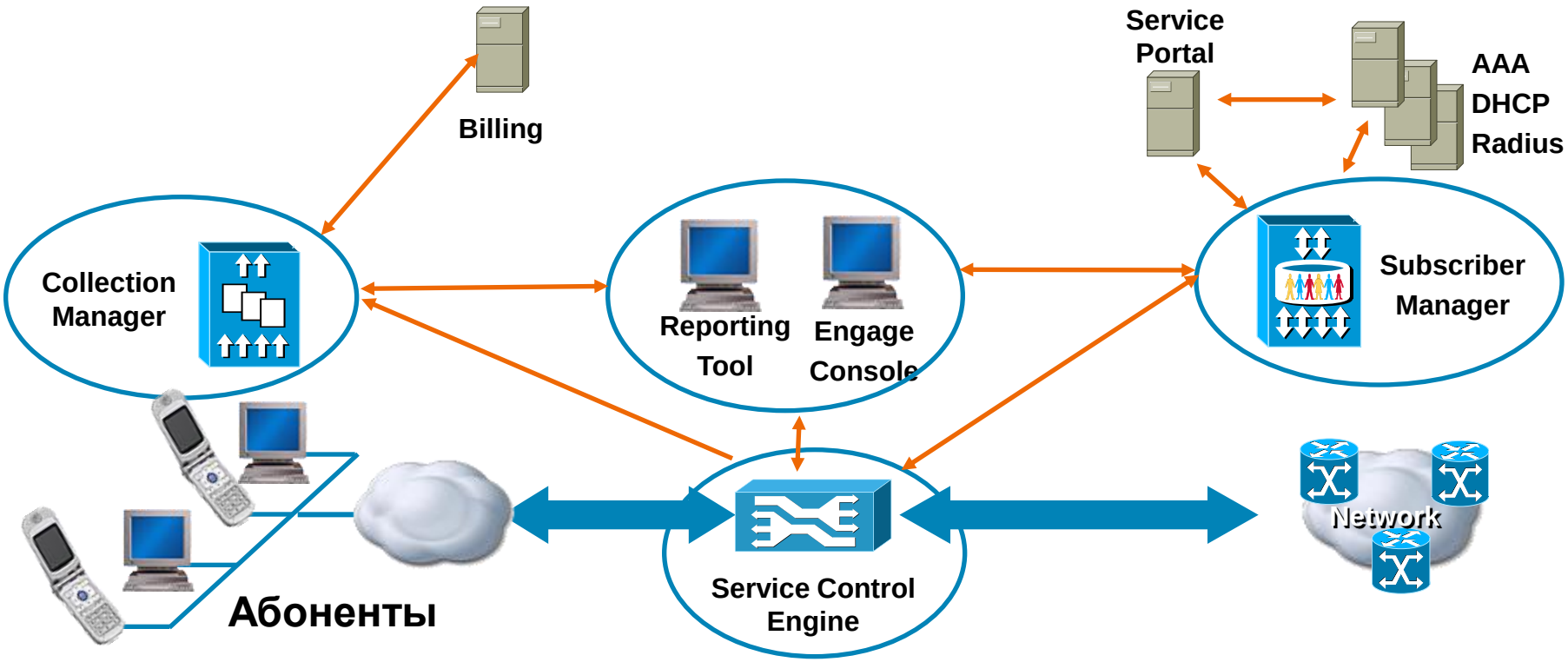
- Топология «Только на прием»
  - •Использование оптического сплиттера или Port-Span
  - •Выполняется только мониторинг трафика



- Топология «в линии»
  - •Устройство устанавливается в разрыв на пути трафика
  - •Выполняется как мониторинг так и управление трафиком



Как выглядит решение с SCE в целом?



