Управляется программно: небо, самолет, девушка

SDN, они же "Программно-Конфигурируемые Сети". В Сети появляется все больше материалов об этой концепции. Особенно на английском. На русском же языке пока материалов катастрофически мало. И поскольку информации мало, кто-то сочтет, что ПКС очередная выдумка маркетологов, кто-то внимательно читает свежие релизы, кто-то просто следит за развитием событий. Мы же взяли и потрогали телекоммуникационный прибор, основанный на концепции SDN и даже включили его в Сеть.

Сразу хочется оговориться - данный материал не является ни руководством по внедрению, ни исчерпывающим технико-коммерческим отчетом, и ни в коем случае не претендует на роль "истины в последней инстанции". Это всего лишь описание системы, которая может быть полезной, во-первых, для понимания (автора, прежде всего) концепции SDN, а во-вторых, возможно заинтересует для практического применения в некоторых подсистемах действующих операторов связи. Наконец, это просто интересно - повертеть в руках и понажимать кнопки у устройства, которого пока ни у кого (в России) еще нет. И вообще, статья не про SDN, а про телекоммуникационный сервис, основанный на идеях SDN.

И выглядит этот прибор так:



Небо

Суть™ ПКС уже была несколько раз изложена на Наге:

1. Самая первая статья "Управляется программно";
2. Обзор критических состояний "Бесчеловечные сети" с упоминанием сабжа на полях;
3. Трендсеттерский обзор Нага "Неоднозначность SDN".

Пока на Наге тема исчерпывается этими статьями. И, разумеется, этого недостаточно.

Попробую еще раз изложить концепцию, чем является ПКС коротко в пять пунктов:

1. Разделение функций передачи данных и управления этими процессами как логически, так и фактически.
2. Централизация управления сетью унифицированными программными средствами.
3. Виртуализация физических сетевых ресурсов.
4. Коммодитизация сетевого оборудования.
5. Протокол управления процессом обработки данных OpenFlow, как основа.

На самом же деле, концепцию SDN можно описать еще проще: это очередной эволюционный виток развития интеллектуальных сетей, когда часть информационных систем имплементируются в

собственно Сеть. То есть ПКС ни в коей мере не заменяет и ни вытесняет привычные методы и оборудование построения современных телекоммуникационных сетей, но дополняет их, расширяет возможности, добавляет новую ценность, как потребительскую, так и технологическую.

Никто не станет ломать существующие построенные инфраструктуры только ради того, чтобы сказать: "у нас внедрена SDN". Но вот добавление новых сервисов и сетевых функций становится проще и понятнее, если использовать концепцию.

Кроме того, коммодитазция ("обезличивание", потеря значимых для потребителей различий между продуктами какой-либо категории и/или брендами) телекоммуникационного оборудования и упрощение управления телекоммуникационной системой, позволяет получить довольно ощутимую экономию. А сэкономил - считай, заработал.

При этом аргументация, что SDN это "разводка вендоров" на новые железки не состоятельна, ибо протокол OpenFlow открыт и доступен каждому, а сертификация Open Network Foundation довольно демократична и доступна как для крупных вендоров телеком-оборудования, так и для небольших стартапов, которых появилось достаточно много, чтобы "крупняк" начинал чувствовать жжение ниже спины.

По сути, наступает новая эра, когда роль ведущей скрипки будут исполнять не "серьезные господа в галстуках", но мелкие (с потенцией превратиться в крупные, разумеется) и гибкие компании, у которых есть Идея. А иллюстрация ниже перестанет быть реальностью:



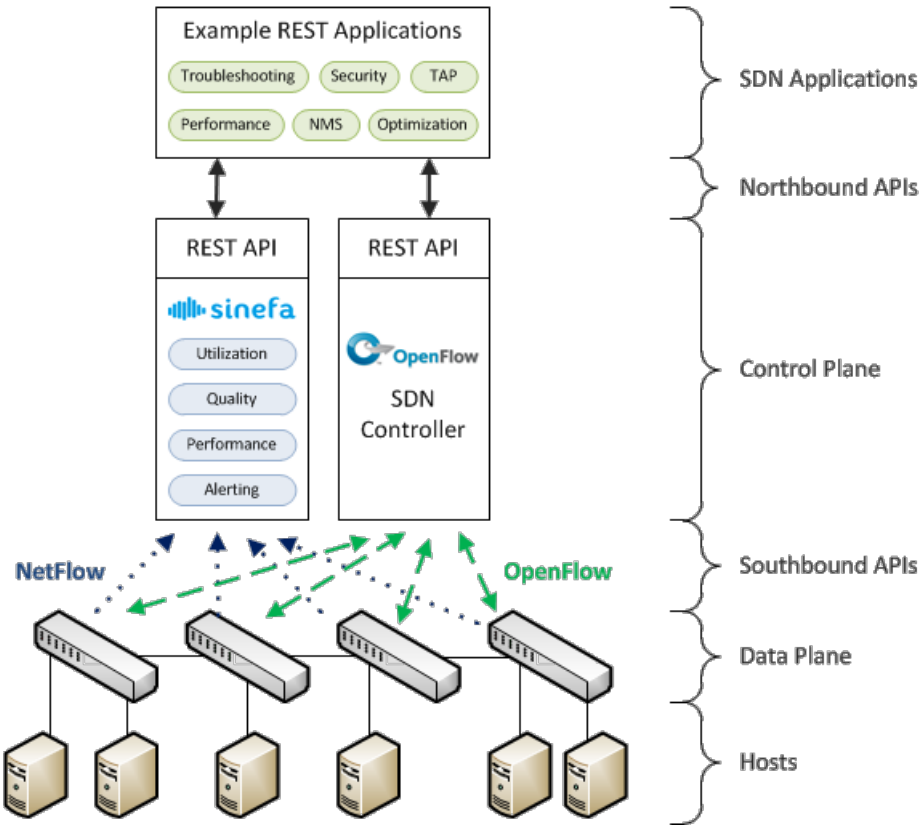
Вот именно решение такой небольшой австралийской компании мы и разберем. Разрешите представить - Sinefa, решение которой представляет собой инструментарий по мониторингу движения битов внутри сетей любой сложности.

