

Занимательная BRAS'ология

Занимательная BRAS'ология.

Пошел в закат 2006 год, а классификация сетей, начатая в [#211](#), [#212](#) так и остановилась на 2005 годе. Это непорядок, пора хотя бы в общих чертах прикинуть, какие изменения прошли за два года в сетестроении.

Наиболее важным фактором, довлеющим над архитектурой, становится (на мой взгляд) переход на 4-х гигабитные каналы. Т.е. идет почти десятикратный рост наиболее востребованной в передаче позиции. С другой стороны, развиваются (вернее сказать, взрываются) приложения р2р. Самого разного масштаба, но с одним следствием - огромным трафиком.

Остается только радоваться, что большинство сетей успело вырасти из детской болезни "медных" воздушных линий, и оптика до дома становится стандартом. В этом Ethernet'чики сильно обгоняют МРК.

Так что можно перейти к вопросу услуг. И первый же интересный вопрос - найти точку, где пользователь получает все сервисы, а провайдер, в свою очередь, удостоверяется в его правах на действия.

На сегодня в подавляющем большинстве сетей этот процесс разделен территориально. Т.е. фактически биллинг управляет доступом в Интернет в ядре сети (считает трафик, выдает полосу), авторизует пользователя на абонентском порту коммутатора (MAC-секьюрити, ACL), и часто дополнительно учитывает потребление с серверов, VoIP, и .т.п.

В принципе, такой распределенный подход недорог и эффективен на небольших и средних сетях (до нескольких десятков тысяч абонентов). Но с ростом рынка услуги усложняются, и не всегда можно быстро ответить на шаги конкурентов. Плюс ничего так не поднимает ARPU, как разнообразие дополнительных услуг (то, что это не всегда благотворно сказывается на прибыли, вопрос уже другой).

Поэтому можно предполагать стремление к упрощению, т.е. появление одной особо интеллектуальной точки, и сведение к минимуму функций оставшихся. Думаю, что именно этот характерный момент будет определять собой "сеть 2007 года".

Вариантов тут немного, концов у сети всего два. Либо выносить все на абонентский порт, либо, наоборот, в ядро. Первое - безусловная классика корпоративного жанра. Там все оптимизированное в пользу быстрого действия, исходя из парадигмы, что ядро должно именно передавать данные, а не заниматься глупостями типа фильтрации и прочей обработки. Про превращение "untrusted user traffic" в "ordinary traffic" на абонпорту можно прочитать [тут](#), или [тут](#)

Однако, единой точки раздачи услуг из абонентского устройства ну никак не получается. По крайней мере, если не выходить за сакральные рамки \$10 за порт. Ограничивать полосу гибко, например, отдельно на ресурсы двух разных типов, нельзя. Считать IP трафик - нельзя. И далее еще длинный ряд подобных ограничений.

Нельзя не учитывать и то, что сеть строится не одномоментно, а несколько лет. И на доступ попадает очень разное оборудование, линейки современных китайских коммутаторов меняются слишком часто даже. Строить управление для такого "зоопарка" можно, SNMP придуман не зря, но сложность системы быстро растет в ущерб надежности.

Впрочем, надо помнить, что все это может вообще не пригодиться. Если нейтральность сетей победит во всем мире (включая Россию) - вероятен сценарий моноуслуги. Бери больше, кидай дальше - в переводе на операторский, полоса мегабит эдак в 5-10 на пользователя, по которой он получает все что угодно от сторонних поставщиков услуг (типа google). А управление сводится к "on" и "off".

Придется держать "коммутатор за пазухой", и оставлять себе возможность для отступления на такой сверхпростой (в технологическом плане) путь с минимальными потерями.

Так или иначе, но на роль единой точки раздачи услуг претендует только центр сети. Либо локальные центры, в которых концентрируется достаточное количество пользователей для "тяжелого" оборудования.