1. Устройство SCE
для разбора и управления трафиком

2. Subscriber Manager
для координации информации об абоненте с сетевым адресом и политиками обслуживания

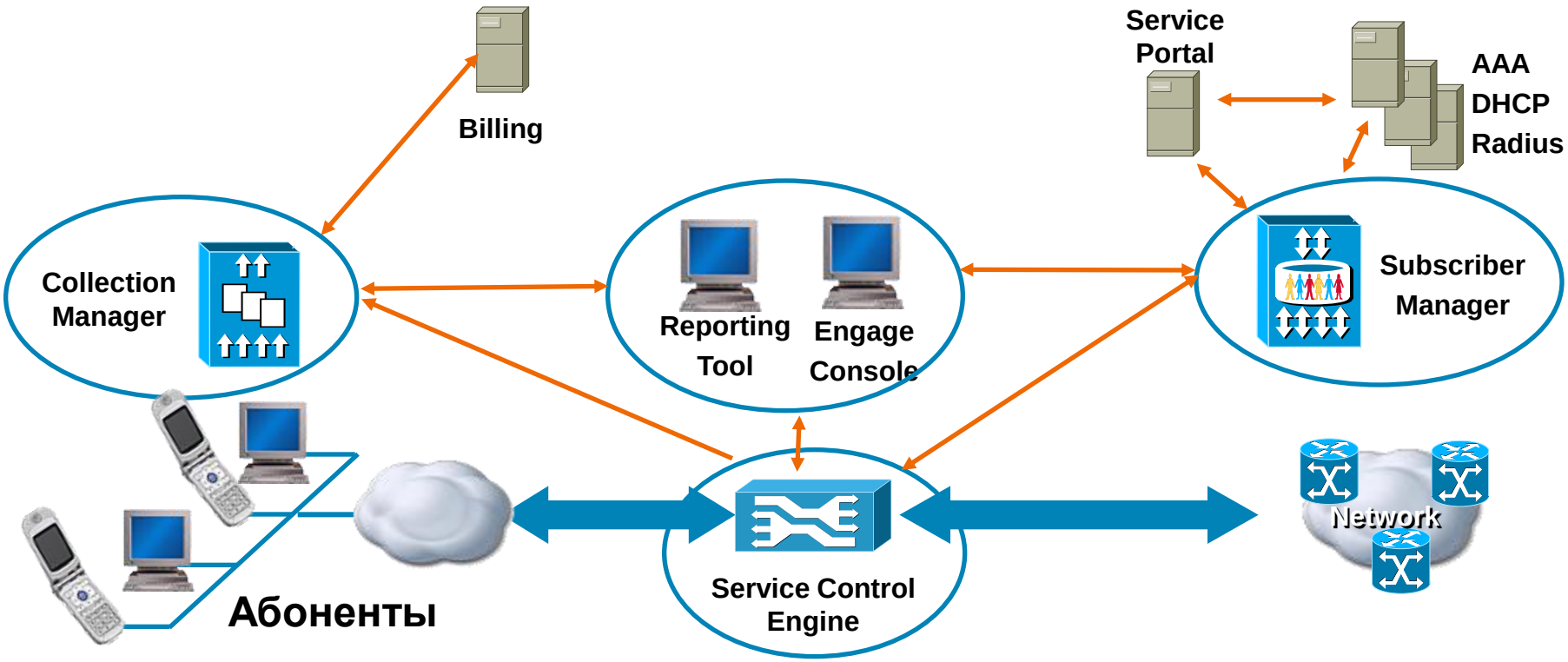
3. Collection Manager
для сбора статистики для отчетов и биллинга

4. Cisco Insight
Предоставление статистики и отчетов

Subscriber Manager (SM)

- Устанавливается на x86 сервер Unix (Solaris, Linux)
- Cisco Subscriber Manager является узлом интеграции
- Контроль и предоставление услуг для абонентов
- Управления абонентскими контекстами
  - ID абонента
  - IP-адрес абонента
  - ID политики (тарифного плана, пакета)
  - Квота для абонента
- Интеграция с системой управления
  - Статическое описание абонента
  - RADIUS AAA
  - DHCP сервер

Как выглядит решение с SCE в целом?



1. Устройство SCE для разбора и управления трафиком

2. Subscriber Manager для координации информации об абоненте с сетевым адресом и политиками обслуживания

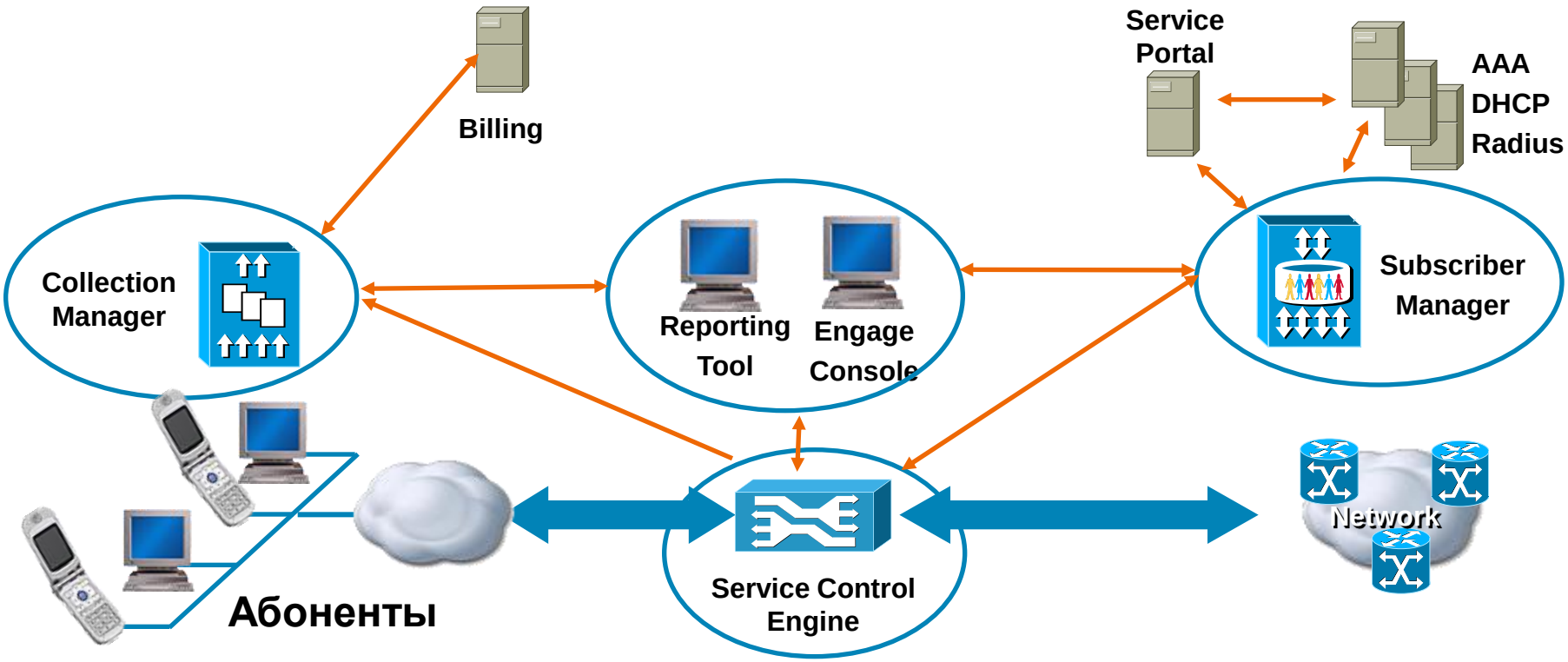
3. Collection Manager для сбора статистики для отчетов и биллинга

