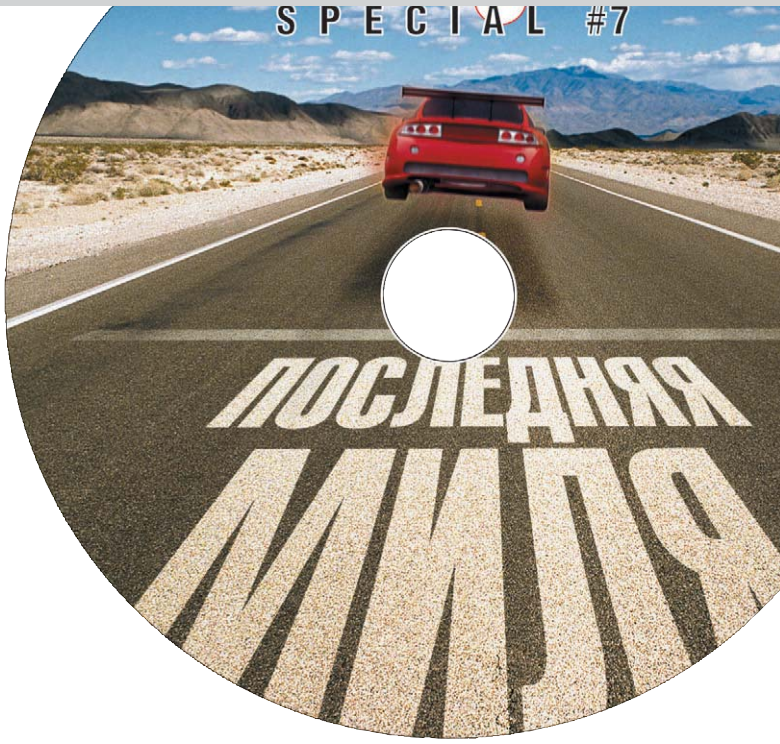


Первое, второе и пакет

Зарождение новой психологии, множество не виданных доселе возможностей и ограничений, появление новых маний и фобий — вот далеко не полный перечень последствий выхода общества на новый уровень организации, имя которому — локальная сеть.

По большому счету, все необходимое для работы в локальной сети уже предусмотрено в операционных системах. Но если вы хотите заставить технику работать на вас в полном объеме, то тут не обойтись без специализированного ПО, о котором пойдет речь ниже.

IPetC Premium — программа, служащая для автоматической настройки параметров локальной сети в любой ОС Windows. Особенно по душе IPetC придется владельцам ноутбуков, которым по долгу службы приходится часто перебираться с места на место. Судите сами, для того чтобы подключить компьютер к любой локальной сети, вам достаточно просто вставить сетевой кабель в соответствующий разъем и запустить эту программу. Пара простых манипуляций и вы увидите рабочие станции своих коллег!

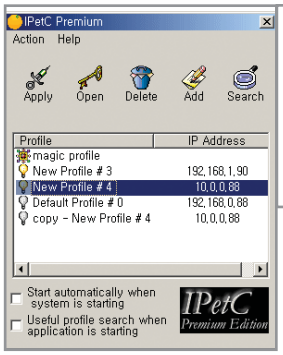
При помощи программы Desktop DNA любое приложение можно не просто скопировать с компьютера на компьютер, но и перенести его полностью со всеми файлами, настройками, системными библиотеками и ключами реестра. Помимо этого, программа может переместить с машины на машину все системные настройки (настройки Рабочего стола, сетевые настройки, настройки принтеров и т. п.). В общем, Desktop DNA позволяет полностью клонировать все настройки компьютера вместе с информацией, хранящейся на жестких дисках.

Локальная сеть

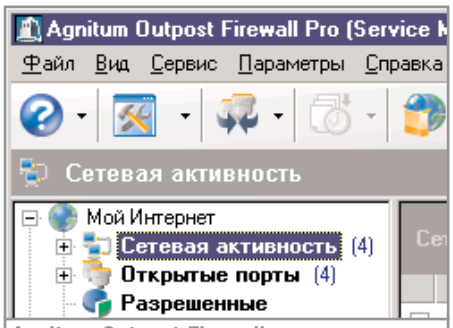
Безопасность

Что такое firewall, сегодня знает почти каждый, но далеко не все спешат пользоваться программами этого класса. В некоторых случаях, например, если вы изредка дозваниваетесь в Интернет из дома, это даже нельзя назвать легкомыслием. Слишком мала вероятность взлома. Однако при работе в офисных и особенно районных сетях защита просто необходима. Всегда может найтись бравый товарищ, который в чисто познавательных целях решит проверить вашу систему на прочность. Если ваш компьютер ко всему прочему сутками напролет доступен в сети, последствия таких проверок могут оказаться непредсказуемыми. Одним из лучших решений для защиты рабочей станции от несанкционированного трафика является Agnitum Outpost Firewall.

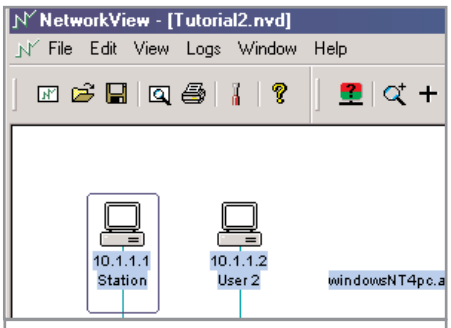
Утилита для обнаружения вторжений Snort известна благодаря своей эффектив- »



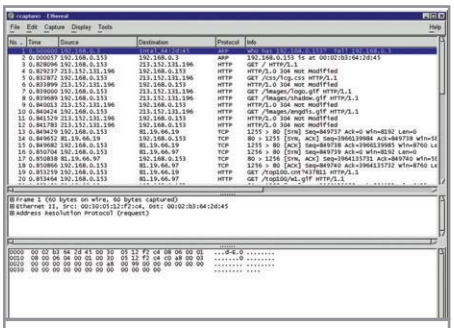
IPetC Premium — настройка сети происходит в несколько кликов мышью



Agnitum Outpost Firewall — мощная защита рабочей станции



NetworkView — узнайте больше о своих «соседях»

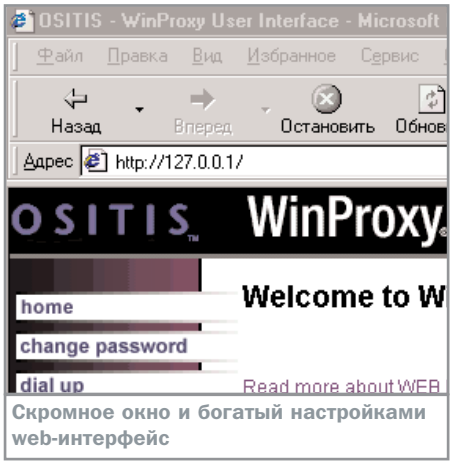


Ethereal — исчерпывающая информация о трафике

» ности и бесплатному распространению. Она может работать в трех режимах: пакетного снифера, регистрации пакетов и обнаружения атак. В последнем из них Snort осуществляет анализ текущего трафика, проверяет корректность структуры получаемых пакетов и соответствие их содержимого определенным правилам. Для описания сетевых инцидентов и определения реакции системы в программе предусмотрен язык сценариев. Встроенная база данных позволяет диагностировать распространенные типы инцидентов, таких как «скрытое» сканирование (использующее флаги сетевых пакетов FIN, ASK), атаки на переполнение буфера различных сервисов, атаки, использующие нарушение структуры сетевых пакетов (ping of death), атаки вида «отказ в обслуживании» (DOS и DDOS). При обнаружении системой любого подобного инцидента можно передать предупреждающее сообщение в службу WinPopup, в лог-файл или сетевому сервису.

Сетевые сканеры

Среди программ для сканирования и диагностики локальных сетей очень много серых и неприглядных. Пользоваться ими могут разве что системные администраторы с большим опытом. Но зачем же так над собой издеваться, когда на свете есть утилита NetworkView? Она сканирует сеть и без посторонней помощи рисует ее схему, похожую на те, что обычно создаются в векторных редакторах. Итоговую модель можно сортировать по IP-адресам, Mac-адресам и т. п. и при необходимости распечатать. Внутри главного окна программы могут существовать несколько окон схем и таблиц. Предусмотрена также возможность передать управление найденным хостом программе VNC, которая опубликована в разделе «Бонус».



Скромное окно и богатый настройками web-интерфейс

Прокси-серверы

Мощные серверные утилиты, которые могут работать в ОС Windows и уж тем более в Windows 9x/Me, сегодня встретишь нечасто. WinProxy как раз является представителем этой редкой категории. Она — не просто прокси-сервер, она — утилита, способная защитить пользователей локальной сети от таких напастей Интернета, как спам, вирусы (для этого используется сервис от Panda Software) и хакерские атаки. Программа поддерживает абсолютное большинство протоколов, позволяет назначить пользователям различные права, кэширует данные и DNS для ускорения работы, позволяет запретить доступ к определенным сайтам и т. д. Все вышеперечисленные сервисы могут быть детально настроены через web-интерфейс, который (при условии того, что программа запущена) доступен через любой браузер по адресу http://127.0.0.1.

Proxy-Pro Professional GateKeeper — мощный профессиональный инструмент для организации доступа в Интернет. Прокси-сервер имеет достаточно большой набор настроек и обладает очень неплохими возможностями. Доступ к основным настройкам программы можно получить не из обычного меню, а через браузер при помощи web-интерфейса. Благодаря этому контролировать программу и вносить изменения в ее настройки можно с удаленной рабочей станции. Программа поддерживает работу с протоколами HTTP, FTP, Telnet, Real Audio, Pop 3, SSL, RTSP, SOCKS4, SOCKS5, MAPPED LINK (TCP), MAPPED PORT (UDP).

Учет трафика

Ethereal 0.9.13 — бесплатная утилита для анализа сетевого трафика может работать в графическом режиме и в режиме командной строки. Отслеживать можно как все пакеты сразу, так и использовать фильтр по определенному протоколу, которых, кстати, Ethereal поддерживает аж 385 (о предназначении большинства из них любой нормальный человек не имеет ни малейшего представления). Полученные данные можно сохранить как в родном формате программы, так и в форматах других утилит. При использовании утилиты в ОС Windows требуется драйвер WinPcap, а в Linux — библиотека libpcap.

Заключение

Закончив подготовку этого номера, мы совершенно случайно для себя обнаружили, что протестированными утилитами регулярно никто из нас не пользуется. Сетевые утилиты не нужны каждый день, но они всегда должным быть под рукой на всякий случай, ведь в одну сеть нельзя войти дважды.

■ ■ ■ Дмитрий Асауленко, Павел Шошин

Для разработчиков

Редакция журнала Chip открыта для сотрудничества с разработчиками ПО и заинтересована в публикации практически полезных и безопасных программ. Предоставляемое ПО должно сопровождаться описанием основных функций. Программы принимаются к публикации не позднее чем за два месяца до появления номера в продаже.

Origin of spicies

На протяжении своей истории человечество испытывало острую необходимость в средствах быстрой передачи информации на большие расстояния. На заре цивилизации использовались примитивные способы — сигнальные костры, барабаны, почтовые голуби и т. д. С развитием науки они совершенствовались: изобретение электричества со временем позволило почти моментально обмениваться данными.

Дальнейшее развитие радио, телеграфа, телефона, изобретение компьютера создали плодотворную почву для проходящей и ныне интеграции различных устройств в глобальное информационное сообщество. На данный момент крупнейшим и самым распространенным во всем мире узлом этого сообщества, безусловно, является Интернет, сейчас насчитывающий более 50 миллионов пользователей и объединяющий около 40 тысяч различных сетей.

Терминал

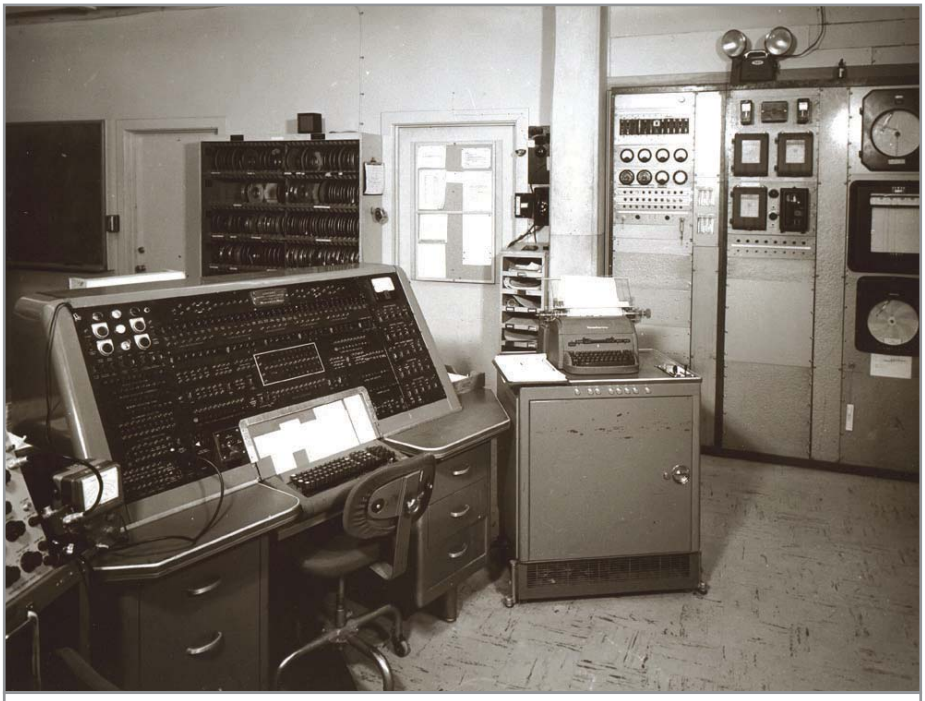
Первые компьютеры появились в 50-х годах и представляли собой огромные, порой занимающие целые здания устройства. Основной акцент ставился на увеличение их производительности, а удобство работы отходило на второй план. Однако в 60-х годах были пересмотрены способы организации вычислительного процесса, и появилась возможность учитывать интересы пользователей. Работать с компьютерами становилось все удобнее и удобнее. Появились так называемые интерактивные многотерминальные системы разделения времени. В таких системах несколько пользователей получали отдельный терминал, подключенный к центральному процессору, и могли в режиме реального времени вести диалог с компьютером, при этом создавалась иллюзия единоличного владения компьютером. Немного позже терминалы из стен вычислительного центра переместились непосредственно на территорию всей организации.

Таким образом, создание многотерминальных систем разделения времени стало первым шагом к появлению современных локальных вычислительных сетей, которы- »

» ми они еще не являлись, так как использовали централизованный способ обработки и хранения данных.

В начале 70-х благодаря многолетним усилиям большого количества разработчиков произошел очередной технологический прорыв, давший возможность создавать мини-компьютеры, которые позволяли обрабатывать информацию быстрее своих гигантских предшественников. Резкое уменьшение их стоимости позволило даже небольшим предприятиям приобретать компьютеры для решения своих проблем, и появилась необходимость распределения вычислительных ресурсов по нескольким подразделениям предприятия. Однако при этом все компьютеры продолжали работать отдельно друг от друга.

Но со временем объем обрабатываемой информации вырос, вычислительных мощностей одного компьютера стало катастрофически не хватать, и появилась острая необходимость в возможности обмена данными между несколькими близко расположенными компьютерами. Предприятиям и организациям пришлось срочно разрабатывать программное обеспечение, позволяющее объединять свои вычислительные мощности. В результате появились первые локальные вычислительные сети, которые во многом отличались от тех сетей, которые мы используем сегодня. В первую очередь это касается устройств сопряжения между компьютерами — каждая компания использовала свои типы кабелей, различные виды разъемов и способы представления данных на линиях связи. Все эти устройства могли работать только с теми типами компьютеров, для которых они были разработаны. Естественно, это тормозило дальнейшее распространение локальных сетей.



UNIVAC 1 (Universal Automatic Computer) — первый промышленный компьютер, который был построен для бюро переписи США в 1951 году. Работал он с тактовой частотой 2,25 МГц и содержал около 5000 электронных ламп

Локальная сеть

Такая разобщенность и несовместимость между различными платформами все больше начинала беспокоить пользователей и потребителей, и в 80-х годах было сделано несколько попыток стандартизировать технологии объединения компьютеров в сеть. В результате из огромного количества технологий было выделено три основных — Ethernet, Arcnet и Token Ring.

В это же время на рынке начали появляться первые персональные компьютеры, которые стали идеальными элементами для построения локальных сетей: их производительности вполне хватало для работы сетевого программного обеспечения, но они нуждались в объединении своих вычислительных мощностей для решения сложных ресурсоемких задач. С течением времени ПК стали преобладать в локальных сетях, причем они уже использовались не только как клиентские терминалы, но и как устройства для централизованного хранения и обработки данных, то есть заняли место сетевых серверов, до этого построенных на мини-компьютерах.

С этого момента для создания локальной сети было достаточно приобрести стандартный сетевой адаптер, кабель и установить на компьютерах одну из популярных сетевых операционных систем. Присоединение каждого нового компьютера к существующей сети также не вызывало проблем — главное, чтобы на нем стоял сетевой адаптер, работающий по той же технологии, что и на остальных.

Сейчас к локальным сетям, также называемым LAN (Local Area Network), относят компьютеры, объединенные в сеть на сравнительно небольшом расстоянии — до 1–2 км. Также в локальную сеть, помимо компьютеров, входят различные периферийные устройства (принтеры, сканеры, устройства для резервного хранения информации и т. п.) и коммутационные устройства, соединенные чаще всего кабелями. Благодаря небольшим расстояниям при построении локальных сетей возможно использовать относительно дорогие, но высококачественные линии связи, позволяющие передавать информацию со скоростью до 100 Мбит/с.

Сейчас при построении локальных сетей основной их концепцией является совместный доступ. Прежде всего, мы говорим о совместном доступе к данным. Благодаря локальным сетям каждый член коллектива, работающего, например, над одним проектом, имеет постоянный доступ к данным, используемым его коллегами.

Также локальные сети предоставляют возможность совместного доступа к аппаратным средствам, то есть принтерами, подключенными к сети, могут пользоваться все ее пользователи, и отпадает необходимость приобретения принтера для каждого компьютера. А, к примеру, файловый сервер обеспечивает совместный доступ к программам. Таким образом, можно сказать, что основной целью создания локальной сети является совместный доступ к ресурсам.

Компьютерные сети делятся на два основных класса — одноранговые сети и сети с выделенным сервером. В одноранговых сетях не используются специальные компьютеры, обеспечивающие работу всей сети. Каждый ее пользователь выделяет в сети ресурсы своего компьютера — дисковое пространство, принтеры и т. д. При этом он может использовать ресурсы других пользователей. В таких сетях все пользователи рав- »

» ны в своих правах и возможностях. Эти сети просты в установке, не нуждаются в специальном программном обеспечении и существенно дешевле сетей с выделенным сервером. Сети с выделенным сервером, несмотря на свою дороговизну и сложность настройки, позволяют централизованно управлять всей сетью. В таких сетях применяется принцип «клиент-сервер». Сервер — это выделенный в сети мощный персональный компьютер, который управляет всей сетью. Клиенты, или рабочие станции, — менее мощные ПК, которые используют ресурсы сервера. Одноранговые сети чаще всего организуются в небольших офисах или при построении так называемых домашних сетей, а сети с выделенным сервером применяются в больших вычислительных центрах.

Глобальная сеть

Одновременно с успешным развитием локальных вычислительных сетей появилось желание соединять компьютеры, расположенные друг от друга на сотни и тысячи километров. Так, в августе 1962 года Дж. Ликлайдер, сотрудник Массачусетского технологического университета, впервые описал возможности информационного взаимодействия, которые станут возможными благодаря сети. В этом документе обсуждалась концепция «Галактической сети» (Galactic Network). Ликлайдер предугадал создание сети взаимосвязанных компьютеров, с помощью которой каждый желающий сможет быстро получать доступ к различной информации и программам, расположенным на любом другом компьютере. Все положения, описанные в этих заметках, по духу очень близки к состоянию современного Интернета. В октябре 1962 года Ликлайдер становится первым руководителем исследовательского компьютерного проекта в Управлении перспективных исследований и разработок Министерства обороны США (Defence Advanced Research Projects Agency, DARPA). Основной целью агентства было создание надежной системы коммуникаций, сохранявшей работоспособность даже в условиях ядерной атаки или природного катаклизма.

Команда специалистов, которая разработала и запустила сеть ARPANET

Но все же первоначально для соединения нескольких удаленных компьютеров использовались обычные телефонные линии, и в 1965 году компьютер TX-2, расположенный в Массачусетсе, связался с ЭВМ Q-32, находившейся в Калифорнии. Связь осуществлялась по низкоскоростной коммутируемой телефонной линии. Таким образом, была создана первая в истории нелокальная компьютерная сеть. Результатом этого эксперимента стало понимание того, что удаленные друг от друга на большое расстояние компьютеры могут успешно взаимодействовать между собой. Также стало ясно, что способов передачи данных по коммутируемым телефонным линиям недостаточно для достижения высокой скорости.

Рэй Томлинсон, изобретатель самого популярного средства сетевого общения — e-mail

В 1967 году появился план разработки сети ARPANET, которая должна была использовать так называемую пакетную коммутацию. В августе 1968 года агентством DAPRA был организован открытый конкурс на разработку одного из ключевых компонентов сети ARPANET — коммутатора пакетов, названного интерфейсным процессором сообщений (Interface Message Processor, IMP). В декабре следующего года конкурс выиграла группа, работающая под руководством Фрэнка Харта (Frank Heart) из компании Bolt, Beranek & Newman (BBN).

И в сентябре 1969 года компания BBN установила в Калифорнийском университете первый интерфейсный процессор сообщений и подключила к нему первый компьютер. Вторым узлом сети стал Стэнфордский исследовательский институт. Спустя месяц после подключения Стэнфордского института к ARPANET из Калифорнийского университета было послано первое межкомпьютерное сообщение.

Следующими двумя узлами ARPANET стали Калифорнийский университет в Санта-Барбаре и Университет штата Юта. В итоге к концу 1969 года уже четыре компьютера были объединены в сеть ARPANET. И с этого момента можно начинать отсчет стремительного развития Интернета. Начало было положено. В последующие годы число компьютеров, подключенных к сети ARPANET, стремительно росло. Однако по мере роста ARPANET стали появляться и другие сети, и вскоре возникла необходимость связывать эти сети между собой.

Общий стандарт

Для организации межсетевых соединений был нужен протокол или, проще говоря, набор соглашений, определяющий способы обмена данными между разными, ранее не совместимыми программами. Для решения этой задачи в 1973 году агентство DARPA запустило проект под названием Internetting Project (проект объединения сетей). И уже в 1974 году Роберт Кан и Винт Керф разработали базовый протокол Интернета, позднее названный TCP/IP (Transmission Control Protocol/Internet Protocol — протокол управления передачей/межсетевой протокол). TCP обеспечивает доставку данных по нужному адресу, а IP отвечает за адресацию сетевых узлов. Однако с момента разработки TCP/IP до его масштабного распространения прошло практически 10 лет, и только в 1983 году »

» Агентство связи Министерства обороны США принимает решение использовать этот протокол на всех узловых машинах ARPANET. Этот переход был запланирован на 1 января этого же года и требовал одновременных изменений на всех компьютерах сети, но все прошло на удивление гладко. Так был установлен единый стандарт, благодаря которому смогла развиваться вся сеть.

Благодаря появлению единого стандарта очень многие университеты стали подключаться к ARPANET, и со временем объем передаваемых сообщений вырос настолько, что мощности сети стало не хватать, она стала просто-напросто захлебываться. На выручку пришел Национальный научный фонд США (National Science Foundation — NSF), который организовал пять суперкомпьютерных центров и стал искать способ, позволяющий ученым со всех концов страны получать доступ к своим машинам. Первоначально велись переговоры о предоставлении линий связи и ресурсов ARPANET, но они по каким-то причинам на такое соглашение не пошли, и NSF в 1986 году создал собственную сеть NSFNET. Новая сеть стала разрастаться, и настолько успешно, что ARPANET к 1990 году была свернута. Постепенно к NSFNET начали подключаться большие корпорации и коммерческие поставщики услуг Интернета, которые стали небезуспешно продавать возможность входа в сеть. С этого момента сеть стала доступна не только военным и научно-исследовательским центрам. Интернет становился доступным всем средством коммуникации.

Тим Бернерс-Ли, создавший систему представления контента в Интернете, названную World Wide Web

К тому времени количество услуг, предоставляемых в Интернете, было не так велико, как сегодня. Пользователям приходилось довольствоваться электронной почтой, разработанной в марте 1972 года Рэем Томлинсоном (Ray Tomlinson) и ставшей более чем на 10 лет крупнейшим и самым востребованным сетевым приложением, и пересылкой файлов и неформатированных текстов.

Но в 1990 году физик Тим Бернерс-Ли (Tim Berners-Lee), работавший в женевском Центре физики высоких энергий (CERN), решил создать такую систему, которая позволяла бы всем физикам в Европе обмениваться иллюстрированными форматированными результатами своих исследований и включать в них ссылки на другие публикации. Так родилась World Wide Web (WWW) — Всемирная паутина. С этого момента Глобальная сеть начала приобретать именно тот вид, который мы имеем на данный момент. Сейчас WWW является самой динамически развивающейся службой в Интернете, и количество текстов, доступных для публичного просмотра, исчисляется миллионами.

Последняя миля

Интернет давно уже превратился из сложного инструмента, доступного и понятного только узким специалистам, в средство для сотрудничества и общения людей, иногда разделенных тысячами километров, в механизм практически мгновенного обмена информацией и новостями, в огромную, постоянно пополняемую библиотеку. Бурное развитие сотовой и спутниковой телефонии, появление протокола пакетной радиопередачи данных (GPRS — General Packed Radio Services) перестает привязывать пользователя к какой-либо географической точке — доступ к Глобальной сети становится поистине мобильным. Можно проверить электронную почту или просмотреть последние новости, находясь в автомобиле или поезде. Пропускные способности каналов растут с каждым месяцем, и уже сейчас во многих странах передача аудио- и видеопотоков в режиме реального времени стала вполне реальным явлением. Однако для того чтобы вкусить все эти прелести, прежде всего необходимо получить доступ к точке входа в Интернет.

Такими точками чаще всего обладают интернет-провайдеры, которые, в свою очередь, соединены высокоскоростными каналами связи с другими центральными компьютерами сети. Финальный участок сети, который

Мэйнфрейм PDP10, который Рэй Томлинсон использовал для отправки первого персонального сообщения

соединяет клиента с провайдером, будь то один домашний компьютер или большая локальная сеть, принято называть «последней милей». Чаще всего именно ее качество определяет скорость взаимодействия конкретного компьютера со всей Сетью. Сейчас домашние компьютеры в большинстве своем подключаются к Интернету посредством телефонной линии, и самым слабым звеном в последней миле при таком соединении является качество телефонной линии и тип АТС. Однако все большее распространение имеют так называемые выделенные линии, которые используют собственные коммутации для доступа к сервис-провайдеру. Их прокладка и организация требует дополнительных, иногда немаленьких затрат, но и скорость передачи информации возрастает в несколько раз. Также все большую популярность приобретают системы беспроводного абонентского доступа. Основными преимуществами такого доступа к Сети являются достаточно быстрое построение канала связи, так как отсутствует необходимость прокладки кабелей, и относительная дешевизна по сравнению с проводными выделенными линиями. Как уже было сказано выше, сейчас появилась возможность использовать и сотовые телефоны для организации доступа в Интернет, а с появлением сотовых сетей третьего поколения скорость передачи данных у них достигнет просто фантастических высот.

В заключение хочется сказать, что вариантов доступа к Глобальной сети большое количество, и каким именно образом организовать свою последнюю милю, решать именно вам. Объем информации, которую можно найти в Интернете, растет с каждым часом, активность не затихает ни на минуту, и если вы все еще не подключены к Сети, поторопитесь.

■ ■ ■ Игорь Пыжов

АНОНС

Их стало двое
Проводные способы связи 10

Как два байта переслать
Соединение с помощью модема 14

Звенья цепи
Связь через сетевые карты 18

Без привязи
Беспроводные технологии 20

Сложности объединения
Гетерогенные сети 24

Верстовые столбы
Обзор сетевого оборудования 28

Простейшие способы связи

Их стало двое

Рано или поздно каждый встает перед задачей объединения ПК и начинает искать пути ее решения. Совет локального гуру «взять шесть частей кембриков на три части проводов и связать пинцетом последовательные шины» способен ввести в ступор любого энтузиаста.

Ethernet

Подробное изучение современной технологии построения кабельных локальных сетей не является целью данной статьи, Ethernet — наиболее распространенный способ коммуникаций между компьютерами. Все рассматриваемые дальше технологии будут сравниваться с достоинствами и недостатками Ethernet, и поэтому несколько общих характеристик привести необходимо.

Ethernet — это набор стандартов на кабельную структуру и передачу сигналов. Первоначальная концепция была разработана корпорацией Xerox в конце 1970 года. В качестве среды передачи использовался коаксиальный кабель. В процессе дальнейшего развития выделилось несколько различных типов Ethernet-сетей, для обозначения которых институт IEEE предложил названия вида: 10Base-2, 10Base-5, 10Base-F, 10Base-T, 100Base-TX.

Коаксиальный кабель (коаксиал) состоит из одного цельного или витого центрального проводника, который окружен слоем диэлектрика (изолирующий материал постоянной толщины и высокого сопротивления). Проводящий слой алюминиевой фольги, металлической оплетки или их комбинации окружает диэлектрик и служит одновременно экраном против наводок на центральный проводник и в качестве второго, возвратного контакта в кабеле. Общий изолирующий слой образует внешнюю защитную оболочку кабеля.

Топология сети на основе коаксиального кабеля представляет собой общую «шину», то есть компьютеры последовательно соединяются друг с другом отрезками ка- »

LINK

» беля. Отсюда следуют и общие ограничения: сложность при сопровождении больших сетей (попробуйте выполнить желание пользователя переставить стол на пару метров в сторону при коротком кабеле), а при повреждении одного из сегментов нарушается работы всей сети. На конечных точках линии устанавливаются специальные устройства — сетевые терминаторы (или обычные резисторы на 50 Ом). Скорость передачи данных составляет 10 Мбит/с. Для тонкого коаксиального кабеля (10Base-2) максимальная длина сегмента между двумя устройствами (компьютерами или повторителями) равна 185 м. Для толстого коаксиального кабеля (10Base-5) максимальная длина сегмента без повторителей составляет 500 м.

Витая пара

Витая пара (Twisted Pair — TP) состоит из четырех пар цельных или витых изолированных проводников. Из них используются только две пары — одна для приема, другая для передачи данных. При использовании защитной экранизации кабеля он маркируется как STP (Shielded TP), без экранизации — как UTP (Unshielded TP). Есть несколько различных категорий этого вида кабелей, для прокладки 100-мегабитных сетей рекомендуется использовать кабели категорий 5 и 5e.

Сеть на основе витой пары имеет звездообразную или древовидную структуру, где в качестве узловых точек используются специальные сетевые устройства — концентраторы (хаб) или коммутаторы (свич). Лучами звезды служат кабели, соединяющие центральную точку и пользовательские компьютеры. При повреждении одного из кабелей отключается только один сегмент, а остальная сеть продолжает нормально работать. Скорость передачи данных при использовании сетевых интерфейсов (сетевых карт) типа 10Base-T состав- ляет 10 Мбит/с, а для 100Base-TX — 100 Мбит/с. Максимальная длина сегмента сети на витой паре без повторителей 100 м. Используя витую пару, можно соединить два компьютера напрямую, без дополнительных сетевых устройств. Для этого используется кабель, в котором перекрестно соединены пары передающих и принимающих контактов сетевых интерфейсов.

На данный момент Ethernet на основе коаксиала используется редко, главным образом для организации длинных линий или в качестве дешевого бюджетного решения. А наибольшее распространение получили сети на витой паре.

Последовательный и параллельный порты

До настоящего времени соединение по последовательным или параллельным портам было одним из наиболее распространенных способов связи двух компьютеров. Для соединения используется нуль-модемный кабель. Схема разводки кабеля достаточно проста, и вместо покупки его можно спаять самостоятельно. Теоретически длина кабеля ограничена расстоянием 15 м. Для передачи данных на обоих компьютерах требовалось запустить необходимое программное обеспечение — Norton Commander или DCC (Direct Cable Connection) из стандартного пакета Windows. Несмотря на соединение таким способом только двух компьютеров, для современных операционных систем это выглядит полноценным сегментом сети. Только из-за ограничений, заложенных в архитектуре последовательного и параллельного портов, скорость передачи данных в такой сети сильно уступает скоростям Ethernet. Например, при работе через последовательные порты скорость будет около 115 Кбит/с, а для параллельных портов возрастет до 1200 Кбит/с. Значит, архив размером 10 Мбайт будет передаваться около полутора минут. В общем-то, это вполне допустимо как временное решение, но по причине перехода производителей оборудования на новые стандарты периферийных портов данный способ коммуникаций отходит в прошлое.

FireWire и USB

Учитывая политику ведущих производителей программного и аппаратного обеспечения по продвижению новых стандартов периферийных портов и постепенный отказ от поддержки старых, следует обратить внимание на знакомых незнакомцев — последовательные шины передачи данных FireWire и USB. Изначально спроектированные для работы с периферийным оборудованием, эти технологии применимы и для связи двух компьютеров или организации локальных сетей.

Несколько фактов: для USB максимальная длина соединительного кабеля 5 м. При использовании стандарта USB 1.1 скорость передачи данных составляет до 12 Мбит/с. При переходе на шину USB 2.0 »

Microdrive-адаптер поможет перебросить данные с накопителя на ПК

Концентратор FireWire позволяет подключить большее количество устройств

скорость возрастет до 480 Мбит/с. При работе с FireWire максимальная длина кабеля 4,5 м, а скорость передачи данных по нему до 800 Мбит/с. Для удлинения сегментов можно использовать аппаратные репитеры или специальный оптический кабель длиной до 100 м.

В обеих ситуациях применяются схожие принципы построения сетевой структуры, где в качестве транспорта используется специфичный для данных шин протокол, поверх которого работают обычные прикладные сетевые протоколы. Следовательно, никаких неудобств для пользователя не создается. Компьютер, который помимо сети на базе FireWire или USB подключен к обычной Ethernet-сети, необходимо настраивать как шлюз для передачи данных из различающихся физически сегментов сети.

Необходимо заметить, что, несмотря на высокую скорость передачи данных, превосходящую максимальную скорость Ethernet в несколько раз, строить сеть на базе USB 2.0 или FireWire будет недешевым удовольствием. Например, для работы по USB-портам требуются специальные кабели с оптронной развязкой, что увеличивает стоимость одного подключения до $40–50. Для организации домашней сети это несколько дорогое решение. Хотя, если требуется именно скорость, то это довольно интересный вариант.

HomePlug

Технология HomePlug позволяет соединять компьютеры, используя в качестве среды передачи данных существующую электропроводку. По стандарту HomePlug Powerline Specification 1.0 скорость передачи данных достигает значения 14 Мбит/с, а максимальная длина сегмента между двумя устройствами — 300 м. Данная технология особенно уникальна, когда прокладка новой кабельной структуры или использование беспроводных сетей невозможны или нецелесообразны. С ее помощью можно быстро создать временную сеть на выставке или в конференц-зале, не рискуя «поймать» в свою паутину кого-нибудь из посетителей. Также можно быстро соединить два компьютера из соседних подъездов в жилом доме.

Для нормальной работы сети все адаптеры HomePlug должны быть подключены к электропроводу с одной фазой. При подключении к электропроводам с разными фазами необходимо их объединить в единую сеть HomePlug с помощью специального коммутатора. Работоспособность сети HomePlug и скорость передачи данных практически не зависят от скачков нагрузки электросети и от включения/выключения мощных энергопотребляющих устройств (нагревательных приборов, холодильников, стиральных машин и т. п.).

Достоинство этой технологии очевидно: никаких новых проводов, мобильность в зоне проложенной электропроводки. Недостаток этой технологии тоже очевиден — относительно высокая цена. Пара адаптеров HomePlug в среднем обойдется около $300. И если в Америке данная технология

Беспроводной вариант

Инфракрасный порт

Использование инфракрасного излучения в качестве транспорта для обеспечения коммуникаций между различным оборудованием позволяет устанавливать соединение без кабеля на коротком расстоянии порядка нескольких метров. Связь осуществляется в режиме точка-точка, длина волны — 880 нм. Изначально при разработке этой технологии ставилась задача осуществлять связь с периферийным оборудованием. Требовалось добиться низкого энергопотребления и невысокой цены реализации решения, что позволило бы использовать эту технологию для мобильного оборудования с автономным питанием. Как можно убедиться, поставленная цель была достигнута, подавляющее большинство современного мобильного оборудования использует для коммуникаций инфракрасные порты. Это ноутбуки, сотовые телефоны, палмтопы и т. д. Ценой решений, заложенных в основу этой технологии, стала сложность ее использования при построении локальной сети, поскольку сетевые интерфейсы достаточно сложны и требуют большой мощности.

В качестве модели при разработке ИК-порта создатели опирались на существующую архитектуру COM-порта, что позволяло передавать данные со скоростью до 115 200 бит. Современные протоколы связи превосходят этот порог в тысячи раз. Например, VFIR (Very Fast Infra Red) позволяет достичь скорости 16 Мбит.

Хотя данная технология предназначалась в первую очередь для мобильного оборудования, сегодня существует целый класс ИК-приемопередатчиков для персональных компьютеров. С их помощью можно передавать файлы с ноутбука на домашний компьютер или упорядочить записи в записной книжке мобильного телефона, не уподобляясь заядлому любителю приставок Dendy.

Для ИК-излучения существует два источника помех: солнечный свет и флуоресцентные лампы, часто применяемые для общего освещения. Хорошо спроектированное оборудование должно предусматривать защиту — полосный фильтр для снижения влияния таких источников помех.

Многопортовые карты дороги, особенно если представлены разные интерфейсы

Кабель FireWire позволяет подключать к ПК и бытовую электронику

Самый распространенный стандарт подключения — USB

» позиционируется как устройство для построения домашних сетей, то в России высокая цена может оказаться главным сдерживающим фактором ее применения.

HPNA

Еще одна сетевая технология, «паразитирующая» на чужой физической структуре, — HPNA. С ее помощью на основе уже существующей телефонной проводки можно обеспечить связь между компьютерами на расстоянии до 400 м.

В качестве основной идеи данной технологии закладывалась задача обеспечить подключение пользователя к серверу доступа интернет-провайдера. Отсюда и вытекает ограничение скоростей в 1 Мбит/с для технологии HPNA 1.0 и 10 Мбит/с для HPNA 2.0. Нецелесообразно подавать пользователю на его абонентском участке скорость, большую, чем обеспечиваемая провайдером Интернета. Дополнительное назначение технологии HPNA — «удлинитель» Ethernet. Вспомним, что максимальная длина сегмента локальной сети на витой паре 100 м, а дальность передачи по технологии HPNA, в зависимости от вида кабеля и топологии сегмента передачи данных, до 400 м.

HPNA-модемы могут подключаться к центральному коммутатору, образуя локальную сеть, по топологии напоминающую звезду. Или работать напрямую друг с другом, образуя соединение типа точка-точка. Пара HPNA-модемов обойдется примерно в $140.

А что если...

необходимо установить связь на расстоянии больше сотни метров? Хотя данный вопрос и выходит за тематические рамки данной статьи, но, установив связь между компьютерами в соседних комнатах, наверняка захочется связаться и с компьютерами в соседнем здании. Кратко рассмотрим несколько фактов. При использовании толстого коаксиального кабеля максимальная длина между двумя соседними точками равна 500 м. Что можно добавить к этому? Старые фокусы — лучшие фокусы.

Если рассмотренной возможности недостаточно, то можно использовать xDSL-технологии. Например, соединив два SHDSL-модема медной парой и включив их через Ethernet-порты в локальные сети двух офисных или домашний сетей, можно на расстоянии до 2 км получить симметричную скорость передачи и приема данных до 2 Мбит/с, то есть файл размером 10 Мбайт передастся где-то за 40 с, а на расстоянии 7 км скорость будет до 70 Кбит/с. Возможно, это не так много, зато далеко. Если вас и это не устраивает, надо работать с оптоволокном, но это уже отдельная тема для разговора.

А что потом...

Исследовательский институт IEEE занимает ведущее место в разработке спецификаций сетевых технологий. На его счету в том числе и разработка современных стандартов беспроводных сетей. В настоящее время идут работы по созданию новой спецификации беспроводных персональных сетей — WPAN (Wireless Personal Area Networks) — на основе заимствованной из военной отрасли технологии UWB (Ultra Wide Band).

Разработанная для применения радарными установками в конце 50-х годов в US Army Research Laboratory технология позволяла исследовать скрытые подземные объекты, не доступные для обнаружения иными методами. Это был революционный прорыв в радарных технологиях. Вскоре от этой технологии ожидают еще одного решительного шага, но уже в области сетевых решений. Предположительно использование UWB позволит достичь скорости обмена данными до 1 Гбит/с. Ожидается, что данная технология будет предназначена для высокоскоростной связи оборудования, передающего большие объемы данных. Помимо организации беспроводных локальных сетей, технология может быть использована для передачи данных между компьютером и монитором, а также в звуковых системах.

В заключение

Выбор одной или другой технологии должен определяется не модой, а практическими соображениями. При всех удобствах беспроводной связи это дорогое решение, оправданное в случае невозможности создания кабельной сети. Выбор технологии связи по USB- или FireWire-портам накладывает ограничение на максимальное расстояние между компьютерами в 5 м, и этого не всегда бывает достаточно. При соединении по Ethernet, что, впрочем, относится и ко всем кабельным решениям (связь по портам COM, LPT, USB, FireWire), необходимо решать проблему укладки кабеля, о чем любят напоминать сторонники беспроводных сетей. Как можно убедиться, все рассмотренные технологии компьютерной связи обладают как преимуществами, так и недостатками. Зачастую при выборе решения необходимо обращать внимание не только на технические характеристики — скорости передачи данных, длину сегмента и т. п., но и на достаточно прозаичные бытовые проблемы. Построив домашнюю сеть, возможно, придется уговаривать любимую собаку или кошку не жевать кабель: он хоть и экранированный, но не вкусный. Или придется убеждать домовладельца не срезать кабель, который совершенно не портит интерьер подъезда. Так что окончательный выбор способа компьютерных коммуникаций должен решаться в каждом случае отдельно, с учетом всех технических и бытовых требований.

■ ■ ■ Александр Красоткин

Соединение с помощью модема

Как два байта переслать

В двадцать первом веке для получения разного рода информации при помощи ПК иметь выход в Глобальную паутину совсем не обязательно. Конечно, он есть в любом более-менее крупном городе, однако, получая электронное письмо с вложением в полмегабайта от друга, живущего в соседнем подъезде, мы каждый раз испытываем чувство вины за бесцельно потраченные ресурсы и собственные деньги.

Давайте попробуем обойтись без Интернета при обмене информацией того или иного рода в рамках одного населенного пункта, имея модем и телефон, но не имея интернет-соединения.

ТЗ и ТУ

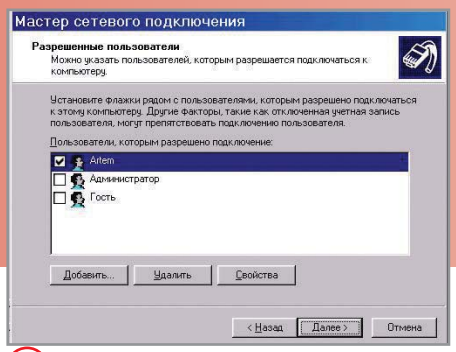
Для начала определимся с тем, что у нас есть: компьютер, модем, телефонная линия и друг в пределах телефонной досягаемости с аналогичным набором устройств и желанием передать нам или получить от нас какую-либо информацию, будь то файлы, сообщения или пакеты при сетевой игре в StarCraft.

Нам потребуется Windows-совместимая операционная система, по мере возможностей мы попытаемся обойтись встроенными в систему программами и утилитами. Как и все программное обеспечение, сделанное Microsoft для рядового пользователя, встроенное модемное ПО имеет минимальный набор функций и не слишком красивый интерфейс, однако пользоваться им все равно можно.

