Применение коммутаторов L3

Новости.

С публичной TV-порки начался спуск собак на сети. Пока достоверно неизвестно кто этим занимается, зачем, и что хочет получить в результате процесса. Рассказ о нелегальных домашних сетях показывался по ТВЦ (в Москве) 26 сентября в 23-50 на программе Петровка, 38 (краткий и безграмотный анонс в сети можно смотреть тут).

Говорили, что сетей много (более 300), пользы от них мало, а вред большой (ну чисто как в Китае при хунвейбинах с воробьями боролись). Обманывают абонентов и не дают работать честным провайдерам. Да еще народную электроэнергию воруют посредством подключения страшных устройств - хабов.

Управление "Р" ГУВД Москвы отработалось по сети "Академ-нет". Деятельность компании остановлена, имущество арестовано, оборудование и линии связи ликвидированы, гендиректор под следствием.

Данная сеть конечно не "Юкос", но своих 800 абонентов имелось (для Москвы это средняя сеть, ближе к небольшой). Полной информации еще нет, и не понятно до конца будет ли, так как маски-шоу в России могут заканчиваться с любым итогом - от освобождения всех схваченных через 2 часа до длительных сроков заключения.

Собственно, докопаться в России можно до любого бизнеса. Особенно такого технически сложного, как сети. Поэтому важно понять, случаен ли разгром "Академ-нет" (может быть там все на самом деле было плохо, или денег кому-то недодали, или подвернулись под горячую руку кому-то), или это начало спланированной волны по монополизации отрасли в Москве.

Не слишком верится (повторюсь, достоверной информации нет), что это исходит от чиновников. Такие действия - не их стиль, да и зачем поднимать шум, когда можно просто не давать выхода на домовые коммуникации.

Скорее похоже на "помощь" конкурентов. Но так или иначе, очередной "гудок тепловоза" о необходимости легализации прозвучал. Судя по всему отрасль (пока только в Москве) накопила достаточно денег для серьезных действий по консолидации рынка в руках нескольких десятков крупных операторов. Поезд трогается от перрона - кто не успеет - тот опоздал. Процесс этот хоть и циничный, но, к сожалению, неизбежный.

Ну а провайдерам остальных городов остается продолжить размещение в вагонах согласно затраченным деньгам и усилиям. И считать месяца (или года) до готовности состава к движению.

Обновления разделов.

- Продолжена вторая глава второй части **книги о домашних сетях**. Если есть поправки и комментарии - прошу в почту.
- Небольшие обновления в **коллекции сертификатов ССС и ССЭ**. Но на неделе ожидаются существенные поступления - читателями были присланы интересные ссылки.
- В разделе **оборудование** наконец-то выложен **полный список** имеющегося на складе железа.
- Единичные пополнения в коллекции . Высылка фотографии на nag@nag.ru активно приветствуется.
- Полностью выложена книга Богдана Ясинецкого (Киев) **"Корпоративный сервер на базе UNIX"** (все 4 части).

Применение коммутаторов L3.

Начало этому материалу положили участившиеся письма читателей, которые спрашивали что либо о коммутаторах 3-го уровня. Причем многие видели в них что-то вроде универсального средства решения всех проблем сети - от увеличения производительности до обеспечения защиты от воровства трафика.

В принципе, такую постановку вопроса нельзя считать неверной - хороший коммутатор L3 действительно способен кардинально изменить возможности управления сетью. Но применение теории к реальности (да еще Российской) никогда не было простым. Поэтому вопросов выходит много, и отвечать на них проще оптом.

Немного теории для тех, кто ее подзабыл. Если сузить поле применения стандартов до конкретной

реальности домашних сетей, то уровень 2 (по семиуровневой модели OSI) соответствует кадрам Ethernet. Соответственно их передвижение происходит согласно MAC-адресам известных CAM-таблицам коммутаторов. Свитчи, которые "не знают" ничего выше по стеку протоколов называются коммутаторами 2-го уровня.

При этом они могут производить весьма сложные операции. Например, ставить и убирать метки VLAN, распознавать приоритеты (QoS), устанавливать кадры в очереди, определять атаки, считать Ethernet-трафик, шейпить его, фильтровать по номерам портов, и т.п. Классическим типом "продвинутого" L2 можно считать 3com SuperStack 3300 или Catalyst 2924.