Слоган Sinefa (это слово в переводе с чуточку искаженного греческого "σύννεφο" означает "облако"): "*See your network - Improve your network*" - "Наблюдая свою сеть - улучшаешь свою сеть". Ну, как-то так.

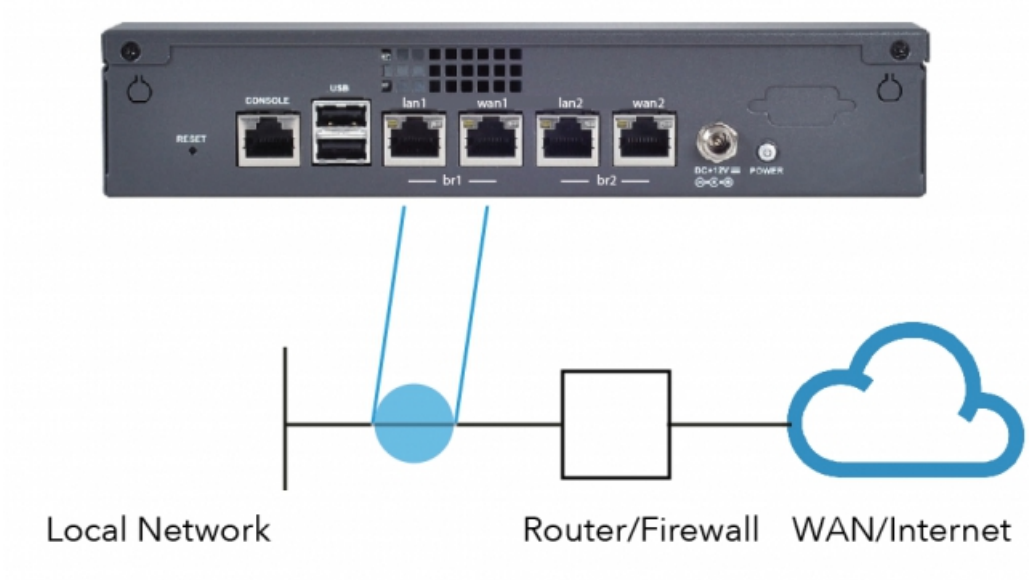
Решение полностью "облачное", то есть не требует долгого и мучительного внедрения, достаточно дешевое и универсальное. И состоит из двух частей: программного обеспечения "в облаке", где происходит обработка и визуализация данных, и специальных зондов (probe), которые устанавливаются физически в точке мониторинга и, собственно, генерируют данные.

К SDN и OpenFlow это решение имеет прямое отношение, но при этом вовсе не обязательно иметь какие-либо устройства в уже существующей сети - для внедрения достаточно просто установить зонды в точке мониторинга и завести аккаунт на специальном сайте. Все остальное достаточно прозрачно и понятно.

Вот так выглядит функциональная схема при использовании Sinefa в сетях SDN.



Но и для использования в "обычных сетях" нет ничего сложного: Probe ставится банально "в разрыв" за маршрутизатором корпоративной сети:



Но на самом деле, зонд Sinefa представляет собой программное решение, которое можно установить на виртуальную машину на любом сервере. И даже самостоятельно соорудить зонд на Raspberry PI!

И, собственно, это и есть реализация концепции "программно-конфигурируемой сети" - приложение, которое выполняет определенные функции, устанавливается на универсальном оборудовании, управляется централизованно, имеет открытый API для интеграции с другими приложениями и суть есть виртуальный сервис во всех смыслах.

Осталось понять, что это дает в практическом плане. Но для начала обсудим аппаратные решения, которые, я уверен, скоро станут привычными и весьма распространенными.

