Неофициальное пособие по глобальной системе местоопределения

А. К. Щербаков

Wi-Fi: Все, что Вы хотели знать, но боялись спросить

Автор этой книги не несет ответственности за использование материалов, которые опубликованы в этом издании. Вся информация дана исключительно в образовательных целях. Ни при каких условиях ответственность за какие-либо последствия от использования этой книги в практических целях не может возлагаться на автора.

Москва

Литературное агентство «Бук-Пресс»
2005

УДК 004.5
ББК 32.973.26-018.2
Щ78

Щербаков А. К.

Щ78 Wi-Fi: Все, что Вы хотели знать, но боялись спросить. Неофициальное пособие по глобальной системе местоопределения, 2005. - 352 с.

Жизнь современного человека – это движение. Мобильность для нас становится одним из самых важных моментов для работы, для общения, для жизни. Многие из нас сейчас уже не представляют жизнь без сотовых телефонов, которые из средства роскоши превратились в предмет, без которого жизнь современного человека стала просто немыслима. Многие уже оценили все преимущества Bluetooth, GPRS. Эти устройства превратили наши телефоны из средств связи в незаменимых помощников в работе. К сожалению, один из самых главных недостатков этих беспроводных технологий – малый радиус действия и низкая скорость передачи данных, что сейчас становится очень важным фактором для всех нас. Поэтому к нам на помощь приходит активно развивающийся во всем мире и в России стандарт Wi-Fi. Особенно радует, что в крупных городах России, особенно в Москве и Санкт-Петербурге, начинается массовое внедрение беспроводных сетей Wi-Fi в публичных местах (так называемых Hot Spot) – отелях, аэропортах, ресторанах, торговых центрах и кафе.

Что же такое Wi-Fi? Очередной мыльный пузырь IT индустрии, который изо всех сил надувают производители и поставщики телекоммуникационного оборудования или новая технология, призванная в очередной раз изменить наш привычный мир, как это случилось когда-то с появлением Интернет и сотовой связи?

УДК 004.5
ББК 32.973.26-018.2

Часть 1. Введение

Глава 1. Беспроводные технологии

На предприятиях и в жилых домах мобильный доступ к информационным ресурсам приобретает все большую популярность. Многие люди уверены в перспективности беспроводной коммерции и очень высоко оценивают возможности радиосвязи в плане повышения производительности своего труда. Однако отделить связанную с этим громкую рекламную шумиху от реальности совсем непросто. Стандарты непрерывно развиваются, но явных лидеров в области беспроводных технологий пока еще нет.

Пользователи хотят, чтобы беспроводные системы работали быстро, имели предсказуемую стоимость и обеспечивали значительную зону охвата. Увы, предлагаемые сегодня на рынке решения не могут удовлетворить всех требований.

В настоящее время разрабатывается множество различных беспроводных систем. И хотя мобильность является ключевой характеристикой многих из них, рынок этих систем развивается в направлении расширения диапазона предлагаемых пользователю услуг, а не просто улучшения доступности связи для мобильных пользователей. Что же касается высокой скорости передачи данных, то в этом отношении для предприятий разных масштабов и поставщиков услуг большой интерес могут представлять фиксированные радиосистемы. Однако помните, что там, где это возможно, лучше задействовать кабельную инфраструктуру, которая всегда работает лучше беспроводной. Если же место, где расположено ваше предприятие, не охвачено традиционными (кабельными) широкополосными службами, тогда вам придется использовать беспроводную систему.

В наше время, когда мобильная речевая связь получила широкое применение (о чем свидетельствуют звонки сотовых телефонов, постоянно нарушающие работу деловых совещаний), неудивительно, что большая часть рекламной шумихи вокруг беспроводных сетей касается служб передачи данных мобильным пользователям. Разрабатываемые

беспроводные сети третьего поколения и микробраузеры создают основу для новой технологической революции. Однако не следует думать, что она произойдет очень скоро. Соответствующие инфраструктуры и приложения появятся только через несколько лет.

Беспроводные сети можно разделить на сети малого радиуса действия, нередко называемые персональными (Personal Area Networks), беспроводные ЛВС, системы фиксированного радиодоступа и беспроводные территориально распределенные сети (WAN). Персональные беспроводные сети используются для организации недорогих соединений между отдельными интеллектуальными устройствами. Беспроводные ЛВС работают внутри зданий и обеспечивают высокоскоростной доступ к информационным ресурсам при максимальной дальности связи 30 или более метров. Благодаря широкой поддержке производителями ключевых стандартов и снижению цен эти сети получают все более широкое распространение. Также растет спрос на системы фиксированного радиодоступа, которые основаны на самых разных технологиях (в том числе спутниковых) и работают в лицензируемых и нелицензируемых диапазонах частот (некоторые из этих систем называют беспроводными DSL-системами). И наконец, на основе беспроводных WAN-сетей, представляющих собой следующее поколение сотовых систем, со временем может быть реализован глобальный мобильный доступ к данным.