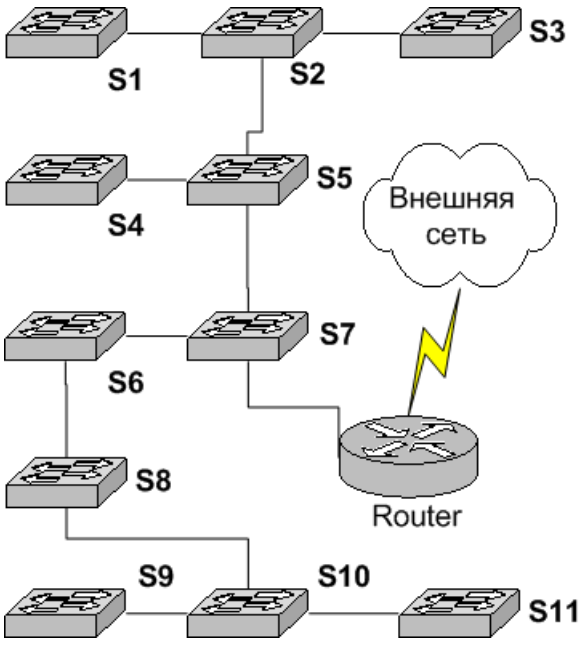
Соединять разные сети Ethernet (т.е. реальные и виртуальные сети 2-го уровня) должны маршрутизаторы, которые обрабатывают данные на 3-м уровне (IP пакетов). Заголовки IP идут по сети Ethernet как данные, и обычным коммутаторам 2-го уровня недоступны.

Ранее сети Ethernet соединялись друг с другом при помощи иной (не Ethernet) канальной средой передачи данных (WAN). Например Frame Relay, X.25, ATM, G.703, и т.п. Для преобразования была нужна гибкость, универсальность, сложный софт, и... хватало небольшой скорости.

Когда сети Ethernet сделались большими, то необходимость в таком подходе отпала, и даже более того, стала мешать (как и любая избыточность возможностей). Тут и появились коммутаторы 3-го уровня, способные в добавление к обычным функциям маршрутизировать трафик между портами на IP-уровне. Быстро, но с весьма ограниченными возможностями (как правило нельзя подсчитать трафик, построить сложные фильтры, добавить скрипты, NAT, и т.п.). Хотя конечно есть и монстры типа Catalyst 6509...

Можно только добавить, что история эта была длинная, и она еще не совсем закончена. Так, сначала различали маршрутизирующую коммутацию, коммутация потоков и коммутирующую маршрутизацию. Эти термины сейчас можно считать в некотором роде анахронизмом, но корни той же MPLS растут из них, и в дальнейшем смогут сильно изменить дизайн сетей. Но это уже лежит далеко за рамками рассматриваемой темы.

Вернемся к сетям. Вернее, к условной схеме сети.



Собственно, большинство небольших сетей так или иначе сводятся к такой простой картинке. А из нескольких подобных сегментов можно построить уже вполне крупную инфраструктуру.

Перечислим варианты установки оборудования.

1. Полностью неуправляемые коммутаторы. Вариант конечно реальный, но для рассмотрения не интересный. Да и перспективность его в общем сомнительна - слишком много неудобств. Достоинство только одно - сверхнизкая стоимость.
2. S7, S5, S10 - управляемые свитчи 2-го уровня, остальные неуправляемые. Такое построение не даст заметного выигрыша. Если два управляемых коммутатора 2-го уровня разделены неуправляемым (с подключенными пользователями) то не все, но большинство функций (VLAN, QoS) будет потеряно. Поэтому имеет смысл поставить мощные устройства только в точках S7 и S5 - тогда их можно будет использовать эффективно.
3. S7, S5, S10 - управляемые 3-го уровня, остальные неуправляемые. Вполне эффективное использование для разделения сегментов в точках S5, S10, но в S7, рядом с маршрутизатором,

функции 3-го уровня могут быть излишни. Ну а в остальных точках контроль над сетью будет неполным.
4. Все коммутаторы управляемые 2-го уровня. Этот вариант дает возможность полностью контролировать и при необходимости маршрутизировать каждый порт сети. Для мультисервисного использования возможно соблюдение QoS, мультикастинг, и прочие функции. Как недостаток - необходим отдельный мощный маршрутизатор, через который пойдет весь междусегментный трафик.
5. S7, S5, S10 - управляемые 3-го уровня, остальные - управляемые 2-го уровня. Этот вариант на сегодня фактически стандарт для серьезных корпоративных сетей, но для Ethernet-провайдеров рекомендовать его явно рановато.
6. Все коммутаторы управляемые 3-го уровня. Это вариант возможно и неплох, но на сегодня избыточен даже для корпоративных решений. Про домашние и говорить нечего.

Из краткого перечисления вариантов видно, что при выборе направления развития можно использовать варианты **3** и **4**. Кстати сказать, производители оборудования пришли (судя по продаваемым линейкам) к похожим выводам, но к этому придется вернуть после небольшого отступления.

Сначала надо ответить на вопрос - "зачем нужно разделять трафик на уровне IP?".

Когда сети строились на хабах, ответ был тривиален - нужно разделять коллизионные домены, поэтому маршрутизаторы (коммутаторы L3 были непозволительной роскошью) ставились между каждыми 5-8 хабами (или 30-40 пользователями). Если этого не делать, то наступала быстрая деградация производительности сети.

Однако, в коммутируемой сети такого ограничения нет. И ее размер ограничивается только бродкастовым трафиком, который постепенно заполняет полосу пропускания. Считается, что "бродкастовый шторм" может наступить при количестве пользователей около 300-500. И это не предел, если в центре сети использовать оборудование с фильтрацией на 4-м уровне (т.е. по протоколам).

Много ли найдется домашних сетей, в которых возможно собрать столько пользователей на территории, не разделенной каналами WAN? Только единичные случаи. Тем более количество одновременно работающих компьютеров в сети провайдера как минимум в 2-3 раза меньше, чем в корпоративной, и предел можно поднять еще выше.

Для чего может быть нужно разделение на отдельные сегменты в случае **4**? Подсчет локального трафика, ограничение скорости отдельных сегментов, фильтрация, построение закрытых корпоративных локалок. В остальном сеть и так полностью управляемая, в ней отдельно **можно маршрутизировать каждый отдельный порт**. Да и с мультисервисными услугами проблем не возникнет.

Минусов два. Приличная стоимость управляемого железа и проведение межсегментного трафика через центральный узел, что плохо сказывается на пропускной способности основной магистрали. Собственно последнее и ограничивает размеры плоской сети Ethernet на управляемых коммутаторах 2-го уровня.

Для варианта **3** вероятные причины сегментирования иные. Подсчет трафика на недорогих коммутаторах 3-го уровня делать затруднительно (а при отсутствии финансовых проблем см. вариант **5**). Закрытые корпоративные сети то же не сделать - разве что ставить управляемые свитчи во всех точках подключения таких пользователей. Так что единственный смысл решения - повысить производительность и управляемость сети в целом, локализовать неисправности, ограничить доступ абонентов друг до друга.

Достоинство - не нужен выделенный маршрутизатор, нет лишнего трафика через центральные магистрали.
Недостаток - из-за многократной маршрутизации на IP-уровне сильно повышается сложность сети - лишние подсети, лишние проблемы. По неволе придется поднимать OSPF, RIP-2 или что-то подобное.

Теперь можно перейти к сравнению коммутаторов L3, например D-Link DES-3326S ($800) и Catalyst 3550-24 ($4500). Конечно не на уровне технических параметров, а по парадигме использования.

Первый, вероятно, предназначен к использованию по варианту **3**, только в расчете на небольшие офисные сети, а не на провайдеров (кто про них в Китае думал?). Так же хорошо вписываются в подобную схему коммутаторы от D-Link с портовыми, нетегированными виланами, для которых L3 на ближайшей развилке - хорошее решение проблемы как скорости, так и безопасности. Но большую разветвленную сеть построить таким образом будет достаточно сложно.

Ну а Cisco 3550 конечно "заточена" под варианта **5**, и проходит в связке с Catalyst 2950 через пособия по дизайну сетей. Как раз один 3550 или 3550-12G, и к нему звездой - десяток-другой 2950. Это

позволяет достичь максимальной скорости передачи данных. Кстати, нет в линейке этого производителя свитчей с портовыми виланами, а вот поддержка тегированных 802.1q на маршрутизирующих портах становится принципиально необходимой...