Рассмотрим хорошо знакомую идейно и технически схему с туннелями PPPoE, PPTP, и подобными механизмами:

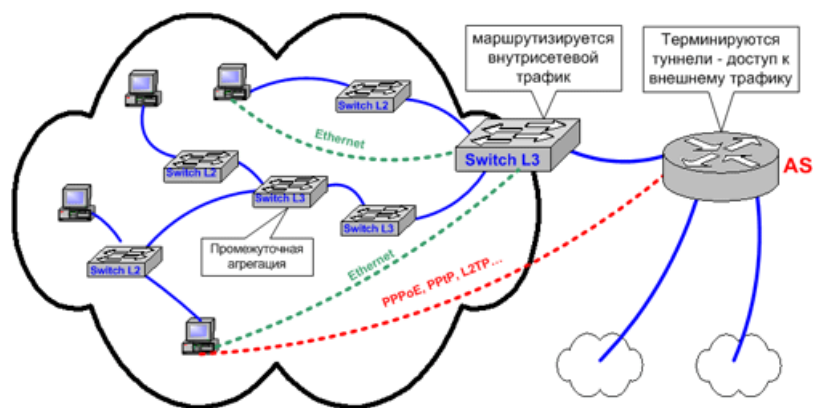


Схема 1. Сеть с туннелями.

- В центре – сервер доступа, или AS (access server), как правило ПК или Cisco. На ней терминируются пользовательские туннели (в основном PPPoE), остальной трафик ходит как хочет и куда хочет. Наоборот, с операторской стороны AS все красиво и гладко - промаркировано, почищено, посчитано.
- Стоимость AS около \$5-10 на пользователя, и мало зависит от масштаба.
- Основной трафик через AS не проходит, он замыкается на предыдущем, агрегирующем уровне, поэтому сервер доступа как правило малопортовый, и расположен подчас географически далеко от терминируемой сети (или сетей).
- Вход во внутрисеть контролируется на порту абонентского коммутатора (MAC-секьюрити, ACL).
- Достоинство – простота и дешевизна решения, много общего с DialUp, xDSL и связанными с ним ПО.
- Недостатки такой сети уже описывались, поэтому приведу только главный. Невозможно контролировать внутрисетевой трафик. Некоторые костыли-фильтры возможны, но базовая проблема остается – терминировать туннели аппаратно не получается, а программно выходит не дешево даже для небольшого внешнесетевого трафика. Ну а обрабатывать многогигабитные внутрисетевые потоки никто даже и не пытается.

Поэтому будущее схемы под вопросом – назвать ее удобной и универсальной язык не поворачивается.

Конкурирующий вариант – это обходиться без туннелей, рассматривая сеть скорее как корпоративную локалку. Вернее, как много небольших локалок – управляемость и контроль никому не мешали.

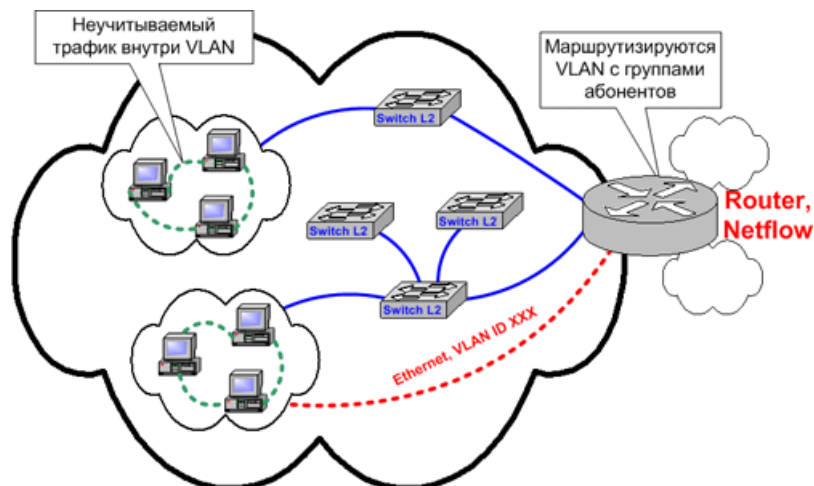


Схема 2. Сеть как ЛВС.