Глава 2. Персональные беспроводные сети

Если у вас есть блокнотный или карманный компьютер, то вполне вероятно, что вы уже имеете аппаратное средство персональной беспроводной сети, каковым является инфракрасный (ИК) порт передачи данных. Однако лишь очень немногие пользуются такими портами. Причинами этого в той или иной степени являются присущие ИК-технологии значительные технические ограничения, неразвитость созданных для нее приложений и сложность пользования ими.

Впрочем, если персональная сеть вам нужна, но вы не удовлетворены возможностями ИК-технологии, обратите внимание на недорогую новейшую сетевую беспроводную технологию Bluetooth, которая обеспечивает передачу данных со скоростью 1 Мбит/с на короткие расстояния — до 10 м. Согласно результатам исследования, недавно проведенного компанией Cahners In-Stat Group, объем рынка средств Bluetooth в 2005 г. составит 5 млрд долл. Следует отметить, что данная технология имеет беспрецедентно высокий уровень поддержки со стороны производителей. Ее сторонниками являются почти все крупные компании, рабо-

тающие на рынке информационных и коммуникационных технологий. Среди них есть производители сотовых телефонов, компьютеров и микросхем.

Технология Bluetooth отнюдь не идеальная, но благодаря широкой сфере применения и низкой стоимости ее успех вполне возможен. И хотя первые поддерживающие данную технологию продукты (включая интерфейсы PC Card для блокнотных ПК) будут стоить дороже 100 долл., конечной целью сторонников Bluetooth является создание интерфейса на базе единственной микросхемы, который будет стоить не более 5 долл. При такой цене каждое информационное устройство станет узлом персональной беспроводной сети.

Однако на пути к успеху технология Bluetooth сталкивается с определенными препятствиями. В частности, вызывает беспокойство реализованный в ней механизм защиты от несанкционированного доступа. Кроме того, нельзя исключать возможность возникновения радиопомех, поскольку диапазон 2,4 ГГц, в котором работают средства Bluetooth, используется и беспроводными ЛВС стандарта 802.11. Следует также понимать, что сотовая «трубка» и карманный ПК, оснащенные однотипными сетевыми радиоинтерфейсами, не будут синхронизировать между собой информацию о контактных телефонах до тех пор, пока не появится соответствующее приложение. Однако технология Bluetooth находится на подъеме, и ни один аналитик не видит достаточно веских причин, способных помешать этому, а значит, соединительные кабели вполне могут уйти в прошлое.

Глава 3. Беспроводные ЛВС

Если технология Bluetooth — это дело будущего, то беспроводные ЛВС — наше настоящее. Объем рынка последних неуклонно растет. По оценкам компании Gartner Group, в 2000 г. он составил 487,5 млн долл., а в 2004 г. будет равен 35,8 млрд долл. В основном такими сетями оснащаются различного рода предприятия, но их также начинают устанавливать в отелях, конгресс-центрах и аэропортах, что весьма привлекательно для мобильных профессионалов.

Благодаря широкой поддержке производителями стандарта 802.11 беспроводные ЛВС прошли первую фазу развития, которая характеризовалась низкой производительностью, высокой стоимостью и плохой совместимостью оборудования. Сейчас для них наступила вторая фаза развития, признаком которой является их растущая популярность. С по-

явлением 11-Мбит/с стандарта 802.11b (также известного под названием Wi-Fi), сети стали работать быстрее, а развитие производства соответствующего этому стандарту оборудования снижает цены на него. Следующая фаза развития беспроводных ЛВС предполагает переход на более высокие рабочие частоты и повышение скорости передачи данных до 54 Мбит/с. И произойдет это в ближайшие два года.

Развитию рынка беспроводных ЛВС способствуют два важных обстоятельства. Во-первых, повысилось качество соответствующих продуктов, да и с самой технологией этих сетей пользователи стали знакомы лучше, чем два года назад (многие предприятия и системные интеграторы завершили пилотные фазы своих проектов, изучили достоинства и недостатки беспроводных ЛВС, приобрели ценный опыт их внедрения на предприятиях). Во-вторых, растущий спрос на эти сети стимулирует конкуренцию среди производителей микросхем для беспроводного оборудования, и хотя основными «игроками» на этом рынке являются всего две компании — Intersil и Lucent Technologies, — активное соперничество между ними способствует снижению цен на оборудование. Кроме того, у них появились сильные конкуренты, в том числе фирма Texas Instruments.

Хотя в настоящее время на рынке доминируют продукты стандарта 802.11b, внимание многих специалистов приковано к деятельности двух новых фирм — Atheros Communications и Radiata Communications (недавно приобретена компанией Cisco). Они заканчивают разработку микросхем, поддерживающих стандарт 802.11a, в котором предусмотрена передача данных со скоростью до 54 Мбит/с в менее загруженном диапазоне 5 ГГц. Пока трудно сказать, как быстро оба производителя доведут опытные образцы своих микросхем до уровня, когда можно будет начать их серийное производство. Однако первые продукты на их основе появятся на рынке в середине или в конце текущего года. С открытием новых возможностей построения беспроводных ЛВС эти разработки ставят перед их проектировщиками сложный вопрос: стоит ли приобретать 2,4 ГГц инфраструктуру стандарта 802.11b сейчас, когда на подходе 5 ГГц продукты стандарта 802.11a?