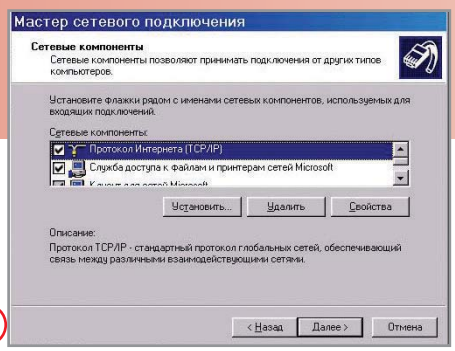
Еще нам потребуются свободное время и не занятый телефон, а также, возможно, крепкие нервы домочадцев с обеих сторон телефонной линии — ведь поначалу наши телефоны будут часто и бестолково трезвонить, а трубку при этом снимать будет категорически запрещено. В случае возникновения протестов со стороны ближайших родственников постарайтесь убедить их в неизбежности торжества высоких технологий, особенно упирая на то, что своими экспериментами вы пытаетесь сэкономить деньги. Должно помочь, проверенно электроникой…

Обмен файлами

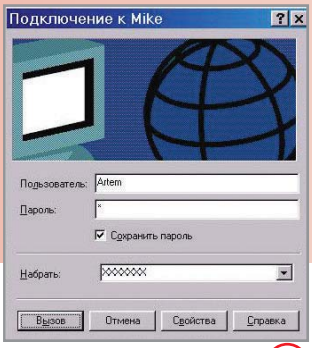
Самое основное применение модемного соединения двух компьютеров — это соединение ради простой пересылки файлов. Может быть, файлы-то небольшие — до- »



7



8



9

» ▸ Заходим в меню «Пуск», далее «Настройка», «Сеть и удаленный доступ к сети» («Панель управления -> Сетевые подключения» в Windows XP). Щелкаем на «Создание нового подключения» (в Windows 2000 это значок, а в XP — ссылка на web-панели слева). Устанавливаем переключатель в положение «Установить прямое подключение к другому компьютеру» и жмем кнопку «Далее». Переводим переключатель в положение «Принимать входящие подключения», нажимаем кнопку «Далее». Оставляем переключатель на варианте «Запретить виртуальные частные подключения». Кнопка «Добавить» нужна для того, чтобы создать нового пользователя, который к нам будет подключаться. Имя или что-нибудь подходящее по смыслу в качестве имени пользователя необходимо вписать в поле «Пользователь». Простенький пароль на соединение в полях «Пароль» и «Подтверждение» — вполне достаточно одной цифры или буквы, но если хотите, можете задать что-нибудь подлиннее. «Полное имя пользователя» — совершенно излишний пункт. Можете ввести туда все что угодно или оставить пустым. Нажмите «ОК». Если вы все сделали правильно, в списке пользователей компьютера появится новый пользователь. Отметьте его галочкой, если он не был выбран автоматически, и нажмите «Далее» (рис. 7).

▸ Перед вами откроется список протоколов. Для игры по сети понадобятся только Internet Protocol (TCP/IP); «Клиент для сетей Microsoft» и «Общий доступ к файлам и принтерам» — лишние пункты. Впрочем, можете их оставить — на производительности это скажется незначительно (рис. 8). Нажмите «Далее», и компьютер порадует вас информацией о том, что создание подключения «Входящие подключения» успешно завершено. После того как вы нажмете «Готово», компьютер станет самостоятельно снимать трубку и пытаться подключиться после примерно третьего звонка телефона.

Так выглядит создание удаленного подключения для доступа к сети со стороны сервера, то есть со стороны того, кому звонят. Тот, кто звонит, получает желаемое еще проще. Первые шаги инструкции абсолютно идентичны, так что начнем сразу с третьего:

▸ Переключатель оставляем в положении «Телефонное подключение к частной сети»: частная сеть — это то самое, что у нас получится в результате. Нажимаем «Далее», вводим номер телефона. Если вам нужно переключаться в импульсный набор или набирать префикс для выхода на городскую линию, настройте правила набора номера и установите соответствующую галочку «Использовать правила набора номера». Как угодно устанавливаем переключатель в следующем окне: хотите — оставьте это подключение видимым для всех пользователей, хотите — спрячьте. На тот результат, которого мы добиваемся, этот выбор никак не повлияет.

▸ Появляется до боли знакомое окно подключения (рис. 9). В поле «Пользователь» вводим имя пользователя, которое ваш друг, выступающий в роли владельца сервера, определял во время настройки. Установленный пароль — в поле «Пароль», галочку — на «Сохранить пароль», чтобы мучительно не вспоминать его в следующий раз, и нажимаем кнопку «Вызов».

После того как произойдет соединение и в системном трее панели задач появится иконка перемигивающихся компьютеров — в точности, как при соединении с Интернетом, — можно открывать шампанское и запускать игрушку: у вас все получилось, удаленный доступ установлен!

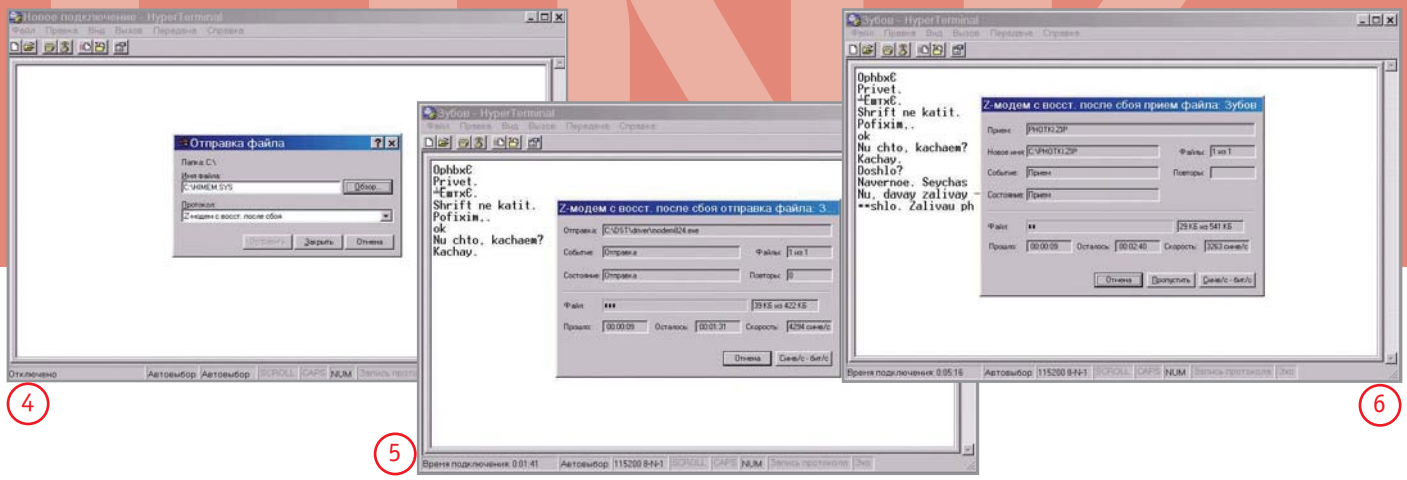
Каждую конкретную игру нужно подключать к получившейся «сети» по-разному, но проблем с этим, как правило, не возникает. Конечно, в Counter-Strike по модему играть получится едва ли, но в стратегию (особенно пошаговую) или старый добрый Quake 2 — что называется, без вопросов.

Последние рекомендации

Модемы необходимо подстроить для наилучшего быстродействия на вашей линии — увы, эта тема слишком обширна для того, чтобы рассмотреть ее в одной статье. Укажем лишь направление, в котором надо начинать «копать»: отмените ненужные протоколы (едва ли вам удастся, например, соединиться на v.90), поиграйте с уровнем выходного сигнала — для координатной (аналоговой) АТС его лучше установить в диапазоне от 6 до 9, на электронной — около 16. Конечно, рекомендация не универсальна, и в каждом конкретном случае есть простор для экспериментов.

Не забывайте удалять «Входящие подключения» после того, как наиграетесь. Во-первых, служба приема входящих подключений мешает всем программам, которые работают с модемом напрямую, а во-вторых, надо ли вам, чтобы модем постоянно хватал трубку после третьего звонка? Если у вас установлена версия Windows, отличная от Windows 2000 или Windows XP, и вы не находите в меню таких пунктов, какие указаны в статье, воспользуйтесь встроенной справкой.

■ ■ ■ Михаил Шахов



трудности, чтобы их героически преодолевать. Но предположим, что необходимость или просто желание пообщаться с другом у нас все-таки возникло, хотя бы из соображений конспирации. Сидите себе, шуршите по клавишам, и ни жены, ни родители в жизни не догадаются, что вы планируете поход на рыбалку и решаете животрепещущий вопрос: брать ли вообще с собой удочки или лучше не рисковать?

Вопрос в том, как это организовать. Как можно понять по приведенным скриншотам, нормально общаться в ненастроенном HyperTerminal можно только транслитом. Но это легко исправить. В меню «Вид» выбираем пункт «Шрифт», устанавливаем какой-нибудь шрифт, поддерживающий кириллицу, выбираем удобный размер — и русский язык появляется во всем своем величии и могуществе.

Нужно только соблюсти несколько рекомендаций. Первое: лучше всего выбирать Courier или любой другой моноширинный шрифт. Вы теоретически сможете пользоваться в терминале псевдографикой — ни таблицы, ни картинки не поплывут. Второе: не стоит задавать слишком большой размер шрифта, тогда окошко, в котором вы общаетесь, может вылезти за пределы экрана, что довольно неудобно. И третье: во время общения вам придется печатать строго по очереди, иначе ваши сообщения перепутаются между собой — и из «Привет!» и «Как дела?» получится «ПКраиквдеетл!а?» Удобно отделять фразы одного собеседника от другого абзацем: допечатали предложение, нажали «Enter», ждем реакции оппонента.

По сети — без сети

Приступаем к самому главному, ради чего и затевается по большей части соединение компьютеров: пробуем играть в игрушки по сети при помощи модема. На самом деле очень небольшая часть современных игр поддерживает игру по модему напрямую, для большинства игр требуется TCP/IP-соединение, или, проще говоря, сеть. Поскольку настоящей локальной сети у нас нет, мы установим такое соединение при помощи удаленного доступа. Вот как это делается (все названия даны для Windows 2000, но в остальных системах настройка практически ничем не отличается:

Дополнительная информация

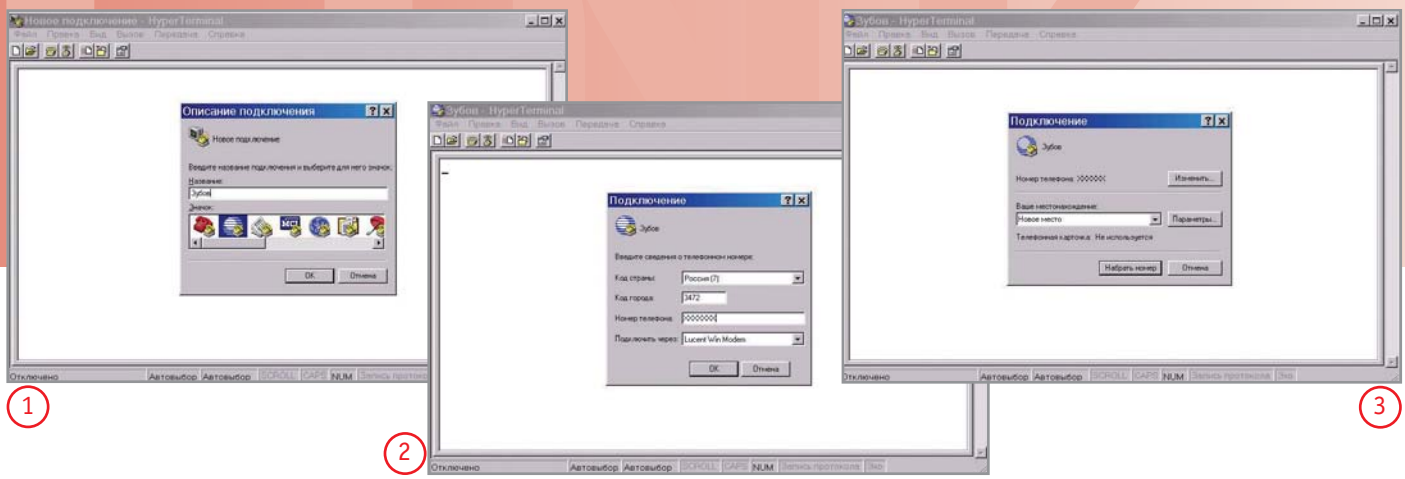
Протоколы модемной связи

У вас вполне может возникнуть вопрос: о каком таком v.90 идет речь и что за протоколы вообще используются в модемной связи? Вот список протоколов, получивших наибольшее распространение (правда, мы оставили в нем только те, с которыми на сегодняшний день можно столкнуться на практике):

v.34. Протокол последнего поколения со скоростью передачи до 28 800 бит/с, промежуточные скорости — 2400–26400 бит/с, дискретность — 2400. В связи с увеличением размера передаваемого за одну модуляцию элемента данных относительно более старых протоколов вместо понятия «бод» используется «символ в секунду» (Caps Per Second, CPS).

v.34bis. Расширение v.34 до скорости 33 600 бит/с с промежуточной скоростью 31 200 бит/с.

v.90. Несимметричный, «полуцифровой» скоростной протокол, позволяющий поднять скорость передачи в одну сторону до 56 Кбит/с. Стандарту предшествовали протоколы x2 (USR/3Com) и k56flex (Rockwell/Lucent). Данная группа протоколов известна также под названиями V.PCM и 56k. Протоколы 56k реализуются только на несимметричных линиях, когда с одной стороны устанавливается блок прямого сопряжения («цифровой модем») с подключением к цифровому каналу, например ISDN, а с другой — аналоговый модем с поддержкой v.90. При таком соединении сигнал со стороны цифрового канала большую часть расстояния передается в неизменной цифровой форме, и только от абонентского комплекта до обычного модема — в аналоговой. Поскольку преобразование из цифровой формы в аналоговую сопряжено с меньшими потерями информации, чем обратно, предельная пропускная способность цифрового канала (64 Кбит/с) понижается только до 56 Кбит/с (на практике обычно до 45–53 Кбит/с). В обратную сторону предельной является скорость 33,6 Кбит/с. Протоколы 56k ориентированы в первую очередь на централизованные системы связи, такие как провайдеры, банковские и информационные сети, где преобладает передача информации от центра к абоненту, а передача от абонента к центру встречается гораздо реже. Увы, но на многих российских линиях из-за высокой зашумленности и «уплотнений» сигнала протоколы этого семейства не работают или работают нестабильно.



кумент на сотню килобайт или драйвер, — но не тащить же их на другой конец города на дискетах? Тут нам приходит на выручку простая внешне, но вполне работоспособная в душе программа HyperTerminal. Она входит в поставку Windows с незапамятных времен, так что ее точно можно найти почти на каждом компьютере.

Программа HyperTerminal служит для подключения к узлам telnet Интернета, электронным доскам объявлений (BBS) и другим компьютерам с помощью модема или нуль-модемного кабеля. HyperTerminal записывает сообщения, передаваемые компьютером или службой с другой стороны подключения в обоих направлениях. Естественно, что вследствие этого программа вполне подходит для организации простейшего двустороннего чата. И, конечно же, она пригодится для связи с устаревшими компьютерами с текстовым интерфейсом, ведь настроить на компьютере, оснащенном DOS в качестве операционной системы, современный протокол передачи данных TCP/IP — задача как минимум нетривиальная.

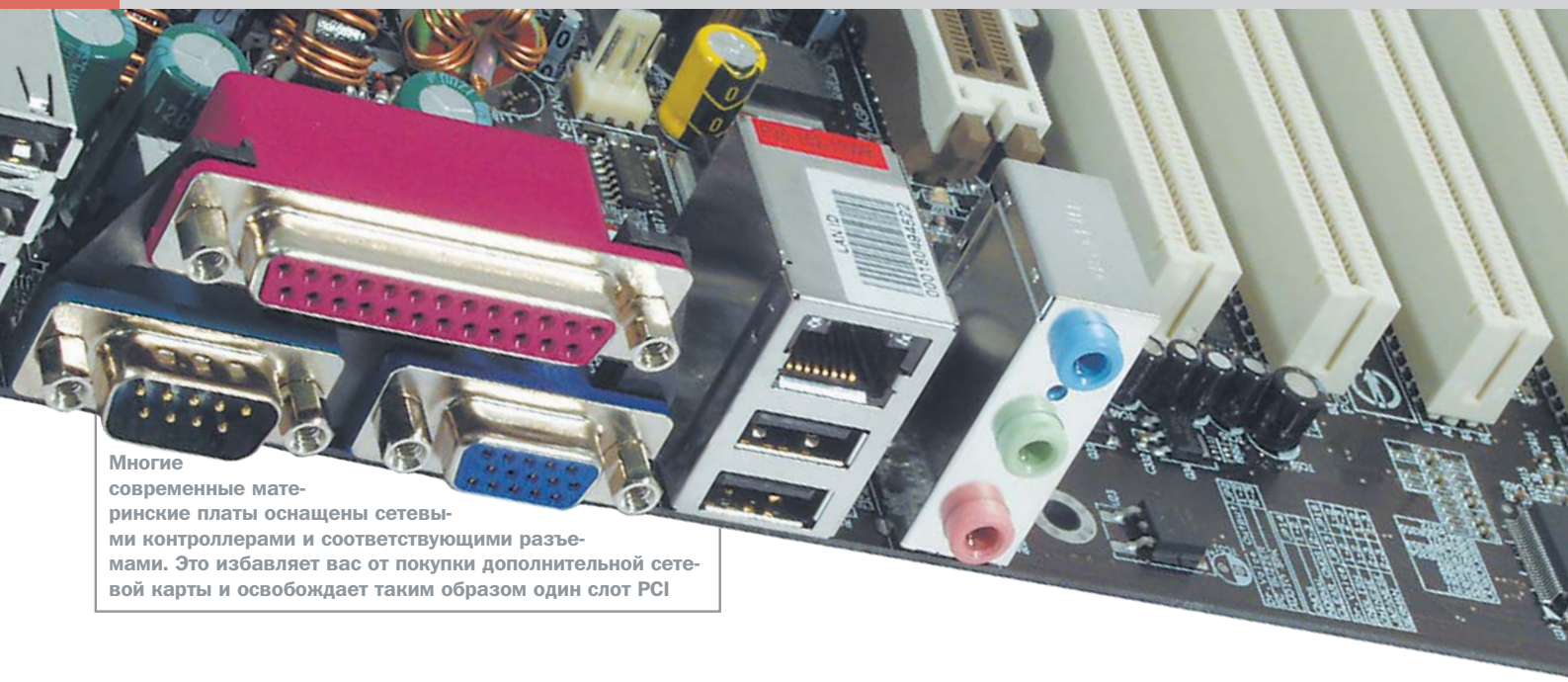
Для того чтобы передать на компьютер второго участника эксперимента файл, нужно сделать буквально следующее:

- Запустить программу HyperTerminal: меню «Пуск -> Программы -> Стандартные -> Связь -> HyperTerminal». Помимо пиктограммы для запуска самой программы, в меню иногда можно увидеть подменю с таким же названием, в котором лежат уже созданные подключения. Если это ваш случай, можете подключаться непосредственно из этого меню — просто выберите то подключение, которое вас интересует. Если же подходящего подключения еще нет или вы вообще запускаете терминал впервые, то сперва надо:
- Создать подключение. Выберите какой-нибудь рисунок для пиктограммы подключения из списка «Значок» и введите название подключения в соответствующем поле. Нажмите «OK» (рис. 1). Выберите страну, введите код города, номер телефона, по которому будете звонить, модем, с помощью которого производится подключение (рис. 2).
- В появившемся окне нажмите «Набрать номер» (рис. 3). К этому моменту у вашего друга, с которым вы пытаетесь соединиться, должна быть тоже запущена программа-терминал. В отличие от вас владелец «ведомого» компьютера должен был отказаться от создания соединения в первом пункте (для этого ему нужно было в приведенном на рис. 1 диалоге нажать кнопку «Отмена» или просто «Esc»). После этого в меню «Вызов» программы HyperTerminal он должен включить пункт «Ждать звонка».
- Если вы все сделали правильно, после набора номера и шума коннекта компьютеры установят соединение. Теперь можете приступать к передаче данных.
- В меню «Передача» программы HyperTerminal выберите пункт «Отправить файл». В открывшемся диалоге (рис. 4) выберите при помощи кнопки «Открыть» тот файл, который вы собираетесь отправлять. В выпадающем списке протоколов, если у вас нет каких-либо особых соображений по этому поводу, оставьте без изменений «Z-модем с восстановлением после сбоя»: этот протокол лучше всего подходит для передачи файлов по модему. Нажмите кнопку «Отправить», сразу после этого начнется передача файла (рис. 5). Чтобы принять файл, никаких особых манипуляций совершать не требуется. После того как вы нажмете «Отправить», на другом конце выскочит окошечко приема файла (рис. 6); сохраняться файл будет в папке C:\ProgramFiles\Accessories\HyperTerminal. Впрочем, есть возможность задать другую папку переданному файлу: для этого надо до начала передачи в меню «Передача» терминала выбрать пункт «Принять файл» и задать папку, в которой его необходимо сохранить. Как только начнется передача файла, кнопка «Принять» станет активной и вы сможете ее нажать. Папка для сохранения принятых файлов останется неизменной, пока вы вручную не поменяете эту установку.

После завершения передачи всех файлов прекратите соединение: «Передача -> Отключить». Осталось добавить всего два момента, чтобы внести полную ясность в вопрос передачи файлов по модему с помощью программы HyperTerminal. Во-первых, чтобы передавать файлы, необязательно дозваниваться самому: после установки связи понятия «ведущий» и «ведомый» перестают быть актуальными и любой участник процесса может файлы как отправлять, так и принимать. Во-вторых, в зависимости от версии Windows названия меню и их пунктов могут звучать по-разному, например меню «Передача» в терминале для Windows 98 называется «Соединение». Все названия в вышеприведенном тексте даны для Windows 2000.

Чатлане нашего времени

Чтобы захотеть организовать чат, имея возможность поговорить вместо этого по телефону, надо быть товарищем из разряда киргизских комсомольцев. Как известно, киргизский комсомолец сам создает себе

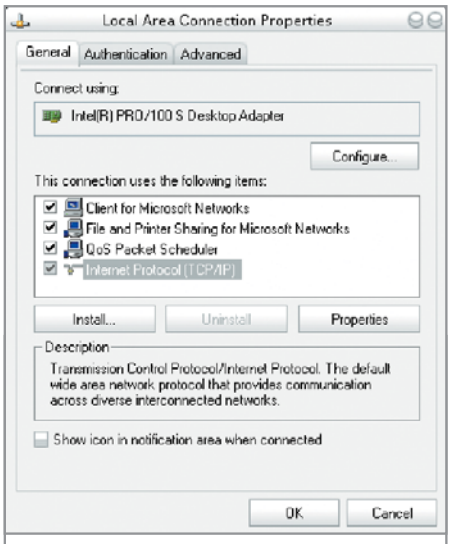


Многие современные материнские платы оснащены сетевыми контроллерами и соответствующими разъемами. Это избавляет вас от покупки дополнительной сетевой карты и освобождает таким образом один слот PCI

Соединение с помощью сетевых карт

Звенья цепи

Вот он стоит дома — новый, пахнущий пластиком, с кучей проводов и большим монитором. Старый на его фоне выглядит пыльным и убогим. И наконец решена проблема бесконечных споров о том, кто сегодня первым сядет за компьютер: теперь их два, на всех хватит. Но через некоторое время приходит мысль о том, что пора бы их объединить.



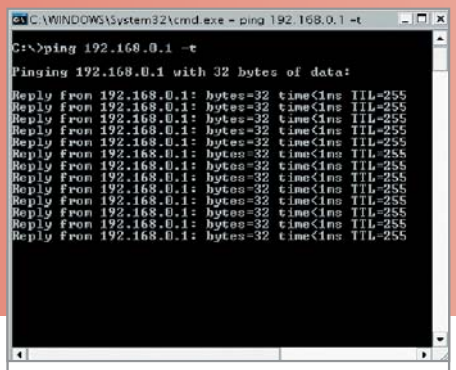
Типичный набор компонентов для только что созданного соединения (Local Area Connection Properties)

Ведь удобно иметь возможность выходить в Интернет одновременно с обоих компьютеров, обмениваться файлами, использовать единственный пишущий CD, да и играть с живым противником куда интереснее, чем с машиной. Можно, конечно, использовать соединение через COM- или LTP-порт (несколько устаревший вариант, да и расстояние между машинами должно быть небольшим) или по USB (необходимы специальные драйверы, скорость работы при этом не очень высока). Но лучше создать свою домашнюю сеть, пользуясь сетевыми картами. Купить их можно в любом компьютерном магазине, стоимость за пару составит примерно $20–30. Установка при наличии драйверов производителя не составляет труда, но может понадобиться диск с дистрибутивом Windows. Единственная рекомендация — не покупать карты безымянных производителей и не пытаться выбрать самое дешевое: это далеко не всегда оптимально.

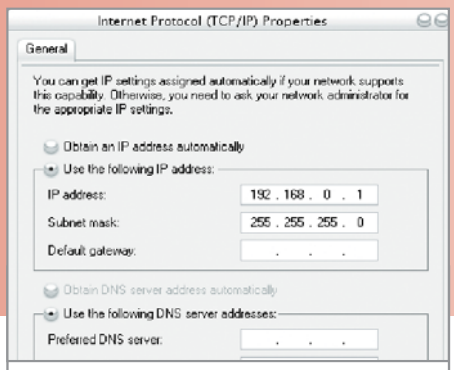
Типы сетей

Есть несколько подтипов сетей. В иерархической сети все задачи выполняет центральный компьютер, или MainFrame; все задачи в ней связаны с обработкой, хранением и предоставлением данных. Пользователи взаимодействуют с центральным компьютером с помощью терминалов. Примером такой сети может служить компьютер под управлением Windows 2000 Server со службой Terminal Services и установленными на компьютеры пользователей клиентами Terminal Service Client. Нагрузка на рабочую станцию при этом минимальна (достаточно конфигурации Pentium 100 и 32 Мбайт памяти), желательно лишь иметь хорошие видеокарту и монитор. Загрузка самой сети также невысока.

В сети типа «клиент-сервер» обработка данных разделена между объектами. Клиент формирует запрос на выполнение каких-либо задач, а сервер его выполняет. В равноправной (или одноранговой) сети каждый компьютер может выполнять и функции кли- »



Окно командной строки с командой ping. В данном случае цель отвечает на запросы — компьютер доступен в сети



Необходимые настройки протокола TCP/IP. Для соединения двух компьютеров этого достаточно

» ента, и функции сервера. Это наиболее распространенный вариант для создания маленькой домашней сети.

Для современной домашней сети следует выбрать Ethernet 100Base-TX, поскольку и платы этого типа, и различные сетевые устройства на данный момент наиболее доступны. Также нет проблем с проводом, инструментами для его обжима и самими разъемами. В качестве протокола рекомендуется использовать TCP/IP, в качестве клиента — стандартный «Клиент для сетей Microsoft», а в качестве сервиса — «Службу доступа к файлам и принтерам сети Microsoft» (все эти компоненты входят в поставку современных версий Windows).

Настройка соединения

Перейдем наконец от необходимой, но далеко не полной теории к практике (на примере ОС Windows XP). После установки сетевого адаптера нужно найти на Рабочем столе значок «My Network Places» и, кликнув по нему правой кнопкой мыши, вызвать контекстное меню. Затем выбрать пункт «Properties», найти в появившемся окне значок «Local Area Connection» и в меню, вызываемом опять по щелчку правой кнопкой мыши, выбрать пункт «Properties» (если значка «My Network Places» на Рабочем столе нет, то аналогичное диалоговое окно можно найти в Панели управления, пункт «Network Connections»). Для работы сети достаточно, чтобы в появившемся окне присутствовали Client for Microsoft Networks и Internet Protocol (TCP/IP). Если предполагается совместный доступ к файлам и принтерам, также должен быть установлен сервис File and Printer Sharing for Microsoft Network. Если каких-либо пунктов не хватает, то следует их добавить (нажать кнопку «Install», в появившемся окне выбрать «Client», «Protocol» или «Service» соответственно и нажать «Add»).

Теперь проведем настройку протокола TCP/IP. Полагаем, что сеть самая простая, без выделенного сервера и автоматического получения настроек сетевых интерфейсов по сети. Выбираем пункт «Internet Protocol (TCP/IP)», нажимаем кнопку «Properties», в появившемся окне ставим точку напротив «Use the following IP address» и набираем 192.168.0.1, «Subnet Mask» — 255.255.255.0. На каждом следующем компьютере настройки должны быть аналогичны, лишь номер узла увеличивается на единичку (192.168.0.2 и т. д.).

Имена машин должны быть различны, а группа, в которой они находятся, желательно (но не обязательно) одинаковой. Проверить это можно, щелкнув правой кнопкой мыши на иконке My Computer, выбрав пункт «Properties», а затем закладку «Computer Name». Для изменения имени компьютера нужно обладать правами администратора.

Соединение компьютеров

А сейчас перейдем непосредственно к объединению компьютеров в сеть. Если есть желание самостоятельно сделать провода — понадобится некоторый набор инструментов и компонентов, а именно:

- клещи для обжима витой пары;
- инструмент для удаления внешней изоляции (иногда совмещен с клещами);
- инструмент для обрезки проводов;
- ножницы;
- разъемы (RJ-45), по два на каждое подключение;
- провод (витая пара (UTP) категории 5);
- тестер (достаточно самого простого).

Нужно, аккуратно сняв изоляцию, расплести пары и выпрямить провода. Длина расплетения — не более 10–15 мм. Как правило, в паре скручены два провода: с изоляцией основного цвета (оранжевый, зеленый, синий, коричневый (в дальнейшем О, З, С, К)) и дополнительного (белый с оранжевым, белый с зеленым, белый с синим и белый с коричневым (в дальнейшем БО, БЗ, БС, БК)). Порядок следования пар внутри разъема очень важен. Если держать разъем проводом к себе (контактами от себя), направив его защелкой (специальная пластиковая пластинка на одной из широких сторон разъема) вниз, то провода должны идти (при перечислении слева направо) так: БО-О-БЗ-С-БС-З-БК-К. Если данным проводом предполагается соединять два компьютера без использования дополнительных устройств, то второй конец должен иметь следующую разводку: БЗ-З-БО-С-БС-О-БК-К. Если же в сети существует хаб или свич, то концы проводов обжимаются симметрично. Операция несложная, но все же требует некоторого навыка. Проверив качество контактов тестером, соединяем компьютеры и включаем их.

После полной загрузки вызываем командную строку («Start -> Run -> cmd.exe»). Предположим, что данные действия производятся на компьютере с адресом 192.168.0.1. В появившемся окне набираем команду ping 192.168.0.1. Если все настроено правильно, приходит ответ от локальной сетевой платы вида: Reply from 192.168.0.1: bytes=32 time<10ms TTL=128.

Затем проверяем, виден ли второй компьютер. Ответ должен быть аналогичным, изменится лишь адрес отвечающего устройства. Все, в принципе, сеть настроена, и в «My Network Places -> Entire Network -> Microsoft Windows Network» должна быть видна рабочая группа, а в ней — компьютеры сети.

Если машин более чем две, требуется дополнительное сетевое устройство — хаб или свич. Число подключаемых машин определяется числом портов на устройстве. Предоставить общий доступ к папке или принтеру можно, щелкнув на ней правой кнопкой мыши и выбрав в появившемся меню пункт «Sharing». Там же можно раздать права доступа к этой папке для различных групп пользователей. ■ ■ ■ Денис Прозоровский

GPRS, Bluetooth и другие

Без привязи

Бум беспроводных сетевых решений имеет сложную природу. Несмотря на то что эти устройства все еще дороже проводных, пользователи «пересаживаются» на беспроводные сети с большой охотой, невзирая на заметную потерю в скорости. Все же соображения удобства пересиливают потребности в высоких скоростях.

Введение

Понятие мобильности в нашем сознании ассоциируется прежде всего с мобильной телефонией, удобства которой оценили все. Мобильные телефоны уже давно стали реальностью нашей жизни. Число пользователей мобильных телефонов в нашей стране постоянно растет и вскоре уже достигнет мирового уровня. Сегодня самый дешевый сотовый телефон в Москве стоит меньше $60, а подержанные аппараты и того дешевле, так что мобильные технологии перестали быть уделом избранных. Какой же следующий шаг в этом направлении? Ответ очевиден — беспроводная компьютерная связь.

Беспроводная компьютерная связь также постепенно входит в нашу жизнь. В развитых странах проблема доступа из любого места решается по-разному, подчас своеобразно. Например, с одним человеком случилась следующая история. Оказавшись в аэропорту одной из мировых столиц, он узнал, что его самолет задерживается с вылетом на пять часов. В связи с чем человек решил выйти в Интернет и послать сообщение по ICQ. Он пошел по стрелке, указывающей в сторону интернет-кафе, где обнаружил комнату и скучающего охранника. Комната была пуста, а охранник на вопрос, где компьютеры, ответил вопросом: а где ваш? Оказывается, интернет-кафе в данном аэропорту понимается как торчащие из стены кабели, к каждому из которых можно подключить ноутбук. Этой истории уже больше года, и, возможно, теперь там оборудована точка беспроводного доступа, известная как хотспот. Так что ноутбук с беспроводным доступом, да и без него тоже, — незаменимая вещь для тех, кому приходится много ездить. Отсутствие постоянной компьютерной связи может серьезно замедлить работу людей многих профессий, которым приходится работать вне офиса.

Wi-Fi — главный стандарт

Сейчас беспроводные сети переживают настоящий бум. Пользователи их приняли, несмотря некоторые связанные с развертыванием проблемы. Известны случаи, когда люди и компании не задумываясь выбирали wireless-решения. Эти решения хороши тем, что беспроводную сеть можно развернуть в любом месте и практически сразу начать работу. Причем пользователи такой сети не привязаны ни к месту, ни к длине кабеля. »

Компактность беспроводных устройств дает весомые преимущества

Точки доступа стандарта Bluetooth хватит для небольшого помещения

» Эта технология изначально была рассчитана на мобильных специалистов, однако сейчас беспроводные технологии используются и в других ситуациях. В некоторых компаниях уже активно применяются беспроводные сети, представляющие собой более удобную и надежную альтернативу кабельным сетям. Беспроводные сети более эстетичны, а в некоторых случаях, например при их прокладке в зданиях, являющихся памятниками архитектуры, и более экономичны, чем кабельные.

Обычно беспроводные сети строятся на основе распределяемых по зданию точек доступа, монтируемых в стены. Точки доступа, как правило, подключаются к внешнему кабельному каналу связи, имеющему выход в Интернет. Таким образом, в данной ситуации кабель нужен только для подключения сети к внешнему миру.

Разумеется, беспроводные сети пока еще дело будущего. Стоимость преобразования обычной сети в беспроводную достаточно велика, к тому же беспроводные сети имеют некоторые ограничения, обычно зависящие от типа связи. Чем меньше ограничений, тем выше стоимость прокладки такой сети.

Однако несмотря на это, беспроводные технологии уже сейчас очень активно используются в компьютерных сетях. Обычно они реализуются в виде радиомодемов или беспроводных мостов, служащих для соединения корпоративных сетей с провайдером для получения доступа в Интернет. Сегодня беспроводные мосты в основном строятся на основе радиомодемов, однако многие уже сейчас рассматривают перспективы использования лазерных технологий. Ограничения таких мостов связаны только с ограничениями видимости, вызываемыми сильным туманом (атмосферные осадки обычно не влияют на качество связи), в результате чего возможны сбои в их работе. Но несмотря на это и на относительно высокую стоимость оборудования, большой радиус действия, очень высокая скорость связи и абсолютная надежность гарантируют жизнеспособность лазерных технологий.

Лазерная технология беспроводной связи

Наиболее дорогостоящей (хотя в последнее время наблюдается тенденция к относительному снижению цены) и высокоскоростной является лазерная технология беспроводной связи. Из-за своей высокой стоимости она не может использоваться на каждом компьютере, поэтому обычно применяются специальные модули передачи, к которым подключаются группы компьютеров. Это позволяет повысить экономическую эффективность данного решения. Лазеры также можно использовать для создания моста между кабельными локальными сетями, расположенными на близком расстоянии. Такой подход обеспечивает более высокую скорость связи и меньшую стоимость по сравнению с выделенными линиями и маршрутизаторами. В качестве основных преимуществ лазерных систем связи, на основе которых обеспечивается весьма существенное повышение безопасности и надежности инфор- »

Немного о стандартах

Быстрые телефонные пакеты

GPRS — это стандарт Европейского института телекоммуникационных стандартов для пакетной коммутации в сетях GSM, функционирующих на частоте либо 900 МГц, либо 1800 МГц. Число пользователей сетей GSM к концу 2002 года превысило 787 млн человек в 190 странах мира. По всем прогнозам, к концу 2003 года эта цифра превысит миллиард.

Теоретическая максимальная скорость передачи данных GPRS при использовании всех восьми тайм-слотов составляет 171 Кбит/с. Реальная скорость, естественно, намного ниже, поскольку очевидно, что оператор не будет выделять одному пользователю все тайм-слоты GPRS. Относительно высокие скорости передачи данных через мобильные устройства останутся не доступными обычным пользователям до тех пор, пока не будут реализованы мобильные сети нового поколения GSM Evolution (EDGE) или Universal Mobile Telephone System (3GSM).

В технологии GPRS применяется новый метод эффективной передачи пакетных данных по радиосетям. Технология пакетной коммутации основана на методах IP и X.25, оба из которых очень популярны и широко используются во многих сетях. Пакетная коммутация GPRS работает в целом так же, как и пакетная коммутация IP, то есть данные расщепляются на пакеты и пересылаются по назначению разными путями по сети, затем снова собираются на принимающей стороне. Пакетная коммутация GPRS допускает любой существующий трафик IP или X.25 для пересылки данных через радиосеть GPRS. Реальная скорость GPRS значительно ниже максимальной, но сравнима с обычной модемной связью. С помощью GPRS нельзя быстро передавать действительно большие объемы данных, но все обычные задачи решаются легко и удобно. GPRS поддерживает передачу данных в различных форматах, в том числе передачу файлов по протоколам FTP, HTTP, Telnet.

Теперь для связи удаленных объектов не приходится тянуть провода

Беспроводная сетевая видеокамера от компании TRENDnet

» мационного обмена, можно выделить практически абсолютную защищенность канала от несанкционированного доступа и, как следствие, высокий уровень помехоустойчивости и помехозащищенности. Это обеспечивает возможность устойчивого криптографирования с высоким уровнем избыточности, а также отсутствие ярко выраженных демаскирующих признаков (в основном побочных электромагнитных излучений) и возможность дополнительной маскировки, позволяющей скрыть не только передаваемую информацию, но и сам факт информационного обмена, а также простоту принципов их построения и функционирования. Кроме того, эти системы безопасны для человека, так как средняя плотность мощности излучения в лазерных системах различного назначения примерно в 10^3-10^6 раз меньше мощности солнечной радиации.

В число недостатков использования лазеров можно включить их высокую стоимость, более высокие требования к мощности, выделение тепла, а также использование видимой части спектра, что приводит к потенциальной угрозе затухания сигнала из-за влияния атмосферных помех.

Скорость лазерных систем беспроводной связи составляет до 622 Мбит/с, а радиус действия — около 9 км. Защищенность системы лазерной связи от ошибок составляет 99,99%, а при использовании резервных систем радиосвязи — и того выше. Лазерные системы беспроводной связи представляют собой наиболее эффективное решение проблемы «последней мили». Они развиваются в направлении повышения скорости обмена и дальности связи. В ближайшем будущем появятся приемопередатчики, поддерживающие скорость до 1 Гбит/с. Их использование будет особенно привлекательным для объединения сегментов ЛВС, в том числе построенных по высокоскоростным технологиям (Gigabit Ethernet и ATM).

Доступ по телефону

Цифровые стандарты мобильной связи всегда позволяли осуществлять по их каналам передачу данных, однако соотношение цена/скорость не вдохновляло пользователей на массовое использование этих технологий. Поэтому появление GPRS, стандарта, который используется в самых популярных сейчас GSM-сетях, заставило многих пересмотреть свою точку зрения на доступ в Интернет по мобильному телефону.

GPRS является промежуточным звеном в переходе от сетей второго поколения к сетям третьего поколения (3G), которые уже начинают появляться в мире. 3G — это беспроводная технология глобальной коммуникации, делающая возможной пакетную передачу оцифрованного голоса, данных или видео. 3G включает в себя широкий спектр конкурирующих беспроводных технологий, таких как CDMA (Code Division Multiple Access) 2000, UMTS (Universal Mobile Telecommunications System) и широкополосный CDMA (WCDMA). Сети 3G отличаются от сетей 2G (GSM) и сетей переходного поколения (2.5G, GPRS) гораздо большей скоростью передачи данных, а также более широким набором и высоким качеством предоставляемых услуг.

Согласно требованиям спецификаций Международного института электросвязи, сети IMT-2000 (3G) должны обеспечивать улучшенную емкость системы и эффективность использования спектра для систем 2G и поддерживать возможности передачи данных со скоростями от 144 Кбит/с при высокой скорости перемещения (до 120 км/ч), до 2 Мбит/с при низкой скорости перемещения (до 3 км/ч) и до 64 Кбит/с при глобальном покрытии (спутниковая связь). Сети третьего поколения в корне изменят концепции мобильной работы, и, возможно, представители еще большего диапазона профессий смогут воспользоваться преимуществами мобильности.

Важным элементом услуг 3G станет мобильная электронная коммерция, когда оплатить товары и услуги можно будет через мобильный телефон, который тем самым превратится в виртуальный кошелек. Разработчики сетей третьего поколения даже всерьез рассматривают возможность запуска такой услуги, как удаленная медицинская диагностика.

Сегодня в мире существуют две основные конкурирующие концепции 3G: UMTS (Uni- versal Mobile Telecommunications System — универсальная мобильная телекоммуникационная система), поддерживаемая европейскими странами, и CDMA 2000 (Code Division Multiple Access — мультидоступ с кодовым разделением каналов), сторонниками которой традиционно являются азиатские страны и США. В принципе, эти технологии предполагают два различных подхода к организации сетей 3G — революционный (UMTS) и эволюционный (разновидности CDMA — CDMA2000, CDMA2000 IX, CDMA2000 IX EvDo). Эволюционный путь подразумевает сохранение частот и постепенный переход к новым технологиям путем наращивания технических мощностей оператора. UMTS — совершенно новый стандарт, в то время как разновидности CDMA, предложенные для 3G, являются развитием уже эксплуатирующейся в мире технологии второго поколения cdmaOne (IS-95).

По данным на 16 декабря 2002 года, в мире было уже запущено 32 сети третьего поколения в 16 странах. Так что день, когда сети 3G вытеснят сети GSM и мир перейдет на качественно новую степень мобильности, уже не за горами, и следует уже сейчас морально готовиться к этому переходу. У нас в России также уже появились первые сети третьего поколения, причем не в Москве.

Как уже говорилось выше, мобильные компьютеры с беспроводной связью полез- »

Владельцы портативных компьютеров получили свободу передвижений

Семейство беспроводных периферийных устройств от Compaq

ны не только для выездных специалистов. Они способны оказаться неоценимым подспорьем в работе для журналистов, переводчиков, редакторов, корректоров и представителей других профессий, которые теоретически могут работать вне офиса. С помощью мобильных компьютеров они смогут работать не только дома, где имеется выход в Интернет, но и находясь, например, на курорте, на даче или просто за городом. Зачем сидеть душным летом в городе, когда можно поехать на природу и при этом выполнить работу в срок, не беспокоясь о том, как ее отправить? Да и вообще, зачем ходить в офис, если можно работать не выходя из любимого ресторана?

Сфер применения технологий беспроводной связи существует огромное множество. Но в основе работы мобильных сотрудников с беспроводной связью лежит в основном использование ноутбуков с модулями Bluetooth, служащими для их подключения к мобильным телефонам. Существуют и другие средства для подключения портативных и карманных компьютеров к мобильным телефонам, однако модули Bluetooth представляют наибольшую гибкость в связи с тем, что они обеспечивают действительно беспроводной доступ. Провода не нужны вообще. Альтернативой Bluetooth является использование инфракрасного порта, однако при этом возникают значительные ограничения расстояния, так как для соединения через инфракрасный порт требуются прямая видимость и небольшое расстояние между устройствами, в то время как Bluetooth обеспечивает высокоскоростное (до 1 Мбит/с) соединение между двумя устройствами в радиусе 10 м и даже в радиусе 100 м (хотя для этого требуется большая мощность, что не всегда возможно в связи с ограничениями устройств). Кроме того, Bluetooth представляет собой универсальное устройство, позволяющее создать беспроводную сеть между компьютером (не обязательно портативным) и различными устройствами (сканер, принтер, плоттер, коммутатор, мобильный телефон).