- Тут AS вообще не нужен, сгодится и бордерный рутер, на котором считается трафик. В случае большой нагрузки можно использовать коммутатор с поддержкой Netflow или Sflow – эти операции не требуют ресурсов процессора.
- Так как практически весь трафик проходит через рутер, он как правило находится рядом с агрегирующим коммутатором. Хотя, конечно, бывают и исключения.
- Вход как во внутрисеть, так и в интернет контролируется на порту абонентского коммутатора (MAC-секьюрити, ACL).
- Достоинства – внутрисеть (как сумма небольших сетей-Vlan) неплохо контролируется и учитывается. Нет особых проблем с обсчетом гигабитных потоков.
- Недостатки – очень ограниченный список услуг (например, резать полосы по такой схеме невозможно). Контроль сети неполный.

И этот вариант не сулит в будущем особых дивидендов. Мне он более симпатичен, как не создающий лишних сущностей в виде туннелей, но не более того.

Однако, развитие обеих схем в предельный, вырожденный вариант приводит фактически к одному и тому же решению. Если взять от схемы туннелей избирательность "до каждого абонента", а от варианта подсчета на маршрутизации - бесперебойную работу на полной скорости, должно, но идея, получится именно то, что нужно.

При этом тип туннеля становится в общем не важным – он просто должен быть дешевым, и поддерживаться базовыми средствами Ethernet. Собственно, на сегодня в этом качестве могут выступать только Vlan'ы 802.1q – при всем богатстве выбора, иной альтернативы нет.

С их помощью фактически можно включить каждого абонента в сервер доступа. А так как это нужно сделать на полной скорости, то и название должно стать (broadband remote access server) или BSR (broadband service router). И то, и другое с упором на **broadband**.

С одной стороны, слово BRAS несет в себе атавизм "remote". С другой, это устройство именно сервер, все сервисы отпускаются клиенту именно в этой точке. А не коммутатор или рутер. По этому поводу даже есть мутноватая и неочевидная [статья](#) Так что, какой термин окажется более распространенным – пока не слишком ясно.

Что же предлагается использовать в качестве BRAS? Единственный аппарат, упоминание о котором можно найти на русском языке [Huawei серии MA5200](#). Например, MA5200G-4 не дорог в масштабах "взрослого" операторства. Шасси MA1BABAS около 10к, софт 16к, порты GE SFP около 25к, System Control Unit 50к... В общем, на 200к\$ за BRAS наберется без труда. Самая младшая модель 5200F весьма демократична, всего 7,5к\$, однако по возможностям это просто AS.

Устройства позволяют связывать порт доступа + VLAN ID + MAC + IP + PPPoE. Предоставляет SSS (Service Selection Server)... В общем, все красиво, на бумаге "настоящие" BRAS'ы.

Нет в мире идеала. Поэтому на сегодня имеет смысл говорить скорее о полуBRASax, которые позволяют реализовать большую часть услуг. Остальное лучше поберечь для "сетей 2009 года".

Мощный коммутатор L3, типа catalyst 6509, может взять на себя многое. Хотя не сервер это, не сервер! Всех возможностей не дает, по щелчку пальцев к услугам не привязывается. Но если добавить к c6509 компьютер, управляющий (фактически) ACL и прочими функциями, можно соорудить комплекс, позволяющий выдавать 80% из списка произвольных услуг. В конце концов, "настоящие" BRAS'ы делают то же самое, но в едином корпусе.

Так что считать потреблённые абонентом услуги, выдавать в биллинг готовые данные в байтах и минутах подобная система сможет. Проводить авторизацию и отключать юзеры при исчерпании баланса - тоже. Ограничивать скорость - и тут справится.

