Тестирование Ericsson SmartEdge 100

 **Несколько сухих фактов**

- Процессорная плата XCRP3
- RAM : 1Гбайт
- Кол-во IPv4 маршрутов – 1 M
- Макс. кол-во интерфейсов – 6x 1 GE
- Макс. кол-во подписчиков (одновременно) – 24к

Собственно сам сервис профиль для инета и для локального трафика.

flow admission-control profile heavy-user
max-flows-per-circuit 100
sustained-creation-rate 10
burst-creation-rate 20
Настраиваем интерфейс с сетью доступа.
no shutdown
medium-type copper
encapsulation dot1q
dot1q pvc 10
bind interface inter local
dhcp relay option
dhcp relay server 91.197.172.18

Настраиваем «фейковый» интерфейс, чтобы SE знал, что делать с абонентами из этой подсети:

interface subs-001 multibind
ip address 172.24.101.254/24

А также профиль субскрайбера:

subscriber profile subs-profile-001
dhcp max-addrs 1
ip interface name subs-001
flow apply admission-control profile heavy-user bidirectional

Терминология
ааа – Аутентификация, Авторизация, Аккаунтинг
субскрайбер – абонент, пользователь, юзер, конечный потребитель ваших услуг

Первые впечатления
SE 100 (дальше по тексту SE), удивительно легкая железка, как по весу так и по стартапу. Загружается сравнительно быстро, во всяком случае на фоне остальных аппаратных маршрутизаторов ждать полной загрузки пришлось всего 2-3 минуты. Интерфейс командной строки (CLI) в общем-то cisco - like , понравилась приятная особенность, после введения команд они применяются либо по выходу из конфиг-режима либо по команде commit: сначала напрягает, а потом думаешь как ты раньше без такого обходился. Разумеется, можно сделать и abort введенных изменений. А также просмотреть сделанные изменения, вызывая show команды не выходя из конфигурационного режима.

Шасси выполнено хорошо, хотя металл мог быть и чуть потолще, особенно у верхней крышки, ну да ладно не книжки складывать. Шум, издаваемый устройством вполне комфортный, можно рядом находится и спокойно разговаривать, чего не скажешь о других моноблочных маршрутизаторах. В общем за исполнение 4+ из 5.

Функциональность
Нас в первую очередь интересовала возможность работы в качестве IPoE BRAS. Но также была протестирована функциональность в качестве LNS сервера. Но обо всем по порядку.

Итак, как SE распознает абонента? Для этого есть 2 варианта: статическая привязка абонента к каким-то механизмам доступа и динамическая по DHCP. Увы, по ARP (unclassified source ip) распознавания абонента нет, потому что все ARP запросы обрабатываются в железе и до софтовой части, т.е. до NetBSD kernel они просто не доходят. К слову кол-во ARP запросов, которое SE может прожевать, равно порядка 8 тысяч запросам в секунду для SE 100 со слов производителя. Именно

этим они и объясняют нежелание поддерживать инициацию сессий по arp, т.к. это потребовало бы доставки пользовательского трафика в control plane. А следовательно это свело бы на нет аппаратную реализацию ARP. Но зато DHCP умеет по всякому. Есть варианты использования DHCP-сервера средствами самого SE, так и для работы в качестве DHCP Relay для L 2 сетей доступа, и в качестве DHCP Proxy для L 2 или L 3 сетей доступа. При этом последний режим не поддерживается ни cisco ни juniper. В общем на любой вкус и цвет.

Про DHCP
Что понравилось в работе DHCP Proxy : при наступлении DHCP Discover, SE стучится на Radius и от имени абонента проходит авторизацию, в случае положительного ответа ретранслирует запрос дальше на DHCP сервер и затем уже отдает ответ клиенту. Т.е. на этапе инициализации сессии, SE уже все знает об абоненте и его услугах, на практике это работает, во-первых, надежно (если у вас умер по каким-то причинам Radius, не будет никаких зависших сессий), во-вторых, быстро: следует отметить, что можно применить на уровне линейных модулей rate - limit на кол-во обрабатываемых в секунду DHCP Discover, чтобы обезопасить back - office , т.е. своего рода защита от dos-атак. Более того, через Radius можно управлять почти всеми параметрами для DHCP (подменить giaddr , lease time , и т.п.). Не знаю как вам, а мне очень понравилось. Все упирается только в возможности вашего Radius сервера.