Самолет

Фотография девайса крупным планом приведена выше. Зонд в данном решении предоставляется как "черная коробочка" - нет ни описания того, что внутри, ни технико-эксплуатационных характеристик, кроме важного в конкретном случае - "два гигабитных порта" и байпас. Это

идеология такая: ставим прибор "как на картинке и все работает".

Фото со стороны портов:



Но неуемное любопытство заставляет взять в руки отвертку:



И внутри это оказывается... почти обыкновенный компьютер. Ну как "почти"... Есть весь комплект, присущий обычным ПК - микропроцессор под радиатором и обдуваемый вентилятором, жесткий диск на 320GB, DDR3 на 4GB. Но все это на одной плате с четырьмя гигабитными портами. По некоторым косвенным признакам (маркировка на плате - ха-ха!) выясняем в гугле, что это ни что иное, как "компактное сетевое устройство" (Compact desktop network appliance) Lanner FW-7540.

По сути, специализированный ПК для сетевых приложений. Подобную машинку можно использовать для чего угодно: маршрутизация, NAT, VPN, proxy, firewall. Можно накатить Asterisk, например. В данном случае - это зонд Sinefa. Винт я (пока) не снимал, и консолью не подключался (консольный кабель в комплекте почему-то выполнен переходником RJ-45 -> RS-232, я просто не нашел компьютера с com-портом), посему, конкретное софт-решение описывать не буду. Рискну предположить, что там банальный Linux, на котором крутится соответствующий daemon, который анализирует проходящий трафик (да-да - это DPI), собирает стату и в соответствии с настройками шлет накопленную стату в "облако" Sinefa.

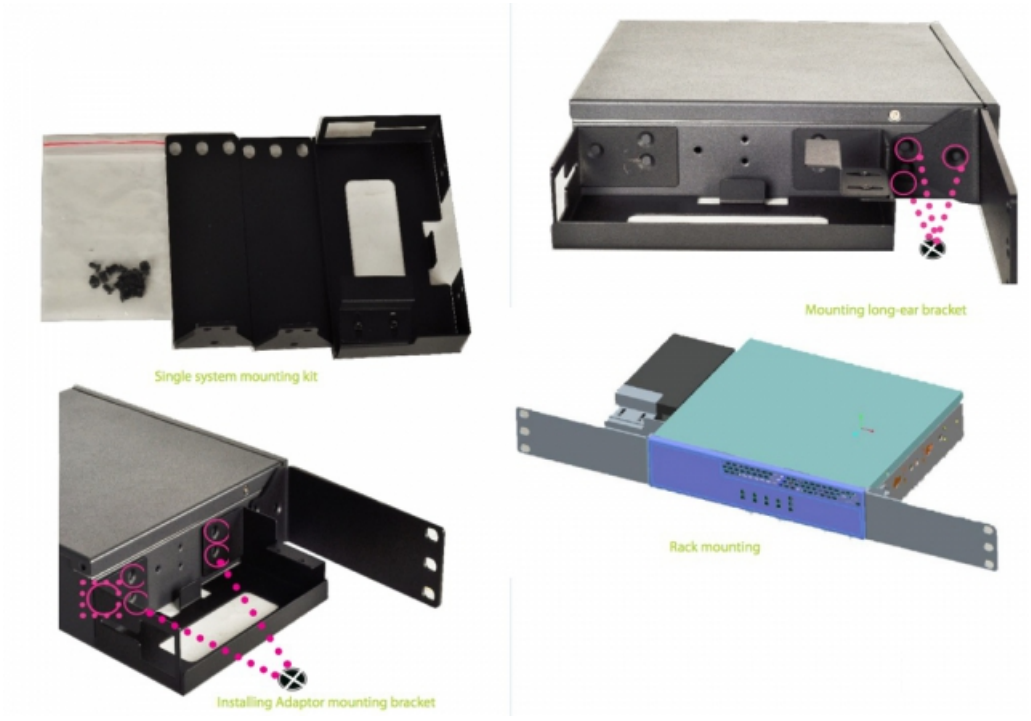
Характеристики сего network appliance по описанию с сайта вендора:

- Intel® Atom™ D425 or Dual Core D525
- Intel® ICH8M Chipset
- Up to 4GB System Memory
- DDR3 800MHz
- 1 x 2.5" HDD Bay (Optional)
- 1 x Type II CompactFlash
- 4 x GbE RJ45
- 2 pairs of G2.5 Bypass
- 2 x USB 2.0
- 1 x Mini-PCIe

Но немного подробностей о конструктиве эплайнса все же стоит сказать. Прибор, по сути, "настольный". Размер его по datasheets - 215.5 x 44 x 190 mm. Но в комплекте есть специальные брекеты, с помощью которых можно вкрутить прибор в стойку:



... я не стал прикручивать, просто приложил. Но в мануале результат нарисован так:

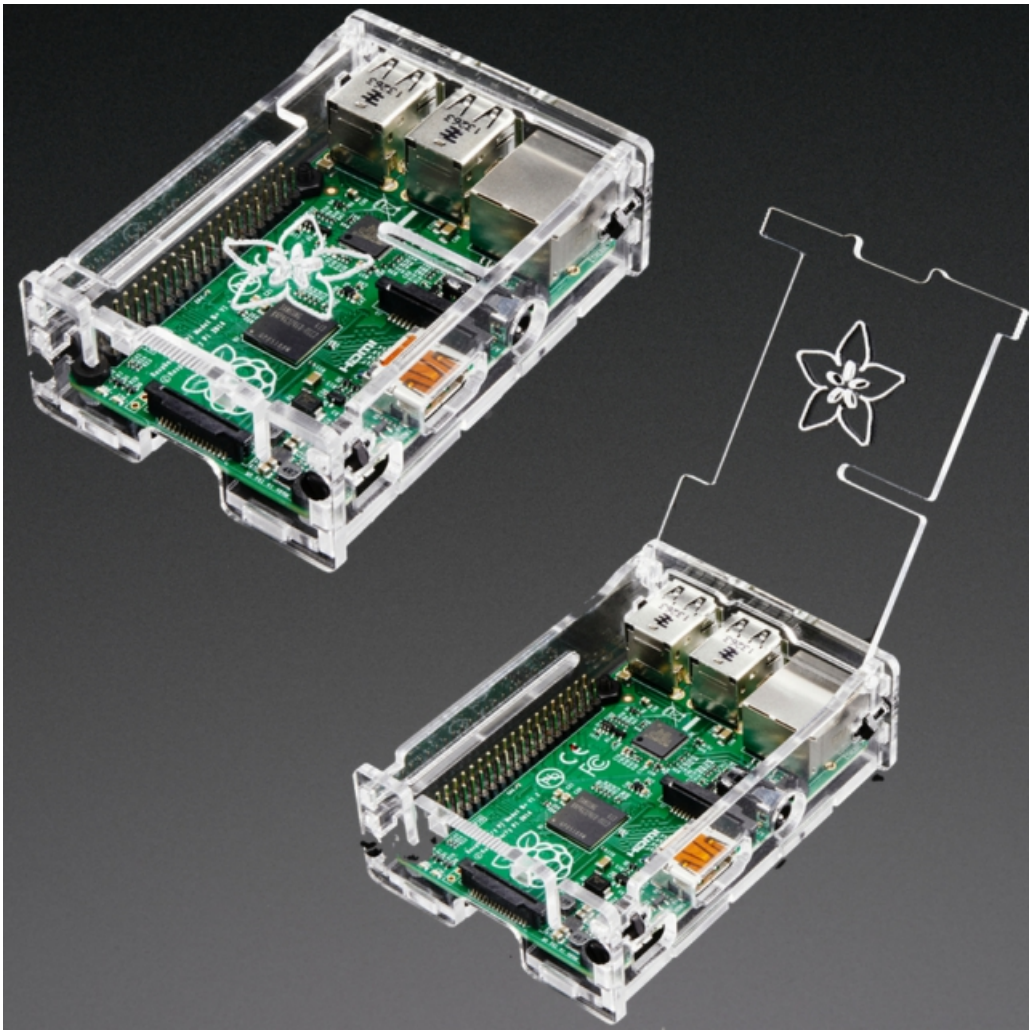


Все эти ушки и винтики в комплекте присутствуют.

На тест мне прислали среднюю модель SF-200. Но в линейке есть еще модель SF-800 - очевидно более мощная, и, очевидно, тоже сетевой компьютер. Что-нибудь похожее на вот это, но я пока не

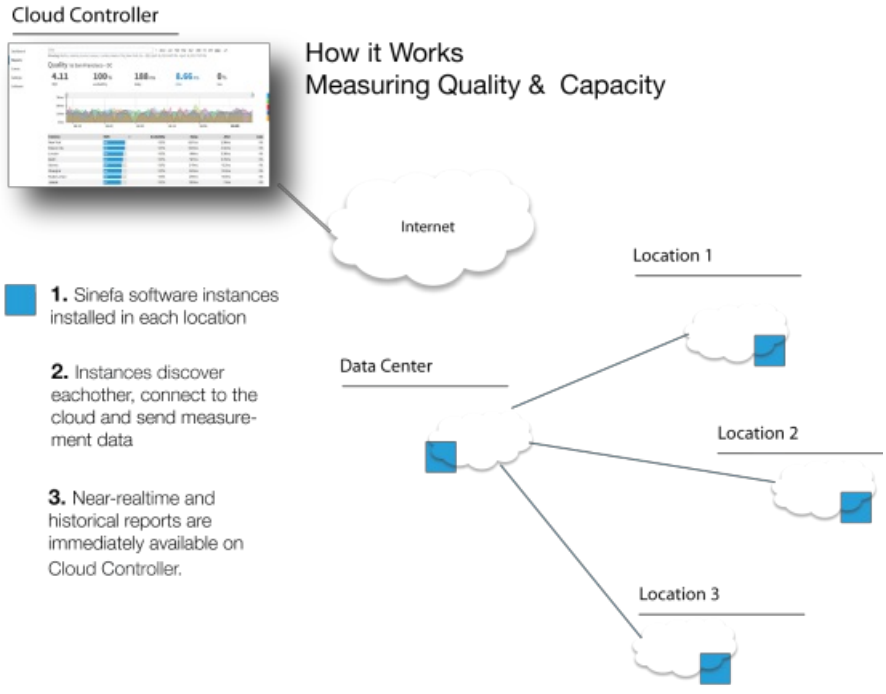
уточнял.

