Динамическое определение и контроль приложений в современных IP сетях

Объемы трафика постоянно растут, а доход от его обслуживания остается неизменным. Хотя для обработки увеличивающего объема трафика зачастую требуется повышение производительности оборудования, на что необходимы дополнительные расходы. Одним из способов ответить вопросы о пользователях сети, типе трафика, источниках проблем в сети и исключить потерю прибыли является механизм определения и контроля приложений. Каков общий принцип и особенности работы механизма динамического определения и контроля приложений?

ТЕКСТ: **Сергей Кремезной**,
консультант отдела сетевых технологий
компании «ЭС ЭНД ТИ УКРАИНА»

Наряду с непрекращающимся развитием и лавинообразным ростом нагрузки в IP-сетях, создаваемой множеством постоянно меняющихся типов трафика, до определенного момента времени остается в тени значительное количество таких вопросов, как:

- Каковы реальные пользователи данной сети?
- Какой тип трафика ими генерируется и потребляется?
- Можно ли определить, что является источником той или иной проблемы в сети: сама сеть в целом, определенный сервер или же непосредственный пользователь?
- Можно ли точно узнать каким образом используются сетевые ресурсы, чтобы избежать или хотя бы минимизировать простои и денежные затраты?
- Соблюдается ли предоставляемый SLA? Какой процент пользователей испытывает трудности с работоспособностью или производительностью сети?

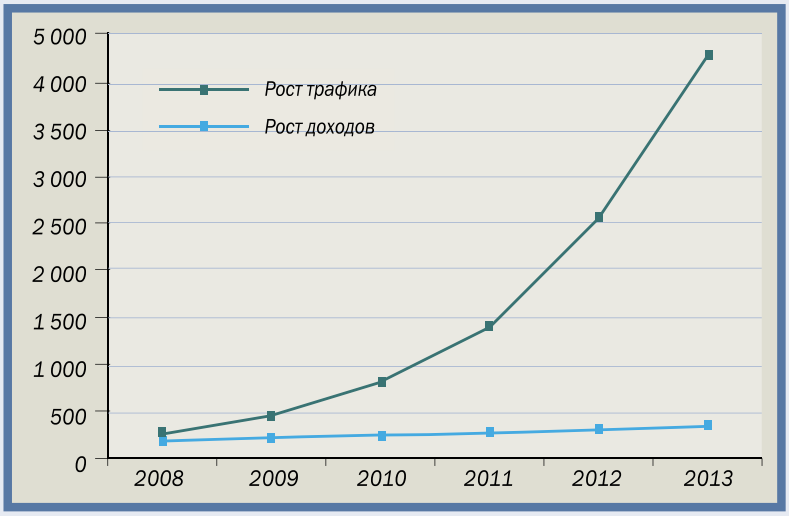
Зачастую даже в больших организациях IT-персонал с многолетним багажом знаний не может полноценно ответить на данные вопросы. И причина тут не в незнании как это сделать, а в том, что не все сети и не все сетевое оборудование готовы предоставить необходимую для этого информацию. Хотя следует также заметить, что не на любом этапе жизни сети существует такая потребность.

Можно обратиться к сравнениям и указать, что потребность в динамическом определении приложений и их последующем контроле необходима в «зрелых» сетях.

Важным также есть аспект увеличения доходов от уже существующего объема трафика в сети, необходимость чего явно видна на следующем графике на основании данных Informa Telecoms & Media.