4. Cisco Insight Предоставление статистики и отчетов

Collection Manager (CM)

- Устанавливается на x86 сервер Unix (Solaris, Linux)
- Принимает данные в RDR от SCE
- Сохраняет данные в JDBC – совместимую базу данных (Oracle, Sybase, MySQL)
- Предоставляет данные для системы биллинга

Как выглядит решение с SCE в целом?



1. Устройство SCE
   для разбора и управления трафиком

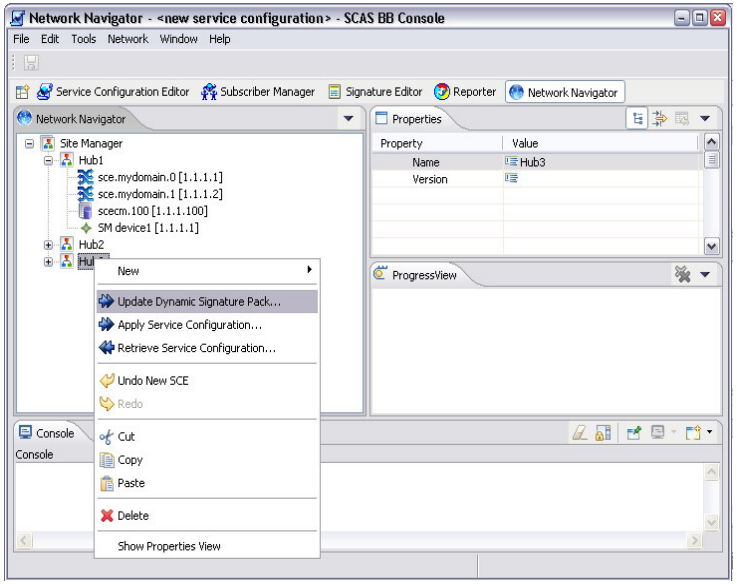
2. Subscriber Manager
   для координации информации об абоненте с сетевым адресом и политиками обслуживания

3. Collection Manager
   для сбора статистики для отчетов и биллинга

4. SCA-BB & Cisco Insight
   Настройка
   Предоставление статистики и отчетов

Cisco Service Control Application (SCA-BB)

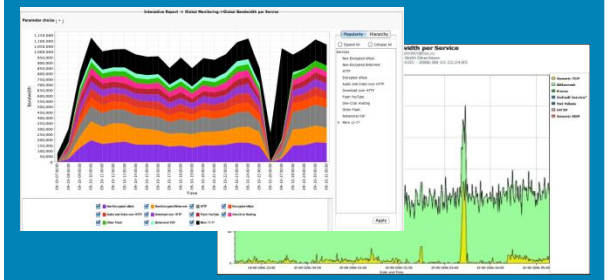
- Программа для OS Windows
- Вся экосистема управляется из одного места
  - SCE
  - SM
  - CM
- Возможнность управления несколькими устройствами
- Встроенные отчеты



Cisco Insight

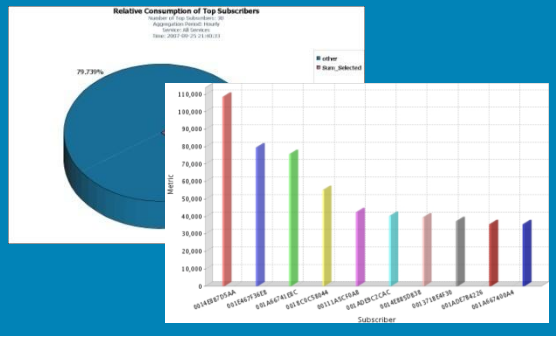
- Высокопроизводительный анализ и централизованная система отчетности для SCE
- Web-based система отчетности (вместо текущего SCA-BB reporter), включающая в себя как все имеющиеся отчеты в SCA-BB, так и новые
- Great usability
- Маштабируется до маштабов любой сети

SCE – примеры аналитики в Cisco Insight



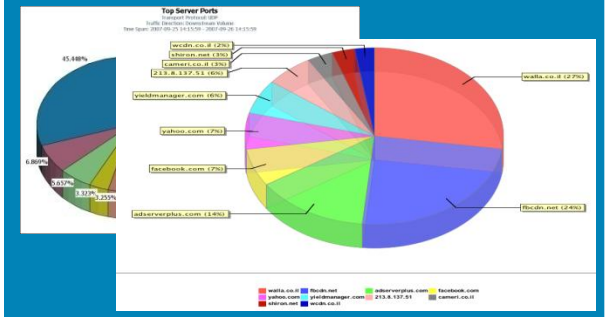
Ресурсные отчеты

- Как расходуются сетевые ресурсы?
- Когда потребуется расширение полосы?
- Где причина congestion?



Демографические отчеты

- Каков процент пользователей P2P/Flash приложений?
- Как выглядят основные профили потребления разными группами абонентов?
- Сколько нам стоят «тяжелые» абоненты?