Про Static
Ну, а что делать, если абонент не умеет DHCP? На помощь приходит возможность статически привязывать абонента к различным сущностям (ip , vlan). Но, увы, тут не обошлось без ложки дегтя. Дело в том, что SE это до мозга костей аппаратная железка, и увы, не умеет делать те вещи, которые с точки зрения софтовой реализации пара пустяков.

Так вот, SE не умеет принять что-либо отличное от /32 с radius сервера, т.е. передать /28 или что-то подобное с Radius для статиков – никак, можно только с локальной БД, что не всегда приемлемо. Решение конечно есть - это использовать статические сервисы с привязкой к vlan, правда в этом случае статистику придется снимать через bulkstats, snmp, netflow. И конечно же, смена сервисов абоненту так же вручную будет производится. Применительно к нам, это не очень критично, т.к. таких абонентов у нас мало и тарифы они меняют раз в «пятилетку» С другой стороны, возможно оно и более идеологически правильно иметь более простую и надежную схему работы для юрлиц. Если свалятся не дай бог DHCP или Radius, они смогут продолжать работать в штатном режиме.

Про LNS
Многим так же интересно будет, а возможно ли терминирование L 2 TP абонентов на SE .

Конечно возможно, и LNS в SE имеет такую интересную возможность как LNS slot redundancy. Что это значит? SE без разницы через какой физический порт подключился и работает L 2 TP абонент. Скажем у вас L 3 сеть доступа (или L 2 в данном примере не важно) подключена через 2 интерфейса, один из интерфейсов упал (сгорел, порвался линк и т.д.), и все остальная сеть доступа только через один оставшийся живой линк. Для LNS данная ситуация не является критической, точнее даже для абонента L 2 TP ничего не произойдет (если конечно у вас есть связанность в сети доступа), он как работал так и будет работать. Но за все надо платить, ряд фитч, которые реализованы аппаратно на линейных картах (flow control, nat, radius service engine), увы, работать не будут (что впрочем логично, не так ли?). Возможно, если отключить функциональность LNS slot redundancy, то использование всех аппаратных возможностей SE станет возможным для LNS .

Про PPPoE
Признаюсь честно, данную технологию не используем, и более того она нам совершенно не интересна. Потому и не тестировали.

Про MPLS
Увы, тоже не было возможности протестировать.

Про Radius, абонентов и сервисы/услуги
Для начала расскажу, что мне очень понравилось: наверняка у многих есть тарифы с разной скоростью в зависимости от дня недели, времени суток и наверняка многие управляют этими процессами через биллинг с изменением в NN часов скоростей на шейпере/полисере (через CoA, скриптами и т.д.). В SE для этого есть возможность создать соответствующий сервис, который автоматически в указанное вами время, будет изменять параметры услуги. Весь трафик в SE описывается классами, причем классы работают абсолютно независимо от используемых служб (сервисы, маршрутизация, l 2 фитчи), т.к. все это реализовано аппаратно в firmware на интерфейсных картах, т.е. фактически без снижения производительности.

К абоненту можно прикрутить flow admission control, т.е. описать кол-во активных IP сессий (flow) у субскрайбера для входящих, исходящих или обоих направлениях. Для борьбы с кровососами (торренты), вирусами и просто раздающим инет соседям – маст хэв. Реализовано это так же

аппаратно и проблем с производительностью не возникает.

Т.к. классы работают независимо, то интересной мне показалась возможность создания услуги «детский фильтр». Скажем, создаем отдельный ACL, в который помещаем IP адреса разрешенных сайтов, а весь трафик, который в них не попадает, перенаправляем на портал, в котором абонента информируем о подключенной в данный момент услуги «детский фильтр», и предлагаем ее отключить (насовсем, на NN часов, NN суток и т.д.). Конечно тут необходима поддержка и со стороны биллинга, но к части SE это уже не относится.

К тому же в SE есть возможность подгружать индивидуальный ACL для субскрайбера через Radius, таким образом реализовав индивидуальные фильтры. Из минусов: ACL фильтрует по IP, а не URL, но тут, увы, ничего поделать нельзя (все таки SE маршрутизатор, а не контент-фильтр). Кстати, если использовать специальный DPI модуль, то фильтрацию можно осуществить и по URL .