Т.е., объемы трафика постоянно растут, а доход от его обслуживания остается неизменным. Хотя для обработки увеличивающего объема трафика зачастую требуется повышение производительности оборудования, на что необходимы дополнительные расходы. Одним из способов ответить на вышеуказанные вопросы и исключить потерю прибыли является

Рис. 1. Зависимость доходов от роста трафика



Источник: Informa Telecoms & Media

Рис. 2. Общая схема работы механизма детектирования приложений

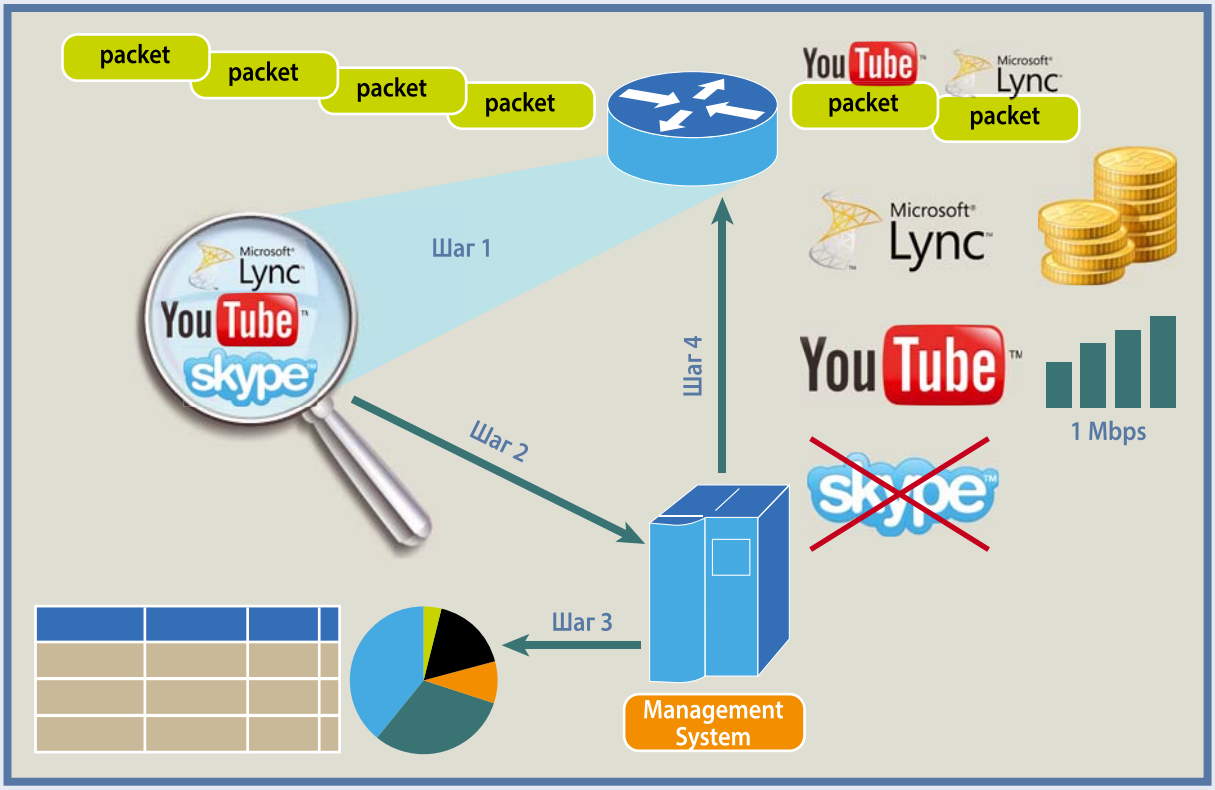
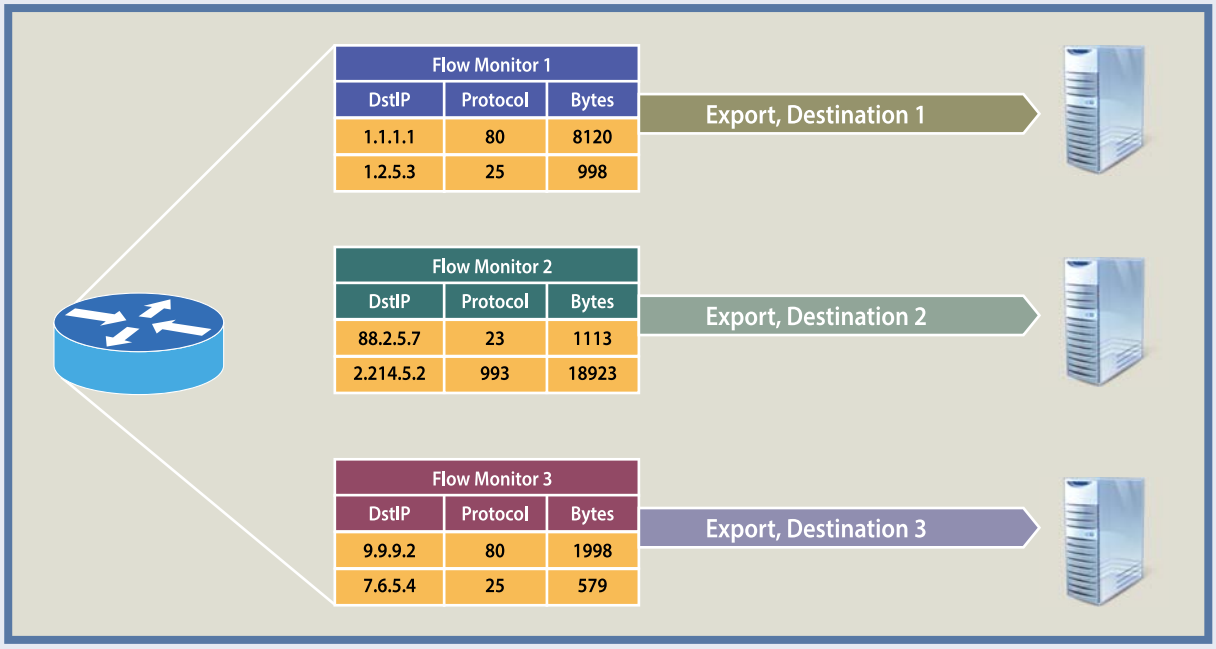