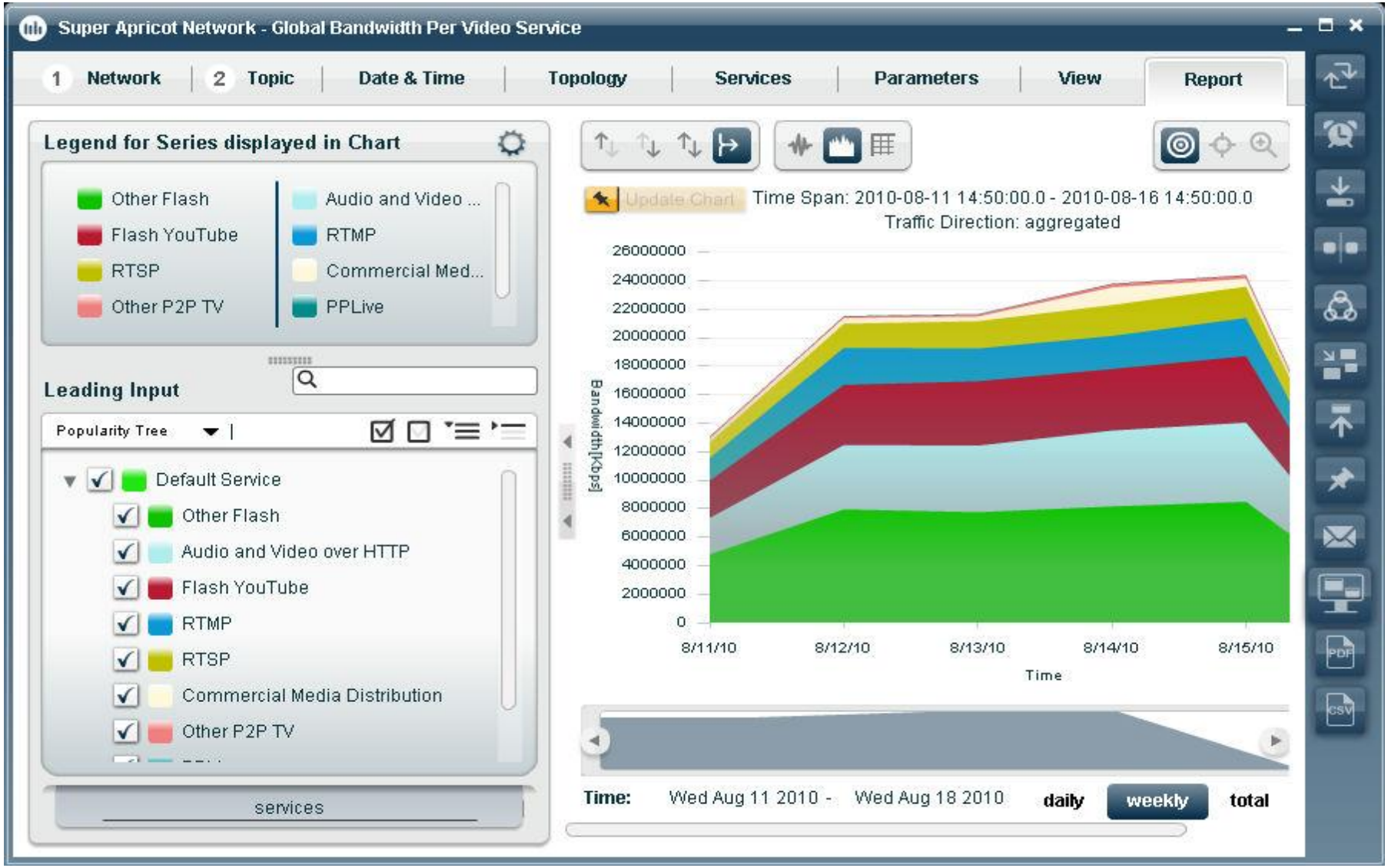


Серверная активность

- Какие web-ресурсы наиболее популярны?
- Какие streaming ресурсы популярны?
- Долгосрочные прогнозы популярности ресурсов