Итак, беспроводная связь постепенно становится неотъемлемой частью нашей жизни. Скорее всего, мы даже не заметим, как человечество перейдет на качественно новый этап своего развития — эпоху всеобщей мобильности. Мобильность — вот девиз нового поколения.

■ ■ ■ Иван Новоселов

Bluetooth

Стандарт карманного масштаба

В настоящее время технология Bluetooth является твердо устоявшимся коммуникационным стандартом для беспроводной связи на малых расстояниях и создания так называемых малых беспроводных сетей.

Технология Bluetooth специально разработана для обеспечения дешевой, устойчивой, эффективной, высокоемкой связи, для работы с голосом и передачи данных со следующими характеристиками:

1. Скорость передачи/приема 1 Мбит/с при использовании канала с максимально возможной шириной полосы.

2. Скорость перестройки частоты составляет до 1600 скачков в секунду. Сигнал перемещается по 79 частотам с интервалом в 1 МГц, что обеспечивает достаточно высокий уровень защиты от помех.

3. Адаптивная выходная мощность для минимизации помех.

4. Быстрое опознавание (подтверждение).

5. Короткие пакеты данных для минимизации мощности во время помех.

6. CVSD (Continuous Variable Slope Delta Modulation) — голосовое кодирование, которое дает возможность работы с высокими частотами ошибок по битам.

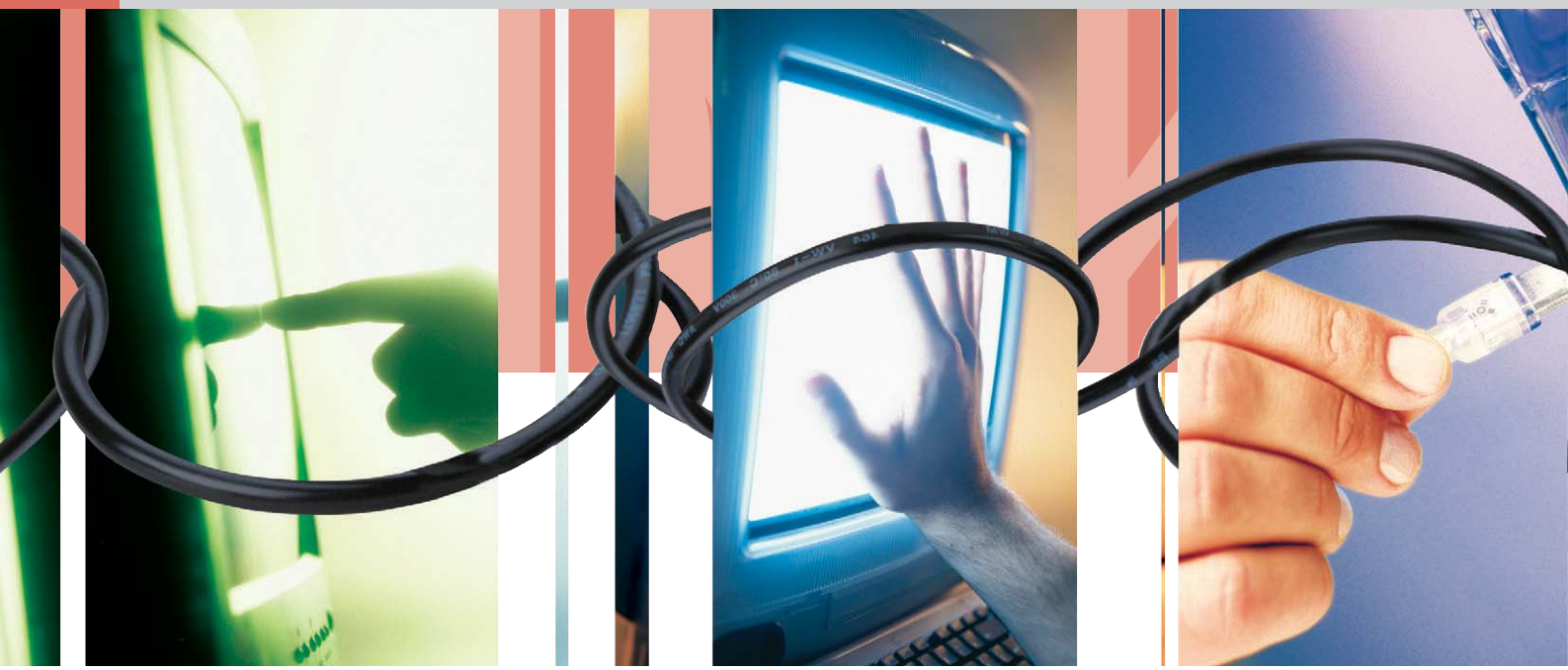
7. Гибкие типы пакетов, поддерживающие широкий спектр приложений.

8. Ненапряженный «бюджет связи», поддерживающий недорогую интеграцию отдельных элементарных сигналов.

9. Интерфейс передачи/приема, специально приспособленный для минимизации энергопотребления.

Спецификация Bluetooth 1.1 поддерживает до семи соединений одновременно.

Суммарная пропускная способность сетей Bluetooth — 780 Кбит/с, а при использовании асинхронного протокола максимальная скорость однонаправленной передачи данных составляет 722 Кбит/с. Перспективы использования технологии Bluetooth велики. Она совместима с большинством популярных протоколов и систем связи, в том числе GSM, GPRS, CDMA, TCP, IP и т. д. Кроме того, стоимость устройств Bluetooth относительно невысока, поскольку технология изначально задумывалась как общедоступная. Технология Bluetooth позволяет обеспечить высокую степень защиты и отличное качество работы. Согласно прогнозу компании International Data Corporation, к 2004 году в мире будет насчитываться 448,9 млн устройств, поддерживающих этот стандарт. Многие мобильные телефоны и некоторые модели принтеров уже поддерживают технологию Bluetooth. А к 2004 году 19% всех цифровых камер будут поддерживать Bluetooth. Использование же Bluetooth в беспроводных сетях достаточно распространено уже в настоящее время и, скорее всего, в будущем будет лишь возрастать.



Практика создания сети

Сложности объединения

До недавнего времени проблемы межсетевого взаимодействия были далеки от пользователей. Однако сейчас, когда повсеместно создаются домашние сети, многие с удивлением обнаруживают, что все не так просто, если речь заходит о соединении компьютеров на разных платформах или с различными операционными системами.

Введение

Локальную сеть можно создавать двумя способами: с нуля и опираясь на существующие ресурсы. Когда сеть создается с нуля, можно ее спроектировать или, если позволяют средства, заказать «под ключ» у системного интегратора. Системный интегратор сделает все и даже возьмет на себя бремя профилактики и обслуживания, однако этот путь не всегда подходит пользователям домашних сетей. Во-первых, услуги интегратора дороги и в гражданском строительстве востребованы лишь на рынке элитного жилья. Во-вторых, увидев подлежащий объединению парк машин, который более уместно назвать «зоопарком», интегратор порекомендует купить все новое, а это может оказаться не под силу добровольному объединению пользователей.

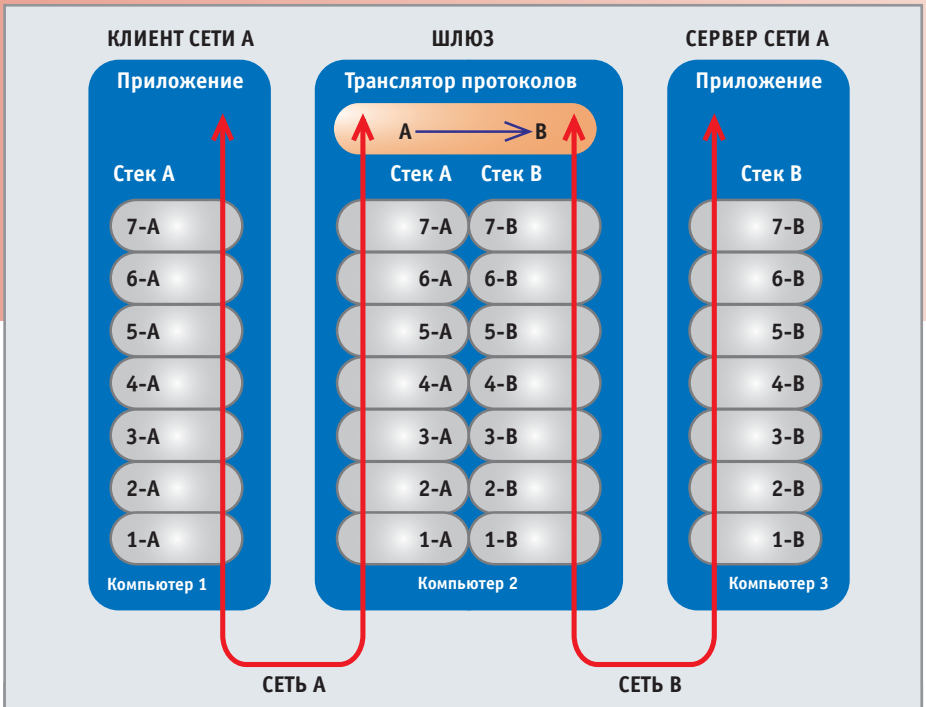
Представим ситуацию, что два десятка инициативных людей надумали объединиться в сеть. При этом у половины пользователей имеются ПК класса Pentium II под управлением Windows 98 или Linux, трое обзавелись продукцией от Apple, у пяти — новейшие машины под управлением Windows XP. Остальные серьезно задумались над апгрейдом и даже выделили на него немного денег, но не знают, с какой платформой связать свою сетевую судьбу. На регулярных посиделках этой разношерстной компании неопределившиеся слушают об удобствах работы с Macintosh, скоростях соединения с Linux и универсальности Windows. Как же договориться между собой этой дружной, но вынужденно разобщенной компании? А вдруг завтра кто-нибудь приобретет себе новый ПК и поставит на него, например, BeOS?

Во избежание путаницы

В принципе, ничто не мешает многочисленным пользователям Windows объединиться в одноранговую сеть. Когда две или более сетей организуют совместную транспортную службу, такой режим обычно называют межсетевым взаимодействием. Так как понятие «номер сети» определяется на сетевом уровне, то оно является относительным, то есть, если в одном компьютере установлено программное обеспечение, поддерживающее несколько протоколов сетевого уровня (например, TCP и SPX), то он может принадлежать нескольким сетям.

Реализация взаимодействия

Если бы в компьютерном мире существовал только один стек протоколов, то у независи- »



Графическое представление алгоритма работы шлюза при трансляции запросов

» мых разработчиков сетевого и программного обеспечения не было бы никаких проблем. Сетевые адаптеры вместе со своими драйверами подходили бы к любой сетевой ОС за счет единого интерфейса между канальным и сетевым уровнями. Разработчики транспортных средств новых ОС могли бы использовать существующие реализации протокола сетевого уровня, а разработчики сетевых приложений — единый API для обращения к сервисным услугам прикладного уровня ОС.

К сожалению, в реальном мире компьютерных сетей существует несколько стеков протоколов, уже завоевавших свое место под солнцем и не собирающихся его уступать. Давайте рассмотрим, как объединять сети на наиболее простом уровне.

Сетевые протоколы

Общность различных стеков протоколов проявляется только на нижних уровнях — физическом и канальном. Здесь почти нет проблем, так как большинство стеков могут использовать общие протоколы Ethernet, TokenRing, FDDI. Соединение компьютеров, использующих на нижнем уровне различные протоколы, а на верхних — одинаковые, не составляет проблемы: задача решается аппаратно с помощью транслирующего моста.

Сложнее обстоит дело с сопряжением сетей, использующих различные протоколы верхних уровней, начиная с сетевого. Задачи согласования протоколов верхних уровней решить труднее из-за их сложности и разнообразия — чем большим интеллектом обладает протокол, тем больше у него граней, по которым он отличается от своего коллеги по функциональному назначению. Сложно осуществить трансляцию транспортных протоколов (таких как IP и IPX), но гораздо труднее совместить протоколы верхнего, прикладного уровня, с помощью которых серверы обслуживают клиентов.

Если рассмотреть наиболее часто используемый в сетях сервис, а именно файловый, то различия в протоколах напрямую связаны со структурами файловых систем. Команды, используемые при работе с файловыми системами, также различаются по названию и содержанию. Кроме того, даже для одной файловой системы в некоторых операционных системах предусмотрены различные удаленные сервисы. Поэтому проблемы, возникающие на верхних уровнях, гораздо сложнее замены заголовка пакета на канальном уровне.

Два подхода

В данном случае это не совсем два подхода, это два пути разрешения подобной коллизии. Естественно, что всем нашим пользователям, создавшим совместными усилиями столь пестрый и причудливый «зоопарк», хо- »

Проблемы Mac OS

Дело в количестве

Если в сети существуют хосты под управлением Mac OS, то понятно желание интегрировать их в сеть. Решить данную проблему можно несколькими способами, и выбор того или иного варианта зависит от соотношения между количеством Macintosh и PC. Если Mac OS доминирует, то кажется разумным установка на PC приложений категории AppleShare for Windows, то есть использование на PC стека AppleTalk. Среди этих продуктов известны AppleShare Client for Windows компании Apple, COPSTalk for Windows компании CoOperative Printing Solutions и Personal MacLAN Connect компании Miramar Systems. Причем последний позволяет компьютеру под Windows выступать в качестве клиента и сервера AppleShare; остальные же — только в качестве клиентов. Подобное решение вполне годится также и для смешанных сетей Macintosh и Windows, когда нет выделенных серверов (в одноранговых сетях). Если же компьютеров с Windows больше, то предпочтительным решением выглядит установка Microsoft Windows NT Server или Novell NetWare 4.x. Эти ОС поддерживают AppleTalk. А для управления компьютерами Macintosh существует продукт от компании Apple — MacSNMP.

С Unix ситуация проще, так как компания Helios выпускает EtherShare не только для AIX, но и для других вариантов Unix. Помимо этого, клиент EtherShare есть и для Windows. Кстати, EtherShare можно применять в сетях, где используются только Unix и Windows.

» чется одного и того же — пользоваться файлами универсальных форматов, которые содержат в себе музыку (MP3), видео и тексты. Поэтому создание файлового обмена жизненно необходимо, хотя и сопряжено с некоторыми сложностями.

Первый подход связан с использованием так называемых шлюзов, которые призваны обеспечивать согласование двух стеков протоколов путем их преобразования (трансляции). Шлюз обычно размещается между взаимодействующими хостами или сетями и служит посредником, переводящим сообщения, поступающие от одной сети, в формат другой.

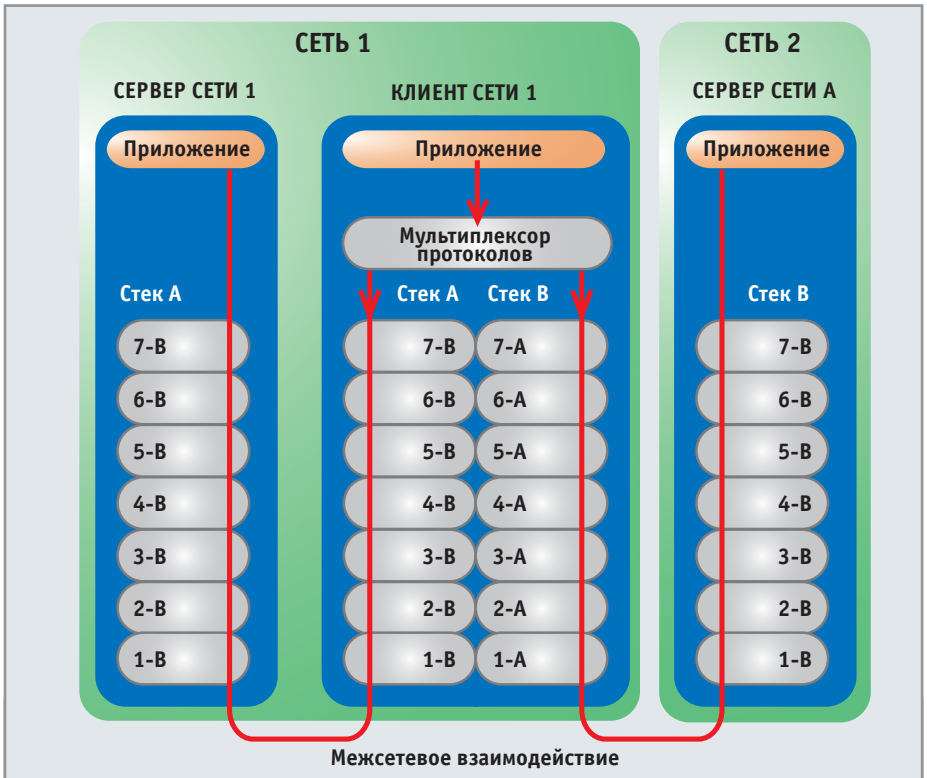
Второй подход заключается в том, что в операционные системы серверов и рабочих станций встраиваются несколько мирно сосуществующих наиболее популярных стеков протоколов. Такая технология получила название мультиплексирования стеков протоколов. Благодаря ей клиентские запросы используют стек протоколов той сети, к которой относятся нужные серверы, или серверы подключают стек протоколов, соответствующий клиентскому запросу.

Шлюзы

Итак, шлюз согласует коммуникационные протоколы одного стека с коммуникационными протоколами другого стека. Программные средства, реализующие шлюз, нет смысла устанавливать ни на одном из двух взаимодействующих компьютеров, гораздо рациональнее разместить их на некотором компьютере-посреднике. Прежде чем обосновать это утверждение, рассмотрим принцип работы шлюза.

Запрос от процесса компьютера поступает на прикладной уровень его стека протоколов. В соответствии с этим протоколом на прикладном уровне формируются пакеты, в которых серверу отсылается запрос на выполнение сервиса. Пакет прикладного уровня передается вниз по стеку компьютера, а затем в соответствии с протоколами канального и физического уровней поступает в шлюз.

Здесь он передается от самого нижнего к самому верхнему уровню стека протоколов. Затем пакет прикладного уровня стека преобразуется (транслируется) в пакет прикладного уровня серверного стека. Алгоритм преобразования пакетов зависит от конкретных протоколов и, как уже было сказано, может быть достаточно сложным. В качестве общей информации, позволяющей корректно провести трансляцию, может использоваться, например, информация о символьном имени сервера и символьном имени запрашиваемого ресурса сервера (в частности, это может быть имя каталога файловой системы). Преобразованный пакет от верхнего уровня стека передается к нижним уровням в соответствии с правилами этого стека, а затем по физическим линиям связи в соответствии с протоколами физического и канального уровней поступает к нужному серверу. Ответ сервера преобразуется шлюзом аналогично.



Обращение клиента с мультиплексированием протоколов к серверам различных ОС

Мультиплексирование стеков

При мультиплексировании стеков протоколов на один из двух компьютеров с различными стеками помещается коммуникационный стек другого компьютера. Для того чтобы запрос от прикладного процесса был правильно обработан и направлен через стек, в компьютер необходимо добавить мультиплексор протоколов, который должен уметь определять, куда направляется запрос клиента. Для этого может использоваться служба имен сети, в которой отмечается принадлежность того или иного ресурса определенной сети с соответствующим стеком протоколов.

Предпосылкой для развития технологии мультиплексирования стало строгое определение протоколов и интерфейсов различных »

Самые распространенные случаи межсетевых транзакций в гетерогенных сетях

» уровней и их открытое описание, чтобы любая фирма при реализации «чужого» протокола или интерфейса могла быть уверена, что ее продукт будет правильно взаимодействовать с другой техникой по этому протоколу.

Сетевое решение

Как видно, любая задача решаема, главное — подобрать к ней соответствующий ключ. Таких ключей может быть несколько. Предположим, что наши пользователи проживают компактно в соответствии с используемыми ими клиентскими машинами. В этом случае напрашивается решение объединить их в несколько сетей в соответствии с типом используемой аппаратно-программной части, а потом уже настраивать межсетевое взаимодействие. Правда, неопределившиеся оказываются под влиянием большинства, но эту проблему тоже можно решить. Кстати, их аппаратная часть, давно нуждающаяся в апгрейде, может в полном составе, если сообщество договорится, стать серверами, шлюзами и коммутаторами.

В то время как расположение программных средств, реализующих шлюз, уже определено — они должны располагаться на компьютере, занимающем промежуточное положение между двумя взаимодействующими машинами, — вопрос о размещении дополнительных стеков протоколов остался открытым. Заметим также, что шлюз реализует взаимодействие «многие — ко многим» (все клиенты могут обращаться ко всем серверам). Очевидно, что наличие программных продуктов для каждого из вариантов сильно зависит от конкретной пары операционных систем. Для каких-то пар может вовсе не найтись продуктов межсетевого взаимодействия, а для некоторых существует даже выбор из нескольких вариантов.

В принципе, можно объединять клиентов в виртуальные сети, но здесь следует проконсультироваться с администратором, имеющим подобный опыт. В случае, если ваш «зоопарк» уже подключен к Интернету и налажены хорошие отношения с провайдером, он не откажется помочь.

Обычно роль шлюзов в сети выполняют выделенные серверы. И никто не мешает докупить оперативной памяти, установить на один из компьютеров Linux и настроить на нем сервер Samba. По крайней мере, так поступает большинство пользователей и компаний, которым надо обеспечить работу гетерогенной сети. При этом может быть задействована значительная часть мощности сервера, потому что преобразование протоколов — дело ресурсоемкое. Под файл-сервер и сервер доступа в Интернет, ради которых все и затевается, стоит выделить по отдельной машине. А поставить их лучше в квартире самого ответственного, чтобы бдил.

Заключение

Как видим, у пользователей гетерогенной сети существует определенная свобода выбора. Мы никоим образом не претендуем на полноту освещения вопроса, однако общие правила и пути развертывания такой сети постарались изложить. После ее создания и отладки вся радость сетевого общения будет доступна каждому пользователю. Единственным камнем преткновения может стать тот факт, что многие сетевые игры не имеют клиентов под все ОС. Конечно же, можно пользоваться эмуляторами, однако они не столь быстры, а мультизагрузка ПК доступна не всем в силу разницы архитектур.

■ ■ ■ Алексей Соколов

Аппаратная часть

Транслирующие мосты и коммутаторы

Транслирующие мосты и коммутаторы выполняют преобразование из одного протокола канального уровня в другой, например Ethernet в FDDI, Fast Ethernet в TokenRing и т. п. Преобразование заключается в изменении формата кадра, в вычислении нового значения контрольной суммы.

Трансляцию протоколов канального уровня облегчает то, что наиболее сложную работу по трансляции адресов, которую часто делают маршрутизаторы и шлюзы при объединении гетерогенных сетей, выполнять не нужно. Все конечные узлы имеют уникальные адреса одинакового формата вне зависимости от поддерживаемого протокола. Поэтому адрес сетевого адаптера Ethernet понятен сетевому адаптеру FDDI, и они могут использовать адреса, не задумываясь о том, что узел, с которым они взаимодействуют, принадлежит сети, работающей по другому протоколу. Поэтому в случае согласования протоколов локальных сетей коммутаторы не строят таблиц соответствия, а автоматически переносят адреса назначения и источника из кадра одного протокола в кадр другого. Единственным преобразованием, которое придется при этом выполнить, является преобразование порядка бит в байте, в том случае, если сеть Ethernet согласуется с сетью TokenRing или FDDI. Это связано с тем, что в сетях Ethernet принята каноническая форма передачи адреса по сети, когда сначала передается самый младший бит самого старшего байта адреса. В сетях FDDI и TokenRing, наоборот, передается сначала самый старший бит самого старшего байта адреса.

Сетевое оборудование

Верстовые столбы

Несмотря на все многообразие видов среды передачи, в случае небольших домашних или офисных сетей наиболее правильным будет говорить лишь о сетях стандарта Ethernet, причем о его конкретной разновидности — Ethernet на витой паре. Так уж получилось, что именно формат 10/100 Base-T к настоящему времени стал основным для организации компьютерных коммуникаций небольших размеров.

Источники и составные части

Процесс передачи данных внутри компьютерной сети можно условно разделить на две составные части. Вначале сетевое оборудование должно сформировать передаваемую информацию и привести ее в соответствие с тем типом кабельной системы, которая будет использоваться. Эти функции реализуют сетевые адаптеры, тип которых определяется не только физической средой передачи (витая пара, коаксиал, оптоволокно и т. п.), но и используемыми сетевыми стандартами, типом шины, разрядностью.

Второй составной частью является процесс распределения и получения информации. Такие процессы реализуются в повторителях и коммутаторах. Разница между ними весьма существенна. Функция многопортового повторителя (хаба) заключается в простом повторении информации, полученной по одному из портов, на остальные. В коммутаторах реализован механизм организации отдельного канала передачи для каждой пары коммутируемых узлов. Этот принцип построе- »

Малый концентратор компании Allied Telesyn (модель AT-MR415T), в котором реализована функция защиты от сбойных пакетов (Jabber lock-up)

» ния центрального сетевого узла позволяет во многих случаях существенно увеличить пропускную способность сети.

Таким образом, рабочий набор для создания небольшой сети включает в себя сетевые карты по количеству рабочих мест, концентратор (хаб) или коммутатор (свич). Дополнительно с этим оборудованием могут использоваться устройства для связи сети с внешним миром — маршрутизаторы (роутеры) и брандмауэры (аппаратные или программные).

Эти устройства часто называют «пограничными», поскольку они могут связывать не только несколько сегментов однотипных сетей, но и неоднородные сети (например, сеть Ethernet и FrameRelay).

Все сетевое оборудование сегодня делается по принципу «купил и включай». То есть, тому, кто впервые приступает к созданию локальной сети, не следует бояться непреодолимых сложностей: все довольно просто и понятно.

Процесс проектирования и создания сети малого офиса надо начинать с выбора производителя сетевого оборудования. Конечно, если разворачивать сеть «по науке», то первым шагом должен стать этап проектирования и структурирования сегментов. Однако практика показывает, что заказ проектирования сети на пять-десять узлов вряд ли экономически обоснован. Более того, обычно прокладка и построение малых сетей происходит совсем без предварительного проектирования. Конечно, это не совсем хорошо, поскольку неправильное построение кабельной системы может существенно снизить общую скорость. Но даже несмотря на это, определяющую роль будут играть оконечные и узловые устройства.

Создаем трафик

Современные сетевые адаптеры можно разделить на несколько типов — по типу шины, по разрядности, по поддерживаемой скорости передачи. Одним из главных определяющих факторов также является то, в каком формате реализован сетевой адаптер — в виде отдельной платы или как составная часть материнской платы.

Основными функциями сетевого адаптера являются формирование, передача и прием кадра данных. Главная часть сетевого адаптера — контроллер, который представляет собой одну из микросхем, выпускаемых сегодня довольно ограниченным числом производителей. Список отличий разных моделей довольно обширен, однако при сравнении следует обратить внимание на две самые важные характеристики — уровень загрузки центрального процессора и скорость работы контроллера в полнодуплексном режиме (или отсутствие поддержки полного дуплекса).

Дешево или сердито?

Наибольшей популярностью на рынке домашних и SOHO-сетей пользуются контроллеры и наборы микросхем от компании Realtek (например, RTL8139 или RTL8029), которые имеют довольно слабую поддержку полнодуплексного режима, однако очень конкурентоспособны на сетевом рынке вследствие низкой цены. Более того, некоторые производители материнских плат при разводке сетевого адаптера непосредственно на плате используют именно контроллеры Realtek, что, во-первых, экономически весьма выгодно, а во-вторых, достаточно функционально.

Второе место по популярности занимают чипсеты и сетевые контроллеры от 3Com. Самое главное преимущество всей сетевой продукции 3Com заключается в том, что она изначально при разработке и впоследствии при производстве оптимизируется для работы с себе подобными. То есть, если вы уж начинаете строить сеть на сетевых платах 3Com, то вам надо быть последовательным в своих намерениях. »

Условия нормальной связи

Переключение скоростей

Технология автоматического определения скорости и режима соединения (Nway autonegotiation) использует импульсы, идентичные по природе сигналам, используемым в спецификации 10Base-T. Именно эти сигналы и заставляют «светиться» светодиодные индикаторы на панели хаба. Если узловое устройство (концентратор или коммутатор) получает от конечного узла одиночный сигнал, называемый Normal Link Pulse (NLP), то делается вывод о том, что связь поддерживается только в стандарте 802.3 со скоростью 10 Мбит/с. Для более интеллектуального управления скоростью используется серия импульсов, называемая Fast Link Pulse (FLP) и состоящая из 17 тактовых и 16 сигнальных импульсов, образующих 16-битное слово. Комбинации битов сравниваются концентратором и конечной станцией, в результате происходит выбор допустимых режимов работы. Сравнение управляющего слова происходит независимо на каждом конце соединения, однако совместимость обеспечивает использование одинакового алгоритма.

Для того чтобы две сети, работающие с разными скоростями, могли обмениваться информацией, в составе устройства Dual-Speed должен находиться модуль коммутации, который, однако, не объединяет эти сети в один «домен коллизий». Отсутствие коммутирующего модуля, который представляет собой буфер для обмена данными, приводит к тому, что один и тот же коммутатор может быть использован лишь для работы двух независимых разноскоростных сетей.

Даже если брать в расчет лишь «голые» технические характеристики отдельного сетевого адаптера 3Com, то и тут картина достаточно впечатляющая. Прежде всего, надо отметить фирменную технологию Parallel Tasking. С ее помощью на сетевых адаптерах организуется конвейер данных, тем самым уменьшается загрузка процессора. Дополнительно к этой технологии при работе с Windows 2000 можно использовать возможности специальной микросхемы, которая самостоятельно аппаратно вычисляет контрольную сумму TCP/IP, еще более разгружая ЦП. Плюс к этому — поддержка приоритезации трафика для мультимедийных и бизнес-приложений. К этому следует добавить возможность установки дополнительного ПО, ответственного за сетевое управление и дистанционное обслуживание компьютера.

Конечно, подобные усовершенствования не могли не сказаться на цене. Но если подходить к построению сети (пусть даже домашней) вдумчиво и серьезно, то не стоит гнаться за дешевизной, а лучше потратить немного больше средств и в результате получить более производительную сетевую конфигурацию.

Концентрируем трафик

Основной принцип работы Ethernet можно выразить одной фразой: «Один говорит — все слушают». Означает это, что каждый пакет, пришедший на общую шину, будет доступен для приема всеми узлами. Однако реально принять его сможет лишь тот узел, которому пакет адресован. Устройства, которые призваны обеспечивать этот принцип работы, называются повторителями. В самом начале истории Ethernet повторители были однопортовыми и выполняли лишь функции репитеров. Впоследствии разработчики поняли, что повторять сигнал можно не только на одном, но и на множестве портов. Таким образом, классическая «общая шина» Ethernet была втиснута внутрь узловых устройств, и внешне сети 10-Base-T стали выглядеть как сети ушедшего в прошлое стандарта Arcnet с топологией «звезда».

Несмотря на то что до сих пор все концентраторы по выполняемым функциям разделяются на три группы, основную часть всемирного парка хабов составляют устройства начального уровня, которые работают в малых сетях и, как правило, являются неуправляемыми «пассивными» сетевыми устройствами. Главное их преимущество — быстрота подключения.

Концентраторы среднего уровня и управляемые концентраторы на сегодняшний день уже морально устарели. Произошло это после того, как стоимость коммутаторов (свичей) из расчета на один порт сравня-

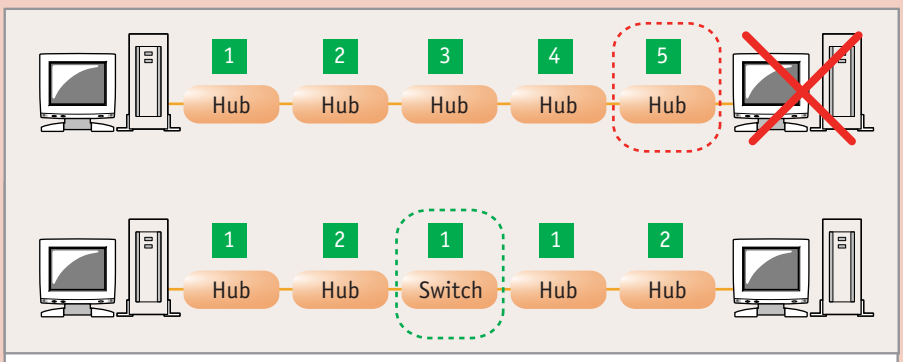
Кто последний?

Скорость как «5-4-3-2-1»

Спецификация IEEE 802.3 определяет скорость передачи в 10 Мбит/с. Пользователю же надо помнить, что это расчетная математическая скорость, которая имеет мало общего с практикой. 10 Мбит в секунду — это скорость передачи «в одну сторону при полном отсутствии коллизий». Реальные же скорости примерно на порядок ниже заявленных. Поэтому при работе сети на первое место выходит не технологическая скорость, а структура, которая должна соответствовать правилу «5-4-3-2-1».

Правило это появилось из-за того, что данные в сети IEEE 802.3 не могут одновременно появиться на всех узлах. Необходимо время (задержка распространения), за которое сигнал проходит все сетевые устройства вместе с проводами. Именно поэтому между каждыми двумя участниками сети не может быть больше пяти сегментов, четырех концентраторов, и только три сегмента могут быть использованы для соединения конечных узлов. Два сегмента, существующие между концентраторами, не могут быть использованы для подсоединения конечных узлов, а вся сеть при построении исключительно с помощью хабов представляет собою один «коллизионный домен».

При использовании коммутаторов правило «5-4-3-2-1» может быть применено к каждому сегменту. Например, нельзя включить последовательно более четырех хабов. Однако если между вторым и третьим хабом включить свич, то сеть останется работоспособной, поскольку он поделит исходный отрезок на два коллизионных сегмента.



Добавление коммутатора разбивает сеть на два сегмента коллизий

Коммутатор Procurve Switch 408 от Hewlett-Packard интересен тем, что производитель предоставляет на него пожизненную гарантию

» лась со стоимостью хабов. Дело в том, что все специфические свойства этих устройств — консольное и SNTP-управление, управление портами и контроль трафика — успешно реализуются и в коммутаторах.

Коробка со скоростями

Существующие сегодня на рынке концентраторы для малых сетей мало чем отличаются друг от друга — каждый из них работает в соответствии со стандартом, имеет ряд светодиодных индикаторов и возможность наращиваемого подключения других коммутаторов (uplink), однако есть и ряд отличий. Например, существуют так называемые коммутаторы Dual-Speed, работающие как по стандарту IEEE 802.3 на скорости 10 Мбит/с, так и по IEEE 802.3u на скорости 100 Мбит/с.

Безусловно, вопрос организации двухскоростной сети далеко не так прост, как это может показаться на первый взгляд. В некоторых источниках встречается определение хаба как устройства, «накоротко замыкающего сетевые интерфейсы». Это не совсем так, но вполне отвечает основным принципам его работы, ведь хабы не имеют внутреннего буфера для хранения передаваемых пакетов, а потому не могут переключать скорости автоматически.

Для того чтобы как-то обойти это ограничение, разработчики решили объединить два разноскоростных концентратора в одном корпусе. Один из них предназначен для соединения сетевых устройств на скорости 10 Мбит/с (стандарт 802.3), в то время как другой — на скорости 100 Мбит/с (стандарт 802.3u). Каждый из повторителей организует свою сеть, в то время как порты подключения у них общие.

Любое устройство, подключенное к одному из двухскоростных портов, должно либо использовать технологию Nway Negotiation для определения наибольшей возможной скорости, либо, если это устройство односкоростное, работать только со своим внутренним хабом.

Интересно, что сегодня на неотвратимо сокращающемся рынке концентраторов можно встретить весьма показательные модели. По заявляемым технологическим параметрам они вроде бы должны работать на двух скоростях. На практике же может получиться так, что при наличии в сети хотя бы одного 10-мегабитного устройства вся подключаемая сеть будет работать только на этой скорости.

Прелести лидеров

Как правило, ведущие производители очень строго следят за качеством своих продуктов. Примером могут служить устройства серии Office Connect Dual Speed Hub вездесущей компании 3Com. Конечно, строго говоря, эти концентраторы следует отнести к промежуточным устройствам между хабами и коммутаторами (иногда их еще называют коммутирующими концентраторами).

Упоминания также заслуживают малые концентраторы компании Allied Telesyn (например, модель AT-MR415T), в которых реализована функция защиты от сбойных пакетов (Jabber lock-up). За счет ее использования предотвращается прием и передача пакетов, длина которых превышает максимально допустимую.

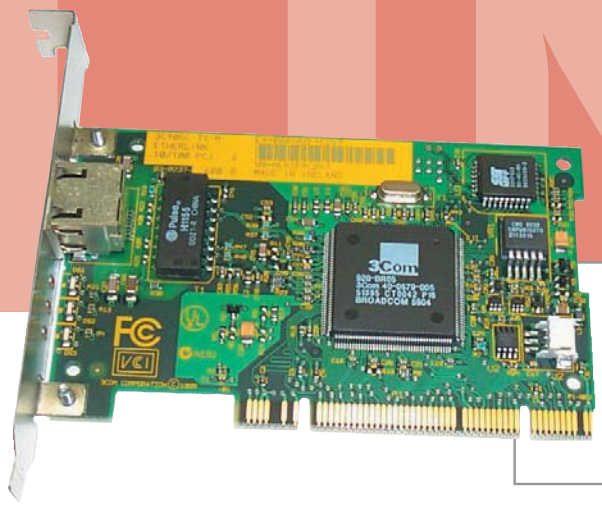
И наконец, нельзя не вспомнить о концентраторах компании D-Link, которые заслужили репутацию надежных и сравнительно недорогих устройств. Основной характерной особенностью некоторых моделей хабов D-Link можно назвать специфический способ наращивания портов. Например, для связи концентраторов DFE-908Dx друг с другом используется не один из рабочих портов на каждом устройстве, а специальные модули коммутации. Получившаяся при этом связка выступает для всех остальных участников обмена трафиком как единое целое.

Если же говорить в общем, то несмотря на глобальное сокращение объемов продаж хабов по всему миру, их еще рано списывать со счетов. Есть еще довольно много задач и приложений, где не требуется большая скорость работы, а важна лишь сама возможность коммутации. В этих случаях применение более дешевых по сравнению со свичами хабов вполне оправданно.

Коммутируем трафик

Коллизионная сущность Ethernet долгое время накладывала определенные ограничения не только на общую протяженность сетей. Расчетным и опытным путем было установлено, что число концентраторов, которые могут быть последовательно подключены друг за другом, не должно превышать четырех. Конечно, для малых сетей этого было вполне достаточно, однако хабы имели еще один недостаток, который вытекал непосредственно из основного свойства «общей шины» — множественного доступа с обнаружением коллизий. Дело в том, что как только загрузка сети превышала некий критический порог, скорость резко падала. Сетевые адаптеры не могли оптимально подобрать случайный промежуток времени, который должен по стандарту IEEE 802.3 разделять попытки передачи, а концентраторы не могли ничем помочь, поскольку по сути своей являются пассивными устройствами.

Для того чтобы хоть как-то решить эту проблему, сетевые инженеры разбивали большие сети на несколько малых сегментов, а проблему межсегментной связи решали с помощью роутеров (маршрутизаторов). По вопросам оптимального разделения сетей на сегменты велись жаркие споры и даже защищались диссертации, пока в 1990 году американская компания Kalpana (купленная Cisco System Inc. четыре года спустя) не предложила решить эту »



Продукция компании 3Com, как правило, отличается совместимостью, хорошим качеством и наличием интересных особенностей, но при этом и стоит дороже

проблему не на уровне организации сети, а с помощью новой технологии.

Идея состояла в том, что внутри центрального узлового устройства, которое называется мостом, или бриджем (bridge), создавались независимые «общие шины» для каждой пары передатчик–приемник. Пользователь получал в свое распоряжение всю ширину канала, а дополнительная буферизация и принцип передачи только включенному в сеть абоненту определяли высокую надежность.

Поначалу казалось, что технология коммутации может быть применена лишь на больших сетевых узлах для снижения их нагрузки, прежде всего потому, что стоимость новых устройств достигала $1500 в расчете на один порт. Тем не менее прошло время, и бриджи из устройств, умеющих связывать лишь два сегмента, превратились в коммутаторы, или свичи (switch), которые есть не что иное, как многопортовые мосты.

Адресата определяет матрица

Работа коммутатора состоит в том, чтобы для каждой пары отправитель–получатель организовать независимое динамическое виртуальное соединение. Реализуется это путем организации внутри коммутатора матрицы передачи или высокоскоростной шины, с помощью которой любые два устройства могут обмениваться данными. Это основная составная схемотехническая часть коммутатора, иначе называемая ядром. Кроме того, в состав свича входят адаптеры для каждого порта, которые преобразуют данные в формат, понятный ядру.

В функции адаптера входит также вычисление MAC-адреса назначения и добавление в поток данных адреса порта назначения.

Сегодня существуют две схемы организации работы свича. Коммутация «на лету» (Cut through) предусматривает передачу трафика получателю еще до окончания приема данных от передатчика. Практически же коммутатору достаточно получить заголовок передаваемого пакета, вычислить адрес приемника и начать передачу. Эта схема самая скоростная, поскольку время задержки не зависит от размера пакета, а определяется лишь характеристиками среды. Коммутация с промежуточной буферизацией (Store and forward), предусматривающая наличие буферов обмена, менее скоростная, однако более надежная, поскольку позволяет избежать ошибок передачи и предотвратить передачу на отключенный порт.

Существует еще промежуточный метод Fragment-Free, мало используемый, однако заслуживающий упоминания. Суть его заключается в том, что если ошибка (или коллизия) присутствует в передаче, то она почти всегда обнаруживается в первых 64 байтах передачи. Поэтому коммутатор принимает первые 64 байта, анализирует их на предмет ошибки и, если таковой не обнаружено, продолжает сеанс связи.

Иногда в современных коммутаторах используются все эти схемы коммутации с возможностью автоматического переключения режимов в зависимости от нагрузки сети, но такие коммутаторы вряд ли найдут применение в малых сетях, поскольку довольно дорого стоят. Самые распространенные сегодня модели свичей, во-первых, обладают буфером для запоминания MAC-адресов, во-вторых, используют метод Store and forward и, в-третьих, умеют работать как минимум на двух скоростях передачи.

Для дома и для дела

Практически все производители коммутаторов при выборе количества портов своих

Безымянность и драйверы

NE2000-совместимость сетевых карт

Изначально в состав чипсета для сетевого контроллера входили три составные части — интерфейс для подключения к локальной шине (Network Interface Controller, NIC), инструмент кодирования и обслуживания коллизий (Serial Network Interface, SNI) и механизм приема и передачи данных по коаксиальному кабелю (Coaxial Transceiver Interface, CTI). До сих пор сохранилась традиция наименования сетевых адаптеров аббревиатурой NIC. Принципиальных изменений эта схема, разработанная некогда Гордоном Кемпбеллом — отцом множества фундаментальных идей (например, технологии 3Dfx), не претерпела и по сей день.

Программная модель поддержки драйверов Novell Eagle (NE) была разработана фирмой Novell в тесном сотрудничестве с малоизвестной тогда компанией Chips & Technologies Inc. (основатель — Гордон Кемпбелл). Спецификация NE2000 определяет состав и методы программирования управляющих регистров для взаимодействия сетевого адаптера с шинами ISA и PCI. Этот документ вот уже более десяти лет является стандартом написания драйверов для производителей сетевого оборудования. Несмотря на то что первоначально сетевые NE2000-совместимые платы существовали только для шины ISA, сегодня, когда в руки специалистам попадает неизвестная сетевая карта без драйверов, но с BNC-разъемом, в первую очередь ее тестируют на работу со стандартным NE2000-драйвером, входящим в состав любой операционной системы.

Определение узла назначения

Что обозначает MAC-адрес

В соответствии со стандартами семейства 802.x канальный уровень подразделяется на два подуровня — управления доступом к среде (Media Access Control, MAC) и логической передачи данных (Logical Link Control, LLC). Для каждого из этих подуровней в современных сетях существуют несколько протоколов, которые абсолютно независимы и могут использоваться в разных сочетаниях. В изначальной технологии Ethernet, которая была изобретена компанией Xerox в 1973 году, подуровни MAC и LLC были объединены в один. И именно тогда появился так называемый MAC-адрес сетевой карты, который, по идее разработчиков, должен идентифицировать каждую сетевую карту и быть абсолютно уникальным. Значение MAC-адреса встраивается в стандартный кадр Ethernet и должно однозначно определять узел назначения. На принципе соответствия MAC-адреса конкретному IP-адресу построены некоторые механизмы сетевой защиты, которые, однако, сегодня можно довольно легко обойти за счет применения сетевых адаптеров с возможностью смены MAC-адреса.
MAC-адрес имеет длину 6 байт и назначается производителем карты. При этом в старших трех байтах адреса «зашивается» код производителя конкретной карты.

» младших моделей руководствуются довольно странной логикой. Портов может быть либо пять, либо восемь. При этом сами по себе свичи мало чем отличаются друг от друга даже по внешнему виду, однако цена из расчета на один порт у восьмипортовых моделей, конечно, ниже. И именно эта цена определяет предпочтения российского пользователя. А также извечная наша привычка покупать все «про запас». Тем не менее в случае с небольшими сетями это вполне оправданно, ведь нет никакой гарантии, что через пару недель вам не придется добавлять в сеть новые узлы.

Конечно, на практике могут возникать самые различные ситуации, тем не менее экономический показатель «цена одного порта» должен быть определяющим. Кроме того, лучше всего выбирать модели того же производителя, что и все остальное сетевое оборудование. Только в этом случае вы можете получить фирменные преимущества, которые производитель закладывает лишь в свое оборудование.

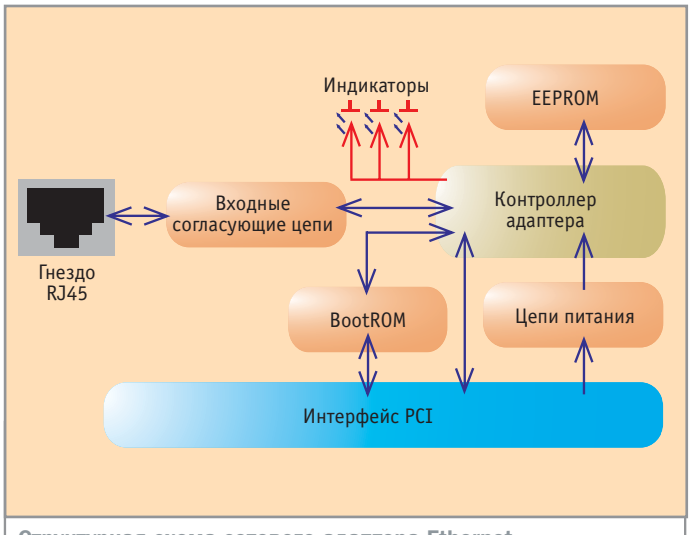
Так, например, все та же 3Com поставляет на рынок восьми- и пятипортовые модели серии Office Connect Dual Speed Switch Plus, которые кроме стандартного набора функций обладают еще и возможностью организации внутренних очередей по приоритетам, определяющимся, в свою очередь, качественным содержанием трафика. Принципиально такая схема должна работать во всех сетях, однако опытные сетевые специалисты говорят, что лучше всего она применима лишь в тех сетях, которые собраны исключительно из компонентов от 3Com.

Безусловно, в каждом конкретном случае необходимо выбирать наиболее оптимальное решение. Однако стоит помнить, что не всегда дополнительные затраты означают повышение производительности. В некоторых случаях пользователь платит деньги не столько за качество, сколько за имя. В качестве примера можно назвать модель Procurve Switch 408 от Hewlett-Packard. Этот коммутатор принципиально отличается от всех остальных только тем, что производитель предоставляет на него пожизненную гарантию. Означает это, что ваше устройство будет заменено на другое в случае его неисправности. Конечно, если вам удастся доказать, что поломка произошла не по вашей вине.

Основную же долю рынка коммутаторов составляют сегодня модели от Compex, Surecom, LG, Genius и еще целого ряда компаний. Модели эти, как правило, обеспечивают заявленную скорость при низких сетевых нагрузках и сильно «проседают», когда нагрузка становится большой. Несмотря на это, все подходящие по характеристикам модели младшего ценового ряда вполне могут использоваться при построении малонагруженных сегментов, которыми в большей своей части и являются домашние сети и сети малых офисов.

■ ■ ■ Сергей Кондращев

Задача роутера сводится к перенаправлению данных с одного сетевого интерфейса на другой в зависимости от заранее определенных маршрутов, но это может быть как обычный компьютер с двумя адаптерами, так и комплексное устройство



Структурная схема сетевого адаптера Ethernet

NET

network

АНОНС

Эфирная сеть
История и эволюция Ehternet 34

Путевая карта
Виды сетевых топологий 40

Сетевой Вавилон
Протоколы передачи данных 46

И закинул он невод
Алгоритм планирования сети 50

Артерии жизни
Услуги Ethernet-провайдинга 54

Хозяйство племени
Обзор сетевой периферии 60

Эфирная сеть

История Ethernet с высоты прошедших трех десятилетий представляется сегодня почти мифологической. Разные источники называют не только разные даты первой реализации технологии, но и разные места ее появления.

Самым первым упоминанием о Ethernet следует считать попытку организации компьютерной сети в одном из корпусов гавайского университета Алоха. Интересно, что в тот момент, когда отец-основатель Ethernet Роберт Меткалф (Robert Metcalfe) представил на защиту свою докторскую работу «Packet Communication» («Пакетная связь»), а произошло это 22 мая 1973 года, речь в ней шла не об университетской сети, а о сети, созданной в тестовой лаборатории компании Xerox в Пало-Альто. Само название среды передачи берет начало от слова «ether» (эфир), которое было написано на эскизе, сопровождающем представленную работу.

Немного позже, в июле 1976 года, в журнале «Communications of the ACM» появилась статья «Ethernet: Distributed Packet Switching for Local Computer Networks», в которой Роберт Меткалф совместно с Дэвидом Боггсом (David Boggs) попытался дать теоретические и, что самое важное, практические рекомендации по реализации технологии. В 1979 году Меткалф создает собственную фирму, которой впоследствии »

» суждено было стать одним из главных игроков на сетевом рынке, и называет ее 3Com (Computer Communication Compatibility). Именно этот момент можно считать началом победоносного шествия Ethernet по всему миру.

Толстый коаксиал

В 1980 году компании DEC, Intel и Xerox разработали и опубликовали первый промышленный стандарт для организации локальной сети, названный Ethernet II. Кроме того, в обиход вошла аббревиатура DIX (по первым буквам названий компаний-разработчиков). Но самое интересное состоит в том, что Меткалф в это время работал консультантом компании DEC и принимал самое непосредственное участие в разработке этого стандарта, а также стандарта IEEE 802.3, который на сегодня является основным документом как для производителей сетевого оборудования, так и для специалистов-практиков.

Первые Ethernet-сети работали на так называемом толстом коаксиальном проводе. Обусловлено это было в первую очередь его широким распространением. Именно толстый коаксиал сопротивлением 50 Ом и диаметром около 12 мм (0,5 дюйма) применяется в телевизионной технике. Подключение узлов в такую сеть производилось с помощью трансиверов, имеющих в своем составе активный приемопередатчик с детектором коллизий и высоковольтный (1–5 кВ) разделительный трансформатор. Высокая помехозащищенность толстого коаксиала обеспечивала большую длину возможного сегмента (до 500 м), что давало возможность использовать разновидность 10Base-5 (именно так называется этот вариант в стандарте IEEE 802.3) для прокладки так называемых базовых сегментов. Но даже несмотря на очевидные преимущества такого вида Ethernet, ему не суждено было стать основной сетевой «рабочей лошадкой»...

Тонкий коаксиал

Построение сетей на толстом коаксиале, может быть, и не составляло особенных трудностей для подготовленных специалистов, однако в повседневной практике даже несомненные преимущества 10Base-5 нивелировались необходимостью подключения каждого узла с помощью трансиверов. Следующий этап развития Ethernet — сети на тонком коаксиале — избавили сетевых инженеров от этого недостатка.

Тонкий Ethernet, или Thinnet (10Base-2), использует в качестве среды передачи коаксиальный кабель диаметром 6 мм. Безусловно, этот факт накладывает определенные ограничения как на количество узлов в сегменте (не более 30), так и на общую протяженность линии (общая длина всех сегментов сети — 925 м).

Тем не менее тонкий вариант коаксиального Ethernet за счет использования топологии «общая шина» получил гораздо более широкое распространение, поскольку основное эксплуатационное преимущество заключалось в снижении количества используемого активного сетевого оборудования. Однако основной недостаток линейного построения сетей — зависимость работоспособности от состояния общего кабеля — удалось устранить лишь на следующем этапе развития Ethernet.

Витая медная пара

В 1991 году Ethernet наконец-то смог вылечится от болезней роста и приобрел те самые незабываемые черты, которые сегодня и определяют его как самую популярную технологию организации локальных сетей. Решением большинства проблем стала так называемая неэкранированная витая медная пара, в которой для приема-передачи данных используются две пары скрученных медных проводов, где передаваемые сигналы имеют разную поляризацию. Хитрость такого технологического приема заключается в том, что потенциально возможные помехи передачи будут одинаковыми по фазе и амплитуде в обоих проводах. А значит, после инвертирования одного из сигналов они взаимно уничтожатся.

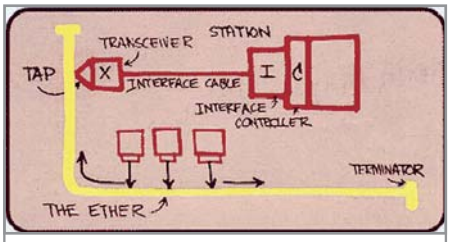
Этот вид Ethernet, получивший обозначение 10Base-T, в самом простом своем варианте может объединять в один сегмент всего лишь два узла, причем провода, отвечающие за прием-передачу, должны быть перекрещены. Понятно, что такие «куцые» сегменты не могли использоваться для соединения многих узлов, поэтому топология была заменена на «звезду», а в качестве соединяющих устройств стали использоваться многопортовые повторители, или хабы.

Несмотря на то что хабы (позже коммутаторы, свичи) стали неотъемлемой частью сетей, а общая протяженность проводов увеличивалась пропорционально количеству узлов, надежность организованных таким образом коммуникаций также возросла. Кроме того что теперь появилась возможность добавления узлов в «горячем» режиме, даже самый простой хаб имеет индикаторы подключения узлов, и это значительно упрощает диагностику неисправностей.

Но самое важное достижение варианта 10Base-T — теперь узлы получили возможность работы в реальном полнодуплексном режиме, поскольку прием и передача данных, разнесенные по разным медным жилам, могли производиться одновременно.

FiberLink

Оптоволоконные соединения, как самые быстрые и наиболее подходящие для про- »



Ставший историческим эскиз Боба Меткалфа, где впервые появилось слово Ether (эфир)

Трансиверный модуль для 10-гигабитного Ethernet

кладки «базовых» сегментов, не могли остаться незамеченными разработчиками и идеологами Ethernet. В самом начале свет увидела спецификация 10Base-FL (FiberLink) — вариант топологии «звезда», где узлы подключались друг к другу с помощью повторителей.

Впоследствии была придумана и спецификация 10Base-FB (Fiber Backbone), целью которой стало регламентирование соединений между повторителями и оптическими хабами. Несмотря на появившиеся преимущества (синхронный режим работы, увеличение общей протяженности каналов, способность повторителей самостоятельно находить и исключать из обмена сбойные порты), разработчики не только не смогли заставить заработать оптический Ethernet в полнодуплексном режиме, но и получили недостаток, который, правда, носил не столько технологический, сколько организационный характер.

Дело в том, что локальные сети уже тогда работали на скорости 10 Мбит/с. Магистрали же, для которых, собственно, и проектировались сети 10Base-F, не могли работать быстрее, хотя, по идее, как элементы, связующие «мелкие» сети, должны были иметь некоторый запас прочности.

Делаем все быстрее!

Развитие простого в инсталляции и надежного в эксплуатации механизма построения локальных сетей на определенном этапе немного затормозилось. Количество узлов в локальных сетях росло достаточно плавно, но скорость работы компьютеров увеличивалась скачкообразно. В результате появились приложения, для успешной работы которых были необходимы самые высокие характеристики процессоров и иного железа. Именно в такой ситуации, когда к сетям все привыкли, но они уже «не успевали» за потребностями в скорости, необходимо было увеличивать сетевую пропускную способность.

В 1995 году организация IEEE опубликовала документ по индексом 802.3u, который, основываясь на пилотных разработках компании Crescendo и исследованиях консорциума Fast Ethernet Alliance (инициатором создания которого выступила все та же 3Com), описывал идеологию и методы построения Ethernet-сетей, работающих со скоростью 100 Мбит/с, которые используют в качестве среды передачи витую пару.

Первоначальная идея разработчиков, получившая свое отражение в варианте под индексом 100Base-T4, подразумевала использование в стандартном кабеле UTP не двух рабочих пар, а всех четырех. При этом три пары отводились для приема-передачи информации (три канала по 33 Мбит), а четвертая — для обнаружения коллизий. Интересно, что для построения таких сетей

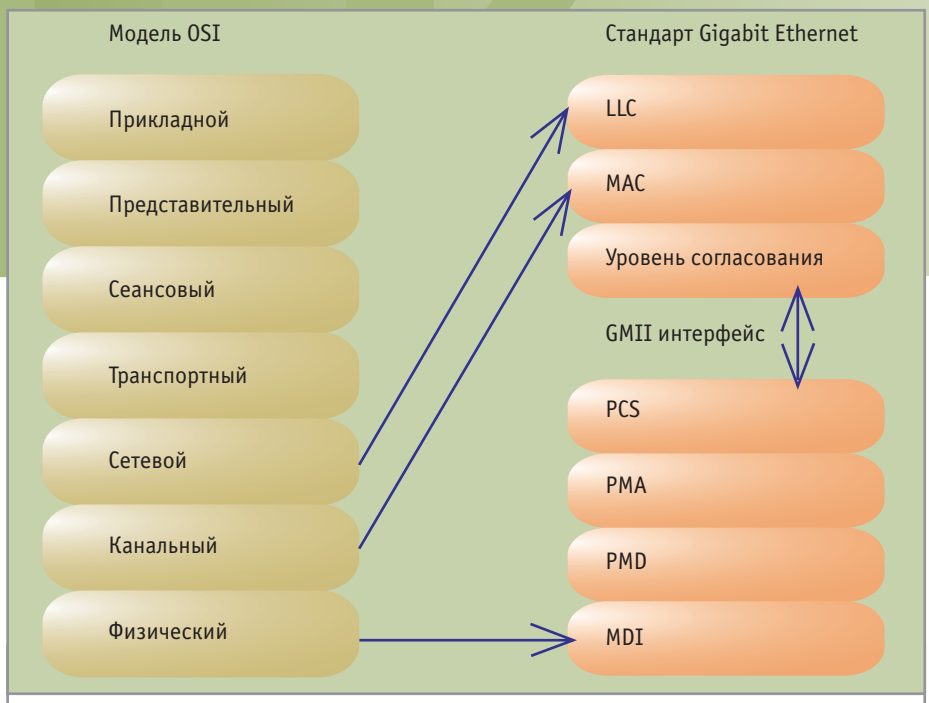
Техническая информация

Общая структура Ethernet

Идеология структуры Ethernet, определенная в свое время Меткалфом, до сих пор остается основой для построения локальных сетей. Физически сеть образуют несколько элементов: среда передачи данных, интерфейс доступа к среде (MDI — Medium Dependent Interface), устройство подключения к ней (MAU — Medium Attachment Unit), интерфейс MAI (AUI — Attachment Unit Interface) и средства управления доступом к среде (MAC — Medium Access Control).

Для наиболее популярного на сегодня варианта реализации средой передачи является кабель (коаксиальный или UTP), MDI — это либо разъем телефонного типа RJ-45, либо разъем BNC. MAU и MAC скрыты от обычного пользователя. Информация передается в виде так называемых MAC-фреймов, по сути являющихся информационными кадрами, в которых информация «обрамляется» служебными октетами и, кроме всего прочего, указываются MAC-адреса отправителя и получателя.

Один занимательный факт: приоритет первенства компании Xerox, который сегодня многие пытаются оспаривать, был навсегда сохранен не столько юридически, сколько технологически. Дело в том, что MAC-адреса, на уникальности которых построена вся технология Ethernet, включают в себя идентификатор производителя (Organizationally Unique Identifiers). Так вот нулевой (самый первый) идентификатор навечно зарезервирован за компанией Xerox.



Реализация модели OSI для стандарта Gigabit Ethernet

можно было использовать витую пару третьей категории. Однако практическая реализация затруднялась тем, что для успешной организации сетевого взаимодействия необходимо было модифицировать протокол физического уровня.

Поэтому наиболее перспективной оказалась реализация 100Base-TX, которая хотя и использовала кабель UTP не ниже пятой категории, но задействовала все те же две пары и отличалась от «классической» 10Base-T форматом передаваемого кадра и временными интервалами. При этом абсолютно неизменными оставались параметры алгоритмов доступа.

Пользователи отреагировали на появление нового «быстрого», или FastEthernet, довольно своеобразно. Несмотря на то что большая часть американских сетей была сделана на UTP третьей категории, самую большую популярность приобрел вариант 100Base-TX, который впоследствии дал начало целому семейству так называемых X-подобных Ethernet (100Base-TX и 100Base-FX).

FastEthernet

С точки зрения конечного пользователя между отцом — «классическим» Ethernet — и его отпрыском — FastEthernet — сходств гораздо больше, чем различий. Однако в тот момент, когда спецификация 802.3u еще только зарождалась, среди ее разработчиков шли жаркие споры по поводу целесообразности использования коллизионного метода. Их инициаторами выступали одни из самых авторитетных членов консорциума — компании Hewlett-Packard и AT&T. Именно они предложили вместо CDMA/CD использовать новый метод Demand Priority, который, с одной стороны, существенно менял алгоритм сетевого обмена, но с другой стороны, при соответствующей «обвязке» мог успешно применяться и в существующих сетях.

Но несмотря на хорошие перспективы Demand Priority, в FastEthernet все-таки решили сохранить возможность возникновения коллизий, однако придумали эффективные механизмы борьбы с ними. Например, признаком свободного состояния среды в Fast Ethernet вместо отсутствия сигнала стала передача символа Idle (не занято).

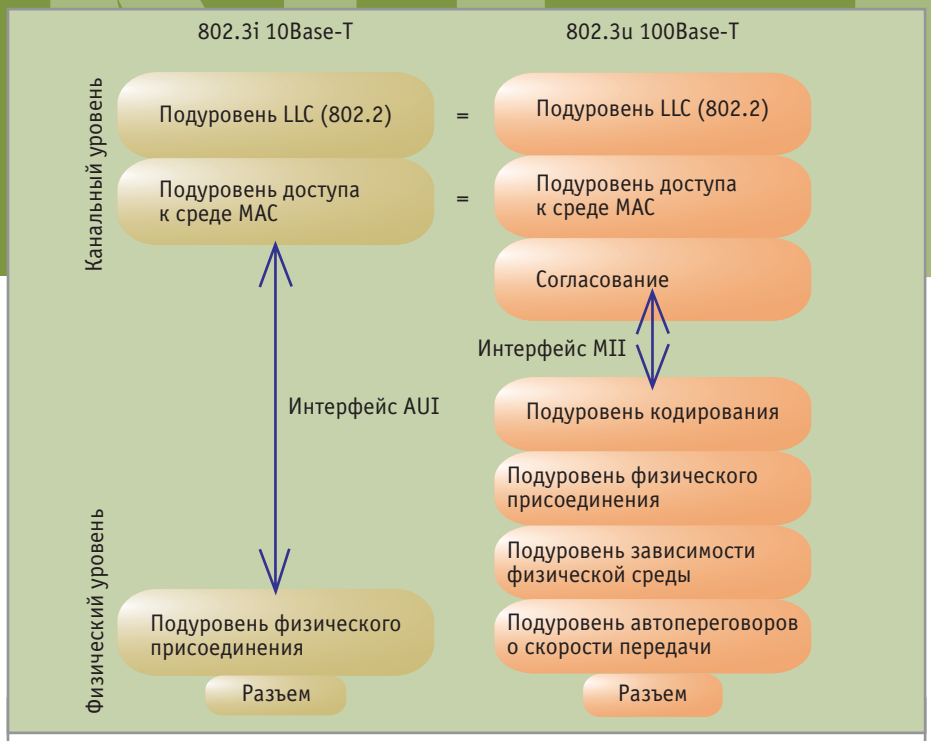
Методы решения проблем

Слушаем несущую и обнаруживаем коллизии

Основной недостаток Ethernet — снижение скорости при одновременном подключении большого числа пользователей — определяется технологией множественного доступа с прослушиванием несущей и обнаружением коллизий (Carrier Sense Multiple Access with Collision Detection — CSMA/CD). Этот метод базируется на трех основных положениях. Первое — «все узлы разделяют общую среду передачи» — вытекает непосредственно из самой идеологии Ethernet. Второе — «один говорит — все слушают» — требует и наличия механизма обнаружения того, что «говорит» именно один, и способов предотвращения одновременной передачи. Именно для этих целей был введен третий постулат, который говорит, что передача может осуществляться лишь в тишине. В случае одновременного начала передачи (коллизии) процесс блокируется и возобновляется через случайно определяемый промежуток времени.

Однако, как водится, в стандарте есть и исключения. Для скоростей, превышающих 100 Мбит/с (FastEthernet и Gygabit Ethernet), предусмотрена возможность работы в так называемом burst-mode. В этом случае один узел может передавать без перерыва несколько пакетов. Промежутки между ними заполняются битами расширения, которые не являются информационными, однако позволяют удерживать приоритет передачи. Если узел не успел осуществить передачу за отведенный ему промежуток времени (burst limit), то такие пакеты отбрасываются.

В качестве альтернативы CSMA/CD компаниями Hewlett-Packard и AT&T был предложен метод Demand Priority, который подразумевает обслуживание запросов станций на передачу в специальном функциональном блоке репитера по принципу циклической очереди. После получения запрос, оформленный в виде специального кадра, передается в порт, к которому подключен адресат. В настоящее время метод реализован в стандарте 100VG-Any LAN (IEEE 802.12).



Различия в реализации уровней модели ISO-OSI для Ethernet и Fast Ethernet

» Но самым важным преимуществом Fast-Ethernet явилось то, что временные интервалы, отведенные для передачи кадра и для паузы между ними, были сокращены на порядок: вместо 100 нс на бит и 9,6 мкс на паузу — 10 нс и 0,96 мкс соответственно.

Особого упоминания заслуживает схема «автопереговоров по принятию режимов работы порта» (Auto-negotiation), цель которой — обеспечение наиболее эффективного режима работы между узлами Ethernet и FastEthernet. При этом схема может определять не только наиболее подходящую скорость (10 или 100 Мбит), но и выбирать полудуплексный режим или режим полного дуплекса.

Gigabit Ethernet

По большому счету, даже сегодня 100-мегабитные сети устраивают большинство пользователей. Но разработчики и лидеры рынка, похоже, не намерены повторять ситуацию, когда сеть не успевала за железом. Наверное, именно поэтому в 1996 году теперь уже почти легендарная 3Com снова выступила в роли одного из инициаторов создания консорциума Gigabit Ethernet Alliance (GEA), в который, однако, на этот раз вошли и крупные производители компьютерного оборудования — Intel, Bay Networks, Cisco и Sun.

Самым интересным фактом в истории Gigabit Ethernet является то, что при разработке официального стандарта IEEE 802.3z использовались не только опыт и умы специалистов, но и средства математического моделирования — язык C и пакет Matlab. Таким образом, гигабитный Ethernet стал первой фундаментально сетевой технологией, которая появилась не «на кончике пера», а практически в недрах компьютерных систем. Может быть, именно поэтому она является на сегодняшний момент хорошо просчитанной, но попадает не совсем «в десятку», если брать во внимание логику развития современных сетей.

Отличия гигабитного Ethernet заключены в основном в реализации так называемого «средонезависимого интерфейса», который здесь именуется как GMII (Gigabit Media Independent Interface). Именно он отвечает за взаимодействие между уровнем MAC и уровнем физической среды. GMII имеет 8-битные приемник и передатчик, а также выдает в среду два служебных сигнала — наличие несущей и отсутствие коллизий.

В качестве физической среды Gigabit Ethernet может использовать как оптоволокно с различными характеристиками лазеров (1000Base-LX и 1000Base-SX), так и экранированную (1000Base-CX) или неэкранированную витую пару, в которой задействуются все четыре пары проводников. Именно поэтому кабель UTP должен быть не ниже пятой категории, а максимальное расстояние не должно превышать 125 м для 1000Base-CX и 250 м для гигабитного Ethernet на неэкранированной UTP (1000Base-T).

Собственно говоря, некоторые аналитики склонны относиться к гигабитному Ethernet с изрядной долей скептицизма. Это связано с тем, что, во-первых, этой технологии присущи те же самые недостатки, что и старшим, определяемые неизменностью принципа «борьбы за среду». Кроме того, ни в одной из сетей Ethernet невозможно управление качеством обслуживания, что в среде с разноскоростными потоками может стать серьезной проблемой.

10 Гбит — это уже не фантастика

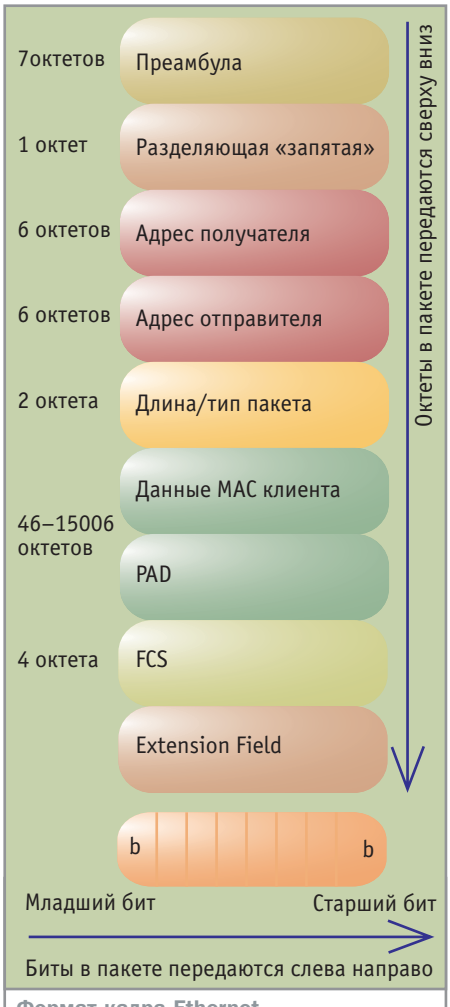
На закате прошлого тысячелетия, а именно в 1999 году, состоялось первое заседание инициативной группы по разработке десятигигабитного Ethernet — 10GEA (10 Gigabit Ethernet Alliance). И снова первая в списке участниц — неугомонная 3Com. Основной целью создания очередной реинкарнации Ethernet стала попытка переноса технологий LAN в инфраструктуру сетей более высокого уровня. Закончилось все это весьма достойной реализацией, получившей наименование IEEE 802.3ae.

Сегодняшняя основа для 10 Gigabit Ethernet — оптоволоконный кабель, который, кстати, пришлось модифицировать специально для новой скоростной технологии. Несмотря на почти полугодовую задержку от анонсированного выхода спецификации, компании-производители сумели представить на рынок отдельные модули для работы по новому стандарту, переведя почти фантастическую скорость передачи данных в реальную плоскость. Несмотря на то что в самом стандарте речь идет лишь об оптоволокне, сегодня уже опубликованы исследования, которые доказывают возможность достижения десятигигабитной скорости и на витой паре. Для »

этого необходимо, чтобы вся существующая кабельная структура была переведена на UTP категории 6. По оценкам экспертов, это произойдет примерно к 2005 году.

Скоро ли финал?

30 лет Ethernet по меркам современных темпов развития IT-технологий — это не просто срок, это целая эпоха. За это время базовая технология построения современных сетей изменилась настолько, что даже сами ее разработчики признают, что от изначального Ethernet осталось очень мало. Во-первых, для обеспечения качества обслуживания и безопасности соединений модифицирован формат Ethernet-кадра.



Формат кадра Ethernet

Во-вторых, «базовая» CSMA/CD в сегодняшних высокоскоростных сетях имеет совершенно иной алгоритм работы. Может быть, единственное, что осталось относительно неизменным, — электрические характеристики сигналов.

Тем не менее эпоха Ethernet окончится еще нескоро. Даже несмотря на серьезную конкуренцию со стороны беспроводных коммуникаций, эфирная сеть была и остается «рабочей лошадью» малых сетей.

Егор Леонидов

Дополнительная информация

Альтернативы Ethernet

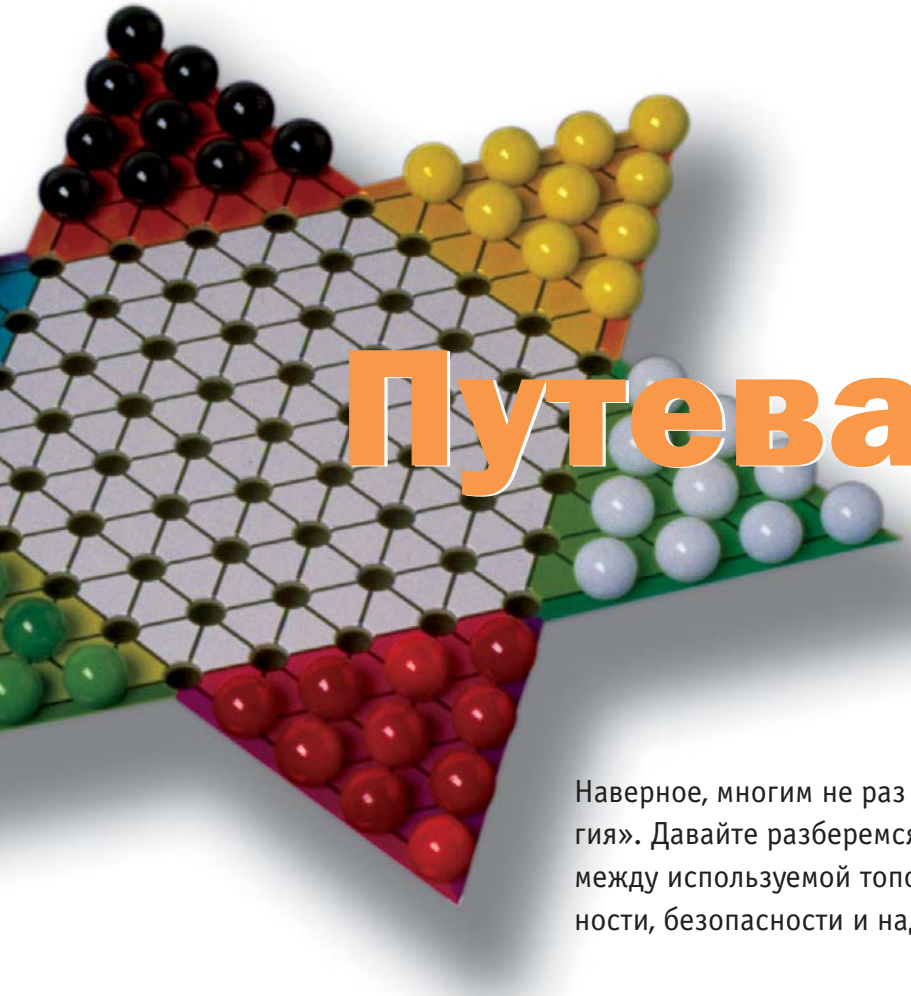
TokenRing. Появившаяся одновременно с Ethernet технология довольно долгое время была одним из основных конкурентов. Идея состояла в том, чтобы в сети, выполненной по топологии «кольцо», от узла к узлу передавался определенный набор битов (маркер), называемый token. Каждая станция принимает маркер, удерживает некоторое время и, если в текущий момент у нее нет необходимости отправлять данные, передает его дальше. Если же необходимо инициировать передачу, то станция модифицирует маркер в метку начала передачи и начинает посылку. Станция-получатель, дождавшись начала потока данных, принимает их, однако пакеты продолжают свой путь, пока не достигнут станции-отправителя, которая, убедившись, что пакет был принят, уничтожает его. Максимальная скорость передачи составляет 4 Мбит/с в соответствии с IEEE 802.5, однако на заключительном этапе развития существовали реализации, в которых скорость была увеличена до 16 Мбит/с.

FDDI (Fiber Distributed Data Interface). Появившаяся в 1980 году технология связи по оптоволоконному кабелю была предназначена для высокоскоростного обмена данными. В качестве среды передачи использовалось двойное кольцо, которое могло охватывать расстояния до 100 км по периметру. Технология напоминает TokenRing — тут тоже используется механизм передачи маркера, но внутри канала FDDI может быть организовано два вида трафика: синхронный, полоса пропускания которого выделялась для непрерывно передающих станций, и асинхронный, передача которого регламентировалась восьмиуровневой системой приоритетов.

Apple Talk, Local Talk. Компания Apple, которая всегда и во всем стремится поступать по-своему, в начале 80-х годов разработала свой стек протоколов, который, естественно, работал лишь на оборудовании того же производства. Малая пропускная способность Apple Talk (246 Кбит/с) некоторым образом компенсировалась возможностью работы практически с любой технологией организации канала — от витой пары (правда, экранированной) до оптоволокна. В настоящее время сетевая аппаратура Apple использует расширенный стек протоколов Apple Talk Phase II, в котором реализованы некоторые дополнительные возможности.

ATM (Asynchronous Transfer Mode). Отличие этой технологии состоит в том, что она единственная работает с применением подтверждения установки соединения. Перед началом передачи специальными процедурами устанавливается виртуальный канал отправитель-получатель, который не может быть использован другими станциями. Одновременно в одном физическом канале могут существовать несколько виртуальных. Передача происходит с помощью небольших (53 байта) пакетов, которые называются ячейками. Взаимодействие осуществляют коммутаторы, производящие управление с помощью таблиц, в которые заносятся номер порта и идентификатор соединения.

NETW



Топологии

Путевая карта

Наверное, многим не раз приходилось слышать термин «топология». Давайте разберемся, каково же его значение, какая связь между используемой топологией и ее параметрами производительности, безопасности и надежности и какую топологию выбрать.

Топология (от греч. topos — «место» и logos — «учение») — это раздел математики, посвященный изучению феномена непрерывности (выражающегося, например, в понятии предела). Можно сказать, что топология изучает способы соединения различных сущностей между собой. Для топологии не имеют значения размер и форма этих сущностей, а важно только то, каким образом они могут быть соединены друг с другом. Применительно к компьютерным сетям под термином «топология» подразумеваются различные виды соединений компьютеров между собой.

Типы сетевых топологий

Топологии компьютерных сетей можно описывать как с физической, так и с логической точек зрения. Физическая топология описывает геометрическое расположение компонентов компьютерной сети. Однако она отнюдь не является картой сети, а представляет собой всего лишь теоретическую конструкцию, которая графически передает форму и структуру сети. Логическая топология описывает возможные соединения между парами конечных точек сети, находящимися в состоянии взаимодействия между собой. Эта информация оказывается полезной при описании наборов конечных точек, которые могут взаимодействовать друг с другом, и при определении наличия прямых физических соединений между парами конечных точек.

В локальных компьютерных сетях существует три основных типа сетевых топологий — шина, звезда и кольцо. В сетях с небольшим количеством узлов могут использоваться и другие топологии (например, полносвязная топология, где все узлы сети соединены между собой), однако в современных компьютерных сетях используются исключительно три вышеперечисленные топологии и их производные или сочетания.

Используемая топология зависит от физической технологии, на базе которой строится локальная сеть. Например, в сетях на базе технологии TokenRing, первоначально разработанной компанией IBM в 1970 году и до сих пор являющейся очень распространенной, по определению должны использоваться кольцевые топологии. Но на практике обычно применяется звездообразное соединение, причем все конечные устрой- »

ства подключаются к так называемому «устройству доступа к многостанционной сети» (MSAU). Так что при выборе топологии необходимо ознакомиться с документацией на используемые сетевые технологии, чтобы не оказаться в ситуации, когда эффективность работы сети будет крайне низкой.

Логические топологии

Логическая топология определяет реальные пути движения сигналов при передаче данных по используемой физической топологии. Таким образом, логическая топология описывает пути передачи потоков данных между сетевыми устройствами. Она определяет правила передачи данных в существующей среде с гарантированием отсутствия помех, влияющих на корректность передачи.

Поскольку логическая топология описывает путь и направление передачи данных, она тесно связана с уровнем MAC (Media Access Control) модели OSI (подуровень канального уровня). Для каждой из существующих логических топологий существуют методы контроля доступа к среде передачи данных, позволяющие осуществлять мониторинг и контроль всего процесса.

В настоящее время существуют три базовые логические топологии: логическая шина, логическое кольцо и логическая звезда (коммутация). Каждая из этих топологий обеспечивает преимущества в зависимости от способов использования.

В настоящей статье мы будем говорить в основном о физических топологиях. Необходимо помнить, что в одной и той же сети могут использоваться разные физическая и логическая топологии (например, физическая звезда и логическая шина).

Шинная топология

Начнем с наиболее простой шинной топологии, которую также называют линейной шиной или магистральной топологией и которая является одной из наиболее распространенных. В ней используется один кабель, именуемый шиной (иногда также называемый магистралью или сегментом), куда подключены все компьютеры сети. В сети с топологией «шина» компьютеры адресуют данные конкретному компьютеру, передавая их по кабелю в виде электрических сигналов. В некоторых шинных технологиях используется более одного кабеля, то есть они в состоянии поддерживать больше одного канала, хотя каждый кабель по-прежнему остается одним каналом передачи.

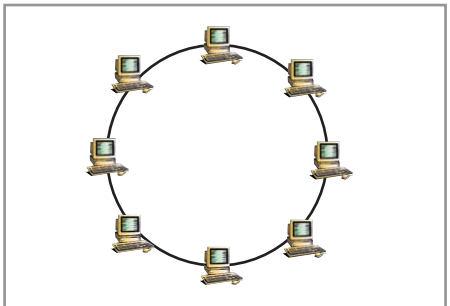
На концах кабеля должны быть согласующие резисторы, предотвращающие отражение сигналов. Когда станция сети передает сигнал в кабель, этот сигнал распространяется в обоих направлениях. Если согласующий резистор не установлен, то сигнал, достигая конца шины, изменяет свое направление и двигается к противоположному концу. В результате одна передача может полностью захватить всю полосу пропускания сети и препятствовать передаче данных другими станциями.

В типичной шинной топологии используется единственный кабель, не требующий установки внешних устройств (например, концентраторов) и соединяющий все узлы сети как равноправные устройства. В шинной топологии данные в виде электрических сигналов передаются всем компьютерам сети; однако информацию принимает только тот компьютер, адрес которого соответствует адресу получателя, зашифрованному в этих сигналах, причем в один момент времени передачу вести может только один компьютер. В связи с этим производительность сети зависит от количества компьютеров, подключенных к шине. Чем больше компьютеров, ожидающих передачи данных, тем медленнее сеть. Однако кроме числа компьютеров на быстродействие сети влияют и некоторые другие факторы, в том числе:

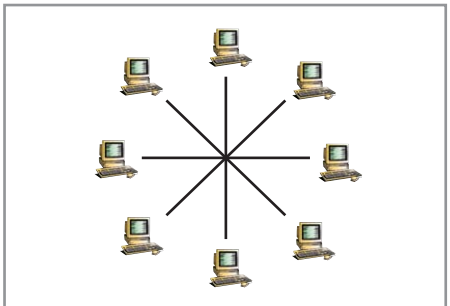
- характеристики аппаратного обеспечения компьютеров в сети;
- частота передачи данных компьютерами;
- тип используемых сетевых приложений;
- тип сетевого кабеля;
- расстояние между компьютерами в сети.

Шина — пассивная топология. Это значит, что компьютеры только слушают передаваемые по сети данные, но не участвуют в их перемещении от отправителя к получателю. Поэтому, если один из компьютеров выйдет из строя, это не скажется на работе остальных.

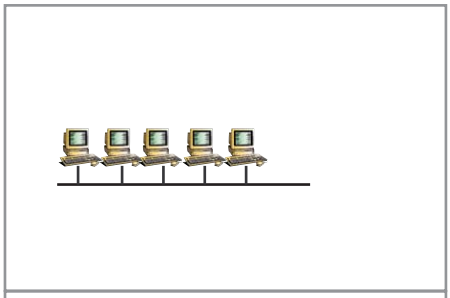
В связи с физическими ограничениями шинной топологии ее целесообразно использовать только в небольших локальных сетях. К числу достоинств шинной топологии можно отнести низкую стоимость и простоту подключения новых узлов. Основной сферой ее применения являются недорогие одноранговые сети. В 100-мегабитных и более высокоскоростных сетях эта топология не применяется, поскольку в число ее недостатков входят низкая производительность, слабая надежность и сложность диагностики. Основным же минусом является то, что при разрыве или повреждении сетевого кабеля из строя выходит вся сеть. Компьюте-



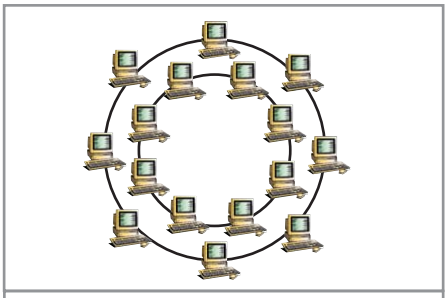
Топология «кольцо»



Топология «звезда»



Топология «шина»



Топология «двойное кольцо»

ры останутся работоспособными, но передача данных между ними будет невозможна.

Хотя в настоящее время шинная топология нечасто используется при создании локальных сетей, у нее все же есть свое применение. Именно на этой топологии основано соединение большинства системных компонентов и периферийных устройств во внутренней архитектуре компьютера (за исключением устройств на базе шины USB).

Звездообразная топология

Локальные сети звездообразной топологии объединяют устройства сети, которые как бы расходятся из центрального узла. Многие говорят о топологии «звезда», имея в виду физическое звездообразное расположение компьютеров, притом что реальная топология не имеет с этим ничего общего. В качестве центрального узла в сетях звездообразной топологии выступают концентратор или коммутатор. Топология определяет не географическое расположение компьютеров, а пути и порядок прохождения данных. Звезда отличается тем, что не предоставляет возможности двум компьютерам в сети обмениваться данными иначе, чем с помощью центрального узла, выступающего посредником.

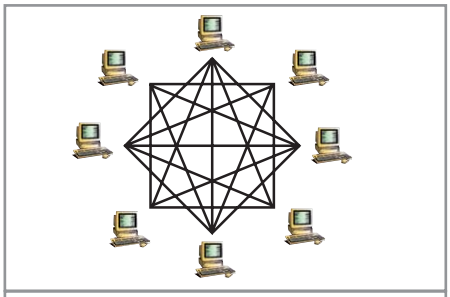
В сетях с топологией «звезда» подключение кабеля и управление конфигурацией сети централизованы. Но есть и недостаток: так как все компьютеры подключены к центральному узлу, для больших сетей значительно увеличивается расход кабеля. К тому же, если центральный узел выйдет из строя, нарушится работа всей сети, поскольку он всегда участвует в обмене данными между двумя компьютерами. Данные компьютера-отправителя сначала достигают центрального узла, а лишь затем транслируются последним компьютеру-получателю. На первый взгляд данная топология кажется не слишком удобной, однако в данном случае несколько компьютеров в сети могут вести передачу данных одновременно, в то время как шинная и кольцевая топологии в каждый момент времени выделяют только один компьютер, которому позволено передавать данные.

В топологии «логическая звезда» используется метод коммутации, обеспечивающий ограничение распространения сигнала в среде передачи в пределах некоторой ее части. Механизм такого ограничения является основополагающим в топологии «логическая звезда».

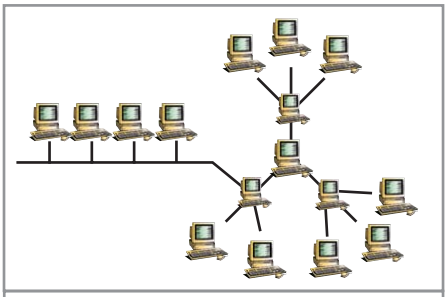
В чистом виде коммутация предоставляет выделенную линию передачи данных каждой станции. Когда одна станция передает сигнал другой, подключенной к тому же самому коммутатору, то коммутатор передает сигнал только по среде передачи данных, соединяющей эти две станции. При таком подходе возможна одновременная передача данных между несколькими парами машин, так как данные, передающиеся между любыми двумя станциями, остаются «невидимыми» для других пар станций.

Звездообразные топологии стали ведущим типом топологий в современных локальных сетях. Причиной их популярности являются гибкость, масштабируемость и невысокая стоимость. В число преимуществ сетей звездообразной топологии также входят более высокая пропускная способность и отказоустойчивость по сравнению с шинной и кольцевой топологиями, удобство подключения новых устройств, возможность использования коммутаторов вместо концентраторов и легкость создания подсетей. Из недостатков звездообразной топологии стоит отметить зависимость работоспособности сети от состояния центрального узла (повреждение центрального узла выводит из строя всю сеть), большой расход кабеля и более высокая стоимость по сравнению с шинной топологией.

В последние годы появился еще один пример сети со звездообразной топологией. Это универсальная последовательная шина (Universal Serial Bus, USB). В случае с USB мы имеем не чистую звезду, а ветвящееся дерево, в котором сигнал от каждого устройства в конце концов доходит до корневого концентратора. Кабельная схема в USB тоже особенная: одна витая пара



Полносвязная топология



Гибридная топология

» для данных, а другая — для питания управляемых устройств.

Кольцевая топология

Сети с кольцевой топологией представляют собой одноранговые сети, где каждый компьютер подключается к общему сетевому кабельному кольцу, по которому передаются данные, и функционирует как повторитель, принимая и отвечая на адресованные ему пакеты. Основным принципом передачи данных в сетях с кольцевой топологией является передача маркера. Этот принцип заключается в последовательной передаче маркера от одного компьютера к другому до тех пор, пока его не получит компьютер, который хочет отправить данные. Компьютер-отправитель изменяет маркер, помещает в данные электронный адрес компьютера-получателя и посылает их по кольцу.

Данные проходят через несколько компьютеров, пока не достигнут того, чей адрес совпадает с адресом получателя. После этого принимающий компьютер посылает передающему сообщение, в котором подтверждает прием данных. Получив подтверждение, передающий компьютер создает новый маркер и возвращает его в сеть. Передача маркера не отнимает много времени и практически не влияет на пропускную способность сети. Кольцо, в котором циркулирует маркер, может иметь размер от нескольких сантиметров до нескольких километров. В первом случае аппаратура кольца сосредоточена в пределах одной платы в небольшом корпусе, к портам которого с помощью кабелей подключаются узлы сети.

Основным преимуществом кольцевой топологии является отсутствие потери сигнала, а недостатками — низкая отказоустойчивость и необходимость разрыва сети для добавления новых узлов. Таким образом, кольцевую топологию можно применять при создании надежных высокоскоростных сетей, расширение которых не планируется.

Выбор топологии

Итак, какую же топологию выбрать? Во-первых, выбор топологии зависит от требований. Если вы собираетесь создать сеть из »

Дополнительная информация

Лучшие производные

Расширенная звездообразная топология

В расширенной звездообразной топологии рабочие станции подключаются к нескольким концентраторам, которые, в свою очередь, подключаются к одному центральному коммутатору. Очевидными достоинствами такой топологии являются экономия кабеля, поддержка большего числа узлов (по сравнению с простой звездообразной топологией) и более высокая отказоустойчивость (при выходе из строя центрального узла остальные концентраторы продолжают работать в локальном режиме, а при выходе из строя одного из концентраторов остальные по-прежнему остаются объединенными в сеть). Недостатками такой топологии являются высокая цена и невозможность использования более четырех концентраторов без применения коммутации (согласно правилу, по которому количество повторителей между двумя узлами не может превышать четырех).

Двукольцевая топология

Как видно из названия, эта топология представляет собой два кольца, первое из которых является основным, а второе используется только при сбое на первом. Преимуществом такой топологии является более высокая отказоустойчивость, главным недостатком — высокая стоимость и больший расход кабеля.

Иерархические топологии

Сети, в которых реализована кольцевая топология, могут быть расширены путем иерархического соединения нескольких колец без снижения их производительности. Вместо кольцевой топологии в качестве топологии второго уровня может использоваться звездообразная или шинная топология. Иерархические топологии применяются для построения крупных сетей и объединения мелких локальных сетей в одну. В них обычно используются такие сетевые устройства, как концентраторы, коммутаторы или мосты.

Смешанные топологии

Сети со смешанной топологией состоят из соединенных между собой сетей с разными топологиями. В качестве примеров можно привести некоторые глобальные и региональные сети и, разумеется, Интернет.

Полносвязная топология

В этой топологии все узлы сети соединены друг с другом, что обеспечивает максимальную скорость передачи данных, чрезвычайно высокую отказоустойчивость и огромное количество возможных путей для передачи данных от одного узла другому. К сожалению, такие сети являются наименее распространенными (за исключением варианта сети из двух компьютеров), это связано с большим расходом кабелей и серьезным ограничением общего количества узлов сети (зависит от количества портов). Такая топология может применяться на высоких уровнях иерархии для обеспечения максимально отказоустойчивых соединений между концентраторами и коммутаторами.

» пяти компьютеров, то можете использовать полносвязную или шинную топологию, однако для сети из ста компьютеров такой вариант уже не подойдет, и вам придется прибегнуть к иерархической системе. Во-вторых, выбор топологии зависит от имеющихся ресурсов. Наиболее производительные и отказоустойчивые схемы обычно являются и более дорогими в связи с большим количеством кабелей и дополнительных устройств. Повышение производительности обеспечивается и за счет использования коммутаторов вместо концентраторов, поскольку коммутаторы обладают значительно более широкими возможностями обработки данных. Однако стоимость коммутаторов на несколько порядков выше. И, естественно, выбор топологии зависит от используемых сетевых технологий. Например, сети Ethernet 10Base-T относятся к звездообразной топологии. Таким образом, прежде чем выбрать топологию, необходимо определиться с требованиям к размеру сети, подсчитать финансовые ресурсы и определить технологию, на базе которой будет построена сеть.

■ ■ ■ Иван Новоселов

Преимущества и недостатки основных сетевых топологий

Название топологии	Преимущества	Недостатки
Шинная топология	Низкая стоимость Простота добавления новых узлов Не требуется концентратор и другое оборудование	Низкая производительность Низкая надежность Сложность диагностики при разрыве кабеля или отказе разъема Повреждение кабеля в любом месте выводит из строя всю сеть При необходимости одновременной передачи данных несколькими компьютерами сильно падает скорость Отсутствие промежуточного усиления сигнала Ограниченный размер сети
Звездообразная топология	Более высокая пропускная способность по сравнению с шинной топологией Выход из строя одного узла не влияет на работоспособность сети Легкость подключения в сеть новых узлов Возможность использования коммутатора вместо обычного концентратора Удобная диагностика	Зависимость работоспособности от состояния концентратора Высокий расход кабеля Более высокая стоимость по сравнению с шинной топологией Ограниченное расстояние между компьютером и концентратором
Расширенная звездообразная топология	Экономия кабеля Поддержка большего числа узлов, чем в звездообразной топологии Более высокая отказоустойчивость, чем в звездообразной топологии	Более высокая стоимость, связанная с приобретением дополнительных концентраторов Невозможность использования более четырех концентраторов без применения коммутаторов
Кольцевая топология	Отсутствие потери сигнала	Низкая отказоустойчивость Необходимость разрыва сети для добавления новых узлов
Двукольцевая топология	Более высокая отказоустойчивость по сравнению с кольцевой топологией	Более высокая стоимость Больший расход кабеля
Полносвязная топология	Максимальная скорость передачи данных Максимальная отказоустойчивость Максимальное количество путей между двумя узлами	Высокая стоимость Большой расход кабеля Ограниченное количество компьютеров (в связи с ограничением количества портов)

Сетевой Вавилон

В период становления сетевых технологий казалось, что для построения распределенных сетей необходимо лишь спроектировать железо и придумать схему его взаимодействия. Позже выяснилось, что на этом пути никто не может существовать в одиночку. Более того, пришло глубокое понимание бесполезности одной отдельно взятой сети.

Появление, развитие и победное шествие семейства протоколов TCP/IP, связавших разрозненные сети в единое технологическое пространство, стало основой для реализации нижних уровней сетевой модели ISO-OSI. После того как вокруг TCP/IP сложилась технологически единая сеть, верхний прикладной уровень стал диктовать необходимость создания единообразных языков сетевого пользовательского взаимодействия. Такие языки, по традиции называемые протоколами, по сути своей принципиально отличаются от того же семейства TCP/IP, поскольку описываемые ими механизмы взаимодействий являются лишь набором правил, которые разные приложения могут реализовывать по-своему. Например, в соответствии с известным всем протоколом HTTP первая строка любого HTML-документа должна иметь вид <!DOCTYPE HTML PUBLIC «-//W3C //DTD HTML 4.0 Transitional//EN»>. Однако, как показывает практика, разработчики web-сайтов очень часто этим пренебрегают. Несмотря на это, такие документы все равно открываются и обрабатываются браузерами. Проще говоря, прикладные протоколы, с одной стороны, являются лишь отражением сложившегося уровня сетевого сервиса, а с другой — сами же этот уровень и определяют.

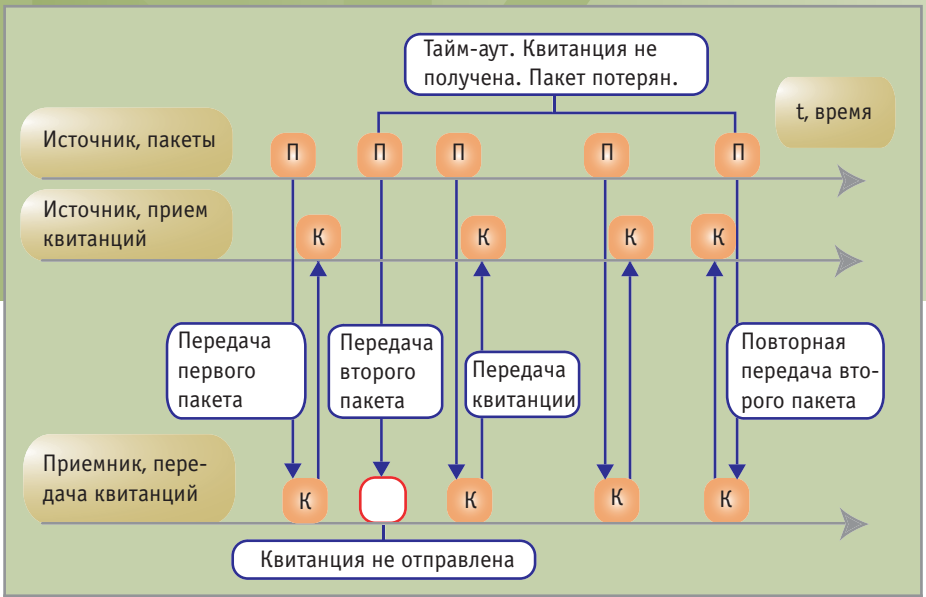
При этом нельзя не отметить, что все уровни сетевой модели тесно связаны между собой. Поэтому начинать путешествие по сетевым протоколам надо с самого начала.

От среды передачи к TCP/IP

Самое нижнее звено сетевой модели ISO-OSI — среда передачи. Компьютеры могут быть соединены между собой не только классической витой парой, но и коаксиальным проводом, оптоволокном, а могут вообще иметь беспроводное сообщение. Во всех случаях среда передачи существует и служит именно для организации передачи данных на физическом уровне.

Сетевой уровень находится на один пункт выше уровня физической среды и отвечает за организацию взаимодействия в данной среде передачи. На сетевом уровне присутствуют, например, средства реализации технологий Ethernet, TokenRing, Radio Ethernet и т. п. Межсетевой уровень, как видно из названия, отвечает за взаимодействие между различными сетями. Именно на этом уровне расположен протокол IP (Internet Protocol), давший наименование всей Глобальной сети. И на нем же существует один из самых удивительных парадоксов современного Интернета.

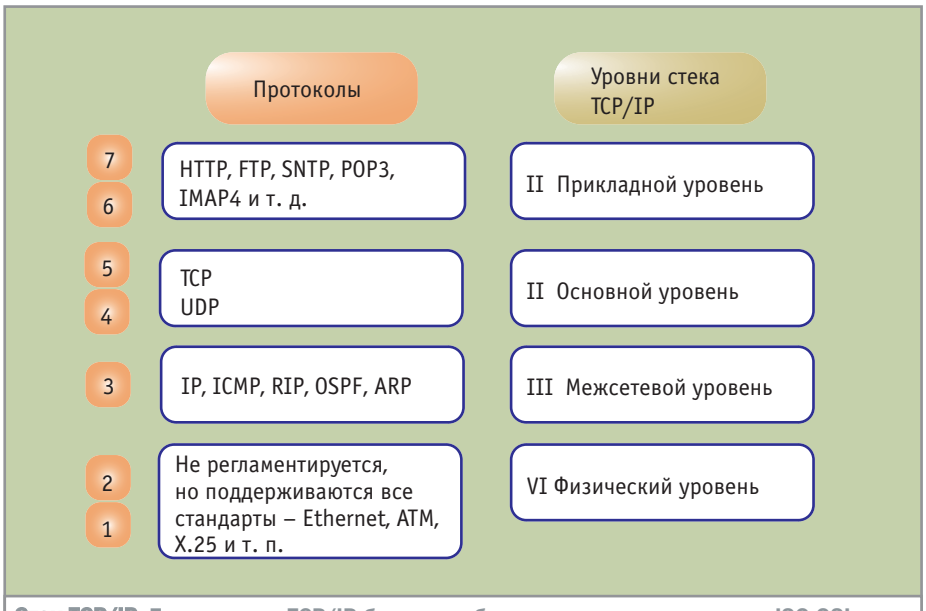
Дело в том, что протокол IP не является средством надежной связи. Это озна- »



Протокол TCP.
Метод подтверждения корректности передачи кадров с использованием тайм-аута

» чает, что, хотя пакеты информации передаются от узла-источника к узлу-получателю, гарантии доставки не существует. Для разрешения этого парадокса существует протокол TCP (Transmission Control Protocol), который призван осуществлять надежную доставку информации, но уже на более высоком транспортном уровне. Таким образом, именно связка TCP/IP является основным механизмом доставки данных, который, кроме всего прочего, еще и не зависит от физической среды передачи.

Однако средства ненадежной доставки тоже нашли свое применение. Протокол UDP (User Datagram Protocol) транспортного уровня в принципе призван исполнять примерно те же функции, что и TCP, однако при использовании UDP в качестве средства доставки информационные пакеты могут быть утеряны, продублированы или прийти не в том порядке, в котором были отправлены. Кроме IP специалисты располагают на межсетевом уровне и протоколом ICMP, который, являясь расширением IP, отвечает за обмен служебной информацией и сообщениями об ошибках.



Стек TCP/IP. Так как стек TCP/IP был разработан до появления модели ISO-OSI, то соответствие уровней стека TCP/IP уровням модели OSI достаточно условно

И, наконец, самым высоким уровнем модели ISO-OSI является прикладной, с различными реализациями которого и встречаются пользователи в своей повседневной работе. Именно эти протоколы определяют сегодня лицо Глобальной сети.

В начале великих дел

Некоторые историки Интернета и просто пользователи с большим стажем склонны считать протокол FTP (File Transfer Protocol) источником и прародителем всего интернет-сообщества. Отчасти так оно и было. По крайней мере, в самом начале, когда FTP-серверы выступали в качестве единственного хранилища информационных ресурсов. В сегодняшнем сетевом мире роль FTP несколько изменилась. Теперь в качестве основного источника информации выступает WWW, а FTP-серверы всемирно используются как файловые хранилища.

FTP корнями уходит в системы Unix, поэтому самый простой FTP-клиент, способный принимать и передавать данные, может быть реализован в виде консольного приложения, которое кроме собственно соединения должно уметь выполнять еще две команды — GET (получить файл) и PUT (послать файл). Примерно так и работал протокол FTP в самом начале своей истории. Несколько позже в нем появились средства аутентификации. Потом — реализация возможности докачки при неожиданном обрыве соединения. С распространением графических оболочек появились и оконные FTP-клиенты, для пользования которыми не требовалось знание внутренних FTP-команд, а сама работа была похожа на работу со стандартным Проводником Windows.

Сегодня протокол FTP можно считать одним из трех китов (наряду с WWW и почтовыми протоколами), на которых базируется современный Интернет.

WWW — бестолковое информационное хранилище

Несмотря на то что первые верхние протоколы (FTP, Gopher) появились практически одновременно с нижними, их катастрофически не хватало для того, чтобы Сеть стала по-настоящему глобальной.

Концепция WWW-сервера и клиента была первоначально разработана в Европейском центре ядерных исследований (CERN). »

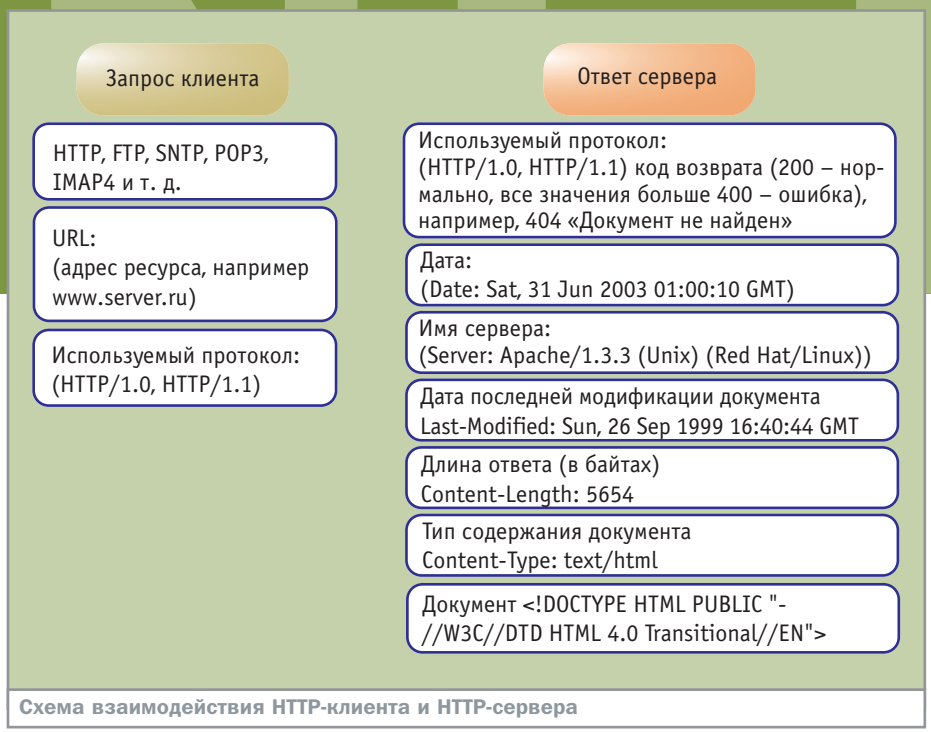


Схема взаимодействия HTTP-клиента и HTTP-сервера

» Это, конечно, никак не снижает ни актуальности, ни исторической и технологической ценности этого открытия, поскольку именно WWW практически стер разницу в географическом расположении того или иного объекта. Глобальная мировая паутина сделала из сугубо технологичного и закрытого Интернета всеобщую систему с открытым доступом для всех желающих.

Основная идея протокола «гипертекста» (HTTP, Hyper Text Transfer Protocol) — глобальная связанность. Любое место любого документа может быть привязано к любому другому месту любого другого документа. С этой концепцией связано определение универсального идентификатора ресурса — URI (Universal Resource Identificator), который абсолютно однозначно указывает на уникальную страницу, расположенную в Сети, или на любое место этой страницы.

При этом за кадром остаются маловажные для конечного пользователя технические подробности: IP-адрес, характеристики сервера и даже его географическое расположение. Все это определило особый имидж WWW у пользователей. Сегодня даже малые дети знают, что Интернет — это, во-первых, большое хранилище информации, которая физически может быть расположена в любом месте Земли, а во-вторых, это хранилище совершенно децентрализованно и для неискушенного взора предстает большой информационной помойкой.

А между тем в протокол HTTP с самого его рождения были встроены средства, которые облегчают и поиск, и структурирование информации. В первую очередь это касается клиент-серверного механизма, который подразумевает один ответ на один запрос. Именно это вместе с поддержкой внешних программ и скриптов (CGI — Common Gateway Interface) дало возможность разработчикам создать промежуточные языки web-программирования (PHP, ASP и т. д.), которые, в свою очередь, смогли заставить работать в Сети системы управления базами данных. Именно приход в Сеть средств работы с СУБД стал основой для появления поисковых машин, которые взяли на себя роль библиотек, хранящих не сами данные, а лишь ссылки, которые на эти данные указывают.

Получите почту!

По личному опыту могу сказать, что почтовый трафик составляет от 30 до 65% всего трафика, если ориентироваться на информационные потребности малого и среднего офиса. Можно сказать даже больше — некоторые пользуются Интернетом только для того, чтобы получать и оправлять электрон- »

Точка входа

Процессы и порты

Основное отличие транспортного уровня от межсетевого — организация связи не между сетевыми узлами, а между пользовательскими процессами. Каждый такой процесс может существовать отдельно в рамках операционной системы и взаимодействовать посредством специально организованных системных очередей, имеющих свою точку входа. Такие очереди называются портами и в прикладных программах обозначаются цифрами от 1 до 65 535. Наиболее распространенные сетевые сервисы получили от организации Assigned Numbers Authority навечно закрепленные номера портов. Например, порт 21 закреплен за протоколом FTP, порт 80 — за HTTP, порт 25 — за SMTP, порт 110 — за POP3. Полный список портов и закрепленных за ними сервисов можно найти в Интернете, хотя серьезные операционные системы (то есть практически все, кроме Windows 98) имеют в составе своих дистрибутивов соответствующие текстовые документы.
Общее количество широко известных портов не превышает двух сотен. Остальные порты могут использоваться прикладными локальными процессами совершенно свободно, чем и пользуются разработчики различного сетевого софта. В качестве примера можно порекомендовать читателю поэкспериментировать с настройками любого из существующих прокси-серверов. Каждому из сервисов, которые поддерживаются подобной программой, может быть назначен практически любой порт. Исключение составляют те порты, которые уже заняты иными сервисами. Для получения текущей картины занятых и свободных портов можно использовать, например, команду netstat.

» ные почтовые сообщения. И дело тут даже не в том, что этот способ связи является довольно быстрым, ведь сегодня существуют более оперативные средства — ICQ, телеконференции, IP-телефония. Причина, как это ни парадоксально, состоит в том, что электронная почта (e-mail) стала сегодня наряду с телефоном и факсом традиционным средством коммуникаций. И поэтому в отношениях пользователей к электронной почте можно увидеть не только стремление к удобству, но и некоторую консервативность.

Кстати говоря, консервативность наблюдается и в почтовых протоколах. К «сладкой парочке» SMTP/POP3 лишь относительно недавно присоединился IMAP4, который по своим функциональным возможностям несомненно превосходит предшественника, однако его повсеместное распространение сильно тормозится. И причина этому — та же самая консервативность пользователей.

Эту консервативность сегодня с большим размахом используют те, кто занимается несанкционированными почтовыми рассылками, или спамом. Изначально протоколы передачи почты задумывались как простое и поэтому надежное средство. Ограниченного набора команд, присущего первым реализациям почтовых клиентов, вполне хватало для работы. Однако в тот момент, когда электронная почта начала становиться всеобщим средством связи, выяснилось, что именно простота и незащищенность почтовых протоколов позволяет использовать их в качестве инструментов для массовых рассылок. Чуть позже, когда спам приобрел черты стихийного бедствия, был разработан «расширенный» SMTP (ESMTP), который, однако, не получил широкого распространения, хотя практически все производители программных почтовых серверов включили его в состав своих продуктов.

IPv6: реинкарнация или новая жизнь?

Начиная примерно с середины 70-х годов прошлого века стек протоколов TCP/IP не претерпевал значительных изменений. А между тем Сеть, получившая благодаря универсальности и широкому распространению большую букву в своем названии, стала сама диктовать пользователям и разработчикам необходимость серьезных перемен.

В первую очередь это касалось пространства IP-адресов, которого с выходом в свет небольших беспроводных устройств стало катастрофически не хватать. Решить эту проблему применением «локальных» адресов (из сетей 10.0.0.0 и 192.168.0.0) принципиально возможно, но в этом случае будет нарушена связность и целостность глобального информационного пространства.

Кроме того, серьезным образом изменился и качественный состав сетевого трафика. Если раньше примерно половину трафика составляли простые сообщения небольшой длины, то сегодня в Сети работают в реальном времени тысячи радиоканалов и сотни телестанций. Новая версия IP-протокола (IPv6) призвана решить все эти проблемы и еще множество других, более мелких.

Самые важные характеристики протокола IPv6

- расширено адресное пространство
- улучшена поддержка иерархической адресации
- введены механизмы аутентификации и шифрования на уровне IP-пакетов
- упрощен стандартный заголовок IP-пакета
- изменено представление необязательных полей заголовка
- введены метки потоков данных
- поддержка многоадресной рассылки multicast (описана и специализирована)
- протокол остался расширяемым
- сохранена преемственность адресации

Новые IP-адреса будут иметь длину 128 бит; в заголовок IP-пакета добавятся поля, которые будут отвечать за управление качеством услуг, то есть каждый пакет сможет иметь разный приоритет отправки. Но самым главным преимуществом IPv6 станет то, что эта версия основного интернет-протокола будет иметь способность к расширению. И, может быть, именно это станет ступенькой, которая приведет к созданию по-настоящему глобальной сети, в которой каждый узел будет связан с другим, а информационное наполнение ляжет в основу мировой библиотеки. ■ ■ ■ Сергей Кондрашев

Почтовые протоколы

SMTP, POP3, IMAP4

Простой протокол доставки почты (Simple Mail Transfer Protocol) является, по сути, именно тем, что и сказано в его названии, а простым он называется потому, что имеет в своем арсенале всего восемь команд, из которых наиболее активно используются лишь шесть (HELO, MAIL, RCPT, DATA, QUIT и NOOP).

Процесс доставки почты заключается в том, что почтовый агент передачи сообщения (MTA — Message Transfer Agent) устанавливает прямое соединение с таким же агентом получателя и пересылает письмо. На стороне получателя письмо в соответствии с внутренними правилами переносится в почтовый ящик пользователя, который может забрать его оттуда с помощью протокола POP3 или IMAP4.

Протокол POP3 по своей простоте напоминает SMTP, однако в его состав включены дополнительные средства аутентификации. IMAP4, кроме того, позволяет прочитать заголовки почтовых сообщений непосредственно на сервере.

Неплохой вариант рабочего места сетевого администратора, но выпадает такое счастье совсем немногим

И закинул он невод

Построение сетей — процесс, к которому в той или иной степени имеет отношение каждый компьютерный специалист. Кому-то везет, и весь процесс рождения, становления и дальнейшего развития происходит при непосредственном его участии. Но в большинстве случаев сетевая инфраструктура становится тем, что существует де-факто, и речь, как правило, идет не о развертывании сети, а о ее модернизации.

Алгоритм планирования

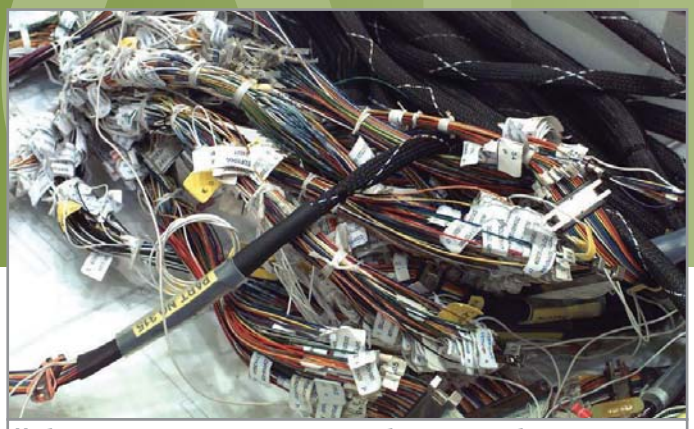
Несмотря на то что локальная сеть (LAN) как частный случай структурированной кабельной системы (СКС) — система весьма сложная, она, тем не менее, довольно проста в эксплуатации.

С чего начать

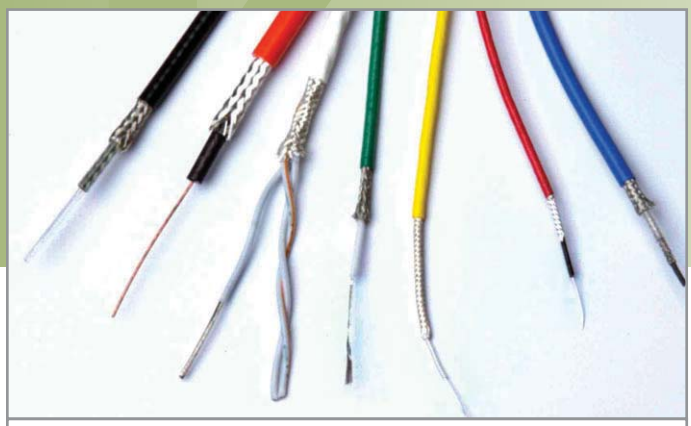
Как утверждают умные книжки и еще более умные пособия, сети должны рождаться не на местности, а «на кончике пера». Безусловно, так оно и должно быть. Более того, до тех пор пока на бумаге не будут проработаны все тонкости и нюансы, включая прямые затраты и затраты на поддержание работоспособности (в том числе на зарплату), начинать строить сеть не только нецелесообразно, но и экономически невыгодно. Что касается эксплуатационных расходов, несмотря на то что однажды настроенная сеть должна работать без вмешательства долгие годы, траты на ее сопровождение и поддержание работоспособности должны быть предусмотрены.

Но самым главный вопрос, который вы должны решить с самого начала, это вопрос «Зачем?» Несмотря на кажущуюся простоту ответа, необходимо в любом случае максимально детально его сформулировать, и лучше всего на бумаге. Цели, которые вы при этом себе поставите, будут в конечном итоге определять не только технологическое и топологическое построение локальной сети, но и последующий за ее развертыванием экономический эффект.

Например, если вы задумали развертывание подъездной локальной сети, то единст- »



Избыточное планирование сети избавит вас в будущем от прокладки дополнительных кабелей



За свою многолетнюю историю построение сетей породило большое количество сред передачи данных

венной вашей целью наверняка станет обеспечение совместного доступа к Глобальной сети. Любые прямые сетевые взаимоотношения между пользователями соседних квартир при этом могут быть вредны с точки зрения сетевой безопасности. Поэтому в таком случае и кабельную структуру, и системную поддержку целесообразнее создавать так, чтобы существенно минимизировать затраты.

Несколько иначе надо подходить к построению высокоскоростных и высокопроизводительных сетей. Здесь необходимо исходить в первую очередь из соображений эффективной сетевой организации и делать ставку на оборудование единого производителя. Конечно, стоимость затрат на построение подобной сети может быть на порядок (или даже несколько порядков) выше, нежели в случае с простой офисной или домашней сетью. Но коммуникации сегодня — это не та отрасль, на которой стоит экономить. Пройдет совсем немного времени, и вы увидите, насколько быстро окупаются ваши вложения.

А теперь нарисуйте подробный план

После первоначального определения целей и задач планируемой (или модернизируемой) сетевой инфраструктуры вам необходимо подробно прорисовать примерный план расположения рабочих станций. В самом простом случае, когда надо объединить в сеть два компьютера, можно просто соединить напрямую две сетевые карты с помощью crossover-соединения. Понятно, что в этом случае этап проектирования и подробной прорисовки можно опустить. Однако, даже если вы соединяете две свои домашние машины, нет никакой гарантии, что завтра любимая бабушка не подарит вам мощнейший ноутбук, что принесет, помимо радости, еще и головную боль при объединении всех машин.

Примерно то же самое, ну, может, за исключением любимой бабушки, происходит и в большинстве офисов молодых компаний. Машинный парк растет, а существующие сети не могут обеспечить необходимой производительности. Поэтому самый правильный подход заключается в том, чтобы планировать сеть с избытком. Кстати говоря, практика показывает, что прокладка дополнительных кабелей поверх уже существующих обходится примерно на 50–70% дороже. То есть всегда надо предусматривать не только достаточное число рабочих мест и сетевых портов, но и избыточное количество кабельных каналов.

Особо стоит обратить внимание на то, что кабельные системы любых сетей разделяются на вертикальные и горизонтальные составляющие части. Например, в случае локальной сети одного подъезда горизонтальная часть — это коммуникации между рабочими станциями и центральным этажным узлом, а вертикальная часть — соединения самих узлов. При этом важно помнить, что вертикальная часть такой кабельной системы должна быть более скоростной, нежели горизонтальная.

Другой альтернативы нет

Ситуация с технологиями построения сетей сегодня довольно парадоксальна. С одной стороны, на рынке можно найти любые, даже самые экзотические сетевые технологии, например беспроводные сети или сети на FireWire (IEEE 1394). С другой же стороны, поискав и взвесив не только соотношение стоимость/производительность, но и другие немаловажные факторы (минимально и максимально допустимое рабочее расстояние, возможность быстрой модернизации, помехозащищенность и отказоустойчивость), пользователь в девяти случаях из десяти придет к сетям Ethernet.

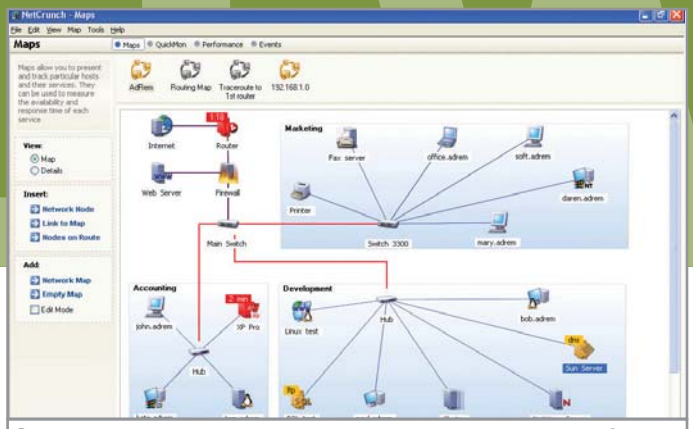
Немаловажную роль в этом выборе сыграет еще и то, что именно Ethernet сегодня является наиболее распространенным на планете сетевым стандартом. При этом основной его недостаток — «коллизионный» способ организации сетевого доступа — абсолютно нивелируется высокой скоростью работы и простотой развертывания. Более того, сети Ethernet удобны еще и тем, что модернизация их структуры (в том числе и кабельной) очень и очень проста. Необходимо лишь выбрать наиболее оптимальную для каждого конкретного случая среду передачи.

Витая пара или что?

Вообще говоря, в случае с Ethernet у любого пользователя есть выбор из трех вариантов среды передачи. Речь идет о витой паре (неэкранированной или экранированной), коаксиальном кабеле (толстом или тонком) и оптоволокне. Оптоволокно, по большому счету, необходимо использовать лишь там, где без него не обойтись. Основная область его применения — магистральные каналы. Однако оптоволоконные вертикальные кабельные структуры можно встретить и в сетях некоторых крупных офисных зданий. Тем не менее оптоволокно даже сегодня удовольствие достаточно дорогое.

Что же касается коаксиального кабеля, причем наиболее популярной его разновидности — «тонкого» коаксиала (стандарт Ethernet 10Base-2), то несмотря на моральное устаревание, сети, построенные на его основе пять и более лет назад, продолжают успешно работать и по сей день. Однако если вам доведется получить в свое распоря-

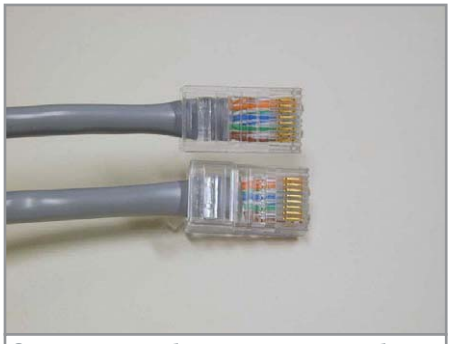
Оптоволоконное соединение оправдывает свою стоимость лишь там, где необходима действительно высокая скорость



Создание сети «на кончике пера» можно воспринимать буквально или воспользоваться специальными программами

» жение подобную сеть, считайте, что вам крупно повезло. Даже несмотря на то что подключение нового узла к такой сети — процесс очень быстрый, вам вряд ли удастся избежать проблем, связанных с нарушением целостности сети. На моей памяти есть несколько случаев, когда работа всей организации останавливалась лишь из-за того, что добросовестная уборщица задевала шваброй один из сетевых разъемов, а в результате вся сеть оказывалась неработоспособной. Ваша же удача состоит в том, что вам как новому специалисту будет гораздо проще убедить начальство в необходимости глобальной замены кабельной системы.

И менять ее вы будете именно на неэкранированную витую пару. Аббревиатурой UTP (Unshielded Twisted Pairwaire) обозначается тип провода, состоящий из четырех пар проводов разного цвета, каждая из которых отличается еще и шагом скрутки. Первоначальное назначение синей и коричневой пар проводов — передача голоса, оранжевой и зеленой — передача данных. Для того чтобы сделать простейшую сеть с использованием концентратора или коммутатора, достаточно обжать одинаково вилки RJ-45 на обоих концах протянутого провода. Однако можно один и тот же проложенный провод использовать как канал не для одной, а для двух пар узлов. Для этого лучше всего задействовать так называемые «двойные» розетки, в которых каждые две пары используются для организации одного подключения.



Одинакового обжатия сетевого кабеля разъемами RJ-45 вполне хватит для создание простейшей сети

К недостаткам UTP следует отнести низкую помехозащищенность и ограниченную длину. Максимальное расстояние между узлами не должно превышать 100 метров. При этом особое внимание надо обратить на то, чтобы линии передачи данных не проходили вместе с силовыми проводами.

Выбор оборудования

Минимальный набор необходимого сетевого оборудования включает в себя сетевой адаптер для каждого рабочего узла и концентратор или коммутатор. Оптимальным вариантом надо признать тот, при котором все сетевое оборудование произведено одной компанией. Это дает потребителю не только гарантию универсальной технической поддержки, но и возможность использования фирменных технологий, которые нередко не работают вообще, если в составе сети есть хотя бы одно устройство иного производителя.

В качестве примера можно привести сетевое оборудование компании 3Com, которое буквально нашпиговано различными фирменными штучками, позволяющими работать ему не только более надежно, но и на больших расстояниях. Другим брендом, на который стоит обратить внимание, является D-Link. Линейка предлагаемых продуктов довольно разнообразна — от простых 10-мегабитных адаптеров до сложнейших сетевых управляющих устройств. Интересно, что особенностью некоторых концентраторов D-Link является то, что их можно объединять в стек без увеличения количества репитеров.

Что же касается аппаратуры остальных производителей, то тут могу лишь привести свое мнение. За семь лет работы сетевым администратором я не заметил особой разницы между продукцией Compex, Genius, Asustek и еще нескольких компаний, производящих сетевые устройства для рынка SOHO (домашние сети и сети малых офисов). Может быть, это связано с тем, что мне так и не пришлось администрировать большие сети (более 50 машин). Но скорее это из-за того, что все сети, с которыми мне приходилось работать, доставались уже готовыми. Поэтому процесс их модернизации шел по принципу «главное, чтобы работало».

Принцип снежного кома

Как только вы выбрали производителя, считайте, что ваша сеть уже готова. Все мелочи, связанные с прокладкой кабелей, определением сетевой политики безопасности, связи с Интернетом и т. п., уже не будут иметь принципиального значения, поскольку развитие любой компьютерной сети идет по принципу снежного кома. Каждое нововведение влечет за собой следующее жизненно необходимое усовершенствование. Так, например, замечено, что установка на каждое рабочее место почтового клиента приводит в конечном итоге к необходимости выработки корпоративной политики защиты от спама. Спастись от подобных ситуаций практически невозможно, но вполне можно ими управлять.

Прежде всего, надо помнить, что любое усложнение снижает надежность всей системы. Поэтому прежде чем приступать к введению глобальных новшеств, хорошо бы провести небольшой анализ последствий, затем потратить пару недель на тесты на одном-двух рабочих местах и лишь после этого вводить что-то новое для всех клиентов сети. »

В связи с этим надо упомянуть о программной поддержке сетей. Тут могу порекомендовать использовать для рабочих станций ОС семейства Windows, а для шлюзов, отвечающих за связь внутренней сети с Интернетом, — UNIX-подобные ОС. Самым лучшим вариантом лично я считаю установку Linux или, например, FreeBSD на каждое рабочее место, но в большинстве случаев это практически невозможно.

Если же остановиться на «смешанной» модели использования операционных систем, то вы получите, с одной стороны, привычную для пользователя среду, а с другой стороны, надежную и производительную систему сетевого администрирования.

Серверы и рабочие станции

Когда-то очень давно, будучи зеленым студентом-второкурсником, я пытался проконсультировать одного своего знакомого, который как раз собирался устанавливать в своем офисе сеть. Попал я тогда в одну весьма неприятную историю. Продавец, который стремился продать подороже все то, что у него было, рассказал мне, что в сети должен обязательно находиться хотя бы один сервер. В тот раз мой знакомый потратил довольно большие по тем временам деньги, а я лишь через несколько лет узнал, что сети бывают разные, в том числе и такие, которые не содержат в своем составе отдельно выделенного сервера.

Хотя, если подходить к этому вопросу строго, то сервер, находящийся в системе, может выполнять самые различные функции. Сегодня именно эти функции определяют в конечном счете и аппаратную часть того или иного сервера. В самом простом случае (два компьютера в сети) каждый из участников может выступать как в роли сервера, так и в роли клиента. Например, один из компьютеров может быть сконфигурирован как сервер удаленного доступа, другой — как почтовый и прокси-сервер.

Безопасность или осторожность

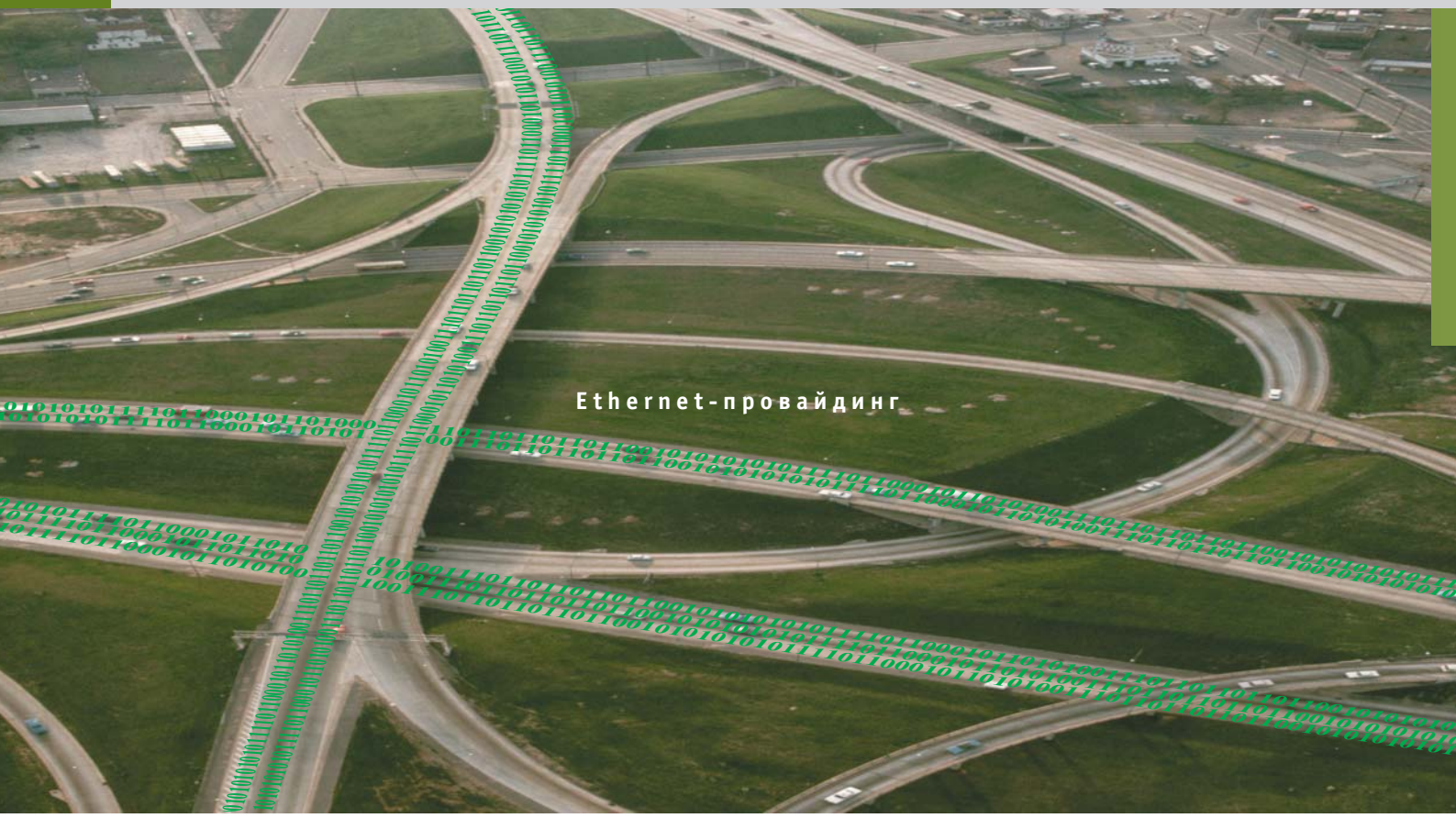
Вопрос обеспечения сетевой безопасности один из самых важных. Несмотря на многочисленные повторения этой нехитрой истины во многих руководствах и изданиях, до сих пор пароли типа «user» или «1234567» являются самыми популярными. Вторыми по популярности, а следовательно и по опасности подбора, являются пароли, повторяющие логин. Бороться с этим, безусловно, надо. Только вот не всегда получается. Причем касается это не только логинов и паролей, но и всех остальных вопросов, забывать о которых не следует, даже если ваша сеть состоит из двух компьютеров.

Особенно остро вопрос безопасности возникает в том случае, когда сеть подключается к Интернету. Персональные и корпоративные брандмауэры, централизованные антиспамерские программы — все эти инструменты необходимо использовать в том сочетании, которое наиболее точно отражает потребности. Если же вам досталась уже готовая сеть, то несмотря ни на какие уверения в самом дружеском расположении, первым делом необходимо очистить все следы пребывания в системе своего предшественника — от системных паролей до файлов с телефонами (хотя последние все-таки можно оставить). Если вам не удается проделать это в полном объеме, то лучше всего провести переустановку системы с форматированием жестких дисков. Пусть вас потом обвинят в администраторской паранойе, но зато вы будете абсолютно спокойны. ■ ■ ■ Сергей Егоров

Неочевидный выбор

Коммутатор или концентратор

В те далекие времена, когда Ethernet только начинал осваивать витую пару, для того чтобы увеличить протяженность одного сетевого сегмента, стали использовать UTP-повторители, основной функцией которых являлось простое повторение на выходе тех электрических сигналов, которые появлялись на входе. Несколько позже такие повторители стали многопортовыми, и основным их назначением стала работа в качестве центральных сетевых узлов Ethernet. Такие устройства называют хабами (hub). Несмотря на то что основной принцип их работы — построение сигнала, полученного на одном порту — на всех остальных не изменился, функционально хабы смогли не только стать на долгое время основными сетевыми кирпичиками, но и дать толчок к появлению иных узловых сетевых устройств — коммутаторов, или свичей. Принципы работы свича, который в представлении мало знакомых с ним людей является лишь более дорогим (по сравнению с хабом) узловым сетевым устройством, совсем иные. Свич, в отличие от хаба, не повторяет сигналы, а организует виртуальный канал связи между двумя абонентами. Кроме того, в своем составе он имеет сравнительно небольшой буфер, который используется как хранилище уже известных устройству MAC-адресов участников сети. Очевидно, что коммутатор — устройство более быстродействующее. Для организации небольших сетевых сегментов вполне можно использовать хабы, однако стоимость свичей сегодня (из расчета на один порт) не намного выше стоимости коммутаторов. Поэтому вполне логичным выглядит решение о построении многосегментных сетей лишь на базе коммутаторов.



Артерии жизни

Повсеместному развитию домашних сетей способствуют рост популярности интернет-услуг, удешевление сетевого оборудования и использование новых технологий, существенно снижающих цены на высокоскоростной трафик. Анализируя существующий опыт, можно утверждать, что создание малых сетей с выходом в Интернет — достаточно прибыльный бизнес.

Основной массе пользователей домашних сетей достаточно хорошо известна лишь та часть работ по прокладке и обслуживанию, которая непосредственно их касается. Самая многочисленная категория пользователей и вовсе не задумывается о том, как такая сеть выглядит изнутри. Эти клиенты ограничиваются лишь доступом в Интернет, а также пользуются услугами биллинговых и авторизационных систем, поскольку контролируют свои затраты. Существенно меньшая часть пользователей понимает, как работает их домашний компьютер в сети и как осуществляется доступ в Интернет. И лишь самая немногочисленная категория пользователей имеет хорошие знания в области технологий построения современных компьютерных сетей и понимает, что не меньшая, а большая часть проблем скрыта от рядового пользователя. Рассказать об этой скрытой стороне функционирования домашних сетей мы попросили Артура Алекперова, руководителя службы по связям с общественностью компании «МТУ-Интел».

Домашние сети как основа Ethernet-провайдинга

В настоящее время основным предназначением так называемых домашних сетей является обеспечение доступа в Интернет для абонентов локальных сетей, развернутых в жилых домах. Поскольку основной технологией для их построения стала Ethernet, то и услуги предоставления с их помощью доступа в Интернет стали именоваться Ethernet-провайдингом. Следует отметить, что подключение через Ethernet как коммерческая услуга не попадало до определенного момента в область интересов крупных интернет-провайдеров.

Большинство домашних сетей начинались стихийно как инициатива группы энтузиастов. Именно на этом этапе технология Ethernet благодаря своей относительной дешевизне стала стандартом. По мере своего развития домашние сети Ethernet неожиданно для многих оказались пригодными для решения пресловутой проблемы «последнего дюйма» при организации широкополосного доступа к Интернету конечного пользователя. Именно это предусматривает так называемая «шведская» модель, заключающаяся в скоростном (как правило, оптоволоконном) подключении проложенной в доме локальной сети Ethernet к оператору связи. При- »



Это вовсе не обычная аптечка, а набор первой помощи сетевых санитаров

» чем в России домашние сети строились не в отдельном жилом доме, а сразу в группе строений, квартале и даже районе. На это есть целый ряд причин, среди которых фигурируют не только экономические.

Безусловно, базовой технологией построения локальных домовых сетей остается Ethernet. Технология эта имеет 30-летнюю историю, однако буквально за последние 3–5 лет произошли существенные изменения, в том числе и в стоимости оборудования. Сначала появились коммутируемый Ethernet (в 1992 году) и поддержка приоритезации (в 1993 году). Затем резко выросли скорости и предельные расстояния между точками одного сегмента сетей Ethernet. В 1998 году был принят стандарт Gigabit Ethernet (IEEE 802.3z), подразумевающий возможность работы по оптоволокну, а также по витой паре на расстояниях до 25 м. Уже в 1999 году появился стандарт 1000Base-T (IEEE 802.3ab), позволяющий работать до 100 м по витой паре. Далее последовала спецификация IEEE 802.3ad, означавшая поддержку агрегации каналов и объединение их в транки. Сейчас на очереди стоит спецификация 10 Гбит.

В условиях взрывного роста популярности домашних сетей Ethernet многие крупные интернет-провайдеры уже не могут позволить себе обделить их своим вниманием. Во многих городах Ethernet-провайдинг превратился во вполне респектабельный бизнес. Крупным компаниям использование домашних сетей вкупе с имеющейся транспортной сетью ADSL позволяет предлагать потенциальным пользователям действительно скоростное и качественное решение. При этом конкурентными преимуществами, возникающими при использовании технологии ADSL (в отличие от прокладки оптоволоконного канала), являются сроки и стоимость создания магистрального канала.

Команда специалистов, с которой в боевых условиях на прокладке сети «Билан-Проект» побывал наш фотограф

Особенности реализации домашних сетей

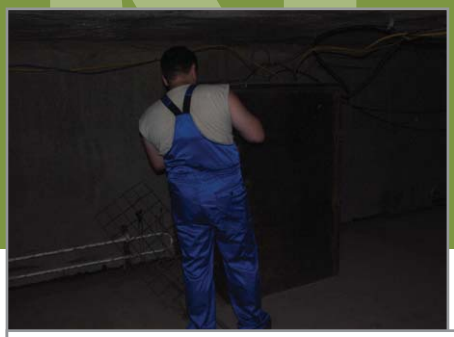
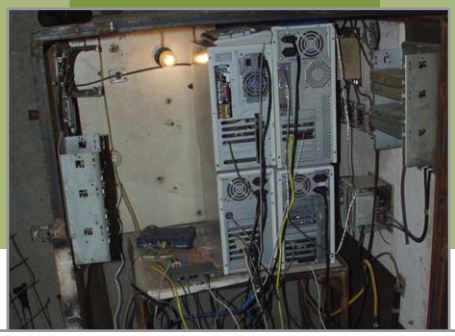
Домашняя сеть, объединяющая клиентов компании, представляет собой некую виртуальную частную сеть. Это означает, что прежде чем получить доступ к Интернету, пользователь должен пройти процедуру авторизации. Внутри сегмента пользователь находится в «бесплатной» области. Если же ему необходимо передать данные из сегмента в сегмент, то за эту услугу уже придется платить. В то же время, чтобы пользователи имели возможность бесплатно общаться между собой, компании развивают некие «условно-бесплатные ресурсы» (чаты, конференции).

Терминология для домашних сетей считается уже сформировавшейся. В соответствии с ней домашние сети состоят из абонентской системы здания и магистральной кабельной системы. Абонентская система здания предназначена для подключения конечных пользователей к активному (реже — пассивному) оборудованию Ethernet-провайдера внутри одного дома. Магистральная кабельная система служит для объединения активного оборудования абонентских систем здания в единую инфраструктуру и соединения их с другими сетями (в том числе с Интернетом).

Обычно магистральная кабельная система (магистральный канал) прокладывается в некую центральную точку района. В дальнейшем магистральный канал по коммуникациям разводится до ближайших зданий в зависимости от распределения клиентов. При этом некоторые компании предпочитают не использовать воздушные коммуникации — так называемые «воздушки», а прокладывают свои коммуникации в основном под землей (при этом достигается наивысший уровень защищенности каналов).

Количество клиентов в пересчете на один магистральный канал в сети должно быть не очень велико. Это приобретает особое значение в тот момент, когда магистральный канал по какой-либо причине все же выйдет из строя. В этом случае утрачивают доступ в Интернет не более 50–100 клиентов, объединенных в рамках одного сегмента сети. И это никоим образом не сказывается на работоспособности других сегментов и других магистральных каналов. Активное сетевое оборудование в домашних сетях традиционно для технологии Ethernet: это коммутаторы и концентраторы. При выборе производителя оборудования в первую очередь надо руководствоваться критерием «цена/производительность».

Перед тем как стать пользователем домашней сети, следует твердо усвоить, что требования, традиционно предъявляемые к обычной СКС (например, к офисной сети), в условиях домашней сети не всегда удается выполнить. Более того, вряд ли вообще можно верить чьим-либо заявлениям о прокладке домашних сетей с соблюдением всех норм и правил, характерных для СКС. Однако это вовсе и необязательно, ведь, по мнению многих специалистов, домашние сети вообще не могут являться СКС, это, скорее всего, самостоятельный класс кабельных систем, который еще только ждет своих стандартов. »


Чтобы сохранить оборудование, приходится использовать специальные «сейфы» и привлекать органы местного самоуправления

Типовые процедуры прокладки домашних сетей

Многие из таких сетей в Москве складывались стихийно, на энтузиазме конкретных жильцов. Они сами тянули кабели, подключали пользователей, заключали договоры с интернет-провайдерами, взимали плату с клиентов. На этом этапе некоторые сети выросли до внушительных размеров. Один из ведущих провайдеров — компания «МТУ-Интел» — ведет свой бизнес в области домашних сетей через своих агентов, представляющих услуги практически во всех районах Москвы. Причем основную долю клиентов по-прежнему составляют энтузиасты — те группы лиц, которые желают подключиться к Интернету. Как правило, никакой проводки в таких домах нет. В этом случае агенты проводят обследование будущей площадки и собирают заявки с потенциальных клиентов. Далее в соответствии с требованиями, установленными в компании «МТУ-Интел», агенты составляют предварительный проект. Затем он согласовывается с технической службой компании. В проекте указывается, какова будет топология сети, какие типы активного оборудования будут использоваться, где это оборудование будет устанавливаться, и в последнюю очередь — как и где будет проложен кабель. Также проект обычно учитывает перспективы наращивания абонентской базы и развития сети. При этом предусмотреть сразу, какова будет плотность клиентов, при составлении проекта практически невозможно, но, с другой стороны, подкорректировать проект по мере роста клиентской базы никаких проблем не составит. Исходя из этого проекта специалистам компании будет понятно, где и какое количество абонентов подключено, какое число портов занято или свободно, каковы пути дальнейшего развития этой сети. Только после утверждения данного проекта агенты приступают к непосредственной прокладке коммуникаций.

После прокладки коммуникаций и подключения оборудования конечного пользователя к сети Ethernet всегда следует период тестирования. Тестирование производится как специалистами агента, так и самим пользователем. Примечателен тот факт, что в течение данного периода поль-

Технологии

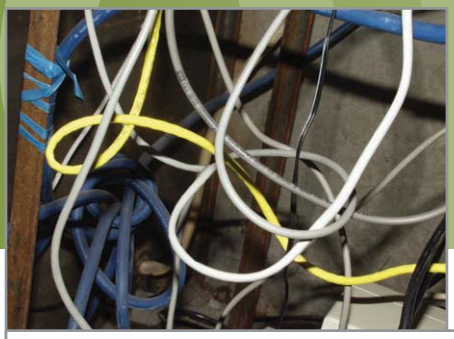
Альтернативные решения для безвыходных ситуаций

Одна из новых технологий создания локальных сетей — HomePNA (www.homepna.org). На сегодня, в том числе и в России, доступно оборудование двух спецификаций: 1.0 и 2.0 (существует версия 3.0 со скоростью передачи более 100 Мбит/с). Суть технологии довольна проста: в телефонной проводке выделяется высокочастотная область для передачи данных. Чем-то это похоже на ADSL, но используются различные частотные диапазоны, благодаря чему технологии не мешают друг другу даже в одной телефонной линии. Компьютеры через специальные адаптеры подсоединяются непосредственно к телефонной сети. Дальность передачи сигнала от одного компьютера составляет около 100 м, так что за пределы дома он не выходит. Однако в спецификации 1.0 существует вариант Long Distance, который позволяет увеличить дальность передачи до 1 км. Изначально технология создавалась для домашних сетей (то есть в пределах одной квартиры или частного дома), однако есть проекты, где на ее основе строится сеть доступа в Интернет. Домашний компьютер подключается через адаптер к телефонной розетке, а там, где сходятся все телефонные линии дома, ставится многопортовый коммутатор HomePNA.

Условием, когда применение HomePNA возможно и оправданно, является наличие единого кросса, куда сходятся телефонные линии из всех квартир, и разрешения владельцев этого кросса на его использование.

В кондоминиумах и элитных домах можно рассмотреть в качестве варианта создание сети на основе HomePNA, хотя стоимость подключения на один порт в среднем все-таки выше, чем у сетей Ethernet. Но есть серьезное преимущество — отсутствие необходимости прокладывать специальную кабельную систему.

Еще одна технология, которая может быть рассмотрена как вариант для домовой сети, — Radio Ethernet (серия стандартов IEEE 802.11x). С HomePNA ее объединяет отсутствие потребности в кабельной инфраструктуре. В некоторых случаях вполне возможно, что локальная сеть на Radio Ethernet будет стоить дешевле, чем сеть Fast Ethernet. Однако надо учесть, что, во-первых, радиосети подвержены помехам (особенно это относится к диапазону 2,4 ГГц в Москве и крупных городах), во-вторых, необходимо получение разрешения от органов радионадзора. Наконец, сети Radio Ethernet в силу открытости среды требуют обеспечения защиты от несанкционированного доступа. В то же время сеть Radio Ethernet может стать незаменимой для прокладки мостов «точка-точка» между домами, если проложить воздушную или подземную кабельную линию невозможно или слишком дорого.



Пестрое разнообразие подвальных коммуникаций

» зователь в случае выявления проблем в работе домашней сети имеет право разорвать отношения с компанией или его агентом, причем затраченные им средства будут компенсированы.

Достаточно часто возникает вопрос о минимальном количестве пользователей, ради которых будет прокладываться домашняя сеть. Решается он всегда индивидуально. Минимальное количество потенциальных пользователей в отдельном жилом доме, для которых компания принимает решение о подаче ADSL-канала, составляет 5–7 человек. Однако эта цифра при условии «перспективности» клиента (величины потребляемого им трафика) может быть уменьшена.

Основные проблемы при прокладке домашних сетей

Одной из главных проблем при прокладке домашних сетей является защита активного сетевого оборудования. По словам Артура Алекперова, в «МТУ-Интел» знакомы со случаями хищения и порчи оборудования не понаслышке. Конечно, собственная служба безопасности компании совместно с органами милиции расследует каждый такой случай, заводятся уголовные дела, иногда оборудование находится и возвращается.

Проблема защиты оборудования решается главным образом на стадии проектирования административными мерами. Безусловно, оборудование размещается не в чистом поле. Оно находится в закрытых ящиках, шкафах, сейфах. Причем чем «мощнее» шкаф, тем сохраннее будет оборудование. Конечно, существует вариант открытого размещения оборудования в щитках, куда вполне влезает специализированный металлический ящик на одно сетевое устройство. Однако в российской действительности от вандалов никто не застрахован. И если принимается решение о размещении сетевого оборудования (концентраторов или коммутаторов) в щитке на лестничной клетке, то надо быть морально готовыми к тому, что на следующий день его может там не оказаться. Поэтому предпочтение отдается чердакам и подвалам, где запираются двери и ограничивается доступ «неблагонадежной публики». Таким образом, проблема решается путем ограничения доступа в помещения, где располагается оборудование. Данные меры реализуют дез и жэк, с которыми компании сотрудничают легально, заключая соответствующие договоры. В этом случае представители компании для доступа в помещения получают ключи, расписываются в книге выдачи ключей, а после завершения работ закрывают помещения и сдают ключи обратно.

Другой вариант решения данной проблемы — использование маскировки и сигнализации. Маскировка подразумевает применение для размещения сетевого оборудования ящиков и шкафов самого неприглядного вида. Задача маскировки целиком и полностью ложится на плечи компаний-агентов. Главное — создать видимость, что оборудование просто не может находиться в рассматриваемых ящиках и сейфах. Сигнализация обычно применяется совместно с другими мерами по защите оборудования и представляет собой последний рубеж защиты.

Несмотря ни на какие меры, потери случаются достаточно часто. При этом подробно изучается и определяется степень вины компании-агента. Если агент не выполнил своих обязательств по сохранности сетевого оборудования, то потери будут компенсироваться за его счет. Если вопросы сохранности были решены на должном уровне, то потери распределятся равномерно.

Другой не менее важной проблемой, возникающей при построении домашних сетей, является обеспечение качества на этапе непосредственной прокладки кабельных линий связи. Проблема важна в связи в тем, что от качества реализации данного этапа зависит качество и надежность функционирования всей сети. При этом самым нежелательным вариантом считается протяжка воздушных кабельных линий. Сама по себе процедура протяжки кабеля по воздуху существенно сложнее в техническом отношении, чем протяжка по подземным коммуникациям. Исходя из этого «воздушки» следует использовать лишь в том случае, когда никакими другими путями требуемые линии провести не удается.

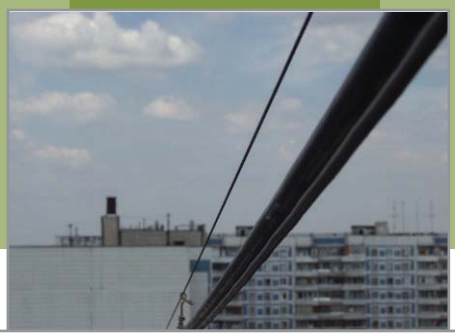
Самая простая процедура протяжки кабеля между домами по воздуху потребует наличия бухты кабеля П-296, используемого для этих случаев, веревок и нескольких комплектов страховочного оборудования для работы на крыше. Данная процедура в самом общем случае включает в себя несколько этапов.

Этап первый заключается в следующем: спуск вниз с крыши первого дома одного конца веревки, привязка к нему свободного конца кабеля П-296, раскатка по двору железной бухты кабеля, сопровождаемая подъемом его на крышу по мере его раскатки, фиксация поднятого конца кабеля на крыше.

Далее следует второй этап, который заключается в спуске с крыши второго дома конца второй веревки, привязке свободного конца кабеля П-296 к спущенному концу, подъеме привязанного конца кабеля на крышу второго дома, его фиксации.

Последний, третий этап — самый сложный в физическом отношении: необходимо осуществить натяжку кабеля между крышами домов, а также его фиксацию и стыковку с сетевым оборудованием провайдера и абонентским оборудованием клиента.

Следует иметь в виду, что в реальных условиях рассмотренная ситуация осложняет- »


Та самая «воздушка». Скоро счастливые соседи смогут обмениваться разнообразной информацией

» ся наличием деревьев на маршруте протяжки кабеля, машин во дворах, а также различиями в высоте находящихся рядом домов. В соответствии с этим процедура усложняется многократно. Иногда даже возникает необходимость протянуть кабель через оживленную улицу или через провода, протянутые вдоль нее. И в том и в другом случае дополнительно потребуется присутствие представителей власти (инспектора ГИБДД и работника жэка).

В отношении надежности воздушные линии связи всегда проигрывают линиям подземным. Представим, что если линия протянута между 20-этажными зданиями, то, несмотря на использование технологий заземления и защиты от молний, она подвержена риску быть поврежденной во время обычной грозы.

Некоторые рекомендации и предложения

Всякий коллектив единомышленников-энтузиастов, вступающих в бизнес Ethernet-провайдинга, должен четко представлять не только технические аспекты будущей деятельности, но и аспекты правовые. Дело в том, что деятельность Ethernet-провайдера попадает под регламентирование различных законов. Регламентирующие органы выделяют по крайней мере семь статей, на основании которых нелегально действующий Ethernet-провайдер может быть привлечен к ответственности (в том числе и уголовной).

Итак, возникает необходимость лицензирования определенных видов деятельности начинающего Ethernet-провайдера, что само по себе вызывает целый комплекс проблем. Несмотря на то что процесс лицензирования достаточно очевиден и понятен, процедура эта трудоемкая и требует больших финансовых вложений. Во-первых, лицензия стоит немалых денег. Во-вторых, лицензия — это не разрешение на ведение деятельности, это лишь первый шаг. Затем потребуется сделать проект разворачиваемой сети. В виду того, что проекты должны составлять организации, имеющие лицензию на проектирование, компании придется обзавестись и этой лицензией. Представим, что начинающая компания добыла требуемую лицензию и разработала проект сети. Однако сеть должна быть построена по этому проекту. А построить ее может лишь организация, имеющая лицензию на строительство. В случае успешного завершения и этой стадии готовую сеть необходимо будет сдать Госсвязьнадзору. При этом все оборудование, используемое в сети, должно иметь соответствующие сертификаты. Биллинговая система учета также должна иметь сертификат. И так далее, и тому подобное...

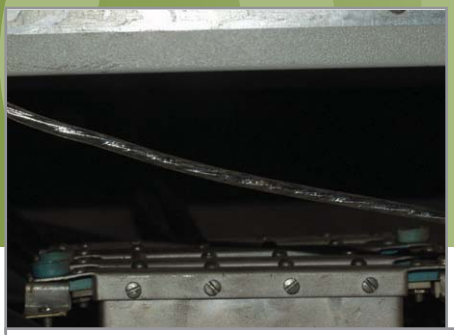
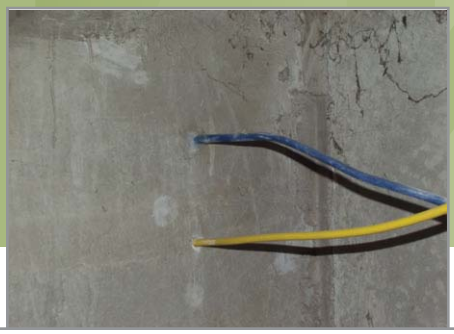
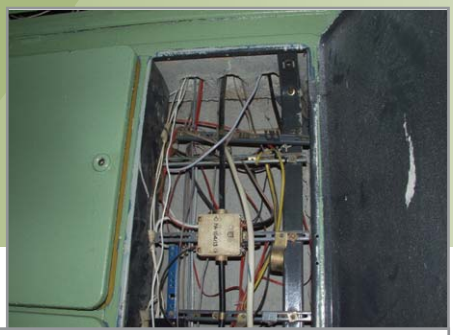
С другой стороны, компания, состоящая из нескольких энтузиастов, на определенном этапе своего развития понимает, что у нее не хватает средств для покупки биллинговой системы или содержания высококвалифицированных программистов, занимающихся ее созданием. И тогда возникает вопрос: можно ли собрать средства с нескольких десятков или неполной сотни клиентов для простого поддержания домашней сети в работоспособном состоянии и обеспечения простейшего сервиса биллинговых и авторизационных систем? Итак, самая распространенная причина краха начинающих Ethernet-провайдеров — нехватка оборотных средств на развитие. Все уходит на поддержание, эксплуатацию, оплату сотрудников, а о расширении своей зоны деятельности не может быть уже никакой речи.

Каким же образом в таких непростых условиях сохранить бизнес Ethernet-провайдинга? Специалисты предлагают в этом случае самое простое и логичное решение — заключение коммерческого соглашения с крупным интернет-провайдером. Организации, приходящие за этим в компанию, подобную «МТУ-Интел», получают возможность сосредоточиться на выполнении своих основных функций, а также различные виды помощи в целях развития своего бизнеса. Фактически обратившаяся к крупному интернет-провайдеру организация становится ее районным агентом и выполняет уже совсем другие функции.

С одной стороны, став агентом, компания перестает исполнять несвойственную ей роль «собирателя денег», подкарауливающего клиента в подъезде. Проблема решается за счет внедрения предоплатной системы интернет-провайдера, которая подразумевает, что при исчерпании на клиентском счету средств доступ в Интернет становится попросту невозможным. В этом случае возможен лишь вход в сеть по гостевому паролю, который позволяет проверку состояния своего лицевого счета и его пополнение.

С другой стороны, масса ежедневных проблем агента разрешима за счет подключения абонентов домашних сетей к мощным службам технической поддержки интернет-провайдера. Поскольку данные специализированные подразделения предназначены для повышения оперативности решения техниче- »

Нетривиальная задача: чтобы соединить соседние микрорайоны (дома 1 и 3), кабель пришлось вести через мост (2) и затем с разбегу натягивать из-за мешающих посередине деревьев

Несмотря на серьезные темпы развития беспроводных коммуникаций, проводную связь еще рано отправлять на пенсию

» ских, финансовых и других вопросов клиентов, агенты сумеют повысить эффективность сервисной функции, что очень важно в условиях конкурентного рынка.

Следует помнить: для того чтобы уже существующей домашней сети стать агентом крупного интернет-провайдера, она должна соответствовать определенному уровню. Как минимум это должно быть юридическое лицо. Компания «МТУ-Интел», например, для выявления уровня потенциального партнера проводит аудит построенной им домашней сети и на основании этого аудита делает заключение о том, насколько грамотные специалисты ее разворачивали и эксплуатировали. Только после этого аудита с заинтересованной организацией начинаются коммерческие отношения.

Таким образом, агент осуществляет деятельность как в своих интересах, так и в интересах крупного провайдера, с которым его связывает соглашение. В отношении интересов партнеров агент осуществляет поиск новых площадок и расширение сети. При этом за счет непосредственного присутствия агента в районе повышается оперативность выезда к клиенту в случае возникновения каких-либо проблем. Интересы самого агента тоже учитываются: ему предоставляются оборотные средства и помощь в лицензировании деятельности. Причем для каждого агента обеспечивается эксклюзивность в том смысле, что на одной территории может работать только один агент в целях исключения пересечений коммерческих интересов.

Заключение

Современные темпы развития и внедрения сетевых технологий позволяют предположить, что в ближайшей перспективе создание домашних сетей с последующим подключением к Интернету найдет своих энтузиастов. Предлагаемые скорости доступа в Сеть уже сейчас находятся на приемлемом уровне, цены на трафик хоть и завышены (безлимитных тарифов с фиксированной оплатой почти не найти), но при рациональном использовании бьют по карману не слишком сильно. Так что если вы чувствуете в себе силы и готовы заняться тяжелым, но интересным делом Ethernet-провайдинга, существующие на этом рынке «монстры» не только не станут мешать, а наоборот, во многом смогут помочь в этом начинании.

■ ■ ■ Аркадий Сорокин

Редакция выражает благодарность компании «МТУ-Интел» за помощь в подготовке материала.

Слабое место

Максимальная длина провода

Коммутатор для подключения пользователей в доме можно установить в подвальном или чердачном помещении в специальном запираемом сейфе, иногда рациональнее поставить коммутатор на этаже. Определенной стандартом Fast Ethernet предельной длины одного сегмента кабеля витой пары в 105 м вполне достаточно для того, чтобы из подвала или с чердака «дотянуться» до любой квартиры в подъезде 16-этажного дома. Как показывает опыт, прокладка кабеля между этажами не вызывает проблем — существенно труднее дается подключение клиентов в соседнем подъезде. Правда, 105 м — это только гарантированная стандартом длина отрезка, при котором сеть будет работать без сбоев. Локальная сеть устойчиво может работать и при несколько большей длине, и здесь как раз могут проявиться лучшие качества оборудования конкретных производителей. Использование вместо витой пары специальных кабелей, например отечественного полевого кабеля дальней связи П-296 (диаметр жилы 1,2 мм), позволяет увеличить длину одного отрезка до 300–400 м, которой может хватить даже для междомовых соединений.

Сеть одного дома может быть либо сразу подключена к Интернету (в этом случае канальное оборудование, например ADSL-модем, устанавливается также в подвальном или чердачном помещении), либо объединена в сегмент с другими домовыми сетями. Во втором случае дома объединяются между собой воздушным (подвешиваемым на специальном тросе) или подземным (проложенным в коллекторе) кабелем. Безусловно, предпочтительней использовать подземные коммуникации для прокладки кабеля между домами (если вообще возможна его прокладка), так как он меньше подвержен агрессивному воздействию окружающей среды (перепады температуры, влажность, ветры, грозовые разряды и т. д.)

Обычно практикуется сегментирование, при котором локальная сеть одного дома (или нескольких — все определяется количеством подключенных клиентов) подключается к магистральной сети. За счет этого во многих случаях удается избегать необходимости прокладывать коммуникации между домами. Если емкости канала не хватает для удовлетворения потребностей клиентов в сегменте, то сегмент разделяется на две части и каждый снабжается собственным ADSL-каналом.

Хозяйство племени

С появлением и развитием сети в офисе или доме несомненно улучшается и ускорятся обмен самой различной информацией: возникают электронные библиотеки, внутренние информационные ресурсы, хранилища фильмов и музыки. Однако вместе с этим появляется желание включить в сеть устройства, покупка которых персонально каждому кажется излишней, а установка локально — неудобной с точки зрения доступа.

К таковым можно отнести высокоскоростные лазерные принтеры (особенно цветные), плоттеры, устройства для записи CD- и DVD-дисков. Для небольшого офиса, например, выгоднее приобрести один мощный принтер с емкими лотками для бумаги и большим ресурсом картриджа, чем два-три менее мощных. Экономия при этом связана не только с разницей в цене на сами устройства, но и с расходными материалами и стоимостью сервисного обслуживания.

Аналогично поступают и с устройствами записи — как правило, устанавливается выделенная машина (при этом скорость ее работы особой роли не играет, лишь бы были быстрыми шина, сетевая карта и диски) с CD-ROM (или DVD-ROM) и устройством записи. При этом без устройства чтения можно и обойтись, но процесс копирования дисков будет более длительным: сначала нужно сформировать образ на HDD, а потом перенести его на болванку. Единственное, чего не удастся избежать без особых ухищрений, — это похода за отпечатками к принтеру и необходимости «загрузки» лотков CD-RW.

Наиболее распространенным сетевым устройством, предназначенным для группового использования, является принтер. Есть очень простой способ, позволяющий печатать на один принтер с нескольких компьютеров: подключить его локально к машине под управлением, например, Windows XP (или любой другой сетевой операционной системы) и разрешить общий доступ к нему. При этом возможно гибкое распределение прав доступа: части пользователей можно разрешить только печатать, части — управлять принтером и заданиями. Но есть и существенные недостатки: при интенсивной печати, особенно если задания большие по объему, производительность системы резко уменьшается, и работать с ней становится затруднительно.

Как правило, сетевой принтер, помимо LPT- или USB-порта, имеет встроенную сетевую карту и может быть подключен непосредственно в сеть. Конфигурировать устройство можно либо с помощью специального ПО, либо кнопками управления. Как правило, такими принтерами поддерживаются все распространенные сетевые протоколы, при этом устройство может иметь как фиксированный адрес, так и получать его по запросу с сервера (в небольших сетях обычно применяется фиксированное назначение адреса).

Если используется операционная система, поддерживающая очереди печати, появ- »

HP LaserJet 2200dn —хорошее решение для небольших групп пользователей и малых офисов

HP LaserJet 9000e — топовая модель в линейке производителя, обладающая поистине огромными возможностями

» ляется возможность привязывания к каждому принтеру большого количества очередей с разными настройками. Например, печать в очередь A — это всегда выбор бумаги A3 из нижнего лотка, максимальное качество и ориентация LandScape; в очередь B — A4, лоток ручной подачи, форматирование текста под бланк, максимальная скорость печати. Также возможны гибкое управление правами пользователей, расстановка приоритетов, разделение заданий листами с «баннером», то есть названием документа и именем пользователя (это, конечно, увеличивает расход бумаги, но позволяет быстро найти свое задание среди множества распечатанных).

Сетевые принтеры

Чтобы вам стали ясны преимущества сетевых принтеров, давайте рассмотрим характеристики нескольких конкретных моделей от крупных производителей этого класса оборудования — компаний Hewlett-Packard и OKI.

Среди популярных для малых групп и офисов стоит отметить принтер HP LaserJet 2200dn. Он имеет встроенный сервер печати HP Jetdirect 610n, модуль двусторонней печати, ИК-порт, USB- и LPT-интерфейсы, 8 Мбайт памяти, печатает до 18 страниц в минуту, общая нагрузка составляет до 40 000 страниц в месяц — почти все, что нужно для обеспечения качественной и быстрой печати в небольшом офисе.

Если этих возможностей не хватает, есть решения куда более мощные, например HP LaserJet 4200n. Он выдает до 33 страниц в минуту, память расширена до 64 Мбайт (и возможно дальнейшее наращивание), встроен сервер печати Jetdirect EIO, тактовая частота процессора составляет 300 МГц, выход первой страницы происходит менее чем через 8,5 с, есть функции проверки документов перед массовой печатью (proof and hold), конфиденциальной печати. Также реализованы динамическая электрофотографическая настройка и механизм автоматического перераспределения тонера в картридже. Возможна установка дополнительных лотков для бумаги (общая емкость до 2600 листов), устройства подачи конвертов, сшивателя и укладчика. Для удобства и простоты управления имеется встроенный web-сервер, позволяющий не только получать доступ ко всем настройкам с помощью стандартного браузера, но и отправлять уведомления о неисправностях по e-mail.

Если и этого недостаточно, существует представитель нового поколения принтеров — HP LaserJet 9000e. Его скорость печати — 50 страниц в минуту, есть возможность управления принтером через Интернет, печать первой страницы проходит менее чем за 8 с, оповещения о неисправностях он может отправлять по e-mail, имеет функции управления заказами на расходные материалы и обеспечения технической поддержки в диалоговом режиме. Тактовая частота процессора — 300 МГц, размер памяти — 64 Мбайт (возможно расширение), нагрузка — до 300 000 страниц в месяц. Можно сказать, что это топовая модель в линейке, обладающая максимумом разнообразных функций и широкими возможностями по управлению.

Пользуются популярностью и принтеры, использующие для формирования изображения LED-технологию. Классическая технология переноса изображения такова: источник света, контролируемый центральным процессором принтера, создает дополнительный заряд на поверхности светочувствительного барабана. Когда барабан, вращаясь, проходит мимо картриджа, частички тонера прилипают к нему, а затем переносятся с барабана на лист бумаги. Закрепление изображения проводится печкой. Источником света служит либо лазерный блок (обычная технология, используемая в лазерных принтерах), либо светодиодная линейка (такая технология используется, например, в принтерах OKI). К преимуществам второй можно отнести отсутствие движущихся частей, независимость качества от скорости печати (не требуется развертка луча), отсутствие необходимости коррекции хода луча (ведь барабан вращается непрерывно, а нужно формировать горизонтальные строки).

Начнем с модели OKI C5100n. Возможности очень неплохие: 12/20 страниц в минуту в цветном/монохромном режиме, 32 Мбайт памяти в стандартной поставке (расширяема до 320 Мбайт), время выдачи первой страницы — 9/14 с в цветном/монохромном режиме, тактовая частота процессора — 200 МГц, разрешение — 600x 1200 dpi, максимальная нагрузка — 50 000 страниц в месяц, емкость лотка — 300 листов плюс 100 листов в лотке ручной подачи, возможна установка модуля двусторонней печати, раздельная замена картриджа с тонером и фотобарабана. Интерфейсы — USB и SoftNIC (Ethernet).

Перейдем к монохромным моделям. OKIpage 14i/n (одна из младших моделей) обладает следующими характеристиками: скорость печати до 14 страниц в минуту, время выдачи первой страницы — 7,5 с, разрешение — 600x1200 dpi, памяти в стандартной поставке 8 Мбайт (расширяет- »

Принтер OKI C5100n способен удовлетворить потребности небольшого коллектива в цветной печати

Модель OKI B8300: впечатляющая скорость, внушительный вид и хорошие возможности расширения

» ся до 40 Мбайт), максимальная нагрузка составляет 15 000 страниц в месяц, стандартный лоток подачи бумаги рассчитан на 250 листов (возможна установка дополнительных лотков на 100 листов/50 конвертов и на 500 листов), USB и параллельный двунаправленный интерфейсы (IEEE 1284 и USB 1.1), встроенный принт-сервер с поддержкой протоколов TCP/IP, IPX/SPX, NetBEUI, Ethertalk, NDS.

OKI B8300 является одним из самых мощных принтеров: скорость печати до 45 страниц в минуту в режиме односторонней или двусторонней печати (при использовании дуплекса, допускающего в одном из вариантов режим ручной подачи), время выдачи первой страницы менее 5 с, разрешение 600 dpi без сглаживания и 1200 dpi со сглаживанием, память в стандартной поставке 32 Мбайт и 8 Мбайт FlashROM (расширяется до 288), максимальная нагрузка до 200 000 страниц в месяц, стандартный лоток подачи бумаги на 500 листов (возможна установка трех дополнительных лотков на 500 листов каждый и податчика на 2500 листов), установка модуля двусторонней печати; сортировщик отпечатков, параллельный двунаправленный интерфейс (IEEE 1284), встроенный принт-сервер с поддержкой протоколов TCP/IP, IPX/SPX, NetBEUI, Ethertalk, NDS.

Пространство для маневра

Иногда возникает необходимость подключения уже существующих принтеров в сеть. Тут возможны два варианта: либо принтер допускает установку встроенной сетевой карты (в этом случае достаточно просто ее купить, установить и настроить с помощью прилагаемого ПО), либо нет. Если нет — проблема может быть решена приобретением внешнего сервера печати. На данный момент фирма Hewlett-Packard предлагает для сетей Ethernet модели Jetdirect 170x, для Ethernet/Fast Ethernet — 175x и 300x, для сетей TokenRing — 500x. Данные сетевые устройства совместимы со всеми моделями струйных принтеров HP, с начальными моделями лазерных, комбайнами и многими принтерами других производителей (в том числе и матричными). Простейшая установка не требует вмешательства администратора, конфигурация сервера производится по сети. Одним из преимуществ является возможность сохранения в памяти задания на печать при перезагрузке принтера, чтобы оно не было потеряно.

Сейчас все большую популярность приобретают беспроводные сети, в этом случае пользователь меньше привязан к своему рабочему месту и может передвигаться, используя переносной компьютер. Для обеспечения аналогичной мобильности принтеров созданы беспроводные серверы печати, например EZ Connect фирмы SMC (модели SMC2622W-U и SMC2622W-P). Первый подключается к принтеру посредством USB-порта (1.1), второй — с помощью последовательного. На борту у данных устройств имеется порт Ethernet (10Base-T/100Base-TX) и слот 802.11b. Возможно приобретение дополнительной беспроводной PCMCIA-карты. Обе модели позволяют использовать как существующую беспроводную сеть point-to-point, так и беспроводную точку доступа. Во втором случае пользователи и проводной, и беспроводной сети имеют равные возможности доступа к сетевому принтеру. При первом варианте, естественно, возможно лишь беспроводное подключение. Настройка осуществляется через web-интерфейс с помощью стандартного браузера, поддерживается SNMP-агент.

Запись дисков по сети

Самый распространенный способ, уже упоминавшийся выше, — найти несколько устаревший компьютер и установить на него операционную систему Windows 98. Наличие монитора, мыши и клавиатуры при этом совсем не обязательно. Дальнейшее зависит от того ПО, которое предполагается использовать для записи болванок.

Если это WinOnCD — проблем минимум, поскольку носитель в устройстве виден как простой съемный диск. Достаточно разрешить общий доступ к нему по сети, установить пароли на запись (если вы хотите ограничить доступ к устройству), и использовать сетевой ресурс можно будет с любого рабочего места внутри сети. Недостатки, конечно, есть: диски, записанные таким способом, требуют перед прочтением установки специального ПО (оно находится прямо на диске, из-за этого, кстати, теряется небольшая часть дискового пространства), также могут возникнуть некоторые проблемы с доступом к ним в DOS. Но удобство работы несомненное, и внедрить технологию труда не составит.

Если же предполагается использовать Nero или подобные программы — нужно предпринять некоторые дополнительные шаги. Самое простое решение — установка программы удаленного управления, например Radmin, VNC, pcAnywhere, Timbuktu или LapLink. Мы воспользуемся Radmin (программа совсем небольшая — 1,4 Мбайт, два EXE-файла и два DLL). Скачать пробную версию можно с сайта www.famatech.com. »

Цветная охранная web-камера AXIS 2100, подключаемая непосредственно в сеть Ethernet

Аппаратная компрессия данных в формат JPEG либо MPEG-4 позволяет камере VN-C10U от JVC передавать изображение даже по низкоскоростным каналам

» На том компьютере, к которому предполагается подключаться, устанавливается и запускается R_server.exe; на машине, с которой производится подключение, — Radmin.exe. На серверной части необходимо задать пароль, который будет запрашиваться при попытке управления извне. Управляющее окно вызывается либо из значка в меню «Пуск», либо выполнением команды r_server.exe /setup. Дальше все просто: создаете новое соединение (можно прописать как IP-адрес, так и HostName машины, к которой будет производится подключение) и активируете его. После ввода пароля на управляющей машине вы получаете копию Рабочего стола управляемой (на которой стоят устройства записи). Запускаете, например, Nero и пользуетесь им в обычном режиме. Передача файлов возможна либо через общие папки в сети, либо с помощью Radmin (если щелкнуть правой кнопкой мыши по созданному соединению, появится возможность выбора режима работы FileTransfer).

Аналогичные действия можно выполнять с помощью служб Terminal Services или Remote Desktop, но они требуют установки более дорогих ОС (Windows 2000, XP), и обойтись машиной класса Pentium 100 с 32 Мбайт памяти уже не получится. Плюс для службы Terminal Services необходима покупка достаточно дорогого клиента и дополнительного пакета лицензий. Эти средства, конечно, гораздо более гибкие и позволяют выполнять очень широкий круг задач, но для самого простого способа подходят мало.

Web-камеры

Рассматривать обычные модели мы не будем, про них все давно известно: качество изображения посредственное, цветопередача «гуляет» (за $10–15 сделать устройство с приличной матрицей очень затруднительно), плюс необходимы близко стоящий компьютер и дополнительное ПО на нем, чтобы обеспечить доступ к изображению по сети.

Нас интересуют камеры, которые возможно подключать непосредственно в сеть (имеется порт Ethernet или для модема) с аппаратным сжатием изображения. Как правило, они подключаются к сети через порт 10Base-T/100Base-TX/1000Base-TX или при помощи модема через последовательный порт. Для работы используется стек протоколов TCP/IP, поэтому камере с помощью специального ПО, стандартного web-браузера либо командой DOS присваивается IP-адрес (статический или динамический). Для идентификации используется MAC-адрес сетевой карты, встроенной в камеру. Фирмы-производители (например, AXIS) также разрабатывают специальные приложения, позволяющие упростить процесс. У такого устройства, как правило, имеется встроенный web-сервер, FTP-сервер и клиент, клиент e-mail, поддерживается работа со скриптами пользователей и Java-апплетами, что позволяет ему функционировать в сети как самостоятельной единице, не связанной непосредственно с ПК. Конструкция предусматривает возможность крепления на кронштейн, некоторые камеры в стандартной поставке оснащаются поворотным устройством, например модель AXIS 2130R. Имеющиеся возможности ПО позволяют обеспечивать доступ к встроенному web-серверу как всем пользователям, так и отдельным группам (часть может только просматривать, часть администрировать). Существуют даже беспроводные устройства (одним из первых было Air DCS-1000W компании D-Link, стандарт 802.11b).

Применение таким устройствам находится почти во всех областях, требующих оперативного контроля. Многие фирмы — владельцы горнолыжных курортов очень любят размещать на своих сайтах ссылку на web-камеру, чтобы направляющиеся на отдых люди могли в реальном времени оценить состояние склонов, количество людей в различное время, мощность и работоспособность снежных пушек. А если камера поддерживает возможность передачи музыки (имеет встроенный микрофон или возможность подключить внешний) — то можно понаблюдать за работой, например, диджея. Также незаменимы подобные устройства, особенно беспроводные, для различных охранных структур. Для этого существуют дополнительные опции в виде детекторов движения (программный модуль, позволяющий оценить не только факт наличия объекта, но и его размеры, скорость), гибко настраиваемых для предотвращения ложных срабатываний, входов и выходов для подключения датчиков тревоги.

Наконец, даже в офисе бывает удобно, просто набрав адрес в браузере, посмотреть, много ли людей в данный момент в буфете, готов ли кофе в горячо любимой всем этажом кофеварке (и не уносит ли вожделенную колбу сотрудник другого отдела), принесли ли бутылку с водой за вас или надо идти и нести самому, поскольку жажда становится невыносимой. Применение можно найти вплоть до размещения камеры в комнате маленького ребенка, что избавит вас от необходимости реагировать на каждый подозрительный звук.

Подключать камеру именно в сеть, кстати, вовсе не обязательно. Существуют модификации, позволяющие использовать обычный телефонный модем, ISDN- или xDSL-технологию, кабельный модем (для передачи данных используются сети кабельного телевидения) или модем для сотовых сетей. ■ ■ ■ Денис Прозоровский

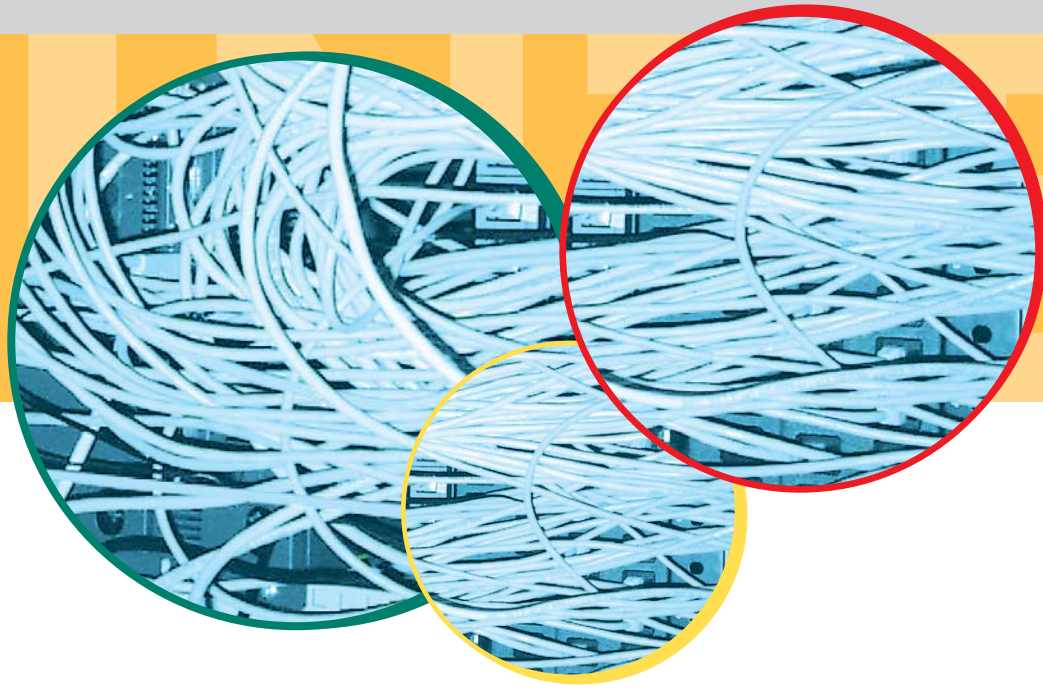
АНОНС

На медной паре
Связь по телефонным линиям 64

Выход в свет
Интернет по выделенной линии 68

Воздушный десерт
Спутники и радиоканалы 72

Обходной маневр
Технологии сетевой защиты 76



Dialup, DSL

На медной паре

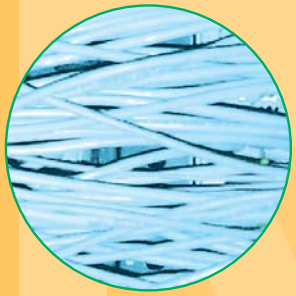
Локальные сети, выделенная линия, спутниковый канал — все это очень нужные и приятные вещи. Однако все начиналось с модема — устройства, способного связываться с себе подобными, используя существующую инфраструктуру телефонной связи.

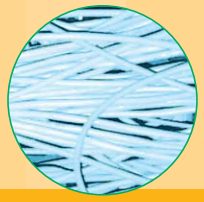
Современные технологии предлагают способы подключения отдельных ПК и локальных сетей к Интернету на любой вкус и кошелек. Вместе с тем, подавляющее большинство из них требуют довольно серьезных начальных вложений, состоящих в основном из прокладки кабелей. Безусловно, скорости доступа никогда не бывает слишком много, но все же пользователю лучше трезво оценивать свои потребности и соотносить свои аппетиты с размером бюджета. К тому же существуют технологии доступа, не требующие дополнительной инфраструктуры, а образно говоря, паразитирующие на существующих проводах. Это очень простой в использовании и настройке аналоговый dialup и его не столь пока распространенный цифровой аналог DSL.

Аналоговое соединение

Соединение называется аналоговым в силу того, что цифровые данные, которые поступают от компьютера для дальнейшей передачи, преобразуются в модеме путем модуляции в соответствии с выбранным протоколом и направляются в телефонную линию. На противоположном конце провода должен находиться модем-приемник, понимающий данный протокол. Если все хорошо, то есть на линии мало помех, приемник осуществляет обратное преобразование (демодуляцию) и пересылает восстановленные цифровые данные в компьютер, к которому он подключен.

Для обеспечения устойчивой связи необходимо, чтобы оба модема поддерживали общий протокол и были подключены непосредственно к компьютерам. »





Долгая история

Телеграф по телефону

История модемов началась в 30-х годах. Именно тогда появилась аппаратура, позволяющая передавать человеческую речь на большие расстояния, официально именуемая «аппаратурой тонального телеграфирования» и лишь особо продвинутыми специалистами называемая «модем». Вообще говоря, человеческая речь передается по телефонным проводам в виде колебаний электрического напряжения. Для того чтобы качество было безупречным, надо передавать колебания с частотами от 50 до 10 000 Гц. Но обеспечить передачу такого широкого диапазона частот слишком дорого, поэтому ограничиваются диапазоном частот, обеспечивающим удовлетворительную разборчивость речи, — от 300 до 3400 Гц.

Сигнал на выходе телеграфного аппарата имеет колебания частот от 0 Гц (то есть постоянного тока) до 200 Гц. Понятно, что такой диапазон частот не попадал в границы полосы пропускания и поэтому не мог быть передан через телефонную аппаратуру, предназначенную для дальней связи, а создавать специальные линии для телеграфа было невыгодно.

Тогда было придумано устройство для подсоединения телеграфного аппарата к телефонному каналу, что потребовало адаптации к полосе пропускания телефонной линии. На выходе телеграфного аппарата напряжение может принимать два фиксированных значения, соответствующие нулю и единице. Если сначала закодировать, а потом по тому же алгоритму раскодировать сигнал, получается прообраз современных модемов. Создание устройства, которое для напряжения отрицательной полярности передавало в телефонный канал сигнал произвольной частоты, а для напряжения положительной полярности — сигнал другой частоты, позволило вписать сигнал в диапазон телефонного канала. На другом конце стояло устройство, определяющее частоту принимаемого сигнала и превращающее сигналы различной частоты в сигналы разной полярности. Первый из процессов называется модуляцией, а второй, обратный ему, демодуляцией. Так как по телефонному каналу возможна одновременная связь в двух направлениях, то на каждом из концов канала ставились устройства, осуществлявшие как модуляцию, так и демодуляцию. От сокращения слов «модуляция» и «демодуляция» и было образовано слово «модем».

Самым первым модемом для ПК стало устройство производства компании Hayes Microcomputer Products, которая в 1979 году выпустила Micromodem II для популярных тогда персональных компьютеров Apple II. Модем стоил $380 и работал со скоростью 110/300 bps. До этого на рынке существовали только специализированные устройства, которые объединяли мейнфреймы.

Кстати, фирма Hayes выпустила в 1981 году и первый модем Smartmodem 300 bps, система команд которого стала отраслевым стандартом и остается им по сей день. Первые модемы с «коммерческой» скоростью передачи 2400 bps были представлены несколькими компаниями в декабре 1981 года на выставке Comdex по цене $800–900. А затем настало время U.S. Robotics. В 1985 году эта компания начала выпуск своей знаменитой серии Courier, существенно снизив планку стоимости модемов 2400 бит/с. В начале следующего года появился первый модем Courier HST со скоростью передачи 9600 бит/с, а в 1988 году — модемы Courier Dual Standard, которые поддерживали протоколы связи HST и v.32 ($1600), и Courier v.32 ($1500). Еще через два года был выпущен модем Courier v.32bis, в 1994-м — Sportster v.34 со скоростью передачи 28,8 Кбит/с ($349), а в 1995-м — Courier v.Everything 33,6 Кбит/с.

» Увы, даже на самых совершенных аналоговых модемах при идеальных условиях связи скорость работы все равно будет на уровне черепашьей. Так, на предельной скорости 57 600 Кбит/с мегабайтный файл будет предаваться около 3–5 минут. Так что 12–15 Мбайт/час — это предельная скорость для этого соединения. Однако в том случае, если выбирать не приходится, следует довольствоваться скоростью аналогового модема.

Для работы в Интернете самой минимальной приемлемой скоростью является 28 800 Кбит/с. А большинство имеющихся в продаже модемов поддерживают протокол связи v.90 и, стало быть, теоретически способны работать на скорости 57 600 Кбит/с. Правда, даже в крупных городах лишь немногие модемы смогут выжать из себя этот максимум. Это связано как с неоднородностью телефонных сетей, так и с тем, что далеко не все интернет-провайдеры могут позволить себе установку модемного пула на каждой АТС.

Протоколы

Конечно же, тип протокола, которым пользуется модем, и даже тип его аппаратной структуры совершенно не важны. Единственный волнующий пользователя показатель — скорость соединения, причем не заявленная в документации, а реальная скорость приема и передачи данных. Прежде всего — приема: известно, что объем отправляемой с компьютера информации при работе в Интернете в 8-10 раз ниже, чем объем информации принятой.

Стандарты обмена данными с помощью модемов подразделяются на четыре группы: протоколы модуляции, протоколы коррекции ошибок, протоколы сжатия данных и протоколы взаимодействия. Вот основные протоколы, каждый из которых отвечает за работоспособность соединения.

Протоколы модуляции. Самыми современными считаются протоколы модуляции »

Внутренний DSL-модем практически ничем не отличается от такого же аналогового, но работает совершенно по-другому

» v.34bis и v.90. Первый устанавливает спецификацию для дуплексного (двустороннего) обмена данными со скоростью до 33 600 Кбит/с (ограничения обусловлены максимальной полосой пропускания аналогового телефонного канала) с помощью модулированных аналоговых сигналов и поддерживается практически всеми модемами. Протокол v.90 относится к последнему поколению и представляет собой асимметричную технологию. На стороне модема-передатчика, установленного на компьютере пользователя и подключенного напрямую к цифровому каналу, нет необходимости осуществлять аналогово-цифровое преобразование. За счет этого скорость передачи данных достигает 56 Кбит/с. На стороне модема-приемника аналогово-цифровые и цифро-аналоговые преобразования происходят обычным образом, поэтому и скорость передачи ограничена 33 600 Кбит/с. Данные на компьютер пользователя поступают с более высокой скоростью, а при работе в Интернете именно это и требуется.

Протокол v.90 работает там, где один из напрямую связываемых модемов имеет доступ к цифровому каналу. Применительно к коммутируемой телефонной линии это означает, что телефонная станция должна быть связана (напрямую или через ряд узлов) с другим модемом цифровым каналом. Если где-то в этой цепи применяется аналоговая линия, то скорость будет равна скорости самого медленного участка.

На практике при подключении к Интернету провайдер должен быть связан с вашей АТС посредством цифрового канала. Такая схема за редким исключением реализована только в крупнейших городах России, только у крупнейших (и, естественно, самых дорогих) провайдеров и только для АТС с электронным оборудованием. Однако обстановка на рынке телекоммуникаций быстро меняется к лучшему. Например, в Москве все АТС уже соединены цифровым волоконно-оптическим каналом связи.

Протоколы коррекции ошибок и сжатия данных. В настоящее время спецификации на коррекцию ошибок и алгоритмы сжатия данных при передаче объединены в протокол v.42bis. При межмодемном обмене информацией по данному протоколу на аппаратном уровне реализован контроль циклическим избыточным кодом (CRC). Это средство позволяет обеспечить достоверную информацию даже на линиях низкого качества. Сжатие данных методом специального алгоритма (Zempel-Ziv) позволяет уменьшить их объем в среднем в четыре раза и тем самым повысить скорость обмена данными. Хороший модем должен поддерживать все спецификации протокола v.42bis на аппаратном уровне.

Протоколы взаимодействия. Для описания форматов, сигналов, способов вызова и других параметров, определяющих возможности взаимодействия модемов, служат спецификации протоколов v.25bis, v.28 и других. В особую группу входят протоколы, описывающие порядок взаимной работы факсимильных устройств, обычно встроенных в модемы — группы 1, 2 и 3. Стандарты на их сигналы определены протоколами v.17, v.27ter и v.29. При покупке модема обратите внимание на его способность поддерживать стандартные протоколы. »

Внутренняя политика

Диалекты и апгрейды

Помимо всем понятных и общепринятых протоколов, практически каждый крупный производитель предлагает и собственные разработки. Среди таких предложений Codex (Motorola), HST (U.S. Robotics), PEP, TurboPEP (Telebit) и ZyXel, созданный одноименной компанией. Эти протоколы хороши исключительно в тех случаях, когда и на том, и на другом конце линии работают модемы одних и тех же производителей. Конечно же, на скорость будут влиять и характеристики телефонной линии, которые определяются качеством прокладки, количеством соединений и даже погодными условиями. Известны случаи, когда пользователи замечали падение скорости в дождливую погоду, и, напротив, резкое увеличение скорости, как только земля просыхала. Поэтому не стоит рассчитывать на прирост производительности, устанавливая связь между двумя однотипными модемами, уж лучше обратить внимание на другие способы ускорения соединения, которые предлагаются производителями.

Сейчас практически у каждой крупной компании на сайте выложены прошивки (микропрограммы для модемов), позволяющие, не меняя аппаратной части, существенно обновить свой модем. Такую же услугу, и тоже бесплатно, оказывают интернет-провайдеры. Поэтому прежде чем идти покупать новый модем, стоит посетить сайт производителя. Вдруг для вашего устройства есть новая версия прошивки.

И еще: даже если вы встретите в многочисленных форумах способы перепрошивки модемов, которые этой процедуре, по утверждению производителя, не поддаются, относитесь к ним с осторожностью: то, что получилось с одним модемом, не факт, что получится с другим. Возможно, тот, кто описал историю своего успеха в форуме, просто перепутал модели.

Внешний ADSL-модем. Возможность USB-подключения развязывает руки пользователю

» DSL

Увеличение потоков информации, передаваемых по Интернету компаниями и частными пользователями, а также потребность в организации удаленного доступа к корпоративным сетям породили потребность в создании недорогих технологий цифровой высокоскоростной передачи данных по самому «узкому» месту цифровой сети — абонентской телефонной линии. Технологии DSL позволяют значительно увеличить скорость передачи данных по медным парам телефонных проводов без необходимости модернизации абонентских телефонных линий. Именно возможность преобразования существующих телефонных линий в высокоскоростные каналы передачи данных и является главным преимуществом технологии DSL.

Впервые аббревиатура DSL была обнародована фирмой Bellcore (ныне Telcordia Technologies). Характеризует фирму уже то, что помимо DSL Bellcore разработала такие технологии, как ATM и SONET. Переименование произошло в 1997 году и было одним из условий приобретения фирмы корпорацией SAIC (Science Applications International Corporation).

Расшифровывается DSL как Digital Subscriber Line (цифровая выделенная линия) и представляет собой различные способы передачи данных со скоростью, существенно превосходящей ISDN, по уже существующим медным телефонным проводам на расстояние до 18 000 футов (5,4 км). Буква «x» означает, что на этом месте могут стоять различные уточняющие обозначения, например A, H и т. д. Объединяет все технологии DSL применение способов модуляции CAP (Carrierless Amplitude and Phase — амплитудно-фазовая с подавлением несущей) или FDM (Frequency Division Multiplexing — частотное мультиплексирование).

Любопытно, что изначально DSL разрабатывалась как технология для реализации видео по заказу и интерактивного ТВ. Однако Акт о реформах в телекоммуникациях 1996 года, разрешивший конкуренцию телекоммуникационных, телефонных, кабельных, радио-, телепередающих и других компаний, связанных с передачей информации, изменил ситуацию. Началась гонка за предоставление скоростных каналов передачи цифровой информации, и единственной более или менее готовой технологией оказалась xDSL. Именно в ней телекоммуникационные фирмы видели способ удовлетворения растущей потребности в передаче большего количества данных, обусловленной взрывным ростом Интернета и интернет-телефонии.

DSL является относительно новой технологией, позволяющей расширить полосу пропускания старых медных телефонных линий, соединяющих телефонные станции с индивидуальными абонентами. Любой абонент, пользующийся обычной телефонной связью, имеет возможность с помощью технологии DSL значительно увеличить скорость своего соединения с Интернетом.

Следует помнить, что для организации линии DSL используются именно существующие телефонные линии; данная технология тем и хороша, что не требует прокладывания дополнительных телефонных кабелей. В результате вы получаете круглосуточный доступ в Интернет с сохранением нормальной работы обычной телефонной связи. Никто из ваших друзей больше не пожалуется, что часами не может к вам прозвониться. Благодаря многообразию технологий DSL пользователь может выбрать подходящую именно ему скорость передачи данных — от 32 Кбит/с до более чем 50 Мбит/с. Данные технологии позволяют также использовать обычную телефонную линию для таких широкополосных систем, как видео по запросу или дистанционное обучение.

Современные технологии DSL приносят возможность организации высокоскоростного доступа в Интернет в каждый дом или на каждое предприятие среднего и малого бизнеса, превращая обычные телефонные кабели в высокоскоростные цифровые каналы. Причем скорость передачи данных зависит только от качества и протяженности линий, соединяющих пользователя и провайдера. При этом провайдеры обычно дают возможность пользователю самому выбрать скорость передачи, наиболее соответствующую его индивидуальным потребностям.

Заключение

Несложно заметить, что даже самый скоростной доступ по коммутируемой линии дает возможность подключения только очень маленькой сети к Интернету. Это связано с невысокой скоростью передачи данных, которая будет делиться между несколькими пользователями. Если все участники такой сети общаются с внешним миром исключительно в текстовом режиме (IRC, ICQ и др.), то с такой скоростью еще можно мириться. А если все одновременно станут скачивать музыку и видео, то ждать каждому из них придется долго.

Совсем другое дело — DSL. В преимуществах у такого способа подключения — свободный телефон и высокая скорость соединения. Однако недостатков у этой технологии тоже хватает. Прежде всего — это ее малая распространенность, поэтому далеко не в каждом городе можно воспользоваться этой альтернативой старому доброму аналоговому модему. Однако ситуация меняется к лучшему, и практически каждый день приходят новости из разных городов о том, что тот или иной провайдер начинает предоставлять доступ в Интернет по DSL. Только не сразу и не везде, потому что ограничение по длине последней мили — пять километров — все еще не преодолено.

■ ■ ■ Михаил Парамонов

Выделенная линия

Выход в свет

Что может быть проще, чем купить сетевой адаптер и протянуть шнур до квартиры соседа? Можно будет играть в сетевые игры, обмениваться файлами и совместно использовать такие ресурсы, как принтеры, сканеры и модемы. Следующий шаг — подключение еще нескольких пользователей. Затем наступает время подключаться к Интернету.

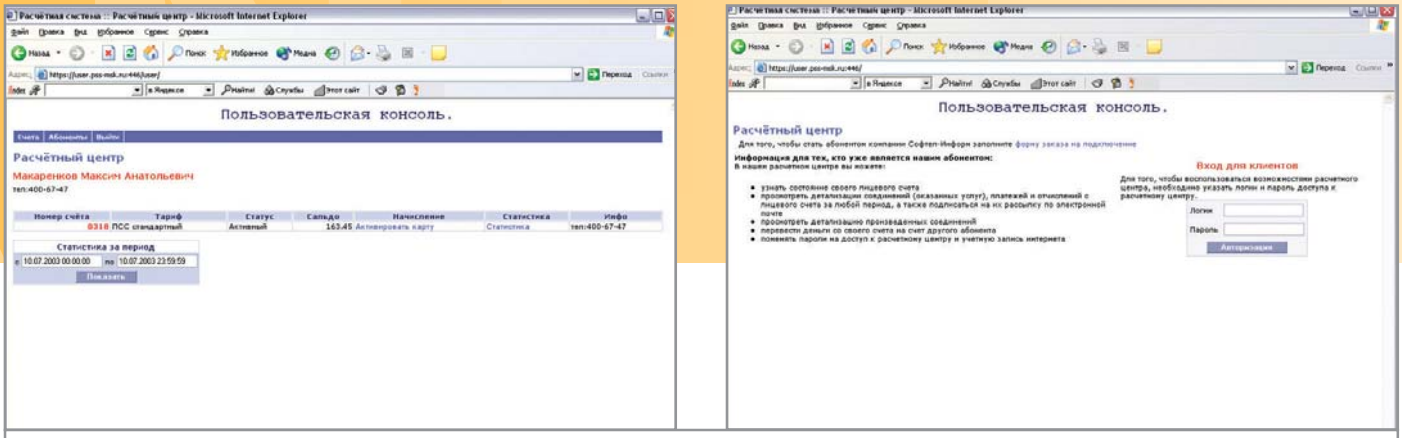
Первые шаги

Домашние сети объединяют несколько компьютеров, расположенных в одном доме. Но что если пойти дальше? Использовать модемы для подключения к Интернету при наличии домашней сети, конечно, можно. Причем с помощью компонента Internet Connection Sharing одним соединением могут пользоваться несколько человек. Однако при существующих скоростях модемной связи такое решение на самом деле не является лучшим. Просматривать сайты в текстовом формате и скачивать, в общем-то, небольшие файлы в течение нескольких дней не очень приятно. При совместном использовании модемного соединения скорость, которая и так в самом лучшем случае редко когда превышает 33 Кбит/с, уменьшится пропорционально количеству пользователей. Не очень хорошая экономия.

Гораздо лучшим вариантом является подключение домашней сети к Интернету по выделенному каналу. Для этого в первую очередь необходим провайдер. Если вы живете в крупном городе, лучше всего выбирать провайдера, расположенного в вашем районе. Особенно это актуально, если количество пользователей домашней сети невелико. Если количество пользователей составляет менее 10 человек, провайдер, скорее всего, не станет связываться с протягиванием кабеля через весь район, поскольку это ему будет просто невыгодно. Обычно провайдеры просят обратившегося к ним человека найти других пользователей, которые пишут заявки на подключение, и начинают работы только после того, как количество таких пользователей достигает хотя бы 10–15 человек.

Перед тем как сделать столь ответственный выбор, необходимо провести небольшое исследование. Узнайте, кто из них расположен ближе всего к вашему дому, есть ли в вашем районе другие дома, подключенные к Интернету, какие провайдеры подключили эти дома. Используйте своих друзей, знакомых и соседей для поиска информации. Правильный выбор провайдера позволит вам сэкономить недели, месяцы и даже, возможно, годы. Известны случаи, когда провайдер обещал начать подключение после того, как наберется более десяти желающих, однако по прошествии двух лет эти обещания так и не воплотились, несмотря на то, что требуемое количество пользователей было набрано. Лучше всего, если провайдер сам проявляет инициативу. В этом случае вам, по крайней мере, не придется долго ждать.

Если количество пользователей вашей домашней сети невелико, не расстраивайтесь. Для провайдера это, по большому сче- »



Провайдер предоставляет пользователю возможность следить за своим счетом. Не забывайте об этой полезной функции

ту, неважно. Он, скорее всего, все равно организует новую сеть. Используемое в домашних сетях оборудование редко когда поддерживает действительно высокие скорости передачи данных, и поэтому провайдеру в любом случае придется установить новые сетевые устройства и, возможно, сменить кабель. К тому же провайдеру нужны возможности расширения, а для этого требуются концентраторы с большим количеством портов. Так что не следует надеяться, что провайдер использует то, что у вас уже есть, и благодаря этому стоимость подключения снизится. Хотя и отметать такую возможность тоже не следует.

Следующий этап

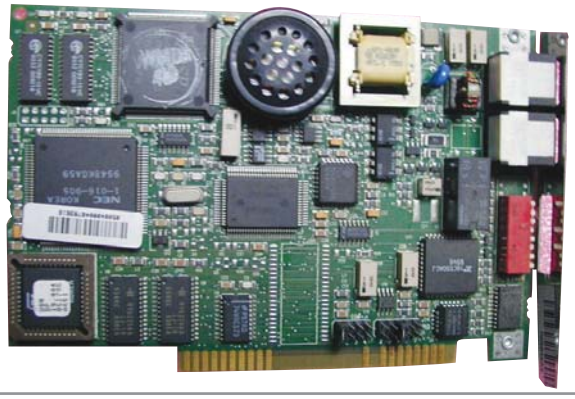
Итак, провайдер найден, требуемое количество пользователей собрано. Теперь наступает самый тяжелый и мучительный период — период ожидания. Прокладка сети занимает много времени, особенно если ваш дом — первая ласточка в районе. Время подключения дома к Интернету обычно варьируется от нескольких недель, если кабель уже протянут до соседнего дома, до нескольких месяцев, а то и года, если кабель приходится тянуть издалека. Однако рано или поздно наступит день, когда в вашем доме раздастся телефонный звонок и голос из трубки попросит вас выбрать тарифный план, сообщить информацию о своем компьютере, заполнить заявку, заплатить аванс или просто скажет, что ваш дом подключен к Сети.

Теперь все зависит от ситуации. Если оборудование вашей домашней сети не устраивает провайдера, у вас нет этой сети или вы к ней не подключены, к вам придут

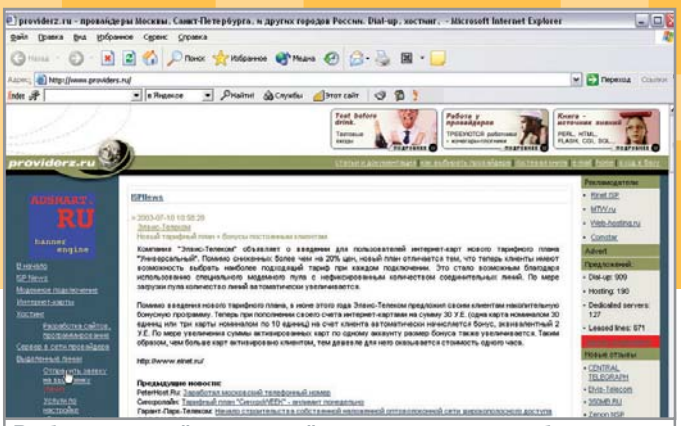
Полезные советы

Страховка от ошибок

- Выбирайте провайдера, расположенного ближе всего к вашему дому.
- Внимательно следите за техниками во время протягивания кабеля по квартире и требуйте устранить любой нанесенный ущерб.
- Отключите в BIOS опции пробуждения по сигналу сети (Wake on LAN) и по событиям управления питанием (PME), если они там есть. Если вы этого не сделаете, ваш компьютер будет включаться самостоятельно в любое время дня и ночи.
- Внимательно читайте акт приемки работ.
- Очень внимательно читайте договор с провайдером.
- Для начала выбирайте не самый дорогой тарифный план, а затем корректируйте его в соответствии с реальными потребностями.
- Никогда не забывайте о трафике. Известны случаи, когда ошалевшие от радости пользователи в первые два дня работы скачивали из Интернета несколько фильмов объемом около 2 Гбайт, а потом платили по $0,2 за каждый мегабайт сверх первых 400. Провайдер останется глух к вашим утверждениям о том, что «это вышло случайно». Ему ведь тоже приходится платить за этот трафик.
- Регулярно проверяйте статистику счета.
- Отключите показ картинок на интернет-сайтах (снимите галочку с пункта «Show Picture» в меню «Internet Options -> Advanced»). Это позволит вам сэкономить очень много денег на трафике. Большая часть картинок в Интернете — это рекламные баннеры, которые не очень интересны для просмотра. Но, разумеется, это дело вкуса.
- Воспользуйтесь программой для блокировки рекламы (Ad Killer, AdsGone, BannerAdFilter, и т. п.). Они также блокируют показ баннеров, экономя вам трафик.
- Обязательно установите на свой компьютер хороший антивирус.
- Обязательно используйте firewall. Помните, что как только вы воткнули кабель в свой сетевой адаптер, ваш компьютер перестал быть чем-то обособленным и стал частью Глобальной сети. А это означает большую уязвимость, чем раньше.
- Берегите свой IP-адрес как зеницу ока. Не раскрывайте его кому попало. Ваш IP-адрес, скорее всего, будет постоянным, и это откроет злоумышленникам гораздо большие возможности для взлома вашего компьютера.
- Убедитесь в отсутствии предоставляемых в общее пользование (shared) ресурсов на вашем компьютере. Лучше всего вообще удалите компонент «File and Printer Sharing». Если вы все же хотите предоставлять ресурсы в общее пользование, откройте их только для чтения, а еще лучше установите пароль для доступа и давайте его тем, кому вы доверяете.
- Связывайтесь с провайдером, если у вас возникнут любые проблемы при доступе к Интернету. Провайдер имеет перед вами некоторые обязательства (подробнее см. договор), однако не лишним будет напомнить ему об этом.



Теперь такие модемы уже история. Между тем они служили людям верой и правдой. Теперь же все мы мечтаем о выделенной линии



Выбирая провайдера, узнайте о нем как можно больше. В этом вам может помочь Интернет, где собрано огромное количество информации

» несколько человек, которые протянут к вашему компьютеру кабель от распределительного щитка в коридоре. Вот здесь и начнется самое интересное. Обычно этот кабель просто протягивается, то есть бросается прямо на пол посреди коридора, и честь убирать его под плинтус, под пол или хотя бы куда-нибудь достается вам. В некоторых случаях провайдеры предоставляют специальную платную услугу, именуемую «прокладка кабеля» (скрытая или открытая). Открытая прокладка кабеля означает, что его бросят не посреди пола, а протянут вдоль стены и, возможно, прибьют парой гвоздиков. Скрытая прокладка кабеля означает, что у вас в квартире отдерут плинтус и протащат кабель под ним, если такая возможность имеется. Здесь самое главное, чтобы при этом не сокрушили все находящиеся поблизости хрупкие и бьющиеся предметы и плинтус прибили обратно (причем именно той стороной, которой нужно).

Если провайдер не оказывает такой услуги, то, скорее всего, работники могут помочь вам, стоит только попросить, причем такой вариант может обойтись вам даже дешевле. Впрочем, они могут предложить сделать все «без бумажек», даже если данная услуга оказывается провайдером. В этом случае на такие предложения лучше не соглашаться, поскольку обычно предоставляется гарантия на прокладку кабеля по квартире, и при возникновении у вас претензий провайдер может прислать к вам людей для устранения недостатков прокладки.

Если это возможно, попросите техников не тянуть кабель прямо к компьютеру, а установить рядом с компьютером розетку, куда вы будете подключать еще один кабель по мере необходимости. Это позволит вам физически отключать свой компьютер от сети и Интернета, облегчит перестановку компьютера и вообще придаст комнате более эстетичный вид. После завершения прокладки кабеля вам, скорее всего, предложат подписать акт приемки выполненных работ. Внимательно читайте то, что подписываете, иначе в конце концов вам может прийти астрономический счет за работы, о которых вы даже не слышали.

После того как ваш компьютер подключили к сети физически, вам потребуется создать и настроить соединение с Интернетом. Для этого наверняка понадобятся имя пользователя и пароль, которые вы можете получить у провайдера. Если вам предоставят возможность выбора имени пользователя и, соответственно, адреса электронной почты, не надо придумывать ничего слишком сложного. Скорее всего, вы будете пользоваться этим адресом много лет, а для того чтобы сменить адрес, в большинстве случаев потребуется платить дополнительные деньги. Не проще ли сразу выбрать простой и удобочитаемый адрес?

За что и сколько платить

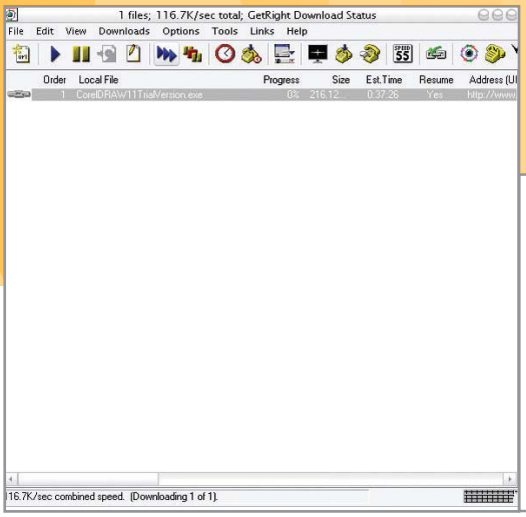
После выбора имени пользователя настанет самое интересное — выбор тарифного плана. Сегодня практически все взимают плату за трафик. И для определения тарифного плана вам понадобится как можно точнее оценить объем трафика, который вам потребуется. Обычно провайдеры взимают некую фиксированную абонентскую плату за определенный объем трафика (например, $30 в месяц за 200 Мбайт трафика), а весь трафик, превышающий этот объем, оплачивается помегабайтно (например, $0,20 за 1 Мбайт). Причем чем выше абонентская плата, тем ниже стоимость превышения. Так что для экономии средств желательно точно оценить свои потребности. Сменить тарифный план несложно, и для начала можно порекомендовать выбрать не самый дорогостоящий вариант. В конце концов, если вы не будете скачивать из Интернета фильмы, музыку и программы в огромных количествах, а ограничитесь просмотром сайтов, общением в чатах и использованием электронной почты, объем трафика будет не очень большой.

Обычно провайдеры предоставляют своим пользователям собственный FTP-сервер, на котором выложено огромное количество полезных вещей, включая музыку, фильмы, игры и т. д. Естественно, плата за пользование таким сервером минимальна или вообще не будет взиматься. Некоторые более продвинутые провайдеры организовывают и дополнительные бесплатные услуги, включая организацию игровых серверов, трансляцию радио- и телепрограмм, создание чат-серверов и многое другое.

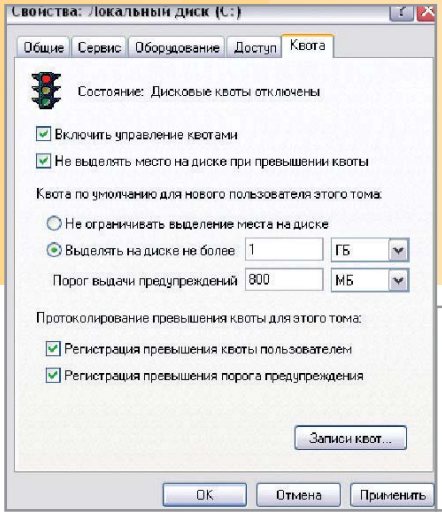
Хотя выделенная линия и имеет преимущества по сравнению с модемом, на ней также могут случаться обрывы связи, причем иногда они могут длиться до нескольких дней. Хорошо, если связь разрывается из-за перезагрузки сервера. Но если происходит обрыв на линии, восстановление соединения займет немало времени. Поэтому, если вы используете Интернет для работы, не выбрасывайте свой старый модем. Он вам еще может пригодиться в трудную минуту. Ведь провайдер не обязан компенсировать вам ущерб, понесенный из-за обрыва связи. Обычно это даже указывается в договоре.

Что будет после

После того как ваша сеть окажется подключенной к Интернету, перед вами откроется множество возможностей. Игры, общение, работа… Все это станет в миллион раз про- »



Одно из преимуществ выделенной линии — скорость передачи данных. Но не забывайте, что за каждый мегабайт придется платить



Помимо других преимуществ, формат NTFS позволяет выделять дисковые квоты для различных пользователей компьютера

» ще, если вы подключитесь к Интернету по выделенной линии. Если до этого вы пользовались только модемом, скорость соединения приятно удивит вас. А ваши домашние наконец-то смогут вдоволь наговориться по телефону. Сегодня расходы на работу по выделенной линии вполне сопоставимы с расходами на модем, а подключение стоит всего в полтора-два раза дороже хорошего мощного модема. О качестве же связи здесь и говорить нечего. Так что выбор очевиден.

Если вы будете постоянно пользоваться Интернетом, подумайте о том, чтобы сменить операционную систему. Файловая система FAT32, применяемая в Windows 98/Me, а иногда и в Windows 2000, не обеспечивает полного контроля над доступом к файлам и ресурсам вашего компьютера. UNIX, Linux, Windows NT или Windows 2000 (с файловой системой NTFS) обеспечат значительно более высокий уровень защиты вашего компьютера от взлома и вирусов. А правильная настройка опций доступа и безопасности защитит ваш компьютер на 99,99%. Правда, для этого уже требуются специальные знания.

Дважды подумайте, прежде чем вызывать для этой цели «технического специалиста» провайдера. Во-первых, эта услуга, скорее всего, будет платной. Во-вторых, нет уверенности, что специалист действительно будет обладать достаточной квалификацией для того, чтобы закрыть все порты, кроме используемых, и полностью регламентировать доступ вашего компьютера к Сети. Такие специалисты встречаются не очень часто и обычно работают не у провайдеров, а в других местах. Чем крупнее провайдер, тем лучше работающие у него специалисты, но это не значит, что они действительно будут возиться с настройками для обеспечения защиты вашего компьютера. Обычно перечень услуг специалистов и расценок приводится в прайс-листе. И число этих услуг обычно ограничивается установкой операционной системы, антивирусов, firewall и различных программ. Так что вызывайте специалиста только в том случае, когда вы не в состоянии справиться с требуемой задачей сами. И обязательно уточните стоимость вызова и количество нормо-часов, которые потребуются специалисту для выполнения требуемой работы. В противном случае счет может вас неприятно удивить.

И помните: доступ в Интернет предоставляется вам провайдером. Так что если у вас возникнут какие-нибудь проблемы — смело звоните в службу технической поддержки. Помогать вам решать проблемы — работа сотрудников этой службы, причем консультации по телефону они должны оказывать бесплатно. ■ ■ ■ Матвей Петренко

Правила безопасности

Прелести и опасности постоянного соединения

При работе в Интернете следует соблюдать осторожность. Не забывайте, что как только к вашему компьютеру подключается сетевой кабель, он перестает быть независимой единицей, а становится частью Глобальной сети. А это означает уязвимость. Интернет кишит желающими поживиться за чужой счет и просто любителями поразвлечься, взламывая чужие компьютеры. Обязательно используете самые последние средства безопасности, если вы хоть немного цените информацию, хранящуюся на вашем компьютере. Внимательно следите за статистикой соединений и немедленно оповещайте провайдера, если увидите, что на ваш счет записан «лишний» трафик. Это может означать, что кто-то из ваших соседей по локальной сети узнал ваш пароль и решил сэкономить собственные деньги. В этом случае необходимо немедленно сменить пароль и принять меры для его защиты. Может быть, даже стоит его запомнить, а не сохранять автоматически. Вернуть деньги или выявить злоумышленника получится вряд ли, но защититься от дальнейшего использования вашего логина вы вполне сможете.

После подключения к провайдеру ваша домашняя сеть перестанет быть чисто вашей домашней сетью, а, скорее всего, будет объединена с другими домашними сетями, подключенными к тому же провайдеру. В связи с этим имеет смысл заблокировать доступ к ресурсам вашего компьютера. Ведь одно дело, когда вашим принтером пользуется с вашего разрешения ваш сосед, а другое дело, когда им пользуется какой-нибудь дядя из соседнего района, которому пришло в голову «немного пошутить» и распечатать на вашем компьютере полный текст файла win386.swp. Закройте доступ к общим (shared) ресурсам или хотя бы защитите их паролем. Ни в коем случае не открывайте ни одну из своих папок для записи. Это позволит любому шутнику напичкать ваш компьютер вирусами.

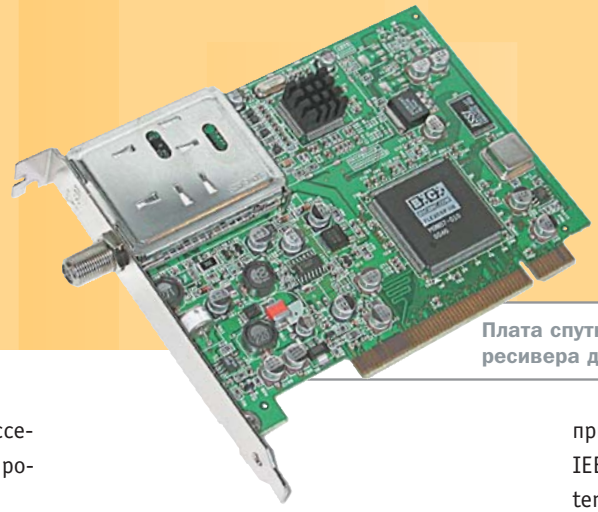
Спутники и радиоканалы

Воздушный десерт

Как только на заре развития информационных технологий два компьютера были соединены проводами, пытливые умы стали искать способы эти самые провода разорвать. Конечно, в те времена эта идея воспринималась многими как еще один сюжет для фантастического рассказа, однако, как показала история, технологические решения, которые могли бы осуществить мечту о беспроводных коммуникациях, уже существовали…

История о механическом пианино

В декабре 1940 года в американский Национальный совет изобретателей поступило описание способа организации помехозащищенной радиосвязи, основанного на методе перескока частоты. Авторы изобретения — актриса Хеди Ламар (Хедвиг Ева Мария Кислер) и композитор Джордж Антейль — предложили использовать в качестве одного из элементов передающего устройства модифицированное механическое пианино. Количество частот, между которыми мог происходить перескок, соответствовало числу клавиш — 88. Изобретение надолго положили под сукно, однако доподлинно известно, что во время Карибского кризиса американские войска получили в свое распоряжение помехозащищенные устройства, использующие перескок частоты. Беспроводной бум, наблюдаемый в настоящее время, начался в 90-х годах про- »



Плата спутникового DVB-ресивера для слота PCI

шлого века. И его причиной стало рассекречивание военных технологий беспроводной связи.

Несмотря на то что Хеди Ламар прожила долгую жизнь, ее роль в становлении беспроводных технологий до самого последнего времени была неоцененной. Большинству пользователей компьютеров она была знакома лишь по изображению на загрузочной заставке Corel Draw. Ее заслуги в мире IT-технологии были отмечены только в 1997 году, когда актриса была представлена к награждению медалью Чести Конгресса.

А сам метод скачка частоты (Frequency Hopping Spread Spectrum — FHSS), являющийся сегодня одним из двух способов организации беспроводной связи, истоками своими восходит именно к тому самому механическому пианино.

Сила и слабость радиоканалов

Самое главное преимущество беспроводных радиосетей, благодаря которому широкополосные технологии передачи данных победоносно шествуют сегодня по всему миру, состоит в том, что отсутствие проводов дает клиентам не только альтернативные, не зависящие от характеристик среды линии связи, но и обеспечивает в общем случае известную мобильность.

Варианты подключения, таким образом, можно весьма условно разделить на две группы — стационарные и мобильные. В первом случае все достаточно понятно: пользователю нужно всего лишь приобрести соответствующее приемное оборудование и антенну и направить последнюю на антенну провайдера. При этом решение возникающих проблем и неприятностей, как правило, берет на себя сторона, продающая трафик.

При мобильном подключении на первый взгляд проблем должно быть меньше, поскольку ориентация принимающей антенны не важна — данные передаются от одной точки (антенна типа «штырь») по всему радиусу действия. Но в этом-то и состоит основной недостаток радиосетей — низкий уровень безопасности. Перехват беспроводного трафика, который при наличии оборудования и соответствующей квалификации особо трудной задачи не представляет, был головной болью всех администраторов с самого начала существования беспроводных сетей. Однако на первом этапе развития эта проблема не казалась особенно серьезной.

Безопасно или без опасности?

Характерно, что ситуация с низкой безопасностью радиосетей могла бы еще долгое время оставаться неразрешенной. Однако огромный потенциал беспроводных технологий привел к скачкообразному росту количества wireless-коммуникаций.

Попытки создания единых рекомендаций обеспечения безопасности предпринимались и предпринимаются постоянно. Например, некогда разработанный стандарт IEEE 802.11x определяет протокол EAP (Extensible Authentication Protocol), призванный обеспечить механизм аутентификации участников беспроводных соединений и механизм шифрования WEP (Wire Equivalent Privacy). Оба этих решения, к сожалению, не оказались удачными. Более того, компании-поставщики очень часто при инсталляции оборудования не устанавливали микросхемы шифрования, держа их «в кармане».

В настоящее время комитет IEEE ведет разработку стандарта 802.11i, который, по замыслу идеологов wireless-сетей, должен решить все проблемы. Но пока этот стандарт находится в стадии разработки, компании — провайдеры беспроводных сетей в основной массе не рискуют предоставлять пользователям мобильные беспроводные соединения. Тем не менее стационарный вариант wireless-сетей остается весьма и весьма привлекательным для широкого круга пользователей. При этом основным способом обеспечения безопасности, как правило, является надежда оператора на то, что сравнительно узкий направленный радиоканал злоумышленнику обнаружить будет довольно сложно.

Симметричный доступ

Спутник в обе стороны

Симметричный спутниковый канал, который обеспечивает прохождение трафика в обе стороны, — удовольствие не из дешевых. Даже если не учитывать затраты провайдера на аренду спутникового передатчика, а посчитать лишь расходы на оконечное оборудование, то получится вполне круглая сумма в несколько десятков тысяч долларов. И даже если вы уже когда-то использовали оборудование для асимметричного доступа, то, скорее всего, вам придется его менять. Это касается как тарелки, так и собственно всего оборудования.

Компании, которые предоставляют пользователям подобные услуги, продают, как правило, полные приемопередающие комплекты, в которые кроме антенны входит спутниковый кабельный модем (или IP-терминал с обратным каналом). Схема работы такой системы довольно проста: спутник выступает в роли связующего элемента между конечным пользователем и земной станцией спутниковой связи (ЗССС). Такие системы называются системами двустороннего спутникового доступа.

Точка беспроводного доступа Radio Ethernet

» Справедливости ради стоит отметить, что многие компании — поставщики беспроводного оборудования пытаются решить проблему обеспечения безопасности своими способами. Делается это, как правило, двумя методами — разработкой собственных аппаратных решений и использованием существующих технологий на транспортном и прикладном уровнях.

Интернет через спутник

Впервые мысль об использовании околоземных спутников для передачи данных родилась еще до создания Интернета. Первые попытки объединения экспериментальной спутниковой сети SATNET с прародительницей Всемирной глобальной сети ARPANET, как известно, не привели к каким-то значительным результатам. Интересно, что побочным продуктом этой разработки стал протокол TCP, который сегодня является краеугольным камнем всей Сети.

Несмотря на относительную неудачность первой попытки, идея спутникового канала все-таки нашла свое продолжение. Более того, как утверждает всезнающая статистика, до 40% всех американцев пользуются услугами того или иного спутникового провайдера. Интересно, что для скоростного и качественного доступа в основном используются так называемые несимметричные спутниковые каналы, идея которых основана на неоднородности интернет-трафика.

Симметрично и не очень...

Асимметричность Интернета, которая сегодня определяется как «перекос распределения трафика в сторону приема информации», проявилась практически сразу после возникновения WWW и многих интернет-приложений, ориентированных не на взаимный обмен данными (как, например, электронная почта), а на выдачу информации клиенту по его запросу.

Первым техническим решением, которое увидело свет во второй половине 80-х годов, стала система DirecPC компании HUGHES Network Systems. Несмотря на свое относительное техническое несовершенство, она стала настоящей технологической революцией, ведь обыкновенный модемный пользователь получал возможность подключения к Сети со скоростью, сравнимой с хорошими оптоволоконными каналами — до 500 Мбит/с. Именно первенство в этой области, а также абсолютная закрытость принципов передачи позволили системе DirecPC примерно на пять лет стать своеобразным монополистом на этом рынке.

И еще довольно долгое время ситуация со спутниковыми интернет-каналами напоминала классическую басню «Лебедь, рак и щука». Каждый разработчик вслед за DirecPC предлагал свое «абсолютно уникальное» оборудование, которое не только не стыковалось с аппаратурой всех остальных производителей, но и работало на корпоративных (proprietary) протоколах.

К числу подобных проектов можно отнести и малоизвестную у нас систему ZakNet (собственник — кувейтская компания ZakSat), которая использовала мощности спутника AsiaSat-2 и была ориентирована на пользователей Ближнего и Дальнего Востока. Представители российского IT-рынка уже тогда пытались выйти на мировой уровень. Проект NetStar предлагал пользователям полосу передачи данных со скоростью 2 Мбит/с. Используемый для этого спутник IntelSat-604 обеспечивал зону покрытия от Восточного Урала до Западной Европы. Система была успешно запущена в 1998 году, когда на смену закрытым корпоративным протоколам пришел новый стандарт.

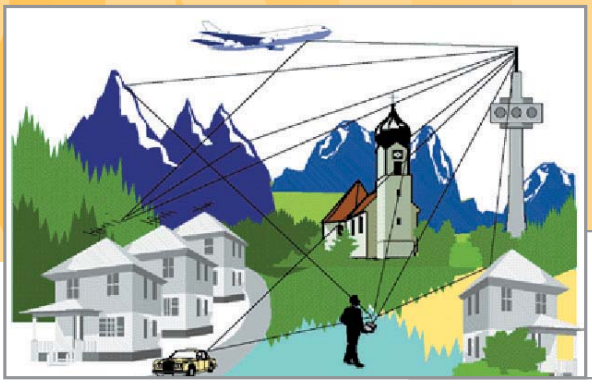
DVB спешит на помощь

Кардинально ситуация на рынке спутникового Интернета изменилась лишь тогда, когда выяснилось, что стандарты MPEG-2, а особенно DVB (Digital Video Broadcast), успешно могут применяться не только для передачи цифрового видео, но и данных. Конечно, речь идет не столько о самой технологии DVB, которая определяет лишь способ передачи цифровых данных по спутниковым или кабальным каналам, сколько о надстройке над DVB, которая называется MPE (Multi-Protocol Encapsulation) и позволяет встраивать в цифровой поток пакеты данных.

Формат передаваемого таким способом пакета очень напоминает формат кадров Ethernet, поэтому разработчикам драйверов под DVB-карты в этом плане особых усилий прилагать не пришлось. Основное преимущество комплексного подхода — возможность объединения в одном нисходящем луче цифрового видео и интернет-трафика — позволило наладить производство универсальных приемных устройств. А это, в свою очередь, привело к тому, что на рынке появился целый ряд компаний, предлагающих пользователям не только прием телевизионных каналов, но и спутниковый доступ в Сеть. Ситуация стала развиваться довольно стремительно, поскольку и схема доступа, и этапы построения соответствующей инфраструктуры были уже известны и отработаны.

Прямой и обратный каналы

Схема работы асимметричного канала довольно проста и интуитивно понятна. Основная идея заключается в том, что запрос на получение данных направляется в Сеть через уже существующую линию — с помощью коммутируемого (модем, ISDN) или »



Благодаря беспроводным коммуникациям человек получает невиданную свободу передвижений, при этом всегда оставаясь на связи

постоянного соединения. Выстроенный таким образом канал запроса называется обратным, и его скорость принципиально не важна, поскольку общий размер пакетов-запросов невелик.

Запросы направляются на центральный узел, который, как правило, оснащен высокоскоростными коммуникациями. Узел, получив информацию из Сети по пользовательскому запросу, формирует пакеты и направляет их на спутник по каналу, называемому uplink. И уже со спутника информация попадает на компьютер пользователя. И именно этот канал является прямым.

Для конечного клиента ситуация асимметричности трафика оборачивается прямой выгодой. Все запросы (до 10% трафика), за которые, как правило, провайдер денег не берет, отправляются по земле, то есть через обратный канал, а ответы (90% трафика) принимаются через спутниковую тарелку (прямой канал). Интересно, что стоимость трафика, приходящего с тарелки, примерно в полтора-два раза ниже стоимости наземного.

Эта цифра, безусловно, разная у всех провайдеров, но порядок примерно таков. Парадокс ситуации заключается еще и в том, что себестоимость наземного трафика несколько ниже себестоимости трафика космического. Однако же эксплуатационные расходы российских провайдеров не позволяют им выйти на приемлемый мировой уровень цен.

Будущее — за беспроводными сетями!

Несомненно, беспроводные сети через некоторое время станут способными завоевать весь сетевой мир. Однако сегодня темпы их развития немного сократились. Некоторые аналитики считают, что это обусловлено достижением точки, за которой «критическая масса» беспроводных коммуникаций должна дать старт глобальному качественному изменению. Вероятно, это связано с разработкой новых, более безопасных стандартов, однако, скорее всего, перелом произойдет не в технологиях, а в умах пользователей, которые должны будут просто привыкнуть к беспроводным коммуникациям. И случится это, будем надеяться, в самое ближайшее время.

Леонид Федоров

Вариации на тему

«Классика» и альтернативы

Наибольшее распространение сегодня получили беспроводные сети стандарта IEEE 802.11b, который с подачи корпорации Microsoft был назван Wi-Fi (Wireless Fidelity). Основные его характеристики определяют скорость передачи до 11 Мбит/с в частотном диапазоне 2,4 ГГц. Основной недостаток этого стандарта наряду с недоработанностью системы безопасности — отсутствие четкого механизма роуминга. Более «продвинутые» IEEE 802.11a и IEEE 802.11g увеличивают возможный диапазон скоростей до 54 Мбит/с за счет изменения способа модуляции и некоторого увеличения мощности передающего оборудования. При этом компании — производители оборудования стандарта 802.11a, который является двухчастотным, постепенно переносят свое внимание на диапазон 5 ГГц, который, во-первых, пока не лицензируется в большинстве стран (но не в России) и, во-вторых, обладает потенциально более высокой устойчивостью к помехам.

Потенциальная перспективность пятигигагерцового диапазона заставляет многочисленных производителей изобретать свои методы и технологии. Особо стоит отметить разработку Nokia и Ericsson под наименованием HyperLAN (и более поздний вариант HyperLAN2) и технологию Canopy от Motorola.

Также внимания заслуживает разработка, называемая Wireless FireWire, которая представляет собой беспроводную реализацию стандарта IEEE 1394. В настоящее время рабочая группа ассоциации 1394 Trade Association работает над технологической реализацией специального «адаптивного» слоя. Этот программно-аппаратный уровень должен будет отвечать за соединение протоколов 1394 с протоколами беспроводных сетей. К числу своих основных задач рабочая группа относит также реализацию схемы защиты информационного наполнения. Речь идет о встраивании в беспроводную реализацию FireWire стандарта защиты Digital Transmission Content Protection, разработанного в свое время для защиты информации в кабельных сетях.

Точка доступа стандарта Wi-Fi (вид спереди и сзади), наиболее продвигаемого сегодня на рынке беспроводных коммуникаций

Обходной маневр

Обзор технологий сетевой защиты

Несмотря на падение рентабельности IT-проектов, вероятно, единственной группой компаний, сохранивших или увеличивших свою прибыль, являются фирмы, специализирующиеся на обеспечении безопасности информационных систем. Угроза утечки конфиденциальной информации или уничтожения корпоративных баз данных не позволяет сократить затраты в этой области.

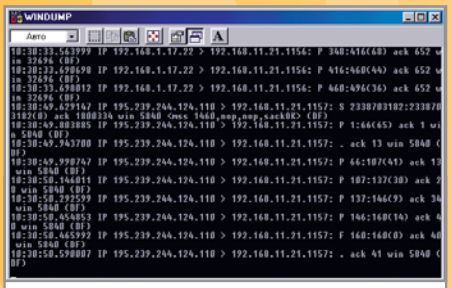
Списки программных и аппаратных решений сетевой защиты, предлагаемых такими гигантами, как Symantec, Internet Security System, Cisco, вызывают у непосвященного человека легкое замешательство. Если поставить межсетевой экран, смогут ли злоумышленники взломать web-сервер компании в Интернете? А если организована корпоративная VPN-сеть, возможен ли перехватит ICQ и e-mail-сообщений? Для ответа на эти и другие вопросы необходимо иметь представление о концепции основных технологий сетевой безопасности. Начнем обзор средств защиты с описаний существующих проблем сетевой безопасности, указывая затем способы их решения.

Перехват трафика

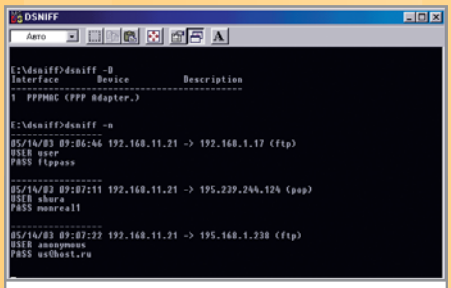
Доступ злоумышленника к сети передачи данных предоставляет ему возможность перехвата и анализа всего сетевого трафика в данном сегменте сети. Исторически сложилось так, что большинство используемых прикладных протоколов передают данные в открытом, не зашифрованном виде. В качестве примеров таких потенциально небезопасных протоколов можно привести протокол передачи файлов FTP, протоколы связи с удаленным терминалом — Telnet и Rlogin, протоколы передачи и получения e-mail-сообщений — SMTP и POP3, протокол передачи гипертекстовых документов HTTP.

В результате злоумышленник имеет возможность перехватывать как верификационные данные пользователя (регистрационное имя и пароль), так и данные с файлами, передаваемые в этом соединении, а также выполнять некоторые виды сетевых атак — принудительно разрывать соединение или принимать участие в этом соединении (технология «man-in-the-middle»), подменяя передаваемые данные и подделывая команды и ответы участвующих сторон.

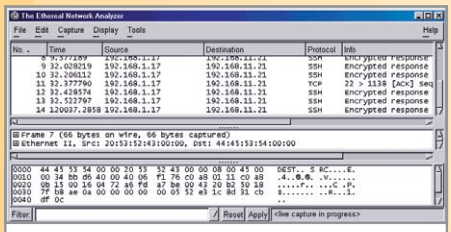
Программы для перехвата и анализа сетевого трафика (снифферы, от англ. sniff — «нюхать», «принюхиваться») появились одновременно с локальными сетями как инструмент диагностики сетевой среды. Вскоре выяснилась возможность двойного использования этого инструментария. Помимо целей сетевого администрирования, техноло- »



Перехват трафика утилитой WinDump



Перехват паролей с помощью DSniff



Анализ перехваченного сетевого трафика сниффером Ethereal Network Analyzer

гии, использованные в снифферах, стали применяться злоумышленниками для перехвата конфиденциальной информации, передаваемой по сети.

В качестве примеров программ-снифферов, используемых в диагностических целях при администрировании сетей, можно привести Tcpdump (только для Unix-платформ, для платформ Windows — аналог программы WinDump) и Ethereal (программа адаптирована как для Unix, так и для Windows). В качестве инструментария злоумышленника можно привести программы DSniff и Cain.

Осуществляя контроль и фильтрацию данных, передаваемых по криптографически не защищенным протоколам, утилита DSniff превращает перехват паролей в тривиальную задачу. На данный момент поддерживается анализ 22 распространенных протоколов. В их числе сетевые сервисы Microsoft — NFS и SMB, пользовательские коммуникационные сервисы ICQ и IRC, службы обмена файлами Napster, утилиты управления удаленным компьютером Symantec pcAnywhere, идентификация пользователей базы данных Oracle SQL.

Утилита Cain предоставляет более широкие возможности. Помимо перехвата определенных данных из сетевого трафика, реализована возможность подбора паролей для взлома защиты передачи данных по криптографически защищенным протоколам. Также реализована возможность выполнения атаки вида APR spoofing (Arp Poison Routing), приводящей к тому, что весь трафик между двумя компьютерами начинает пересылаться через компьютер злоумышленника (технология «man-in-the-middle»). В результате даже при использовании шифрования данных злоумышленник имеет контроль над всей передаваемой информацией.

Приведенные примеры иллюстрируют угрозу и последствия применения злоумышленниками технологий перехвата данных. Для противодействия этой опасности разработаны несколько методик, включающих аппаратные и программные решения. Рассмотрим примеры их типичного использования.

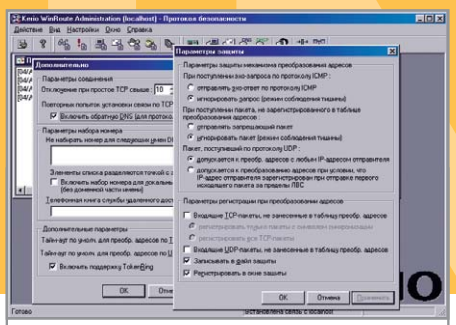
Для защиты информации, передаваемой по небезопасной среде, где существует потенциальная возможность перехвата данных (например, связь между несколькими компьютерами и локальными сетями через Интернет), рекомендуется использовать технологии VPN (Virtual Private Network — виртуальная частная сеть). В этом случае весь обмен данными между компьютерами, образующими VPN, кодируется невидимо для клиентов этой сети. Даже при использовании клиентами VPN криптографически незащищенных прикладных протоколов для связи между собой (Telnet, FTP и т. д.) анализ перехваченного злоумышленником трафика потребует декодирования данных, что при использовании современных аппаратных возможностей требует значительного времени, сравнимого с несколькими годами. Правда, это только в том случае, если не были допущены ошибки при реализации алгоритмов кодирования или разработчики не оставили возможность (черный ход) для универсального декодирования данных.

При невозможности организации VPN следует отказываться от небезопасных прикладных протоколов, заменяя их аналогами, поддерживающими криптозащиту. Например, SSH — адекватная замена небезопасным протоколам связи с удаленным терминалом Telnet и Rlogin, для FTP — замена SFTP, для web-сервисов — HTTPS. Для разработки защиты собственных прикладных протоколов можно использовать методики и технологии проекта OpenSSL.

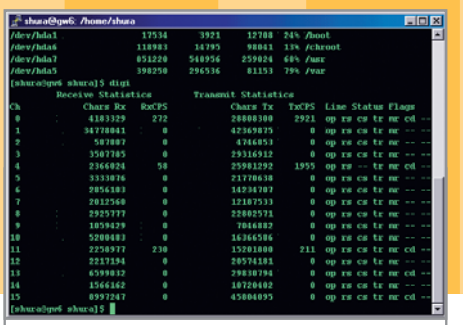
Использование обычных сетевых коммутаторов для устранения возможности перехвата злоумышленником трафика в локальной сети неэффективно. В теории коммутатор строит таблицу динамической маршрутизации, определяя, с каким портом коммутатора работает определенное сетевое устройство, и передает все данные, адресованные этому устройству, только на данный порт. Упоминаемая выше утилита Cain предназначена, в частности, для работы в такой среде — локальной сети, использующей коммутаторы, и, как можно быстро убедиться, позволяет перехватывать трафик между клиентами сети. Как следствие — использование обычных коммутаторов позволяет увеличить производительность сети, но не безопасность.

Более целесообразно использовать коммутаторы, поддерживающие протокол 802.1Q, технология VLAN. Настраивая VLAN-коммутатор, можно жестко регламентировать сетевую активность клиентов сети. В качестве примера VLAN-коммутаторов можно привести хорошо известную серию оборудования Cisco Catalyst 1900.

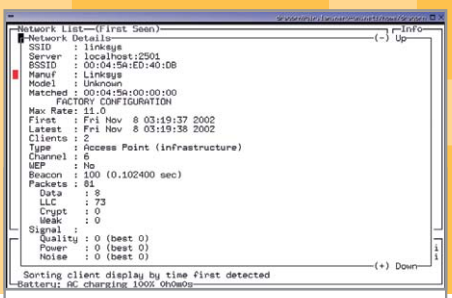
Использование беспроводных локальных сетей (WLAN — Wireless Local Area Network; стандарты IEEE 802.11a, 802.11b — «Wi-Fi», 802.11g), помимо преимущества по сравнению с кабельными сетями в виде мобильности клиентов на определенной территории, имеет и потенциальные недостатки. В частности, это невозможность ограничения зоны покрытия немеханическими способами. Она определяется максимальным удалением от оборудования центральной точки сети с сохранением приемлемого качества приема сигнала. Таким образом, доступ к ресурсам беспроводной сети возможен не только на территории офиса компании, но и в соседних помещениях или на улице. Несмотря на поддержку оборудованием беспроводных локальных сетей стандарта кодирования данных WEP (Wired Equivalent Privacy) для передачи информации, халатность администрирования — отключение WEP — стала распространенной причиной взлома беспроводных сетей. Для диагностики Wi-Fi-сети можно использовать сниффер Kismet. Аудит надежности защиты WLAN можно провести утилитой AirSnort.



Настройка параметров работы брандмауэра Kerio WinRoute Firewall



Putty. Работа с удаленным сервером по SSH-протоколу



Kismet. Просмотр статистики работы клиента беспроводной сети стандарта Wi-Fi

» Сетевая разведка

Цель проводимого злоумышленником перед атакой сетевого исследования — определить тип и версии операционной системы и используемого программного обеспечения. Затем на основании полученных данных выбрать цель (какой-либо уязвимый сервис) и осуществить атаку. Не дожидаясь взлома системы, можно предпринять следующие шаги:

- осуществить аудит сетевой защиты и настроек системы;
- ограничить доступ к сетевым сервисам;
- установить отвлекающие сетевые системы;
- ограничить возможности пользователей по использованию ресурсов Интернета.

Рассмотрим эти действия более подробно.

Аудит сетевой защиты и настроек системы

Для исследования сетевых систем используют специализированное программное обеспечение — сетевые сканеры. Проводимый сканером анализ системы показывает доступные TCP/UDP-порты, через которые работают сетевые сервисы. Сканирование позволяет определить тип сетевого протокола, вероятный тип сетевого сервиса и статус порта — открыт ли он для доступа, или доступ к нему закрыт брандмауэром. На основании полученных во время исследования данных об особенностях реализации стека TCP/IP-протоколов удаленной системы делается предположение о типе и версии операционной системы. Заслуженно одним из лучших сетевых сканеров считается NMap для платформ Unix/Linux. NMapWin — адаптированная версия сканера для Windows-платформ. Для идентификации операционной системы лучше использовать сканер Xprobe.

При сканировании могут использоваться различные методики анализа систем, часть из которых ориентирована на сокрытие факта исследования системы или на затруднение идентификации системами защиты сетевого адреса, с которого осуществляется сканирование.

Для автоматизации поиска уязвимых к взлому сетевых сервисов используется другой класс программ — сетевые сканеры вторжения. Исследуя выбранную систему, сканер вторжения пытается определить доступные сетевые сервисы. Затем, применяя методы хакерских атак, анализирует устойчивость сервиса к взлому. При идентификации типа и версии сервиса сканер осуществляет атаку, нацеленную на специфичные для данного сервиса уязвимости. В реальности на исследуемую систему проводится серия сетевых атак с применением всех известных на данный момент методик. По результатам анализа системы строится отчет с описанием обнаруженных явных или потенциальных уязвимостей, их анализом и рекомендациями по устранению. Возможны случаи ложного срабатывания, когда сканер сообщает об обнаруженной уязвимости, которой на самом деле не существует.

Возможна и обратная ситуация. Сканер безопасности не является абсолютным средством аудита надежности сервисов, поскольку использует уже известные методики сетевых атак. Необходимо учитывать, что с момента обнаружения какой-либо уязвимости и публикации ее описания до включения этого описания в базу данных сканера вторжения пройдет определенное время. Поэтому, помимо регулярного обновления баз данных уязвимостей и методик анализа используемого сканера вторжения, необходимо обращать внимание на информационные бюллетени специализированных ресурсов по сетевой безопасности, таких как организация CERT/CC. В любом случае, для анализа отчета сканера и исправления уязвимостей требуется компетентный специалист.

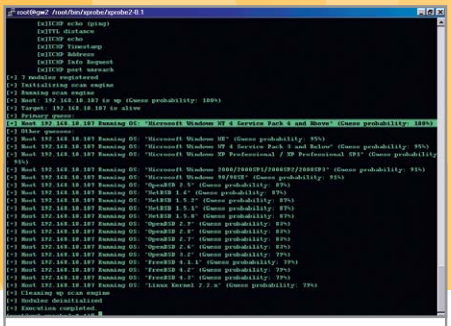
В качестве примера персональных сканеров вторжения можно привести ISS Internet Scanner, GFI LANguard Network Security Scanner, XSpider и Nessus. К достоинствам последнего, помимо бесплатного распространения по лицензии GNU GPL, можно отнести возможность самостоятельной разработки новых методов исследования систем. Для этой цели предоставлен язык сценариев NASL (Nessus Attack Script Language). »

Основные организации

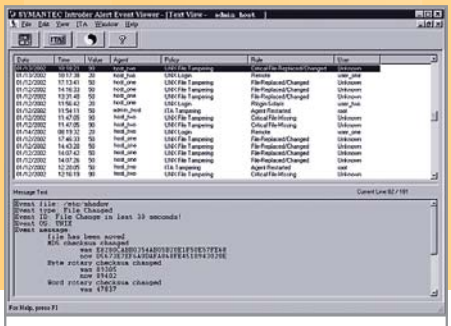
Кто есть кто

CERT Coordination Center (CERT/CC)
Координационный центр CERT (Computer Emergency Response Team) был организован несколькими институтами и Defense Advanced Research Projects Agency (DARPA) в 1988 году как группа реагирования на обнаруженные проблемы в сетевой безопасности. Поводом к созданию такой группы послужил инцидент с вирусом Морриса. В настоящее время проект является экспертным координационным центром по вопросам компьютерной безопасности.

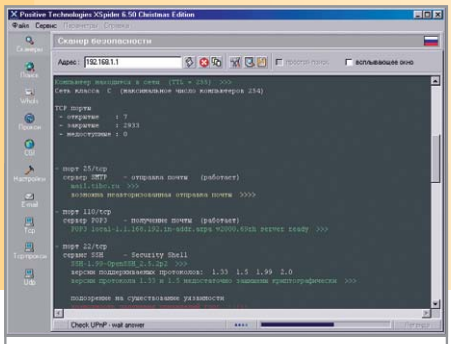
Institute of Electrical and Electronics Engineers (IEEE)
Институт инженеров по электротехнике и радиоэлектронике IEEE — некоммерческая организация, находящаяся в Нью-Йорке, членами которой являются инженеры, ученые и студенты, занимающиеся электроникой, а также работающие в смежных областях. В составе этой организации более 300 тысяч членов. В ее задачи входит установка стандартов в области вычислительной техники и телекоммуникаций.



Отчет сканера Xprobe о проведенном анализе сетевого компьютера



Анализ действий взломщика, записанный Symantec Intruder Alert



Проверка сервисов сканером XSpider

Если возникли сложности при установке или работе с персональными сканерами вторжения, можно воспользоваться сервисами онлайнового аудита защищенности сетевых систем, предоставляемых на web-ресурсах проектов COTSE и Void.ru.

Ограничение доступа к сетевым сервисам

Эта задача решается использованием брандмауэра — аппаратно-программного средства сетевой защиты. Для обозначения этого типа защиты употребляется еще и другой термин — firewall. Основное назначение брандмауэра — контроль и фильтрация обмена данных между компьютерами в сети. Фильтрация (разрешение или запрещение) осуществляется на основе правил, определенных администратором или пользователем.

Выбор брандмауэра определяется постановкой задачи по обеспечению сетевой защиты определенных ресурсов, эффективностью и стоимостью реализации решения. Для связи двух удаленных офисов на магистрали с интенсивным обменом данных можно использовать аппаратные брандмауэры компаний Cisco или D-Link.

При поиске программных решений задачи обеспечения сетевой защиты для сервера или шлюза локальной сети в Интернете на основе Windows обратите внимание на разработку компании Kerio Technologies Inc. — Kerio WinRoute Firewall. Та же самая задача, только для Linux-платформ — Open Source проект Netfilter, брандмауэр Iptables. Для обеспечения сетевой защиты небольшой локальной сети или одного компьютера с подключением к Интернету можно использовать персональные программные брандмауэры компании Agnitum Ltd — Outpost Pro и Outpost Free. Применение этих брандмауэров позволяет жестко регламентировать сетевую активность пользовательских и системных приложений, контролировать целостность пользовательских программ (необходимо для определения факта модификации программы вирусом или обновлением), блокировать загрузку интернет-рекламы и выполнять другие задачи. Помимо возможности подключения к брандмауэру дополнительных модулей, расширяющих функциональность систем защиты, к названным достоинствам программы можно добавить адаптацию интерфейса брандмауэров для русскоязычных пользователей.

Отвлекающие сетевые системы

«Война — это путь обмана. Поэтому, даже если [ты] способен, показывай противнику свою неспособность. Когда должен ввести в бой свои силы, притворись бездеятельным. Когда [цель] близко, показывай, будто она далеко; когда же она действительно далеко, создавай впечатление, что она близко. Изобрази выгоду, чтобы завлечь его.

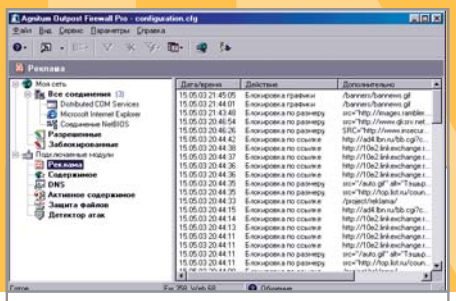
Ограничение пользователей

А Интернета тебе будет совсем чуть-чуть

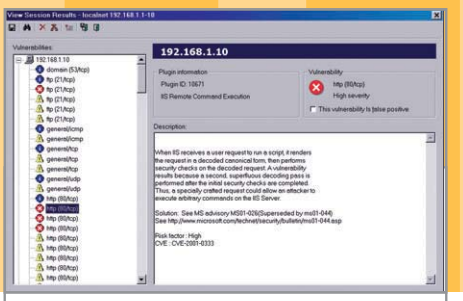
В первую очередь необходимость этого ограничения вызвана опасностью использования злоумышленниками в своих целях определенных интернет-технологий. Например, после загрузки активных компонентов интернет-документов — ActiveX, Java-апплетов — на компьютере пользователя исполняется неконтролируемый им код, имеющий потенциальную возможность доступа к записанной на диск информации. Сценарии на языках JavaScript и Visual Basic Script могут изменять без контроля пользователя настройки web-браузеров. Исследуя cookies, можно не только отследить траекторию перемещения по web-серверам, но и получить регистрационную информацию пользователя к интернет-ресурсам.

Ограничивать использование активных компонентов web-документов и cookies можно несколькими способами — соответствующими настройками интернет-браузера или программного персонального брандмауэра. При ограничении использования этих технологий лучше придерживаться гибкой политики: разрешать их использовать для web-ресурсов, которым вы доверяете, и запрещать для остальных.

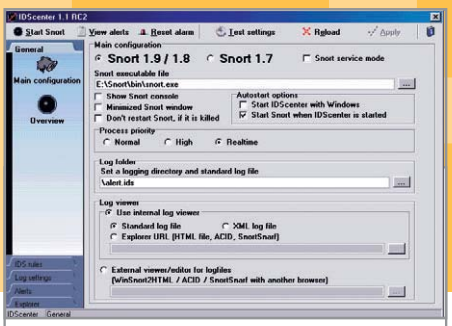
Специальное программное обеспечение, прокси-сервер, позволяет расширить возможности регламентирования использования интернет-ресурсов. Прокси-сервер функционирует как посредник при обмене данными между клиентским приложением пользователя и реальным интернет-сервером. Он перехватывает все запросы пользователя к интернет-ресурсу и проверяет, не может ли он их выполнить, предоставив сохраненные данные из своей кэш-памяти и экономя время пользователей. Если прокси-сервер не может предоставить данные, запрос передается реальному серверу. Обслуживание запросов пользователя происходит в соответствии с ограничениями, установленными администратором для этого пользователя. В качестве примеров прокси-серверов можно привести Squid для Unix/Linux-систем и разработку компании Ositis Software Inc. — WinProxy. Последний позволяет проводить онлайновую антивирусную проверку получаемых пользователем файлов из Интернета.



Просмотр статистики работы программного персонального брандмауэра Agnitum Outpost Firewall Pro



Анализ отчета сканера вторжения Nessus об обнаруженных уязвимостях сетевой системы



Конфигурирование параметров работы Snort утилитой IDScenter

» Сотвори беспорядок [в его силах] и возьми его. Если он полон, приготовься; если он силен, избегай его. Если он в гневе, беспокой его; будь почтителен, чтобы он возомнил о себе. Если враг отдохнувший, заставь его напрячь силы. Если он объединен, разъедини его. Нападай там, где он не приготовился. Иди вперед там, где он не ожидает. Таковы пути, которыми военные стратеги побеждают».

Уже две с половиной тысячи лет идеи, изложенные в трактате «Искусство войны» китайским военным стратегом и философом Сунь Цзы, находят применение в практике единоборств, экономике, повседневной жизни. Нашли они применение и в области информационной безопасности. Последние несколько лет развивается новая концепция обеспечения сетевой защиты — использование имитаций уязвимых сетевых систем и сервисов. Идеология такой защиты — привлечение внимания взломщиков кажущейся доступностью имитируемых систем плюс документирование всех действий злоумышленника при попытке взлома. Такие системы называются Honeypot. Название образуется от английских слов honey — «мед» и pot — «бочонок», подразумевая приманку для лакомки. Практическое применение этой концепции дополняет традиционные способы защиты, позволяя с большой точностью выявлять злоумышленников среди пользователей сетевых ресурсов.

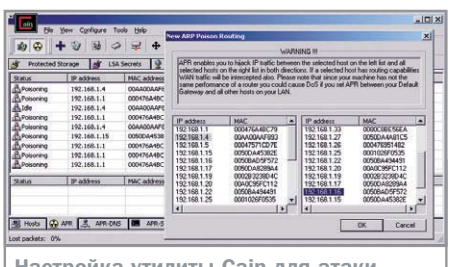
Основной вклад в развитие систем Honeypot вносит некоммерческий исследовательский проект Honeynet. В рамках этого проекта выделилось два вида систем Honeypot — исследовательские и промышленные. Первые служат для сбора информации о методиках сетевых атак и действиях злоумышленников после взлома. Назначение вторых — отвлечь внимание взломщиков от рабочих систем. При атаке на промышленную систему Honeypot о взломщике собирается вся доступная информация и передается системе защиты сети.

В качестве примера промышленной Honeypot можно привести систему Honeyd. Она позволяет создавать виртуальные хосты в сети, имитирующие различные операционные системы, вплоть до уровня сетевых протоколов. Что примечательно, для достижения полной имитации используются базы данных характеристик протоколов различных операционных систем и сетевых устройств — сканеров Xprobe и NMap. Созданные системой Honeyd хосты можно объединять в виртуальные сети, определяя их топологию, схемы маршрутизации, загруженность и потери пакетов. Имитация работы сервисов виртуальных хостов достигается переброской соединений на рабочие сервисы или использованием специально разработанных интерактивных сценариев.

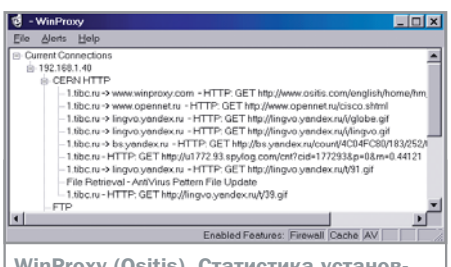
Атака

На основании данных, собранных злоумышленником во время разведки, на систему проводится сетевая атака. Это может быть одновременное открытие множества соединений; определенная последовательность команд и данных, переданных определенному сервису; серия сетевых пакетов с преднамеренно нарушенной структурой. Для обнаружения начала атаки используют специальное программное обеспечение — сетевые системы обнаружения вторжений (Network Intrusion Detection System, сокращенно NIDS). Эта система защиты осуществляет контроль устанавливаемых соединений, проводит анализ структуры и содержимого сетевых пакетов. NIDS может работать как на отдельном компьютере, контролируя его собственный трафик, так и на выделенном сервере (шлюз, маршрутизатор, зонд), просматривая весь межсетевой поток данных. При обнаружении атаки NIDS (в зависимости от разработки) может послать сообщения на e-mail, рабочую консоль администратора, пейджер, телефон, факс, SNMP, реконфигурировать брандмауэр или маршрутизатор; блокировать устанавливаемые соединения.

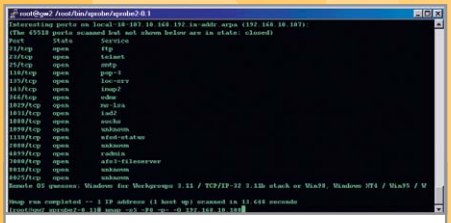
Проиллюстрировать применение NIDS можно на примере системы Snort. В режиме реального времени Snort осуществляет анализ сетевого трафика, проверяя корректность структуры сетевых пакетов и соответствие содержимого пакетов определенным правилам. Для описания сетевых инцидентов и определения реакции системы используется гибкий язык сценариев. Встроенная база знаний позволяет определить распространенные типы инцидентов, таких как «скрытое» сканирование (использующие установленные в сетевых пакетах флаги FIN, ASK), сбор баннеров сетевых сервисов (Services & OS fingerprinting), атаки на переполнение буфера различных сервисов, атаки, использующие преднамеренное нарушение структуры сетевых пакетов (ping of death), атаки вида «отказ в обслуживании» (DOS и DDOS). Включено описание множества атак, эксплуатирующих определенные уязвимости различных »



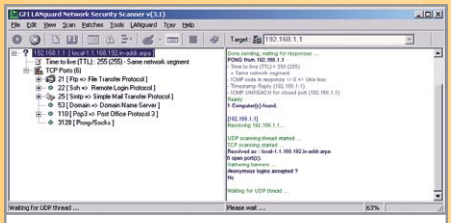
Настройка утилиты Cain для атаки «man-in-the-middle»



WinProxy (Ositis). Статистика установленных соединений



NMapWin — Windows-аналог сканера Nmap



Аудит сетевых сервисов сканером GFI LANguard Network Security Scanner

Результаты анализа сканером NMap удаленной системы

сетевых сервисов. При фиксировании системой Snort сетевого инцидента можно, конфигурируя брандмауэр, блокировать атаку и/или передать предупреждающее сообщение в службу Windows WinPopup, в пользовательский файл или сетевому сервису.

Идея использовать методы активной сетевой защиты, то есть автоматическая контратака нападающего при фиксировании сетевого инцидента, имеет несколько уязвимых позиций. Первый аргумент против использования такой защиты — сомнительная законность контратаки. Второй аргумент — вполне возможна ситуация, когда злоумышленник имитирует атаку со стороны постороннего хоста, направив реакцию системы защиты не против себя, а против выбранного хоста.

Последняя линия защиты

Предположим, что, несмотря на принятые меры защиты, система была взломана. Какие действия необходимо предпринять для своевременного обнаружения и расследования факта компрометации системы:

- анализ журналов системных сообщений;
- контроль работы пользовательских и системных приложений;
- контроль целостности файлов;
- антивирусная проверка.

Большинство системных и пользовательских приложений ведут запись своей деятельности в специальные файлы — журналы сообщений (логи). Например, обычно ведутся журналы, в которых фиксируется, когда и кто вошел в систему, список вызванных пользователем программ, параметры запросов к системным сервисам. Анализируя эти журналы, можно легко выявить действия взломщика: например, сетевой сервис получил странный запрос, затем в системе появился новый пользователь с администраторскими правами, который принялся активно модифицировать используемое программное обеспечение. На первый взгляд все выглядит не очень сложно. Но учитывая, что первой задачей злоумышленника после взлома системы будет сокрытие следов, нельзя доверять информации в журналах сообщений на скомпрометированной системе. С большой вероятностью они будут модифицированы взломщиком. Поэтому запись информации в локальные журналы лучше дублировать пересылкой копий сообщений по сети специально выделенному серверу Syslog, запретив к нему любой сетевой доступ (кроме пересылки сообщений). Таким образом, взломщик, скрыв следы своего входа на скомпрометированной системе, не сможет взломать удаленный сервер Syslog и изменить там журналы сообщений.

Для мониторинга работы системных и пользовательских программ и выявления нетипичной деятельности используют специализированное программное обеспечение под общим названием Host Based Intrusion Detection System (HIDS). В качестве примера можно привести Symantec Intruder Alert.

Контролируя целостность файлов, можно определить, какие программы были модифицированы злоумышленником. Для этой цели можно использовать утилиты Tripwire или AIDE (Advanced Intrusion Detection Environment).

Самый ожидаемый шаг для поиска вредоносного кода, внесенного взломщиком в программное обеспечение системы, это использование антивирусных программ типа Chrootkit для Linux-систем и AVP «Лаборатории Касперского» для Windows.

В заключение

Завершая обзор средств сетевой защиты, хотел бы заметить, что задача обеспечения информационной безопасности является постоянно эволюционирующим процессом, требующим внимания, тщательности и интеллектуальных усилий. Никакие методики защиты не могут считаться абсолютно надежными по определению. Ведь соревнование технологий меча и щита идет от зари появления человечества и до сих пор не окончено. ■ ■ ■ Александр Красоткин

Полезные ссылки

Ресурсы и проекты

Agnitum	www.agnitum.com
AIDE	www.cs.tut.fi/~rammer/aide.html
AirSnort	airsnort.shmoo.com
AVP	www.avp.ru
Cain	www.oxid.it
Cisco	www.cisco.com
CERT/CC	www.cert.org
Chrootkit	www.chkrootkit.org
Cotse	www.cotse.com
Dlink	www.dlink.com
DSniff	naughty.monkey.org/~dugsong/dsniff
DSniff (Win 32)	www.datanerds.net/~mike/dsniff.html
Ethereal	www.ethereal.com
GFI LANguard NSS	www.gfisoftware.com
Honeynet	www.honeynet.org
Honed	niels.xtdnet.nl/honeyd
Honeyd (Win 32)	www.securityprofiling.com
IDScenter	www.packx.net
IEEE	www.ieee.org
ISS	www.iss.net
Kismet	www.kismetwireless.net
Kerio	www.kerio.com
Nessus	www.nessus.org
Netfilter/Iptables	www.iptables.org
Netsec	www.netsec.ch
NMap	www.insecure.org
NMapWin	www.nmapwin.org
OpenSSH	www.openssh.org
OpenSSL	www.openssl.org
Ositis	www.ositis.com
Putty	www.chiark.greenend.org.uk/~sgtatham/putty
Symantec	www.symantec.com
Squid	www.squid-cache.org
Snort	www.snort.org
Syslog (Win 32)	www.kiwisyslog.com
Tcpdump	www.tcpdump.org
Tripwire	www.tripwire.com
XSpider	www.ptsecurity.ru
Xprobe	www.sys-security.com
Void.ru	www.void.ru
WinDump	windump.polito.it

СПЕЦВЫПУСК ПО КОММУНИКАЦИЯМ

ЧИП CHIP®

ISSN 1609-4212

SPECIAL #7

ЧИП CHIP®
Журнал информационных технологий
ISSN 1609-4212
CHIP Special 4/2003 (7)

Учрежден и издается ЗАО «Издательский дом «Бурда»
Адрес издателя: 109240, Москва, Гончарная ул., 12
Адрес редакции: 125040, Москва, ул. Правды, д. 8, корп. 35
тел. (095) 787-33-88, факс (095) 787-94-31
Отдел распространения: тел. (095) 797-45-60
Отдел курьерской доставки: тел. (095) 787-94-06
Издание зарегистрировано в Комитете по печати и информации РФ. Рег. номер 019376
Журнал CHIP издается по лицензии немецкого издателя Vogel Burda Communications, Мюнхен, Германия

Тираж 35 000 экз. Цена свободная
Advertising International
Vogel Burda Communications,
Poccistr.11, D-80336 Munchen:
Erik N.Wicha *(ewicha@vogel.de)*
Phone.(+49 89)74642 326, Fax (+49 89)74642 217
More information about the publishing house and its products is also available on *www.vogel-media.com*

Типография
Reproprint, s. r. o.,
Podebradska 26/540, Praha 9

Реклама в номере

Philips . . . . . 2-я обложка
Rambler . . . . . 3-я обложка
SAMSUNG Electronics . . . . . 4-я обложка