Через Radius в SE можно управлять всем. Список VSA достаточно обширен и навскидку я просто не нашел в нем того, что мне не хватает.
Из особенностей Radius можно выделить следующие моменты: аккаутинг работает с частотой не чаще раз в 15 минут, ограничение не существенное учитывая тот момент, что 99% абонентов используют безлимитные тарифы, к тому же никто не запрещал использовать netflow для тарификации, тем более что SE может включать netflow индивидуально для каждого абонента. Также SE может работать с квотой, т.е. если выдана квота на объем, то он может либо уронить сервис/сессию на момент ее исчерпания, либо послать в этот момент незапланированный acct - alive , при этом не роняя сессию/сервис и ожидая указаний по CoA со стороны билинга/радиуса. По сути, это полностью нивелирует 15 минутный лимит по update-ам. Второй момент, SE не умеет конструировать User-Name из различных атрибутов (Option 82, Vlan и т.д.) , т.е. User - Name всегда показывает MAC адрес абонента, для случаев использования DHCP, либо вручную указанный в конфигурации в случае static. Поэтому если вам для биллинга нужен User-Name отличный от MAC и при этом нужен DHCP на доступе, то извольте конструировать его самостоятельно средствами Radius-сервера из различных VSA атрибутов, которые SE передает в большом количестве, в том числе практически все опции DHCP отображаются в свои VSA .

Что с SE можно еще сделать
Как и большинство современных маршрутизоторов SE поддерживает виртуализацию. Можно создавать сколько угодно виртуальных маршрутизаторов (далее BM), добавлять им различные интерфейсы, вланы и т.д. Но увы, по внутренней шине BM умеют обращаться друг с другом только через IS - IS или статическими маршрутами. Если вам нужен BGP, OSPF, RIP или что-то еще, придется гнать трафик через внешние интерфейсы, попутно навесив на него различные сервисы (если конечно вам нужно).

Зато есть интересная технология кросс-коннект, которая позволяет соединить два различных интерфейса L 2, абсолютно не вмешиваясь в то, что происходит внутри этого виртуального коннекта. Если же вам нужно объединить в одну сеть несколько разных вланов, для этого можно создать виртуальный бридж, причем на каждый влан в отдельности можно повесить также различные сервисы (конечно без ааа, но оно в данном случае и не нужно).

Разумеется, можно также использовать SE и в качестве пограничного маршрутизатора, поддержка всех необходимых для этого протоколов есть, но признаюсь честно, не тестировал, хотя опять же не думаю, что в данном функционале могут возникнуть проблемы.

Ограничения
Идеального оборудования не бывает, и у SE есть свои ограничения: в текущей версии нельзя использовать LACP (Ethernet - channel) совместно с по-сервисным аккутингом с их инициализацией через Radius . Но тут есть такой момент, что другие производители не умеют терминировать абонентов поверх LACP вообще. Также нельзя использовать бридж для ааа через Radius. Положительный момент: обещали устранить эти ограничения в следующих версиях ПО.

Примеры конфигураций
Создаем сервис профиль для полисинга трафика по направлениям в зависимости от времени суток.

У нас 3 класса: Локальный, Ночной внешний (с 00:00 до 08:00), Остальной внешний.

Профили классов.

Профили для QoS (задаем параметры по умолчанию также).

Эта была сама самая сложная часть в конфиге. :-)

Например, так выглядит flow admission control. Разрешаем субскрайберу создать сразу 20 IP сессий и затем прирост по 10 сессий в секунду, но не более 100.

А вот пример конфигурации IPoE для L 3 сети. Абоненты находятся в сети 172.24.101.0/24, которая терминируется где-то далеко от SE. Но до SE нам нужно только доставить DHCP запросы от субскрайберов. Для этого настраиваем DHCP Relay на коммутаторах доступа на интерфейс SE и все. С сетью доступа SE соединен через vlan 10 с 172.24.10.1/30.

interface inter
ip address 172.24.10.1/24
port ethernet 2/2
service clips dhcp

Последняя строка говорит о том, что на этом интерфейсе мы ждем абонентов DHCP - IPoE. Настраиваем DHCP Proxy:

dhcp proxy 252

Разумеется, не забыть указать, что начинать аккаунтинг при наступлении dhcp события
aaa accounting event dhcp

Конфиг в Radius (для простоты использовать авторизацию по MAC), разрешающий доступ к локальным сетям на 8Мбит/сек, в Инет днем - 2Мбит/сек, ночью - 4Мбит/сек.

Если кому-то нужны дополнения или разъяснения, пишите, постараюсь всем ответить.

Примеры Radius пакетов
Авторизация IPoE абонента с назначением сервисов.
Подтверждение получения абонентом IP адреса
Update пакеты IPoE абонента

Ермишин Андрей, руководитель департамента управления сети оператора связи ООО "Шупашкартранс-К"