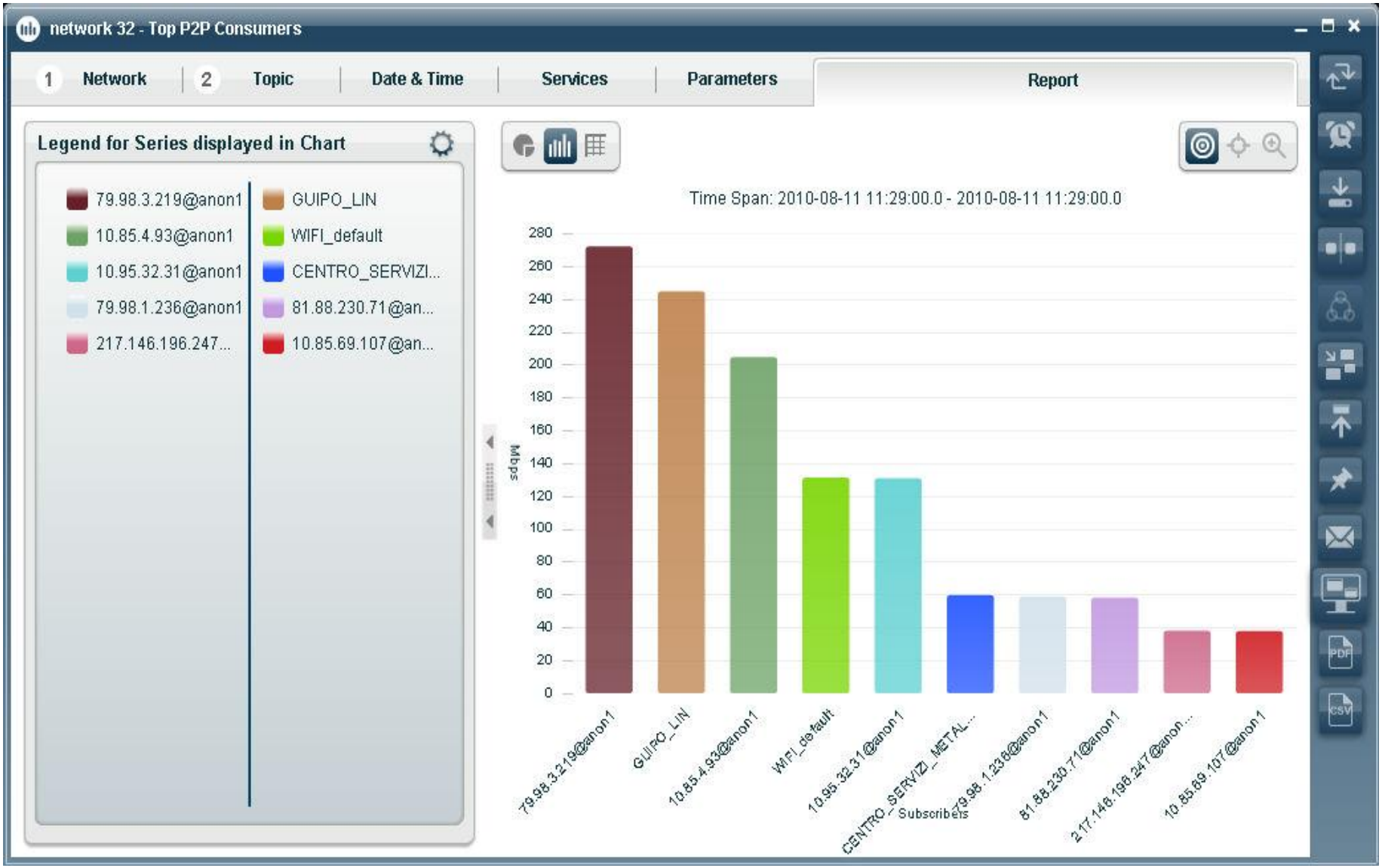
Отчет: Распределение типов трафика

Детальный отчет по каждому типу трафика

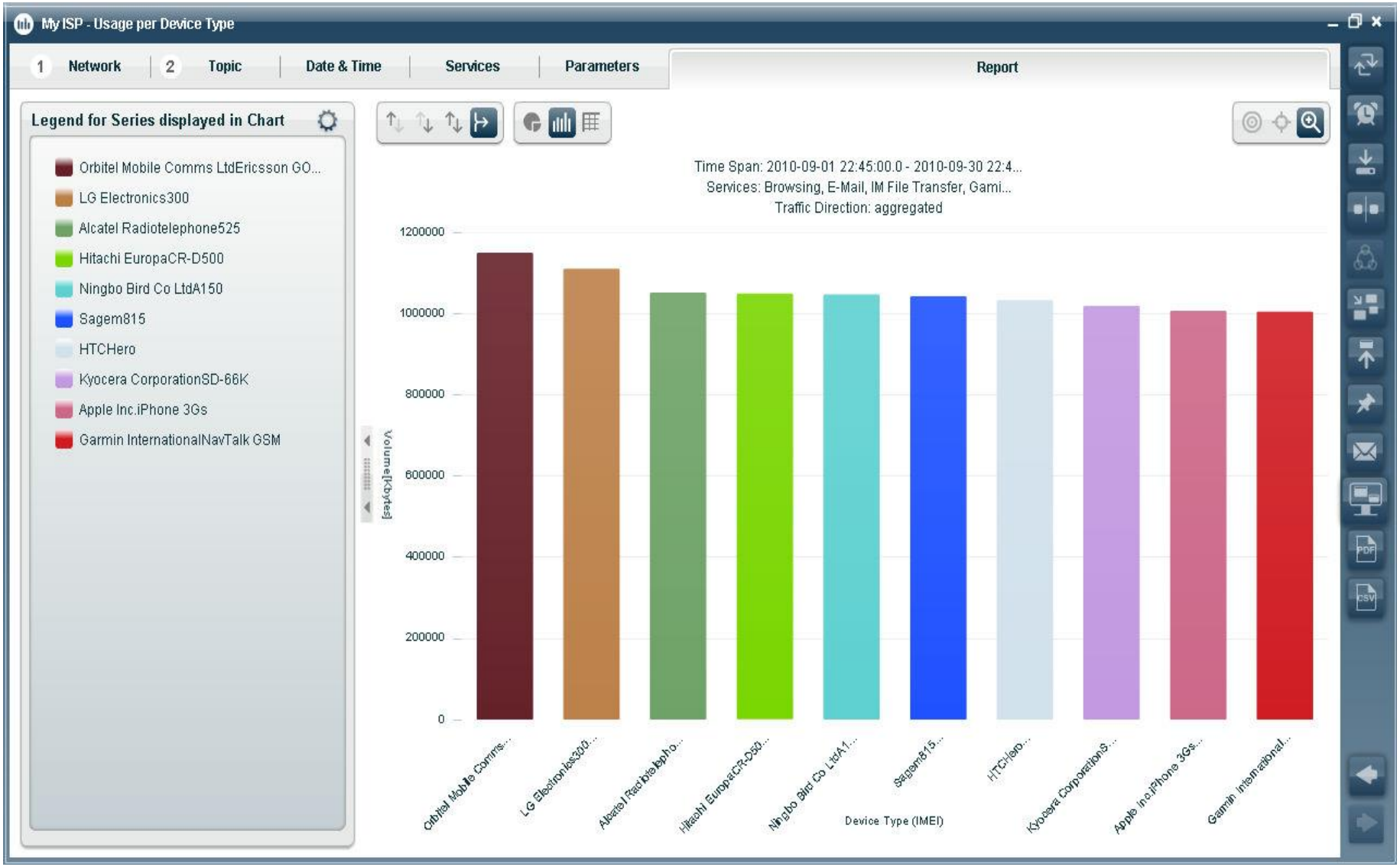


Абоненты, просматривающие больше всего видео

Абоненты, злоупотребляющие torrent программами

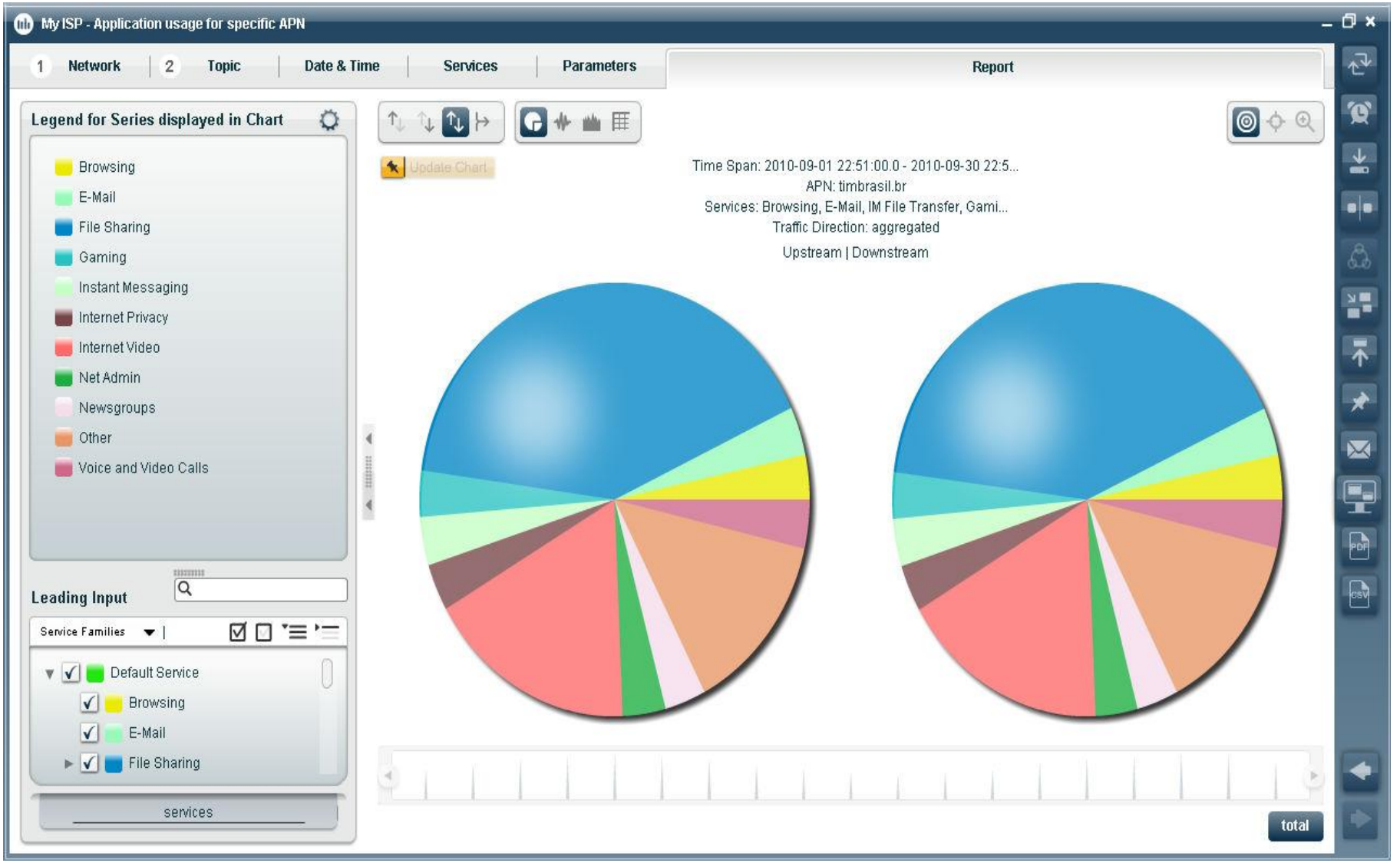


Mobile reports
Volume Usage per Device Type

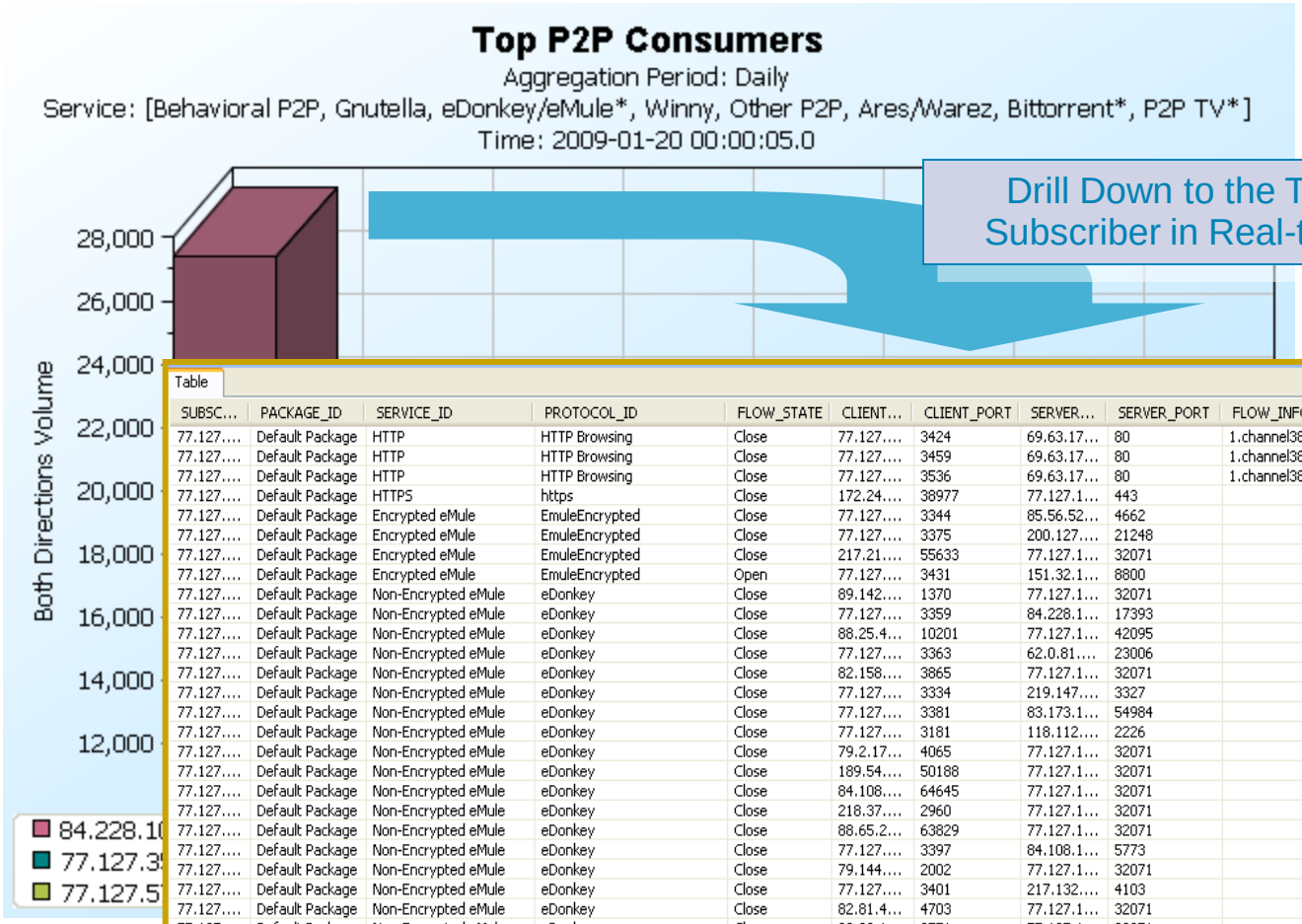


Mobile reports
Application Usage for specific Network

Mobile reports
Application Usage for specific APN



Детальная информация об абоненте



Drill Down to the Top Subscriber in Real-time

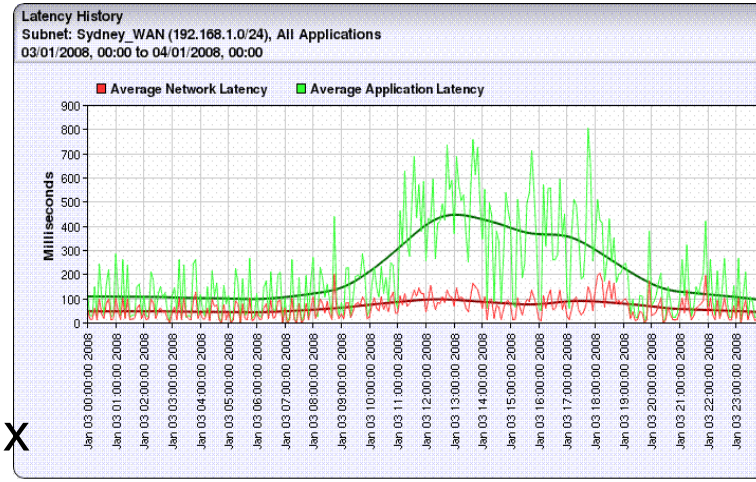
Реальные данные

Table

SUBSC...	PACKAGE_ID	SERVICE_ID	PROTOCOL_ID	FLOW_STATE	CLIENT...	CLIENT_PORT	SERVER...	SERVER_PORT	FLOW_INFO1	F	INITIATING_SIDE	TIME_STAMP	FLOW_DURAT
77.127....	Default Package	HTTP	HTTP Browsing	Close	77.127....	3424	69.63.17...	80	1.channel38.facebook.c...	/...	Subscriber Initiated	Wed, 21 Jan 2009 11:50:26	58.6200
77.127....	Default Package	HTTP	HTTP Browsing	Close	77.127....	3459	69.63.17...	80	1.channel38.facebook.c...	/...	Subscriber Initiated	Wed, 21 Jan 2009 11:50:35	3.0700
77.127....	Default Package	HTTP	HTTP Browsing	Close	77.127....	3536	69.63.17...	80	1.channel38.facebook.c...	/...	Subscriber Initiated	Wed, 21 Jan 2009 11:58:01	301.7300
77.127....	Default Package	HTTPS	https	Close	172.24....	38977	77.127.1...	443			Network Initiated	Wed, 21 Jan 2009 11:53:20	2.4600
77.127....	Default Package	Encrypted eMule	EmuleEncrypted	Close	77.127....	3344	85.56.52...	4662			Subscriber Initiated	Wed, 21 Jan 2009 11:49:12	103.9200