Где грань пригодности, что считать BRAS, что не считать? Наверно, это пока не так важно. Да и 2007 год не наступил, мало ли что успеют придумать китайские друзья. Значительно важнее посмотреть, какие изменения в топологию сети принесет единая точка раздачи услуг. **Очевидно, что BRAS'ы новой формации (т.е. действительно broadband) будут многопортовыми. Иначе как в них ввести несколько тысяч пользователей на 10-100 мегабитных каналах?**

А значит, схема с маршрутизатором, вынесенным в сторонку от коммутатора агрегации, совершенно не годится. **BRAS нельзя поставить вместо AS, его нужно ставить на место коммутатора.**

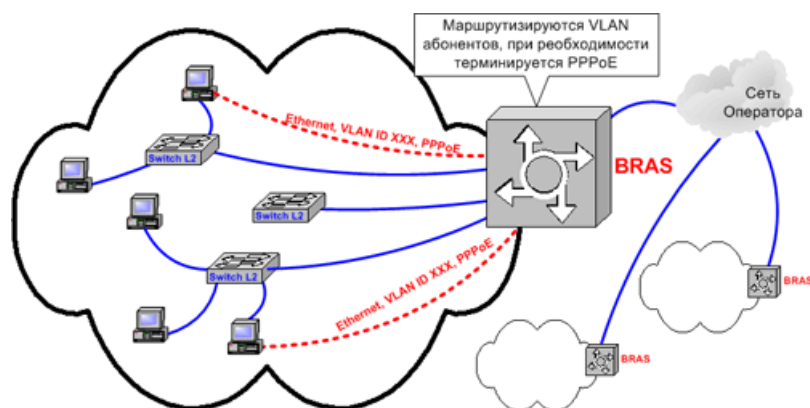


Схема 3. BRAS в сети.

- Все услуги контролируются на порту BRAS, в центре (или центрах) сети.
- Весь трафик без исключения проходит через BRAS, там он может учитываться, получать приоритеты. Вход в сеть контролируется там же, дополнительно можно терминировать туннели

PPPoE, либо другие.

- Недостаток – сейчас на рынке отсутствуют устройства таких возможностей за обозримые деньги. Но никто не запрещал использовать самосборные комплексы.

И не во всякой сети это получится сделать красиво. Типовая древовидная структура с 2-3 промежуточными уровнями агрегации (см. Схему 1), с простенькими коммутаторами L3 на каждом уровне, становится неудобной. Работать-то, конечно, будет, но ненужным станет интеллект на промежуточной агрегации, и станут лишними несколько слотов в BRAS'е.

Так что пока массовое строительство еще идет, нужно стараться укрупнить узлы, на сколько это возможно. В идеале, желательно вообще избавиться от промежуточных уровней агрегации, делая узлы примерно на 100 волокон-домов (и соответственно на 3-4 тысячи абонентов).

Второй нюанс – вложения в дорогие интеллектуальные абонентские порты имеют шанс не окупиться. Если в качестве туннеля используется Vlan, то это означает фактический вынос порта L3 BRAS'а на абонентский порт. **Так что все, что нужно от коммутатора доступа - поддержка 802.1q. Все остальное можно просто не использовать.**

Красиво? Не очень. Подводных камней в схеме с BRAS хватает. Один из них носит гордое имя "мультикаст". Действительно, если на каждого пользователя свой Vlan, то для передачи мультикаста придется дублировать потоки во все Vlan, что, соответственно, вызовет большую нагрузку на линии.

Бороться с этим явлением непросто. Хрестоматийный (и такой же проприетарный) MVR от Cisco красив, но дорог - к абонентскому порту без Catalyst не подходит. Есть и кучка самоделок "по мотивам MVR" - асимметричные Vlan, IVL, и другие попытки реализовать механизм "IPTV ready".

Все это сыровато, несовместимо, и на мой взгляд на сегодня для массового использования просто непригодно. Да и дорого, чего греха таить.

Думаю, что решение проблемы на практике будет "в духе Ethernet". Не интеллектом, а дешевой полосой. Действительно, в гигабите вполне поместятся около 200 TV-трансляций (по 5 мегабит каждая). Это много меньше, чем должно приходиться на BRAS в "средней" схеме использования (4000 абонентов, 50 портов - 80 абонентов на гигабит).

Ну а в схеме, когда волокно идет в центр от каждого дома в отдельности - по идее хватит даже 100 мегабит - 20 абонентов, одновременно потребляющих TVoIP - это больше, чем бывает даже в очень хорошем доме.