Рис. 3. Механизм Flexible NetFlow



механизм определения и контроля приложений.

Давайте разберем общий принцип работы рассматриваемого механизма динамического определения и контроля приложений.

Определенно, что необходимо «заглядывать» вглубь пакетов трафика, который функционирует в сети. И дабы более точно определить, что за приложение сгенерировало этот пакет и с какими ключевыми параметрами, необходимо разбирать или декапсулировать порцию данных до наивысшего 7-го уровня. Ведь знаний об IP-адресах и используемых портах, которые зачастую динамически меняются, недостаточно. Чаще всего этот процесс именуется, как DPI – Deep Packet Inspection. Некоторые производители оборудования возлагают задачу DPI на маршрутизирующее оборудование, т.к. оно по своей природе уже участвует в процессе разбора пакета, правда не на таком глубоком уровне (Рис. 2, Шаг 1). Учитывая доступные процессорные мощности на сегодня, эта идея выглядит вполне логичной.

Далее, изъятая из пакета данных информация обо всех характеристиках трафика зачастую отдельным протоколом отправляется для сбора, хранения и дальнейшего анализа на оборудование Системы управления (Рис. 2, Шаг 2). Возможны также варианты, когда Система управления в полном объеме или частично также интегрируется с маршрутизирующим оборудованием.

На основании внутренних правил Системы управления, полученная в результате DPI статистика агрегируется, предоставляется необходимому персоналу в графическом виде (Рис. 2, Шаг 3) и создается определенный перечень правил, которые применяются к дальнейшему прохождения трафика через сетевое оборудование (Рис. 2, Шаг 4).

Многие могут отметить, что идея не нова, и будут правы. Но следует отметить, что ранее данный механизм был не настолько актуален, как сегодня. Можно даже попробовать обобщить и сказать, что относительно недавно основной задачей сети была передача клиентского трафика, ведь:

- изначально емкости линий связи были невелики;
- позже возникало ограничение из-за операционных мощностей сетевого оборудования (процессоры, буферы памяти);
- далее камнем преткновения могли стать либо архитектура сетевого оборудования, либо архитектура сети в целом.