Это решение для довольно серьезных систем мониторинга трафика, но, как уже упоминалось выше, для удаленных точек мониторинга есть возможность "накатить" систему на простецкие Raspberry Pi стоимостью несколько десятков долларов:



... или на виртуальную машину в дата-центре. Кстати, для Amazon уже есть готовый AMI-образ, разворачивание которого занимает считанные секунды.

А общая схема, разъясняющая принципы "как это работает", выглядит так:



Где имеются следующие элементы:

1. Облачный контроллер Sinefa, где через веб-интерфейс можно управлять всей системой мониторинга.
2. Программные инсталляции зондов Sinefa, которые не требуют специального оборудования и можно установить в ДЦ клиента-оператора.
3. "Железные зонды" - вот та же SF-200, например. Предназначены для мониторинга трафика в корпоративных сетях, либо на сетях оператора.
4. "Простые зонды" на Raspberry Pi, которые можно установить в удаленных второстепенных узлах корпоративной сети.

Девушка

И вот мы добрались до самого главного. Какой профит даст нам использование этого решения?

Ценность Sinefa в том, что можно достаточно быстро реализовать полный мониторинг трафика в корпоративной сети. Очень быстро - это буквально в течение нескольких часов, причем, 95% времени займет игры с интерфейсом облачного контроллера, а собственно установка зонда не более 15 минут.

Система управляется через веб-интерфейс, а с настройкой может справиться даже такой несведущий специалист, как автор этих строк.

[Управляется программно: небо, самолет, девушка]

Мониторинг же интересен в следующих случаях:

- Quality (мониторинг банальный - качество трафика, доступность и все вот это);
- Utilization (мониторинг углубленный с разделением по типу трафика, источнику трафика и конкретным сетевым ресурсам - тот самый DPI).

Есть и небольшое учебное видео, но на английском:

Попробую описать применимость системы в реальной жизни, по направлениям, которые мне показались важными и интересными. Возможно, читатели в комментариях напишут другие интересные мысли о тех проблемах, которые смогла бы решить обозреваемая система в реал-лайф. У меня же есть следующие варианты:

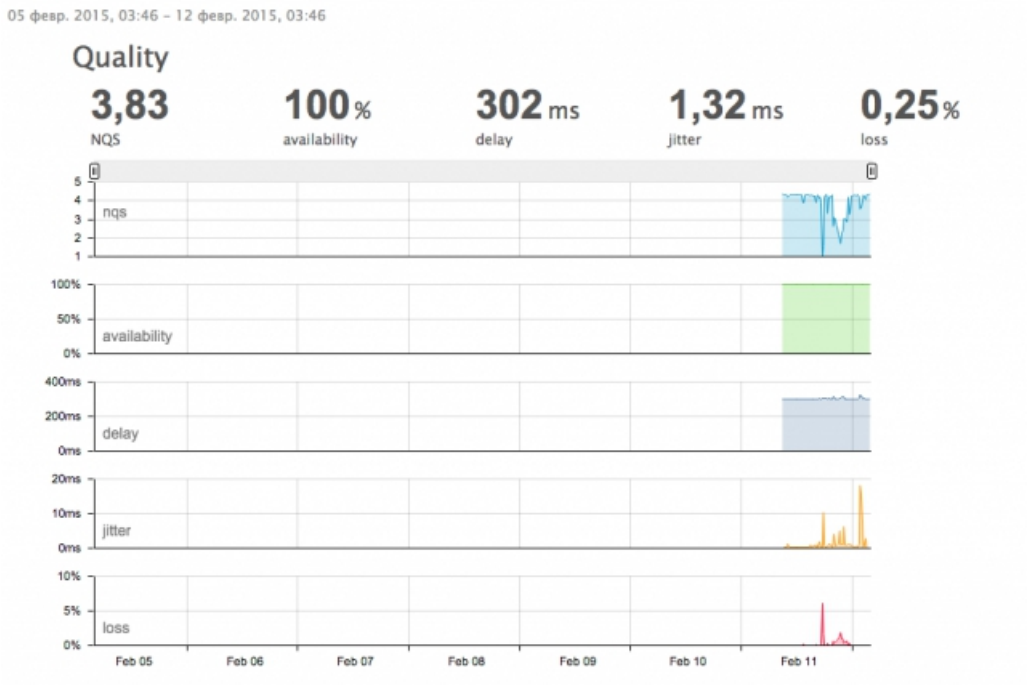
Поддержка SLA

Инсталлируем систему и предлагаем клиентам (корпоративным, разумеется) инструмент для мониторинга исполнения "соглашения об уровне сервиса" по принципу "стороннего арбитра" (third party). Причем Sinefa не только даст полный отчет о качестве услуги, но и просигнализирует (пока только по электронной почте, но принципиально это может быть и SMS, мессендежеры или даже социальные сети - API открыт) о выходе параметров качества за оговоренные пределы.

