

Мозги. Доступ или агрегация?

Осталось немного больше месяца до ежегодной Конференции Российских Операторов Связи (КРОС-2009), регистрация скоро завершается (база более 280-300 человек просто "не прокормит"). На сегодня "записались" 260 участников, более 120 компаний. Все подробности можно узнать на сайте cros.nag.ru.

Мероприятие пройдет 20-22 мая, на б/о Иволга, около Екатеринбурга. Программа и формат традиционные, проверенные 2006-2008 годами.

Разное

Мода на блогводство добралась и до "отцов" российского провайдинга. Отличился Александр Ермолаев.

Интересны заметки о гаджетах, например о Siemens Gigaset C470IP, это SIP-DECT телефон за 3990 рублей. Причем база поддерживает до 6 трубок, и до 6-ти SIP-аккаунтов (т.е. можно сделать настоящую домашнюю мини-АТС).

Следующее "открытие недели" - блог Михаила Климарева. Взорвала мозг заметка [о судьбе Связьинвеста](#). Не удержусь, приведу одну из иллюстраций:



Другое дело, что тут не обойдется без политического решения. И если оно будет... Объективным факторам и субъективным предпосылкам придется мужественно подстраиваться.

Вскоре предстоят выборы члена Исполнительного Комитета RIPE NCC от России. В настоящее время это место занимает Дмитрий Владимирович Бурков, почитать о котором можно [здесь](#) и [здесь](#). Ну а участники КРОС-2008, вероятно, помнят его доклад на конференции.

Полагаю, избрание Дмитрия на второй срок в Исполнительный Совет RIPE NCC принесет большую пользу. Подробнее о RIPE NCC GM можно посмотреть [тут](#)

Если LIR не планирует прислать своего представителя на General Meeting, можно участвовать в голосовании "по факсу" через доверенное лицо. В качестве одного из таковых - сотрудник Российского НИИ развития общественных сетей Горбунов Сергей Александрович, pr@ripn.net.

Подобралось несколько ссылок под "школьный проект"

Для начала - [История об интернетизации отдельно взятой школы](#). Оказалось, что школа не имеет права своими силами разводить интернет по локальной сети. Все подобные работы должны быть выполнены Оператором. В результате все ученики ...пользуются единственным подключенным компьютером.

Другие предлагают отметить 100 дней с момента [трагической смерти](#) Школьного Портала. Нет, сайт-

призрак все еще виден в Сети - просто он не обновляется...

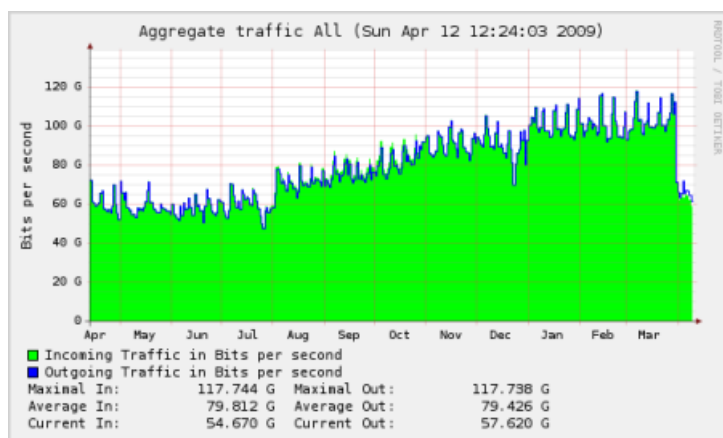
Как тут не вспомнить, что связь в России [хуже, чем в Африке](#). Всемирный экономический форум опубликовал ежегодный "Глобальный отчет по информационно-коммуникационным технологиям", опустив при этом нашу страну с 72-го на 74-е место среди 134 обследованных стран.

Основной причиной отставания стала высокая стоимость всех услуг связи по отношению к душевому ВВП. По стоимости подключения стационарного телефона Россия и вовсе оказалась на 106-м месте в мире.