Поборов эти преграды, введя глобальное использование механизмов Quality of Service и продажу клиентам SLA (Service Level Agreement), естественно встал вопрос «как это делать более точно, красиво, с наименьшими затратами и с наибольшей выгодой?»

Давайте рассмотрим, как этот механизм реализован у известных вендоров сетевого оборудования, и

какие новшества были введены в последнее время.

Компания Cisco Systems предлагает продукт под названием AVC, что расшифровывается, как Application Visibility and Control. Он создан для решения вышеперечисленных вопросов и работает по уже рассмотренному принципу. Но, конечно же, имеет свои особенности.

Состоит AVC из следующих компонент:

1. **NBAR2** – специализированный протокол, способный определять, к какому типу приложений относится каждый проанализированный им пакет;
2. **Flexible Flow** – протокол, собирающий статистику по обслуживаемому трафику в форме, удобной для дальнейшей ее агрегации и анализа;
3. **Performance Monitoring and Routing** – механизм, позволяющий определять, обслуживается ли определенный тип трафика в соответствии с требуемым качеством.

Первое, что следует отметить, AVC работает на основании обновленного протокола NBAR (Network Based Application Recognition) версии 2. Cisco ставит акцент на том, что сегодняшний HTTP – это новый тип трафика, где приложения стали не прозрачны, где увеличивается количество использований шифрования, где сессии состоят одновременно из потоков нескольких приложений (голос, видео, данные), и где, конечно же, увеличивается процент использования IPv6 (IP протокол 6-й версии).

Изменился также подход к систематизированию типов приложений – появились категории, подкатегории, группы приложений и прочее. Т.е. можно более точно определить, к какому типу приложений относится определенный пакет.

Появилась возможность выполнять загрузку специализированных баз сигнатур приложений PDLM (Protocol Description Language Module) на маршрутизаторы в виде целых пакетов, а не поодиночно, что значительно упрощает их администрирование и сокращает необходимое для этого время. Подход загрузки этих модулей «на лету» без необходимости перезагружаться остался неизменным.

Механизм Flexible NetFlow позволяет выборочно собирать статистику по трафику и отправлять такие выборки на различные сервера (кол-

Рис. 4. Пример использования механизма контроля приложений для качественного использования нескольких каналов связи