Мониторить мы можем все измеряемые параметры качества передачи данных:

1. Доступность (availability)
2. Задержки (delay)
3. Джиттер (jitter)
4. Потери (loss)

Все вместе по хитрой формуле высчитывает главный параметр NQS (Network Quality Score), который выражается по пятибалльной системе от 5 (excellent) до 1 (bad). Вот пример качества сети у меня в офисе, которую назвать прекрасной все же нельзя, хотя бывает и хуже.

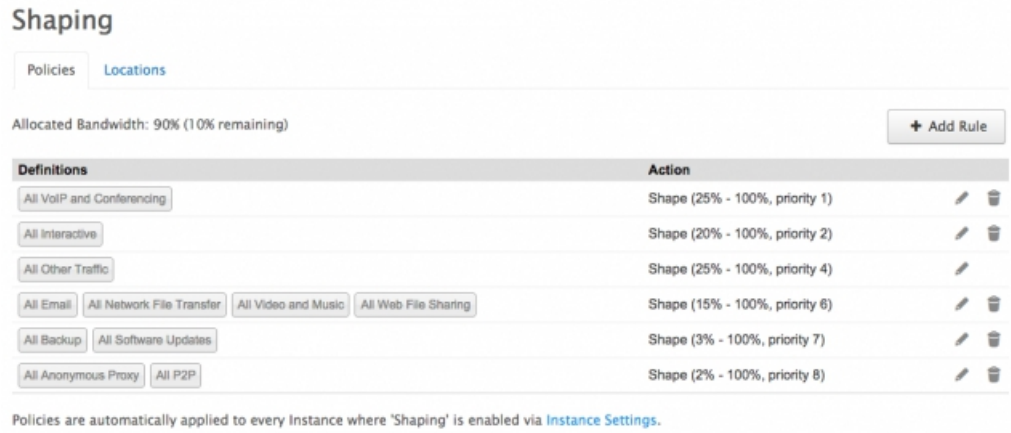


Мониторинг NQS полезен тем, что, во-первых, об авариях в сети администраторы будут узнавать быстрее пользователей. Во-вторых, появляется возможность организовать проактивную поддержку сложных корпоративных сетей, выявляя и локализуя проблемы до того, как все обрушится. И в-третьих, автоматизировать процесс отчетности по качеству.

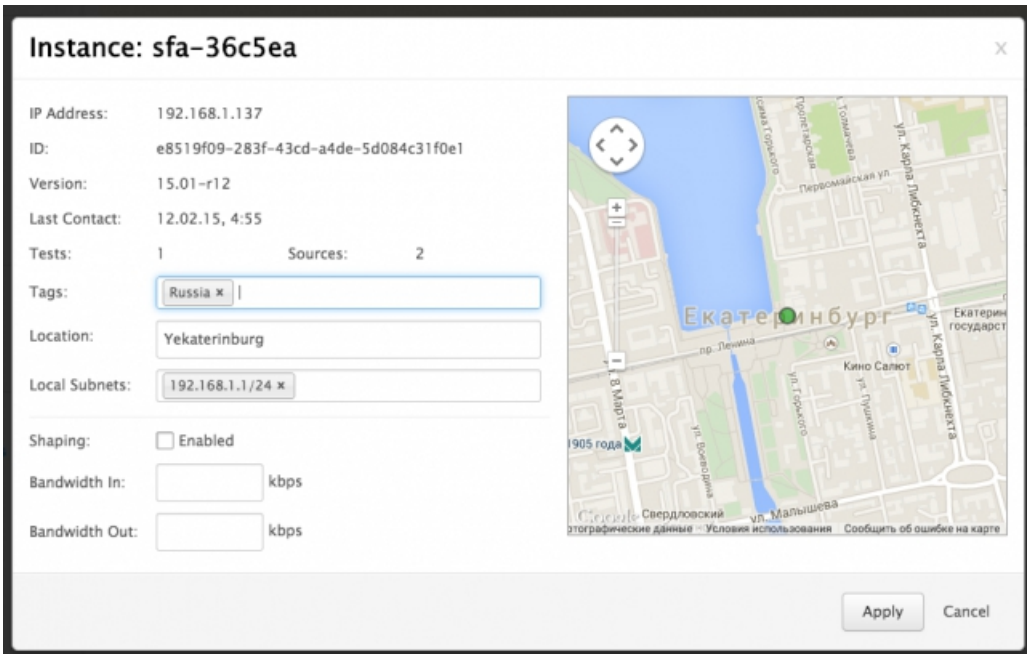
Характерно, что мониторинг качества ПД можно организовать не только между узлами сети, но и внутри сети с детализацией до каждого пользователя. Причем, пользователей можно собирать прямо из корпоративного справочника Active Directory просто подключив его к Sinefa.