77.127....	Default Package	Encrypted eMule	EmuleEncrypted	Close	77.127....	3375	200.127....	21248			Subscriber Initiated	Wed, 21 Jan 2009 11:49:16	74.2700
77.127....	Default Package	Encrypted eMule	EmuleEncrypted	Close	217.21....	55633	77.127.1...	32071			Network Initiated	Wed, 21 Jan 2009 11:49:51	76.0400
77.127....	Default Package	Encrypted eMule	EmuleEncrypted	Open	77.127....	3431	151.32.1...	8800			Subscriber Initiated	Wed, 21 Jan 2009 11:50:06	19.5500
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	89.142....	1370	77.127.1...	32071			Network Initiated	Wed, 21 Jan 2009 11:48:30	666.9400
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	77.127....	3359	84.228.1...	17393			Subscriber Initiated	Wed, 21 Jan 2009 11:48:34	48.9600
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	88.25.4...	10201	77.127.1...	42095			Network Initiated	Wed, 21 Jan 2009 11:48:41	22.0100
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	77.127....	3363	62.0.81....	23006			Subscriber Initiated	Wed, 21 Jan 2009 11:48:44	51.7300
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	82.158....	3865	77.127.1...	32071			Network Initiated	Wed, 21 Jan 2009 11:48:45	73.3500
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	77.127....	3334	219.147....	3327			Subscriber Initiated	Wed, 21 Jan 2009 11:48:46	76.2100
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	77.127....	3381	83.173.1...	54984			Subscriber Initiated	Wed, 21 Jan 2009 11:48:54	10.4100
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	77.127....	3181	118.112....	2226			Subscriber Initiated	Wed, 21 Jan 2009 11:48:56	301.8800
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	79.2.17....	4065	77.127.1...	32071			Network Initiated	Wed, 21 Jan 2009 11:48:58	74.7700
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	189.54....	50188	77.127.1...	32071			Network Initiated	Wed, 21 Jan 2009 11:49:00	53.6700
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	84.108....	64645	77.127.1...	32071			Network Initiated	Wed, 21 Jan 2009 11:49:23	55.0700
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	218.37....	2960	77.127.1...	32071			Network Initiated	Wed, 21 Jan 2009 11:49:29	67.4300
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	88.65.2...	63829	77.127.1...	32071			Network Initiated	Wed, 21 Jan 2009 11:49:32	733.0200
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	77.127....	3397	84.108.1...	5773			Subscriber Initiated	Wed, 21 Jan 2009 11:49:35	52.4000
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	79.144....	2002	77.127.1...	32071			Network Initiated	Wed, 21 Jan 2009 11:49:36	57.4900
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	77.127....	3401	217.132....	4103			Subscriber Initiated	Wed, 21 Jan 2009 11:49:37	51.5300
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	82.81.4...	4703	77.127.1...	32071			Network Initiated	Wed, 21 Jan 2009 11:49:41	51.2500
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	89.29.1...	2771	77.127.1...	32071			Network Initiated	Wed, 21 Jan 2009 11:50:07	62.9300