Но никто не сомневается, что новый проект объединения МРК в единую госкорпорацию последовательно отстоит принцип качественной связи для разных социальных систем, и даст решительный отпор агрессивным силам британскихзарубежных ученых... :-)

Антипиратский закон от 1-го апреля [обрушил](#) шведский интернет-трафик. В соответствии с новыми правилами, владельцы авторских прав, считающие, что их интересы ущемлены, могут через суд принудить интернет-провайдеров раскрыть данные пользователей, незаконно обменивающихся файлами.

Эффект неожиданно серьезный, его можно видеть невооруженным глазом на netnod:



Спад минимум на треть - с 110 гигабит до 70-ти. Статистика [в Амстердаме](#) практически не пострадала, но небольшое понижение заметно и там, и даже на M9.

Эксперты обещают, что скоро объемы "вернутся". Пользователям надо понять, как обеспечить свою безопасность. Но что-то подсказывает, что для начала просто увеличится "зарубежный" трафик...

Ссылки про кризис™

Некоторые спутниковые каналы на территории России (в том числе популярные Animal и Discovery) [будут перезаключать](#) договоры только с кабельными операторами, которые смогут оплатить за канал не менее \$10000 в год. А не как сейчас, \$0,13-0,15 с абонента в месяц, от 1000 абонентов. Т.е. минимальный платеж увеличен в 10 раз. Вот это и есть "звериный оскал капитализма".

Более того, обязателен ежегодный рост абонентской базы не менее 15%! Надо понимать, что КТВ не растет такими дикими темпами, как ШПД. Тем более в кризис. Многие небольшие города охвачены полностью, и там абонентскую базу можно увеличивать только демографическими методами, через подъем рождаемости.

Так что придется и тут продвигать отечественного производителя. Или просто воровать.

Не сильно отстают и отечественные ОПСОСы. Статья Каганова [Осторожно, кидалово: как МТС борется с кризисом](#). Временно бесплатные услуги, которые сами активируются, а потом неожиданно становятся очень даже платными.

Ссылки в одну строку:

[Видеозапись](#) про тяжелые будни монтажников "Эр-Телекома". Как только живы остались...

[Наступает эпоха бесплатных телефонных разговоров](#). Для профессионалов не интересно - слишком просто и популярненько, но можно рассматривать как показатель - тема VoIP добралась до массовых изданий.

Divx.com отказался развивать divx кодек и перешел на h.264.

We're now introducing the next generation of DivX technology with DivX 7 - our new software that lets you create and play full HD H.264 (MKV) videos. H.264 is a new standard that is poised to power the high definition video revolution by offering incredible visual quality, performance and efficiency.

Закончилась целая эпоха...

Замдиректор красноярского филиала "Сибирьтелекома" [оштрафован](#) за отключение абонента (вернее, отключение телефона за неуплату интернет). Сумма штрафа 15 тысяч рублей.

Глобальная карта интернет. Одна из лучших, на мой взгляд.

Борьба сотовиков с вандалами, Пермская область



Обновление в разделах:

- На **карте городов** каталога "Провайдеры России" теперь **1632** компании (т.е. за время, прошедшее с прошлого обзора, добавилось **26** провайдеров). Коэффициент самоадминистрирования вырос и составляет **32%**. Если кто-то желает дополнить информацию по городу или провайдеру - прошу писать на prov@nag.ru.
- Пополнение в разделе [сертификатов](#) для сетевого оборудования: [маршрутизатор Cisco 1841](#).
- Пополнение в разделе [фотографий](#) внутренностей сетевого оборудования: 16-портовый коммутатор [D-Link DES-1016D](#).
- В разделе [shop.nag.ru](#) добавлена линейка мультиплексоров CWDM, поддерживающих, кроме прочего, **одноволоконные 10Gb с использованием DWDM XFP|X2|XENPAK** (индекс 10GR-4A). Кроме того, запущены в серию недорогие (140 рублей) узлы крепления к столбам SNR-UK-III, SNR-UK-I, и вращающийся каркас-барабан для хранения кабеля на опоре SNR-K2-B.

Наиболее интересные темы форума (TOP-3):

- [В чем главная Техническая сложность в предоставлении VLAN на пользователя;](#)
- [Что делать, если провайдеру пох...?;](#)
- [NetFlow, как хранить весь этот мусор.](#)

Мозги. Доступ или агрегация?

Последнее время производители телекоммуникационного оборудования все больше и больше наращивают функционал коммутаторов доступа. Их можно понять - "чем умнее, тем дороже". Эту идею, кстати, продавцы-вендоры вполне поддерживают, и охотно проталкивают всеми способами - от прямой рекламы до презентаций и учебных курсов.

Но с точки зрения провайдера все наоборот - расходов должно быть как можно меньше. Причем как

первоначальных, на покупку "железа", так и эксплуатационных, на ремонт и замену изуродованного вандалами и грозами, сворованного, залитого, перегоревшего, и просто вышедшего из строя "без объяснения причин". И тут логика столь же тривиальна - "чем дешевле, тем лучше".

Поэтому вопрос выбора "схемы" сети далеко не праздный и не дешевый. Стоит ли, жертвуя функционалом, использовать на доступе экстремально недорогое оборудование? Ведь разницу в функционале можно компенсировать более производительным, надежным, и интеллектуальным оборудованием агрегации (или ядра, в зависимости от схемы организации сети). Таких узлов мало, они обычно во вполне сносных условиях - защищены, имеют гарантированное питание, хорошее, часто регулярное, обслуживание. Это позволяет почти полностью устранить основные негативные факторы.

Зададим технические требования. В современных условиях жесткой конкуренции операторов ШПД сеть должна:

1. Защищать абонента от атак вида IP spoofing, MAC spoofing, ARP spoofing, DHCP spoofing;
2. Давать возможность абоненту получать услугу TVoIP, VoIP;
3. Предоставлять оператору контроль над легальностью сетевых реквизитов абонента;
4. Фильтровать нежелательный трафик (вирусные порты, netbios).

I. Схема с "интеллектуальным" доступом:

Вариантов построения много, и рассматривать каждый в отдельности в рамках данной статьи нежелательно. Поэтому ограничимся требованиями к коммутаторам доступа поддерживать достаточные комбинации следующих функций:

IP-PORT-MAC binding (D-Link) – осуществляет привязку IP address + MAC address к физическому порту коммутатора. Позволяет защититься от подмены IP/MAC абонента. С точки зрения простоты обслуживания и сокращения трудовых издержек данная функция имеет один большой недостаток – привязка MAC адреса к порту (если клиенту потребовалось подключить любое другое устройство к своему кабелю, то придется на стороне абонентского коммутатора или на стороне клиентского оборудования переписывать MAC адрес, что очень неудобно). Особо надо обратить внимание, что функция не дает 100% защиты от атаки ARP spoofing (Man in the Middle attack).

ACL Packet Content Filter (D-Link) – позволяет анализировать первые 80 байт информации в Ethernet фрейме. Гибкий механизм позволяет создавать почти любые правила для фильтрации трафика. Позволяет защититься от L2 атак, фильтровать нежелательный трафик и осуществлять контроль над легальностью сетевых реквизитов абонента.

ISM VLAN (D-Link)/ **MVR** (Cisco) – (IGMP Snooping Multicast VLAN)/(Multicast VLAN Registration) функция позволяет создать одну запись Multicast VLAN на коммутаторе доступа, который будет "прослушивать" все сообщения о вступлении в многоадресную группу из различных VLAN и не допускать дублирования потоков, т.е. передавать потоки multicast в одном общем VLAN для всех подписчиков.

Dynamic ARP Inspection (Cisco) – функция коммутатора, предназначенная для защиты от атак с использованием протокола ARP. Коммутатор проверяет, не передается ли "невалидные" записи IP/MAC в теле ARP-пакета. Если будет обнаружена "невалидная" запись, то коммутатор отбросит пакет. Может использоваться как в схемах с динамической, так и статической адресацией.

IP Source Guard (Cisco) – защищает порт коммутатора от подключения злоумышленников с фиктивным IP адресом на основе данных статической таблицы IP+MAC Binding или динамической таблицы DHCP Snooping. Обеспечивает защиту от IP spoofing.

ACL (Access Control List) – позволяет классифицировать трафик по полям L2, L3, L4. В зависимости от производителя и конкретной модели существует много нюансов и ограничений. ACL предназначены для фильтрации нежелательного трафика, а так же для классификации трафика требующего приоритизации.

QoS (Quality of Service) – Качество обслуживания определяется как мера производительности передающей системы, отражающая качество передачи и доступность услуг. Доступность услуг является важнейшим элементом QoS. Функция необходимая для приоритизации трафика в мультисервисной сети для увеличения доступности критичных к задержкам и полосе пропускания услуг.

При этом основная фильтрация и классификация трафика происходит на доступе, поэтому можно использовать сравнительно дешевые L2 коммутаторы для узлов агрегации. Ведь из списка "дешевое, производительное, функциональное" можно выбрать только два параметра.

II. Схема с "простым" доступом:

В коммутаторах доступа понадобится:

Поддержка **802.1q VLAN** + желательно (но необязательно) **SSH** для удаленного управления. Необходимо ограничить обмен Ethernet трафиком между абонентами, чтобы у него был только один путь – в сторону агрегации, где будут решены проблемы сетевых атак (ARP spoofing, IP spoofing и т.д.), приоритезации, классификации и фильтрации трафика на аппаратном уровне.

"Односторонние" **MRV** или **ISM Vlan** для IPTV (в связи с провальным ходом внедрения этой услуги, потребность в данном функционале неочевидна).

На агрегации:

Поддержка функций **IP Source Guard, Dynamic ARP Inspection, DHCP snooping, DHCP option 82 insertion, QoS, VLAN ACL** или аналогов на оборудовании агрегации.

Опционально: наличие **L3 интерфейса** на абонента как точки для применения политик.

Решения поставленных в первоначальных технических требованиях задач можно добиться при использовании схемы vlan-per-user (CVLAN – Client VLAN). Минус в данном случае – необходимость выделения сети с маской /30 на абонента. В случае с раздачей реальных адресов использование схемы затруднено.

Для устранения этого недостатка можно применить [ip unnumbered](#) на L3 интерфейсе абонента.

Функция [IP unnumbered on SVI interface](#) на данный момент есть только в коммутаторах Cisco Catalyst + маршрутизаторы [Juniper MX Series](#) (которые не годятся на роль агрегации).

Возможно, скоро [появится](#) поддержка данного функционала в коммутаторах Allied Telesys.

Второй существенный недостаток в данной схеме – каждый VLAN (абонент) должен иметь доступ к источнику multicast трафика. Без этого использование функции IGMP Snooping (есть почти в любом коммутаторе) в каждом VLAN'е пойдет отдельный multicast поток. При большой популярности услуги TVoIP нагрузка на uplink коммутатора доступа резко возрастает.

Решение – использование функции Multicast Vlan Registration (Cisco) или аналогов, например ISM Vlan (D-Link). В результате весь multicast трафик попадает на коммутатор в отдельном VLAN'е (все абонентские VLAN получают к нему доступ в пределах коммутатора, дополнительная нагрузка на uplink отсутствует).

Схему сети в этом случае можно представить следующим образом:

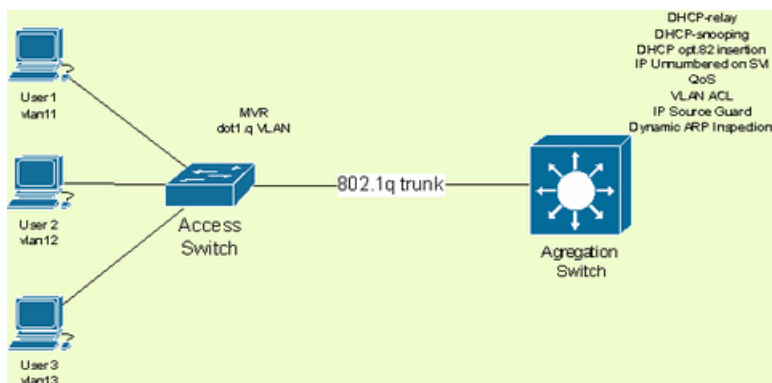


Рис. 1 Схема VLAN-per-User (CVLAN – Client VLAN)

Есть похожий вариант, в котором нет предыдущих недостатков, но в котором отсутствует персональный абонентский L3 interface. Для организации такой схемы коммутаторы доступа должны поддерживать функцию **Privat VLAN Edge port** (Cisco) или аналоги, например, **Traffic Segmentation** (D-Link).