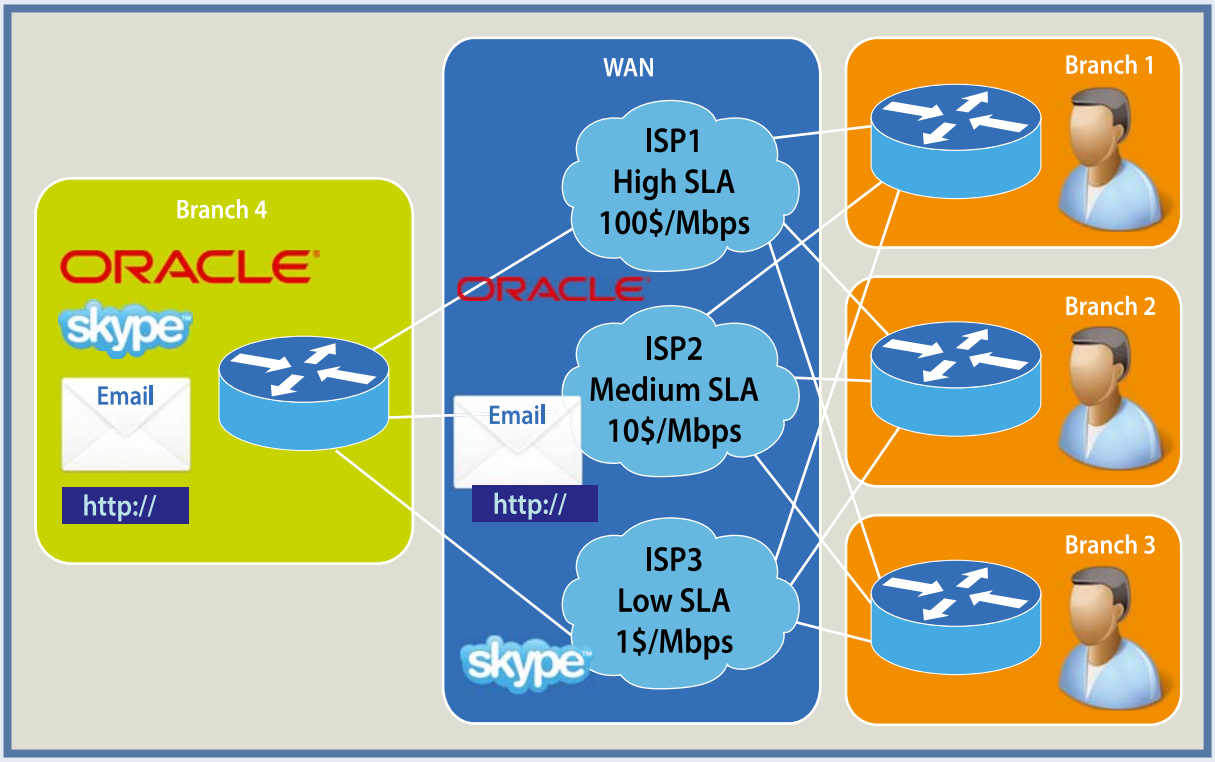
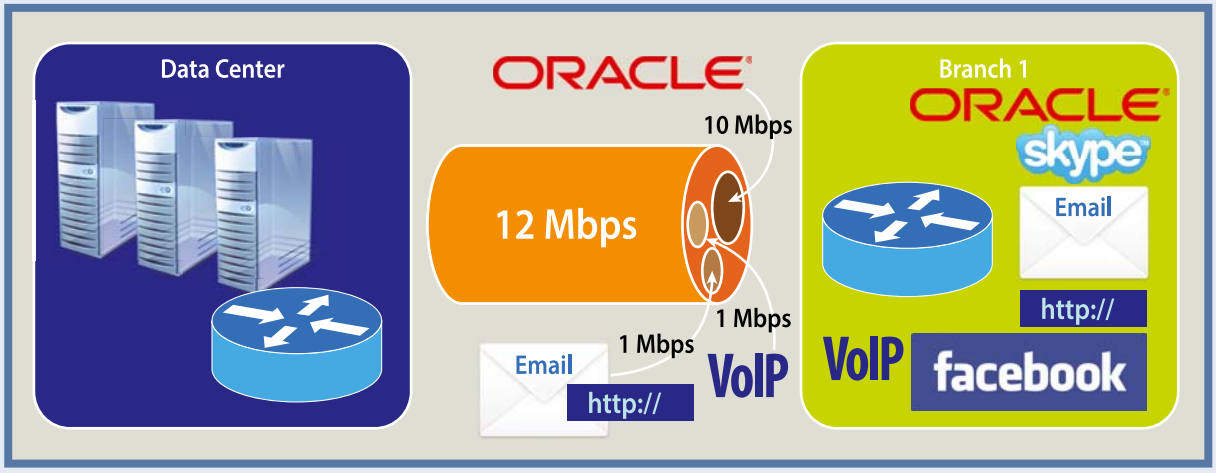


Рис. 6. Пример использования механизма контроля приложений для качественного использования доступной полосы пропускания



лекторы) для анализа. Это позволяет организовать более гибкий процесс «Пассивного» мониторинга за состоянием сети. Напротив, для «Активного» мониторинга можно использовать функционал Performance Agent-а.

Функция Performance Monitoring позволяет следить за основными метриками трафика: jitter, задержка, потеря пакетов и др. Например, можно настроить оповещение оператора или системы управления о возникновении 1% потерь пакетов для трафика приложения Lync. Опция Performance Routing позволяет принимать решение о передаче трафика в определенном направлении на основании типа приложения, которое его сгенерировало. Т.е., критичный трафик направляется в более надежные и емкие каналы связи.