Оптимизация сети

Мониторинг качества связи - это не все возможности системы. Sinefa может выступать и в качестве маршрутизатора с возможностью приоритезации/шейпинга трафика. Причем, настройки довольно гибкие и уже имеются преднастроенные паттерны, которые достаточно просто активизировать.



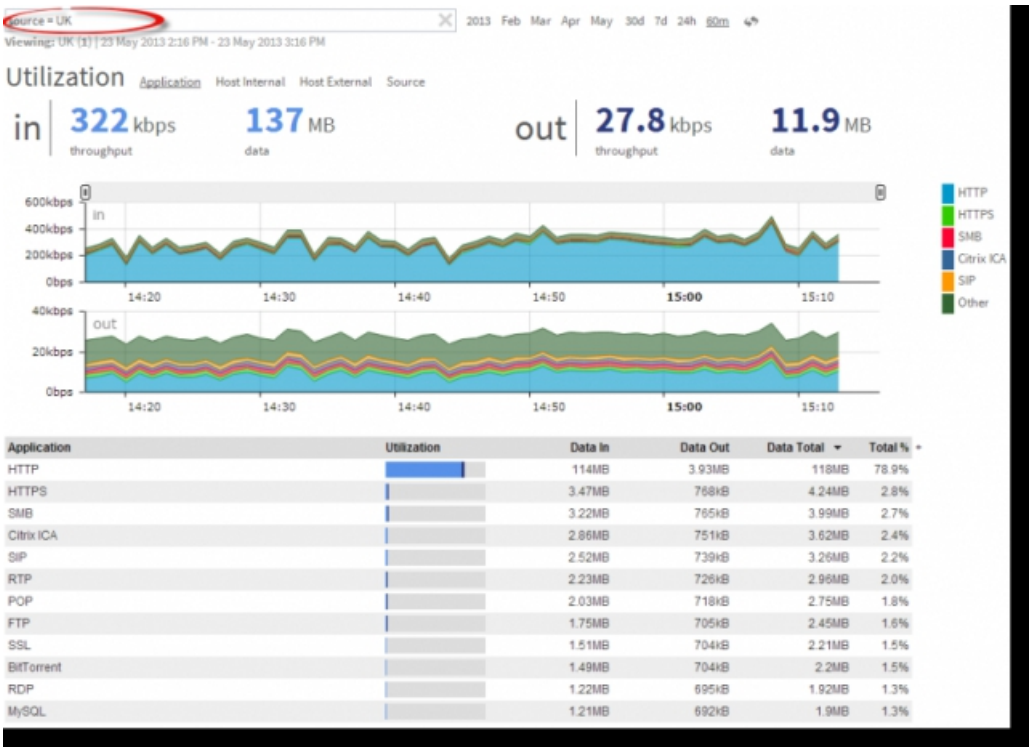
Причем, правила шейпинга можно назначать различным узлам, сегментам и подсетям - см. "галочку" Shaping - Enabled.



Параметры для настроек различных сегментов сети сведены в табличку:

Segment Property	Description
IP Version	Match the Internet Protocol version, e.g. IPv4 or IPv6.
IP Protocol	Match the IP transportpProtocol, e.g. TCP or UDP.
Internal/External Address/Subnet	Match the internal or external IP address or subnet, e.g. 192.168.0.1 or 10.0.0.0/16.
Source/Destination Address/Subnet	Match the source or destination IP address or subnet, e.g. 192.168.0.1 or 10.0.0.0/16.
Source/Destination Port	Match the source or destination ports of TCP or UDP flows, e.g. 80.
Application	Match the application classification, e.g. HTTP, YouTube, Facebook, etc.
Direction	Match the flow direction, e.g. inbound or outbound.
Virtual Circuit	Match the Virtual Circuit name of flows exported from Exinda devices performing QoS.
VLAN	Match the VLAN ID where flows contain 802.1Q VLAN tags, should be a number between 1 and 4095.

В итоге, отчет по типу проходящего трафика в конкретном сегменте сети выглядит следующим образом:



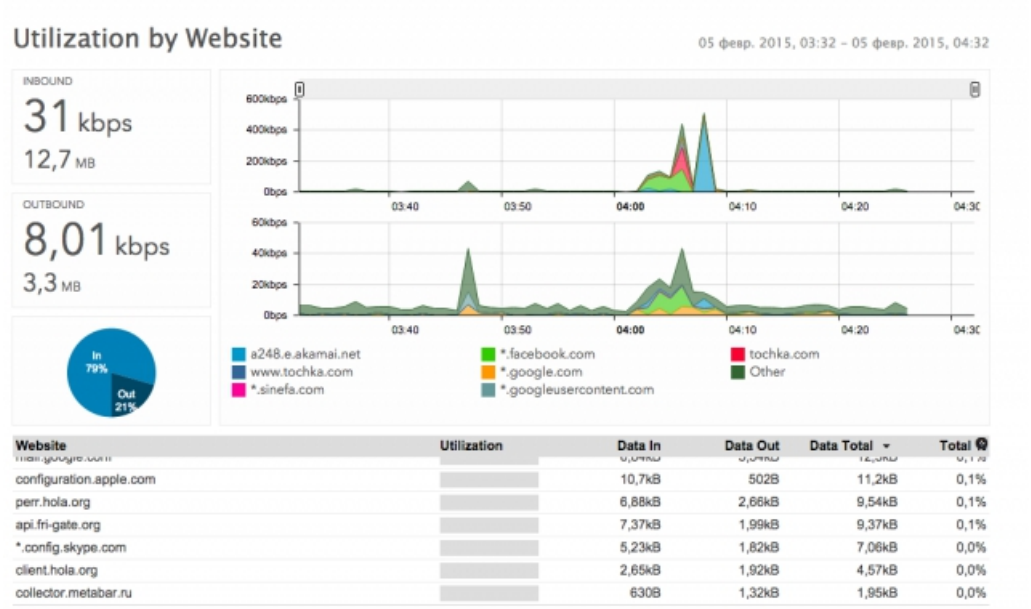
Ну а уж принимать решения по оптимизации сегментов отдельное искусство. По меньшей мере, можно добиться экономии на каналах, просто отказавшись, например, от излишней полосы. Или наоборот - повысив пропускную способность там, где ее действительно не хватает.

Безопасность и продуктивность персонала

Аппаратный зонд Sinefa может работать и как DPI для пропуска трафика. Система анализирует проходящий трафик и аккуратно собирает всю статистику ~~в папочку под подпись компетентным органам~~ в базу данных для последующего анализа.

Опять хочу обратить внимание, что решение это - облачное. И, следовательно, оператор связи может оказывать эту услугу в рамках пакетного предложения за дополнительную плату. Впрочем, и достаточно крупный корпоративный заказчик может так же озадачиться реальной сетевой активностью своих сотрудников.

А служба информационной безопасности получает инструмент анализа проходящего трафика. Как пример, мой опыт: буквально через полчаса после установки зонда, я начал просматривать трафик моего серфинга по Сети и обнаружил ссылку на интернет-порожняк под названием metabar (это такое расширение для браузера, которое ставится, не спрашивая пользователя, а потом пихает свою отвратительную рекламу куда ни попади). Поскольку я несколько раз уже удалял из браузера оный порожняк, очень удивился наличию трафика на этот ресурс:



Оказалось, что порожняк устанавливает вместе с собой другое расширение Fri-Gate, которым я пользовался для доступа к "запрещенным сайтам" (не подумайте плохого, - например, к сайту RCR Wireless, который заблокирован "за одно" по IP с какой-то глупостью). Оказывается, этот самый Fri-Gate таким незамысловатым образом монетизируется, не предупреждая, кстати, пользователей. Фактически, это банальный шпион-malware, паразитирующий на теме "черных списков" - фу таким быть. Расширение было незамедлительно удалено без всякого сожаления, чего и вам советую - ну, мало ли что эти шлемазлы еще придумают. Сегодня они рекламу подсовывают, а завтра будут доносы строчить.

В общем, это третье применение системы Sinefa, которое пришло мне в голову. Но я надеюсь, что читатели придумают еще кейсы.

Хеппи Энд

Пока же хочу превентивно ответить на некоторые вопросы, которые наверняка возникли.

Где купить систему?

В России пока только готовится соглашение с вендором. Будет ли Sinefa в принципе поставляться зависит, в том числе, от реакции на данную заметку. Если будет спрос - будет и предложение. На Наге, разумеется, система появится всенепременно.

Сколько стоит?

Ответ аналогичный предыдущему - пока определенности нет. Пока можно назвать только порядок цен и принцип ценообразования. А принцип заключается в том, что железки продаются отдельно, а услуги - отдельно.

Порядок цен на зонд SF-200 как оборудования - $600 по курсу.

Порядок цен на услуги зависит от нескольких параметров: объем трафика, количества точек в сети, заказанных услуг. Есть, по меньшей мере, два тарифных плана - Lite и Pro. Но возможно для России сделаем третий. Порядок цен начинается от $15 в месяц за бизнес-юнит на тарифе "Лайт", и $45 м месяц за тариф "Про". Принцип ценообразования для ЮВА и Австралии можно прочитать вот тут.

Как там с исполнением "сервера в России"?

Пока все работает "на серверах в Калифорнии". Если будет спрос - сделаем инсталляцию в России, не вопрос. Ни один супостат не узнает о ваших профилях трафика.

А можно ли хотеть странного?

Всегда можно. Но пока есть только вот это. :)

Ну, и на другие вопросы я постараюсь ответить в ЛС, почтой, скайпом или просто в комментарии. Пока же - вот небо, самолет и девушка:

