Организация надежного канала Интернет

Уровень проникновения Интернет в нашу деловую жизнь сейчас настолько стал велик, что пропадание канала связи с внешним миром даже на пару часов может привести к серьезным проблемам в работе или даже прямой потере денег (упущенной выгоде). В современном коммерческом предприятии многие бизнес-процессы напрямую зависят от каналов связи, где самым доступным и наиболее часто используемым на сегодняшний день является Интернет соединение. Бухгалтерский АРМ "Интернет-банк", сдача налоговой отчетности по электронным каналам связи, IP-телефония, деловая переписка, интернет-торговля, B2B-системы обслуживания клиентов, корпоративные порталы, маркетинговые исследования, информационный поиск - вот далеко не исчерпывающий список бизнес-приложений, которые повсеместно используют современные компании в своей работе каждый день, не говоря уже о банках, электронных торговых и аукционных площадках и т.п., где роль каналов связи чрезвычайно высока. В этих условиях одна из главных задач ИТ отдела современной компании - организация и поддержание бесперебойного и достаточно скоростного интернет канала. В этой статье я хочу рассмотреть основные аспекты выполнения данной задачи для типовой организации Н.Новгорода из сектора СМБ и привести некоторые конкретные решения ее технической реализации.

Итак, шаг первый. Выбор Интернет-провайдера.

В последние годы в Н.Новгороде настолько бурно строились оптические опорные сети сразу несколькими альтернативными провайдерами телеком-услуг (сейчас в городе активно действуют более десяти таких компаний), что привело во многих районах города к серьезной конкуренции между ними и, как следствие, к существенному падению цен на высокоскоростное подключение абонентов, как физических так и юридических лиц. Например, наша компания имеет возможность выбирать сразу из четырех провайдеров, предлагающих оптическое подключение на скорости до 100 Мбит/с, а также из двух традиционных операторов ADSL-подключений: АДС("Билайн-бизнес") и "Волгателеком". Не буду останавливаться на персоналиях, но отмечу, что качество каналов и стоимость подключения (тарифные планы) у провайдеров сильно отличаются, и сисадмину компании-абонента нелегко выбрать среди этого множества оптимальный вариант. Возникает дилема - какой канал выбрать: надежный, но дорогой или экономичный, но без гарантий стабильной работы? Уточню, что качество канала определяют три основные характеристики: соответствие определенной тарифным планом скорости соединения в течение всего рабочего дня, бесперебойность работы и действия технической службы провайдера при аварийных ситуациях (время восстановления), скорость доступа к различным ресурсам в интернет (сюда же относится организация работы в Нижегородском кольце). Не буду останавливаться подробно на характеристике нижегородских провайдеров, это отдельная тема, но цель любого нормального клиента - получить максимальное качество услуги по минимальной цене.

Наш опыт показывает, что оптимального во всех отношениях провайдера в Н.Новгороде не существует, а решение обозначенной задачи достигается путем одновременного подключения сразу к 2-3 провайдерам, правильном выборе тарифных планов и тонкой настройке оборудования. При таком подходе компании вполне реально получить стабильный канал с полосой 4-8 Мбит/с с месячным порогом скоростного трафика 10Гбайт всего за 1,5-2,0 тыс.руб.

Шаг второй. Определение и выбор типа основного и резервного канала.

Как только вы определитесь со списком доступных для вашего местоположения провайдеров и технологий, которые они предлагают, необходимо выбрать оптимальный тип соединения для основного и резервного каналов. В Нижнем Новгороде сейчас доступны следующие технологии доступа в интернет:

1. ADSL.

Самая массовая технология, предлагаемая в основном традиционными телефонными операторами (АДС, Волгателеком), располагающими собственной кабельной базой - проложенными в квартиры и дома медными парами. Работает на расстояниях до 4-5 км от абонента до кросса АТС, а при использовании нового подпротокола Annex L - до 7 км. Максимальная скорость в направлении

абонента у ADSL2 - 24 Мбит/с при длине медной пары до 1,5км, но её провайдеры дают далеко не на всех тарифах и не в любом районе города. Обычно она ограничена 8 Мбит/с, а для длинных пар и того меньше. Доступность такого подключения в Нижнем сейчас очень хорошая, но тарифная политика телефонных компаний такова, что интенсивное использование этих каналов "влетит в копеечку". Кроме того, по задумке ADSL - технология ассиметричная, т.е. скорость соединения в направлении от абонента примерно в 8 раз меньше, что мешает работать с некоторыми корпоративными приложениями, например закачкой по FTP файлов на удаленный сайт. В некоторых случаях, в индивидуальном порядке, с оператором можно договориться об организации соединения на той же медной паре по симметричной технологи SHDSL.bis (до 5,7 Мбит/с) или VDSL2 (до 40 бит/с при длине пары до 1 км). Я бы рекомендовал канал ADSL для резервного соединения, если, конечно, доступны другие варианты для основного подключения.

2. Оптика до здания (FTTB).

Я уже в начале статьи отмечал, что данный вид подключений в последнее время рос лавинообразно, и сегодня им охвачены практически все бизнес-центры и большие учреждения в городе, будь то институт или завод. Основные компании, предлагающие этот тип подключения - Р-Телеком, МЕГА-НН, Комстар-регионы (экс-Сенди), Старт-телеком, Инфолинк, АБВ и некоторые другие. Недавно, опомнившись, спешно начал строить опорную оптическую сеть и наш основной игрок на рынке - Волгателеком. Канальная скорость такого оптического подключения обычно 100 Мбит/с, доступная полоса делится между всеми подключенными абонентами в здании, в офис которых приходит уже обычная "витая пара" от распределительного узла. Типовой тарифный план предусматривает скорость подключения абонента до 10Мбит/с, которая может в течение дня варьироваться в зависимости от загрузки оптического подключения как вашего строения, так и всего магистрального участка до центрального узла провайдера. При недостатке клиентов у провайдера в отдельных местах можно на приемлемых условиях получить и все 100Мбит/с. Все остальные типы выделенной линии Ethernet являются частным случаем этого вида.

3. Беспроводной канал WiFi (2,4Ghz) или WiMax (2,5Ghz).

Первый вид подключения распространен в местах общего пользования и обычно предназначен для подключения отдельных абонентов, хотя скорость выделенного WiFi соединения может быть вполне прилична – около 20Мбит/с. Но незначительная радиус действия точек доступа мешает их широкому распространению для подключения корпоративных абонентов. Близкие по смыслу технологии Radio Ethernet с большим радиусом действия типа Breezcom и Revolution (полоса 3.5 Ghz) в Нижнем Новгороде распространения не получили из-за сложностей с органами гос. регулирования.

Более приспособленная для городских сетей технология WiMax (иногда называемая 4G) теоретически сегодня может обеспечить канал до 70 Мбит/с на сектор 60гр, которая делится между подключенными абонентами. В нашем городе уже около двух лет 4-5 провайдеров (Энфорта, Старт-телеком, Unitline, Virgin Connect) предлагают такие подключения. За канал 1-2 Мбит/с они просят 3-3,5 т.р., поэтому обычно их разворачивают там, где другие виды подключений просто не возможны. Инфраструктура сетей этих операторов (опорная оптическая сеть + базовые станции) пока слабо развита, а стоимость оборудования и тарифы весьма высоки. Надеждам на скорый приход самого агрессивного российского оператора WiMax «Скартел» (марка YOTA), предлагающего в Москве юр. лицам канал 10Мбит/с за 2,5 т.р., похоже, не суждено сбыться - трудное финансовое положение региональную экспансию «Скартела» приостановило. Реальная скорость этого канала в Москве при наборе клиентской базы в часы пик редко превышает 1Мбит/с. Вывод - в "тяжелых" случаях WiMax может быть основным каналом, а в других – только резервным (при помегабайтной оплате).

4. Беспроводной мобильный канал 2G/3G. Здесь основные игроки - сотовые операторы, так как технологии базируется на уже существующей у них инфраструктуре. К сетям 2G относят GPRS (до 56Кбит/с) и EDGE (до 384Кбит/с), а к 3G - UMTS/HSDPA (до 3.6/7.2Мбит/с) и CDMA/CDMA2000 EV-DO (до 2.4Мбит/с). МТС, Билайн и Мегафон уже около года подключают в Н.Новгороде абонентов по технологии UMTS/HSDPA, а Скайлинк - по технологии CDMA/EV-DO. Данные варианты в потребительском плане почти равнозначны, хотя по опыту последний ввиду небольшой абоненткой базы выдает реальные 2Мбит/с, а перегруженные сети большой тройки показывют реальную скорость около 600-800 Кбит/с, чего, впрочем, вполне достаточно для обычного серфинга в Интернет. Наличие недорогих начальных тарифов (100Мб за 250 руб. у МТС),

условно безлимитных (до 512Кбит/с у Билайн за 695 руб), приличная зона покрытия (Н.Новгород, Арзамас, Саров, Кстово, Бор, Дзержинск, Б.Козино) и наличие недорогого абонентского оборудования в виде USB модемов делают данный тип интернет соединения вполне привлекательным для создания резервного канала в офисе или основным для мобильных сотрудников и подразделений.

5. Спутниковый однонаправленный беспроводной канал.

В некоторых неосвоенных районах нашего города и в пригородах такое решение может быть весьма эффективным. Слабая сторона этой технологии - нестабильность скорости от загрузки транспондера и влияние погоды. Поэтому ее применение нужно планировать в сочетании с каким-либо проводным каналом, тем более, что для обратного трафика от абонента в спутниковом канале задействован именно земной канал. Такая связка (спутник + ADSL) успешно работала в нашем офисе 2 года и позволяла иметь 7 Гбайт трафика в месяц на скорости около 1Мбит/с за 2,5 т.рублей. Выбор провайдеров довольно широк, наиболее известный из них немецкий SkyDSL, у которого в России есть представитель в Екатеринбурге. Недавно в тестовом режиме начал предоставлять такую услугу отечественный оператор спутникового телевидения Tricolor. Цены обещаются более чем демократичные. Также нужно учитывать, что реализация спутникового канала предполагает наличие прокси-сервера на базе ПК для спутниковой карты PCI.

Шаг третий. Выбор технического решения.

Прежде чем выбирать оборудование, исполнитель проекта должен четко ответить себе на следующие вопросы:

- сколько всего пользователей интернет в компании, сколько из них в среднем одновременно будут использовать канал и сколько в среднем они будут генерировать интернет сессий (некоторые любители открывания окошек в браузере генерируют до 100-150 сессий).

- какую максимальную скорость канала могут потребовать те или иные приложения, например, участие в вебинарах, видеоконференциях, аренда "облачных" ресурсов и приложений и других требовательных до полосы сервисах (следует помнить, что доступная скорость и скорость подключения к интерфейсу провайдера - не одно и тоже)

- будут ли приниматься меры для ограничения трафика некоторым пользователям (квотирование) и будут ли выделяться привилегированные группы пользователей.

- будет ли и как интенсивно использоваться шифрование трафика по технологии VPN или какой-то иной для образования закрытых корпоративных каналов с филиалами, складами и т.д., а так же какова должна быть скорость этих каналов.

- планирует ли компания разворачивание системы IP-телефонии

- в каком виде и в каком месте будет организовано ограничение пользователей к некоторым ресурсам интернета, а так же антивирусная защита и защита от спама.

- будет ли необходимость в доступе сотрудников к локальным ресурсам компании из вне офиса через канал интернет, а также в размещении собственного ВЕБ-сайта внутри корпоративной ИТ-инфраструктуры на собственной площадке.

- каков реальный технический уровень исполнителя проекта и каков бюджет времени и денег может быть выделен руководством компании для решения поставленной задачи организации надежного интернет канала и решения сопутствующих задач.

Приведем несколько вариантов технических решений, различных по количеству пользователей (масштабу компаний), набору функциональных возможностей и стоимости, двигаясь от самых простых решений к более продвинутым.

1. Перенаправление внешнего трафика на резервный шлюз.

Некоторые производители интернет маршрутизаторов и модемов предусмотрели возможность резервирования канала через дополнительный низкоскоростной порт (RS232), к которому может быть подключен dial-up или GSM модем. Кроме того, данные тип оборудования может быть запрограммирован на перенаправление всего поступающего трафика на другой внешний шлюз, IP-адрес которого заранее записан в настройках. В качестве последнего может выступать абсолютно любой роутер, реализующий резервное подключение по одной из вышеописанных технологий.

+ небольшая стоимость решения
- вхолостую постоянно работающий резервный маршрутизатор
- простой резервного канала в штатном режиме
- использование в качестве встроенного резервного соединения низкоскоростных, морально устаревших технологий

Последний минус, правда, уже есть возможность исправить с появлением на рынке 3G/4G недорогих USB модемов и недорогих абонентских устройств, умеющие работать с USB модемами 3G/4G (D-Link DIR-320, ASUS WL-520gP, Zyxel Keenetic) Правда, они пока не умеют штатно работать с 2-мя WAN соединениями одновременно и автоматически переключаться с проводного интерфейса на беспроводной и обратно, но вполне могут выполнять роль либо основного, либо беспроводного резервного шлюза (прошивка для DIR-320 от YOTA допускает ручное переключение). Учитывая стоимость 3G модема и маршрутизатора вместе менее 5 тыс.руб. организация такого канала по карману даже начинающей компании.

2. Балансировщики нагрузки с 2-мя WAN интерфейсами.

Довольно редкое, но очень эффективное решение, т.к. "убивает сразу двух зайцев": обеспечивает автоматическое резервирование основного канала вспомогательным и распределяет весь пользовательский трафик по каналам в некоторой заданной пропорции. У "продвинутых" балансировщиков доступны минимум четыре алгоритма распределения трафика (клиентских сессий) по каналам: процентный, равномерный, с превышением порога в основном канале и временной (по расписанию). Самым доступным представителем данного класса оборудования (реализующим только первый алгоритм) еще недавно был D-Link DI-LB604 по цене около 3 тыс.руб. Сейчас доступно несколько более дорогое оборудование: Asustek RX-3042H, TP-Link TL-R480T+, DrayTek Vigor 2820 и некоторые другие.

+ небольшая стоимость решения и легкость настройки
+ полное использование обеих каналов (провайдеров)
+ незаметность для пользователей переключения на запасной канал и обратно
- неумение распределять по каналам трафик по пользователям и по приложениям
- как правило, неумение создавать и резервировать VPN соединения
- слабое присутствие данного оборудования на российском рынке

3. Сетевые экраны фиксированной конфигурации с 2-мя и более WAN интерфейсами.

Данный класс оборудования используется достаточно давно и лишен почти всех недостатков, перечисленные выше, а также организуют доступ к внутренним ресурсам ЛВС удаленным пользователям. Классическими представителями данного класса на рынке являются D-Link DFL-800, Zyxel ZyWall-35, Netgear FVS336G, DrayTek Vigor 2910, а вот совсем недавно анонсированный Netgear SRX5308 является пока уникальным продуктом на рынке, т.к. имеет 4 гигабитных WAN порта и способен "обслужить" клиента любого размера или даже провайдера среднего масштаба. Цены на данный тип оборудования начинаются от 12 т.р., а некоторые модели позволяют организовать вдобавок к базовым функциям за дополнительную плату такие UTM-сервисы как, антивирусная защита непосредственно на входе в корпоративную сеть, борьба со спамом с использованием специализированной интернет базы, контентная фильтрация, система фиксации и предотвращения хакерских атак извне. Следует заметить, что эти дополни-

тельные сервисы следует использовать очень осмотрительно, только при незначительной загрузке процессора этих устройств, иначе можно получить резкое падение производительности по основным функциям, т.е. общей пропускной способности. Еще год назад эти устройства стоили немалых денег, но с появлением мощных процессоров с малым потреблением типа Intel Atom и резкое падение цен на память сделали свое дело, и сейчас все основные игроки на рынке предлагают такие устройства – миникомпьютеры, обычно реализованные на базе ОС Linux, по цене уже менее 20 тыс. руб. (Zyxel ZyWall USG-50, D-Link DSR-1000 и некоторые другие), причем, с гигабитными WAN и LAN портами.

+ комплексное решение задачи по резервированию каналов, защищенному доступу удаленных пользователей, фильтрации интернет контента и т.п.
+ возможность организации DMZ зоны для размещения публичного WEB-сервера
+ возможность различать и распределять трафик в каналах по множественным критериям, такими как используемый приложением сетевой протокол, принадлежность пользователя к привилегированной группе и т.д.

- относительно высокая цена и необходимость тщательной настройки
- невозможность организации 3-х и более WAN-интерфейсов
- сильная загрузка центрального процессора задачами шифрования и контроля трафика

4. Модульные универсальные маршрутизаторы.

Сама идеология этого оборудования (модульность) позволяет доукомплектовывать базовую конфигурацию роутера по мере необходимости и получить в итоге достаточное количество WAN и LAN портов, причем различных по технологии типов. Несмотря на победное шествие технологии Ethernet на городских магистралях провайдеров многие компании еще используют синхронные протоколы передачи данных типа ISDN PRI, Frame Relay, X.21. Бесспорным лидером этого сегмента рынка является компания Cisco Systems, линейка маршрутизаторов с универсальными сервисами которой SR1800/2800/3800 имеет решения для самых нестандартных задач. Самый "младший" представитель этого семейства с 2-мя WAN интерфейсами Cisco 1841, способный одновременно работать с различными провайдерами, стоит от 30 тыс.руб.

+ огромная номенклатура интерфейсных модулей для WAN-подключений
+ способность прокачать через роутер WAN-LAN полноценные 100Мбит/с и более
+ наличие вычислительных спецмодулей и большой внутренней памяти позволяет интегрировать в роутер такие "сторонние" приложения, как менеджер IP-телефонии или антивирусный контроль
+ гибкая настройка резервирования каналов, в т.ч. защищенных по VPN
- цены, не подъемные для малого бизнеса
- необходимость докупки необходимых программных модулей (расширенного функционала)
- трудность (дороговизна) организации билинга (учета трафика по пользователям)
- необходимость высококвалифицированного персонала для настройки оборудования
- дефицитность некоторых моделей по причине не простых правил ввоза оборудования с аппаратным шифрованием в Россию

5. Программные прокси-серверы на базе обычного ПК.

Не трудно догадаться, что и описанные выше устройства, по сути, так же являются компьютерами, где есть процессор, оперативная и постоянная память, слоты расширения и где при старте загружается и работает некая операционная система (микропрограмма), которая и управляет всем процессом передачи трафика. Но поскольку эти устройства имеют уникальную аппаратную часть и закрытую архитектуру, пользователю самому трудно что-то изменить в функционале маршрутизатора. Естественно, спрос на продвинутые интернет маршрутизаторы и готовность пользователей платить десятки и сотни тысяч рублей не остался без внимания опытных программистов, и как грибы после дождя в начале 21-го столетия начали появляться программы для стандартных PC-совместимых ПК, реализующих в той или иной мере функционал

классических маршрутизаторов. Наиболее доступными и легкими в развертывании являются программы для Windows, например, WinGate, Traffic Inspector и другие, но уважение пользователей и большее распространение получили программные прокси-серверы под управлением Linux и FreeBSD. Последние гораздо лучше изначально подходят для реализации данной задачи, более стабильны в работе, не расположены к вирусным заражениям и, к тому же, не так требовательны к аппаратным ресурсам ПК, что позволяет в качестве платформы такого решения использовать устаревшие ПК 5-летней давности (если Вы уверены в его достаточной надежности - смотри заголовок статьи). Если в компании есть приличный "линуксист" (и вы в нем уверены на долгие годы вперед), то достаточно функциональный роутинг, с несколькими интерфейсами LAN/WAN можно настроить не прибегая к какому-либо коммерческому ПО, остальным же рекомендую не тратить массу времени на изучение основ UNIX-программирования и купить готовые к эксплуатации программы. Одним из таких коммерческих российских продуктов является Ideco Control Server, имеющий обширный функционал и гибкую систему лицензирования. Главной изюминкой его является то, что он устанавливается на абсолютно "голую" машину (не надо тратиться на легальное системное ПО) и позволяет, кроме всего прочего, администрировать работу в Интернет персонально каждого пользователя. Удобный графический русскоязычный интерфейс, работа с меню, обилие информативных отчетов, электронная почта, все это легко настраивается обычным пользователем "средней руки", который может и не подозревать, что работает на Linux машине. Подробнее о системе можно почитать на сайте производителя http://www.ideco-software.ru/ Производительность и количество интерфейсов этого программно-аппаратного решения определяется используемым ПК (сервером) и может масштабироваться в достаточно широких пределах.

+ гибкий, почти безграничный, добавляемый по необходимости, функционал
+ возможность использования нестандартных каналов, например, спутниковых
+ легкость в развертывании и сопровождении, архивировании данных
+ русскоязычный интерфейс, удобная и гибкая система отчетов, экспорт форматов
+ наличие сертифицированной ФСТЭК версии (конкретно для Ideco Control Server)
+ бесплатная техническая поддержка производителя ПО
- требуется дополнительный, аппаратно совместимый, выделенный под задачу ПК.
- стоимость лицензии на ПО растет пропорционально количеству учетных пользователей
- переключение на резервный канал и обратно происходит достаточно долго, что связано с перезагрузкой программных модулей.

Предвидя замечания "продвинутых" специалистов, сразу поясню, что:

* да, можно, например, у недорогого экрана D-Link DFL-210 порт DMZ заставить работать, как 2-й WAN, но это даже у опытного специалиста займет немало времени, а приемлемую балансировку каналов сделать не получится. Уж лучше дополнительно к экрану использовать отдельный балансировщик (см. п.2 выше) и получить одновременно используемые балансируемые каналы.

* да, китайские фирмы в угоду рынку сейчас выпустили массу совсем недорогих noname роутеров с большим количеством интерфейсов, которые призваны потеснить авторитетов этого бизнеса. Ответ на это простой - количество портов и их номинальная скорость еще не означает, что процессор роутера сможет обработать трафик для всех портов одновременно на этой скорости, особенно, в защищенном режиме шифрования, а создание «безглючных» прошивок подобных устройств требует многолетнего опыта в этой области.

И последнее замечание. Не доверяйте маркетинговым цифрам провайдеров и изготовителей оборудования, особенно малоизвестных китайских фирм. Ориентируйтесь на опыт работы конкретных пользователей и испытания в независимых лабораториях. И покупайте там, где знают, что продают.

Об авторе:
Генеральный директор ЗАО «Сети» Дементьев Андрей
Вопросы и замечания можно присылать на seti@sandy.ru или связаться по тел.(831) 246-40-73