Таким образом, можно сказать, что главная причина применения L3 в корпоративных сетях - повышение скорости передачи данных. Но... Для провайдера актуальность этого момента сомнительна. Основной трафик невелик, и имеет вертикальную структуру (от серверов к пользователю и обратно). Межпользовательский обмен данными прибыли не приносит, и во многих случаях просто вреден.

Что же выбрать, на какой путь ориентировать сеть? Сказать сложно - факторов много, и они весьма разные. Кто-то перейдет на снижение внутреннего обменного трафика ограничительным путем или на его прямой подсчет. Да и поставить стремительно дешевеющий гигабит на магистрали не сложно, разгрузив узкое место для прохода межвилановых данных.

Кому-то покажется проще брать абонентскую плату и поднимать скорость сети, замыкая трафик на свитчах L3. Это особенно удобно в небольших, но многочисленных сетях, связанных между собой xDSL. В этом случае ставить маршрутизатор на каждый сегмент дорого, а расширение магистрали трудноосуществимо.

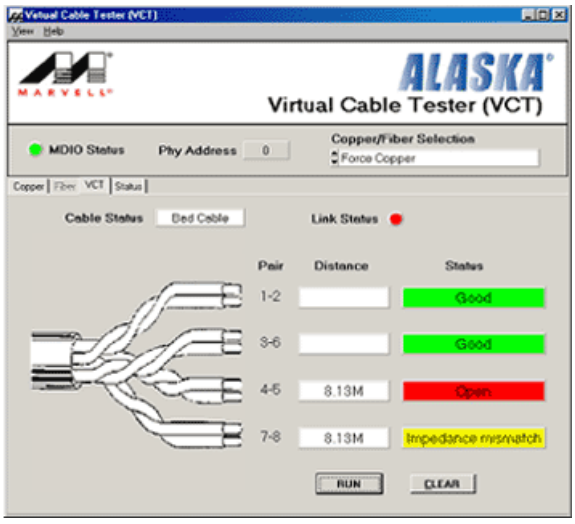
Решений много, выбирать или комбинировать нужно в каждом конкретном случае по разному. Но на мой взгляд, даже широкое применение устройств L3 с неуправляемыми или частично управляемыми коммутаторами (без поддержки полных возможностей L2) не позволяет получить значительных преимуществ для продажи услуг сети. По крайней мере до тех пор, пока с избытком хватает гигабита.

Однако безусловно, есть локальные варианты использования, в которых свитч L3 будет очень удобен, или даже незаменим. Поэтому о их наличии стоит помнить при проектировании сети. Но так же надо учитывать, что "третий уровень" совсем не волшебное средство решания всех проблем, а лишь инструмент. Который нужно применять к месту и в нужных количествах. Как лекарство. :-)

Интересное в сети.

Вот что бывает если позволять пользователям слишком много и при этом не следить за проходящим трафиком. Этим могут быстро воспользоваться непорядочные конкуренты, выстроив коммерческие туннели через чужую сеть.

Интересную новость прислал Юрий. Asus выпустила серию материнских плат AI (например P4P800) с сетевым контроллером 3Com 3C940 на борту. В комплекте с платой идёт программа-кабельный тестер.



Кажется не слишком вероятным, но сетевая карта измеряет (кроме прочего) расстояние до обрыва конкретной пары. Таким образом, можно собрать очень бюджетный и универсальный кабельный тестер.

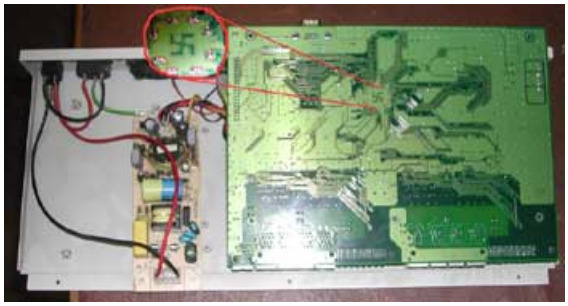
Сеть Академ-нет из Новосибирска запустила интернет-вещание ТВ канала Fashion в формате MPEG-4, 640x480 25 кадров (т.е. лучше, чем VHS). С учетом мультикастинга на основных магистралях поток занимает всего 2 мегабита.

Но вот видео-серверу приходится тяжело. У разогнанного Атлона 2500(333) утилизация составляет до 99%. Так что без специальных видео-ускорителей вещание через IP будет непростой, но перспективной задачей.