Стоит также отметить, что весь этот функционал доступен лишь на определенном перечне оборудования Cisco Systems: линейках ISR SG и ASR. Лицензирование на данный момент обязательно и является платным.

На оборудовании Juniper Networks функционал динамического определения и контроля приложений реализован на базе технологии Dynamic Application Awareness. Состоит он лишь из механизма DPI (Deep Packet Inspection) и J-Flow, аналоги которых были рассмотрены чуть выше – NBAR2 и Flexible Flow. Компания Juniper решила дополнить данное портфолио механизмом динамического определения и контроля пользователей (subscribers) под названием Dynamic Subscriber Awareness.

Принцип работы Dynamic Application Awareness использует классическую схему, рассмотренную нами выше, а именно:

- маршрутизатор использует механизм DPI для классификации трафика на основании типа приложения, что его сгенерировало;
- принимает решение о том, какую политику применить к трафику – отправить дальше, удалить пакет, применить ограничение или видоизменить его;
- отмечает данные в общей статистике трафика приложений.

Классификация приложений также может описываться вручную или же с помощью загрузки на оборудование готовых специализированных баз сигнатур приложений без необходимости перезагружать оборудование или процесс.

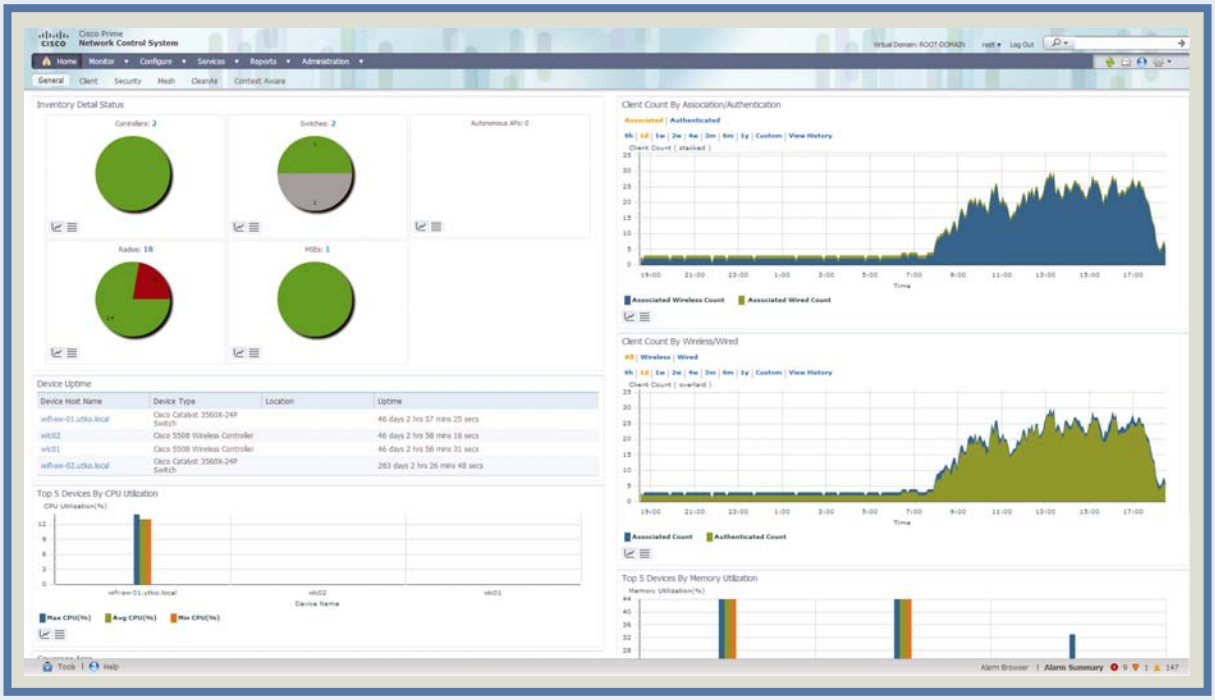
Стоит отметить, что не смотря на заявление Juniper о более «дружелюбной» политике, чем у конкурентов, предоставления полного и единого набора сервисов практически на всей линейке сетевого оборудования компании доступны лишь на маршрутизаторах MX240, MX480, MX960 (линейные платы MS-DPC) и M120, M320 (линейные платы MS-400 and MS-500) после докупки специализированных лицензий.