Остальные "грабли" (а их в BRAS'ологии) раскидано достаточно, перечислять не буду. Их так или иначе можно обходить, например, выдавать Vlan на дом, а не на пользователя, или вместо маршрутизации подсетей использовать inter VLAN bridging. Это работает, но лишает дизайн красоты простоты.

Но решения лучше - пока просто не вижу. А недостатки этого - на форуме припомнят "доброжелатели и Гости". :-)

Разное

Письмо от Ростелекома...

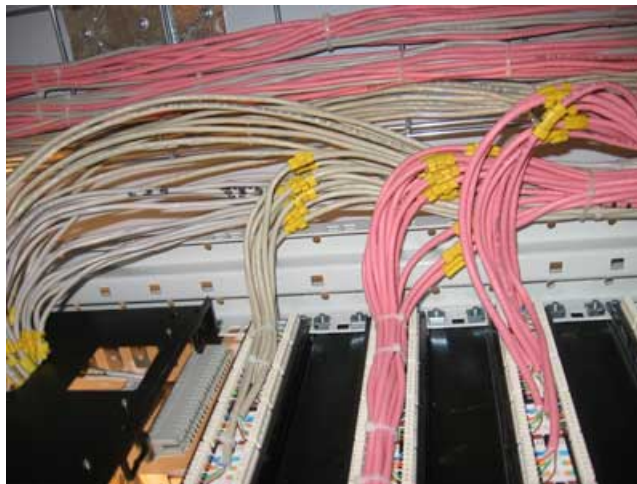
Фотозарисовки.

В Волгограде застрявший проходчик с оборванным кабелем. Самый центр города. Добром это не кончится.



Прислал **Vitaly**.

Монтаж внутри строящихся зданий в г. Белгороде



- [Вид под стеновой панелью;](#)
- [Вентиляция;](#)
- [Коммутационная стойка;](#)
- [Кабельный лоток;](#)
- [Кроссовые панели;](#)
- [Кабеля;](#)
- [И опять кабеля...](#)

Прислал **Ежеченко Геннадий**.

В последний месяц резко увеличилось количество краж кабеля. За последнюю неделю было вырезано кабеля на общую сумму около 10000\$, выведены из строя более 18 жилых домов (некоторые по 2-5 раз). Это без стоимости восстановления, времени, нервов.

Заведено 5 уголовных дел, 4 уголовных дела на подходе. Задержано 7 (семь!) человек, резавших кабель. Причём самое интересное, что помимо откровенных бомжей, этим "балуются" и 20-летние оболтусы.



Все магистральные линии на оптике с самонесущим кабелем, но и их, бывает, режут, видимо, принимая за медесодержащие. Появились и откровенно вредящие - просто-напросто сжигающие целиком ящики с оборудованием. На одном из чердаков после принятия мер против поджога, стали перекусывать витую пару.

Бригады монтажников уже звереют и есть серьёзные опасения, что следующие пойманные будут доставляться не в милицию, где на них заводятся уголовные дела (как это было с предыдущими), а куда-нибудь ещё.

- [Первый поджог](#)
- [Второй поджог](#)
- [Всё восстановлено](#)

Прислал **Dennis Yusupoff**, системный администратор сети ozerki.net.

Анонс

- Развитие FoD;
- Ethernet сеть на оборудовании Siemens;
- Письмо - как сетям использовать ADSL в своих целях;
- Выгодно ли покупать небольшие сети? (сбор статистики, жду писем);
- Послегрозовой ремонт управляемых коммутаторов;
- Оптические магистрали Турции (фотографии);
- Традиционный пункт - ссылки на интересные места Сети. Присылайте письма - они очень нужны для обзоров. Обязательно сообщайте, нужна ли Ваша подпись, ссылка, или лучше обойтись без нее;
- В "ужастиках" - кабеля в подмосковье.

Долгострой:

- Пример настройки сервера для терминирования PPPoE (перенесен в долгострой);