Еще один "бесконечно далекий" от реальности обзор технологий выделенных линий. Читать только если хочется немного развлечься (ссылку прислал **Grumbler**).

Внутренности свитча Xnet SH9016A (прислал argus). Агрегат проработал не выключаясь около полутора лет, потом вышел из строя. Вскрытие показало, что это произошло из-за некачественных конденсаторов в блоке питания.

Но самое интересное обнаружилось с обратной стороны платы.



Не иначе, постарались неонацисты из Китая.

Небольшая ссылка от Michail - Локальные сети Ethernet в АСУ ТП. К сожалению, в сеть выложены только анонсы.

Ведомство Чубайса создает свою сеть передачи данных. Хоть строительство и не такое масштабное как у Трансгелекома (предполагается активно использовать сети сторонних операторов), все равно тенденция проглядывает знакомая...

Заметка Школа остается с пустой "тарелкой" (прислал Aleksei). Собственно, давно не понимаю, почему проблема информатизации сельских школ не решена простым спутниковым способом.

Односторонний канал с единой по России программой стоит в общем копейки как для вещающей стороны (одна полоса), так и принимающей (односторонняя тарелка стоит не более $200). Объем данных, которые можно без труда "свалить" с орбиты, очень велик - можно уложить как часовые обновления нескольких сот ведущих новостных сайтов, так и неторопливо пополнять файловые архивы.

При современной стоимости жестких дисков каждая школа может позволить себе вполне актуальный микроинтернет гигабайт на 300. Это **очень** много при разумном использовании. И будет работать даже на полярной зимовке, там, где нет **никакой** связи.

Ну а обратный канал... Если есть телефон - нет проблем. Но в заметке пишут, что 22 тысячи школ не имеют экстренной связи. Однако, отправить почту и немного сообщений можно через межгород по радио - пусть на скорости 9600 или 2400 (и черт с ним, с качеством кабелей). Или даже на дискете отнести до сельсовета - если там есть компьютеры.

В общем, совершенно не понимаю, зачем зарывать большие деньги в какую-то программу. Достаточно обеспечить централизованное вещание, и предложить (обязать) школы поставить тарелки. Ну может быть еще софт специальный (дуракоустойчивый) написать и распространить. Если у них есть компьютеры, уж 200 баксов найдут или в своем бюджете, или соберут в конце концов с родителей.

Вот только преодолеть бы проблемы в мышлении. Когда не хотят что-то делать, находят поводы. Ну а способы, судя по всему, никто искать еще и не пробовал...

Фотозарисовки.

Данный материал прислали из Ульяновска. Для начала, несмотря на фактическое окончание сезона, опубликую еще одну грозовую фотографию. Красивая и опасная стихия.



Что бы Ethernet-провайдеры не сильно расслаблялись, и помнили о неизбежном приходе лета. А то уж скоро 7 лет как в Екатеринбурге весна наступает неожиданно. :-)

Далее, радиосеть в г. Ульяновске (есть все нужные лицензии и разрешения на частоты).

Базовая станция на высоте 120 метров расположена на законсервированной трубе ТЭЦ1.



Монтажник-высотник Илья (слева) и параболическая антенна на расстояние 62,4 км (справа).

Вверху большая белая всенаправленная антенна 12db для раздачи интернета части города. Вверх ногами работает лучше по неизвестной (несмотря на более чем 6-ти летний опыт работы) причине.



Слева маленькая антенка 9db для раздачи инета части другой города (вверх ногами работает лучше).

Внизу справа лючек, где расположено все оборудование (Cisco BR342 2шт. Orinoco AP-2 1шт). Есть еще несколько D-Link, но их антенны расположены ниже ярусом чтобы не было помех на основные каналы.




Вид на город. На фото слева антенна Harvest, с его помощью получается использовать телефонную связь почти по всей области. Справа - вида на завод УАЗ. Вдали река Волга.

Хождение админа в народ.

Кто-то спрашивал: "...как обеспечить точку доступа на улице?".



Как видно на фото (прислал Sergey) легко, и не только точку, но и рабочее место самого админа.

Анонс

- Муниципальная городская информационная сеть города Северска (Томская область).
- Ссылки на интересные места Сети. Присылайте письма - они очень нужны для обзоров. Обязательно сообщайте, нужна ли Ваша подпись, ссылка, или лучше обойтись без нее;