Давайте рассмотрим варианты практического применения механизма динамического определения и контроля приложений:

1. Схема использования нескольких каналов связи между различными приложениями в сети.

Как и оговаривалось выше, в современной сети функционирует трафик различного назначения – трафик различных приложений. Задача заключается в том, чтобы под критичные приложения (в данном примере Oralce) и только под них выделить надежные и не дешевые каналы связи

Рис. 7. Пример результатов анализа типов приложений в системе Cisco Prime



(High SLA). Это даст гарантии их требуемого функционирования. Также нужно быть уверенным, что никаким другим приложением сети (на схеме это Skype, e-mail, web) дорогие и высоконадежные каналы связи не используются – для них закуплены и организованы более дешевые каналы связи (Medium и Low SLA).

Таким образом, не докупая новых канальных емкостей можно более качественно распределить их применение, используя не только информацию об IP-адресах и TCP/UDP-портах, но и тип приложения.

2. Классическая схема запрета трафика определенного приложения.

Данная схема преследует практически ту же цель, что и в п.1. Разница лишь в том, что определенный трафик – в этом случае трафик в сторону социальной сети Facebook – не направляется в более дешевый канал связи, а попросту удаляется из сети на маршрутизирующем оборудовании.

3. Схема выделения определенному типу трафика определенной полосы пропускания.

Основываясь не на информации о порте включения, метках CoS (Class of Service), IP-адресе и других параметрах L1-L4 уровней, а на точном названии приложения (Oracle, VoIP, Mail, Youtube, etc.) можно более качественно манипулировать доступными емкостями каналов связи.

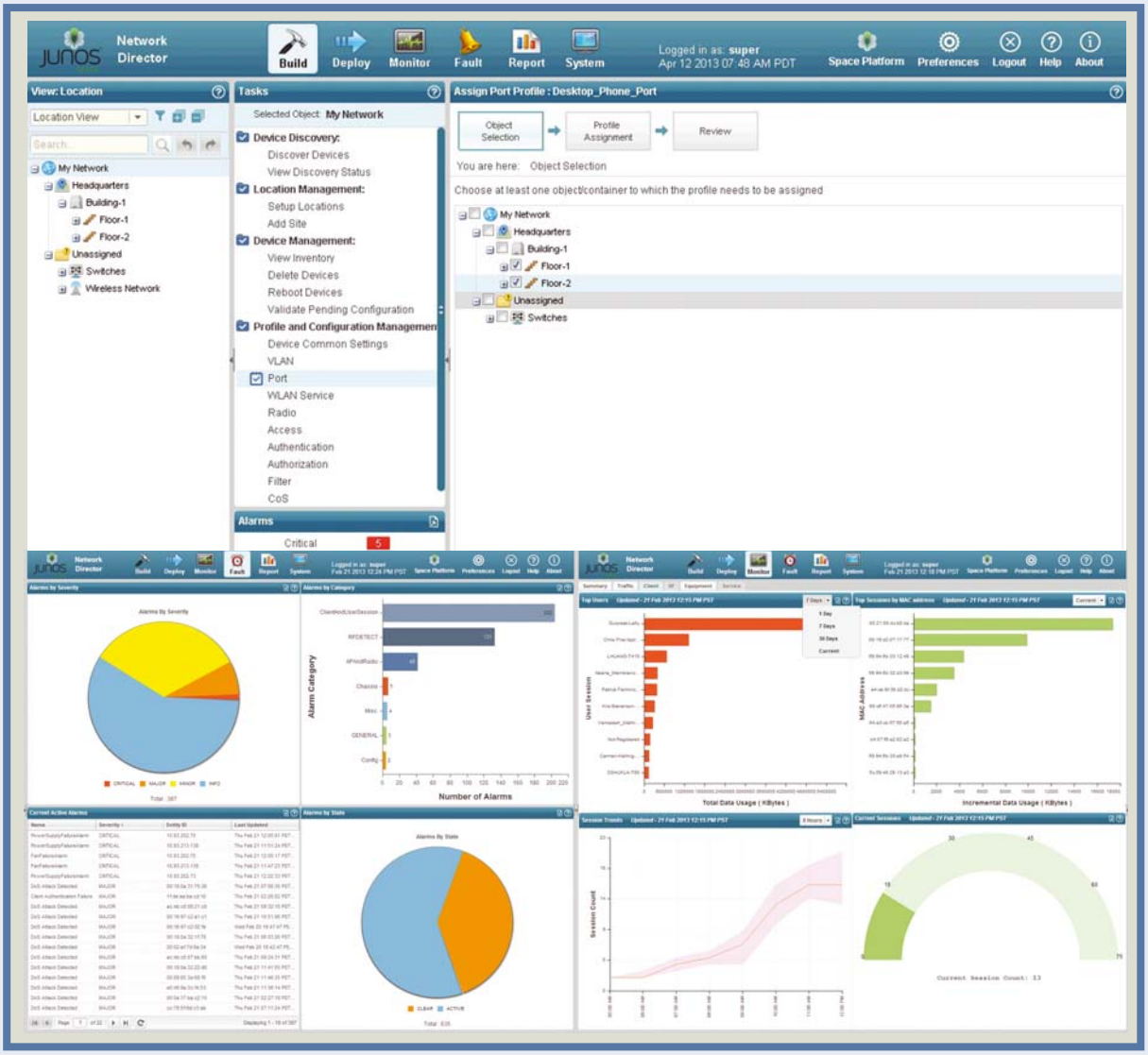
4. Мониторинг за состоянием трафика для определенного приложения.