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Open	90.44.2...	61838	77.127.1...	32071			Network Initiated	Wed, 21 Jan 2009 11:50:18	0.0000
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	79.178....	44816	77.127.1...	32071			Network Initiated	Wed, 21 Jan 2009 11:50:19	59.6500
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Open	81.67.2...	50836	77.127.1...	32071			Network Initiated	Wed, 21 Jan 2009 11:50:20	0.0000
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	83.38.2...	22841	77.127.1...	32071			Network Initiated	Wed, 21 Jan 2009 11:50:24	55.1700
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	83.196....	57337	77.127.1...	32071			Network Initiated	Wed, 21 Jan 2009 11:50:25	68.9700
77.127....	Default Package	Non-Encrypted eMule	eDonkey	Close	82.224....	49262	77.127.1...	32071			Network Initiated	Wed, 21 Jan 2009 11:50:26	123.8800

Какие проблемы SCE решает

- **Неудовлетворение пользователя от услуг** (загруженная сеть)
  - Нежелательный или не важный трафик занимает слишком большую полосу
  - Business important/real-time трафик страдает от задержек
  - Меньшее количество пользователей занимает большую полосу пропускания канала
- **Необходимость регулировать доступ**
  - Составление отчетов о посещении
  - Блокировка URL
- **Угрозы безопасности**
- **Снижение ARPU (**введение премиальных тарифных планов)



Вопросы и Ответы

Сергей Великанов

Дополнительные вопросы Вы можете задать по электронной почте svelikan@cisco.com

Мы хотели бы узнать Ваше мнение

Пожалуйста, заполните анкету


CISCO