В этом случае выделяем один VLAN на абонентский коммутатор. Обмен трафиком между абонентами возможен только через uplink порт. Соответственно, отпадает необходимость в поддержке MVR на коммутаторах доступа и IP Unnumbered on SVI на коммутаторах агрегации.

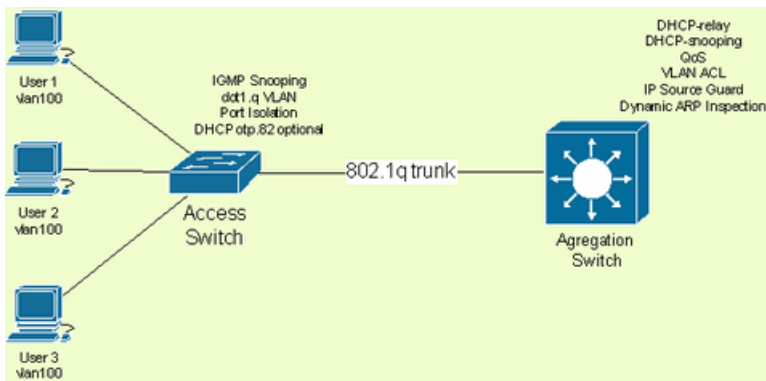


Рис. 2 Схема с изоляцией портов + VLAN-per-switch

В рассмотренных схемах есть один большой плюс – это простота администрирования. Основной акцент ставится на узлы агрегации, которых небольшое количество. Узлы доступа нуждаются лишь в небольшой стандартной (в некоторых схемах даже абсолютно идентичной) конфигурации. Соответственно, обслуживание и траблшутинг многочисленных коммутаторов намного упрощается.

III. Посчитаем приблизительную стоимость в схеме с "интеллектуальным" и "простым" доступом.

1. Интеллектуальный доступ.

Access Switches:

D-Link DES-3550 ~ 670\$ (за 48 портов)

D-Link DES-3052 ~ 630\$ (за 48 портов)

Linksys SPS224g4 ~ 340\$ (680\$ за 48 портов)

L2 aggregation:

D-Link DGS-3100-24TG ~ 700\$

D-Link DGS-3426 ~ 1 700\$

L3 aggregation:

DES-3828 ~ 600\$

DGS-3312SR ~ 767\$

DGS-3627G ~ 3 002\$

2. Упрощенный доступ.

Access Switches:

Digital China DCS-3950-26C ~ 150\$ (300\$ за 48 портов) (MVR)

б/у WS-C2950G-48 = 300\$ (за 48 портов) (MVR)

Edge-Core ES3526XA ~ 230\$ (460\$ за 48 портов)

D-Link DES-3026 ~ \$170 (340\$ за 48 портов)

Agregation Switches:

б/у Cisco WS-C3550-48 ~ 500\$

б/у Cisco WS-C3750G-24T ~ 2000\$

Cisco WS-C3750E-24TD ~ 8000\$

Allied Telesyn AT-x900-24XS ~ 5200\$

3. Упрощенный доступ без IPTV.

Access Switches:

Любой коммутатор с поддержкой 802.1q ~ 200-250\$ за 48 портов.

Посчитав разницу в цене между "интеллектуальными" и "простыми" коммутаторами, и учитывая, что на каждый узел агрегации приходится не менее 20-ти устройств доступа, можно получить неплохую экономию (около \$1000), которая более-менее покрывает затраты на использование более дорогого оборудования агрегации.

Важный момент - при строительстве новой сети есть возможность выбирать. Но в кризис проекты "с нуля" редкость. Что делать в случае модернизации, когда есть десятилетнее "наследство", сотни или даже тысячи коммутаторов доступа от Comrex 1008 до c2960? В этом случае схема "VLAN на пользователя" представляется едва ли не единственной возможностью получить универсальное решение без замены оборудования.

Дальше - проще. При эксплуатации недорогое оборудование на доступе приносит только плюсы - оно

дешевле в замене, проще в обслуживании, допускает одновременное применение коммутаторов разных "поколений" и марок.

P.S. Еще один момент, которым давно уже пугают – переход на IPv6. Что придется делать со всеми «интеллектуальными» коммутаторами на доступе, которые не поддерживают и никогда не будут поддерживать IPv6?

Автор - Дмитрий С.