Используя пассивный (на основание Netflow/J-Flow) или активный (IP SLA механизм) методы мониторинга за состоянием сети можно всегда точно ответить, сколько канальной емкости и каким приложением была занята сеть в тот или иной момент времени, а также какие наблюдались показатели задержек (rtt), джиттера (jitter) или потери пакетов (packet loss). Учитывая большие объемы таких данных и их специфику, мониторинг работает в связке с графической системой управления. У Juniper таковой является семейство продуктов Junos Space, а у Cisco – Cisco Prime.

Хочется также отметить ряд проблем, с которыми описанное выше решение может столкнуться при рассмотрении и внедрении. А именно:

- сложность в определении выгоды. Она на самом деле является косвенной и, как описывалось в начале статьи, не исчисляется в повышении количества обслуживаемого трафика или росте абонентской базы и пр. Нужно понимать, что динамическое определение и контроль трафика является дополнительной услугой

Рис. 8. Пример результатов анализа типов приложений в системе Junos Space



к уже существующим и, в конечном счете, позволяет уменьшить расходы на функционирование существующей сетевой инфраструктуры в разрезе потребляемого ею трафика.

- Высокое требование к ресурсам. Технология является очень требовательной к ресурсам сетевого и серверного оборудования, поэтому требует очень тщательной проработки схемы ее использования: на каких участках сети, для каких конечных пользователей и с какой детализацией.

Подводя итог, хочется еще раз отметить высокую актуальность механизма определения и контроля приложений в сетях любых масштабов и назначения. Так Enterprise сегмент может более гибко и экономнее использовать покупаемые у провайдеров каналы связи, а также иметь в своем распоряжении предсказуемую сеть, зная какие приложения в ней функционируют в каждый момент времени. Центры обработки данных, как коммерческие, так и корпоративные, а также провайдеры связи, учитывая огромные объемы трафика, могут по требованию активировать данный механизм на определенных участках сети или же использовать его на них на постоянной основе за дополнительную плату со стороны клиентов. СТ