Производители оборудования стандарта 802.11b признают важность продуктов стандарта 802.11a, поэтому альянс Wireless Ethernet Compatibility Alliance (WECA) планирует сертифицировать их. Сторонники стандарта 802.11b считают, что средства стандартов 802.11a и 802.11b можно будет использовать в одной и той же сети совместно, если реализовать ее на основе точек доступа, каждая из которых должна быть оснащена двумя разными (соответствующими этим стандартам) радиоинтерфейсами. Однако объем рынка точек доступа, поддерживающих два радиоинтерфейса одновременно, существенно ограничен, поскольку

их выпускают всего две фирмы — Intermec Technologies и Lucent Technologies. Кроме того, данный вывод сделан на основе предположения, что продукты стандартов 802.11a и 802.11b будут иметь одинаковые характеристики передачи. Если же это окажется не так, то развертывание в настоящее время сетевой инфраструктуры на основе вышеупомянутых точек доступа в долгосрочной перспективе может оказаться не оправданным. В связи с этим большинству организаций стоит подождать с крупномасштабными инвестициями в беспроводные ЛВС; за исключением тех случаев, когда речь идет о перспективных приложениях для этих сетей, способных окупить затраты на них за два года.

Стоит отметить, что весьма перспективной сферой применения беспроводных ЛВС являются малые и домашние офисы. Площадь большинства из них соответствует дальности действия беспроводных сетевых средств, к тому же многие люди не хотят прокладывать дополнительные кабели в своих домах. Производители оборудования стандарта 802.11a тоже собираются работать на этом рынке, предлагая использовать свои продукты для поддержания развлекательных приложений, в основном тех, в которых предусматривается передача видеоизображений в формате MPEG.

Глава 4. Системы фиксированного радиодоступа

СВЧ-системы типа «точка—точка» и оптические системы (но в меньшей степени) уже многие годы применяются для организации каналов связи между зданиями в черте города. Хотя лицензируемые СВЧ-системы дороги и установка их сложна, при удачном конструировании они обеспечивают высокую пропускную способность и имеют уровень надежности 99,99% даже при самых неблагоприятных погодных условиях. Для успешного функционирования этих систем требуется соблюдение условия прямой видимости, а дальность их действия ограничивается только кривизной земной поверхности.

Относительно недавно стали популярными более дешевые системы, работающие в нелицензируемых диапазонах 2,4 и 5 ГГц, которые используются вместо проводных каналов T1 или в качестве мостов между удаленными ЛВС. Поскольку для применения этих систем не требуется лицензия Федеральной комиссии по связи (ФКС) США, их можно развернуть очень быстро. Данные системы имеют разную производительность — от 1,5 до 50 Мбит/с и более. Их широко применяют для подключения удаленных базовых станций сотовых сетей к их центральным узлам, а также для объединения ЛВС, расположенных в разных зданиях

кампуса (в тех случаях, когда отсутствие кабелепроводов между зданиями не позволяет проложить оптоволокно). Некоторые небольшие Интернет-провайдеры стали подключать к Сети клиентов, используя рассматриваемые средства. Однако из-за ограниченности доступной полосы пропускания и необходимости минимизировать стоимость пользовательского оборудования построение многоточечных систем является сложной задачей.

В нелицензируемых диапазонах велик риск возникновения помех, но хорошо спроектированные системы довольно устойчивы к ним. И даже когда помехи сильно влияют на эти системы, их производительность, как правило, снижается постепенно. При наличии в системе хороших средств мониторинга возникшую проблему можно обнаружить и решить до серьезного сбоя в ее работе. За последнее время улучшены средства обеспечения информационной безопасности систем.

Устройства DSL и кабельные модемы считаются лучшими средствами высокоскоростного доступа для оснащения малых и домашних офисов, однако широкополосные радиосистемы могут стать достойной альтернативой им, особенно в тех местах, где услуги DSL и кабельные сети не доступны.

Недавно ФКС приняла новые правила, позволяющие поставщикам услуг более гибко предоставлять услуги на базе мультимегабитовых беспроводных систем MMDS (Multichannel Multipoint Distribution Service), работающих в диапазоне 2,5 ГГц, который первоначально был выделен ФКС для цифрового телевидения. Вероятно, что эти системы получат широкое применение в течение ближайших нескольких лет. В июле прошлого года для разработки открытых стандартов на MMDS-доступ был создан консорциум Wireless DSL (очевидно, что те, кто выбирал такое название, хотели извлечь выгоду из рекламной шумихи вокруг технологии DSL). По сравнению с ранее разработанными системами LMDS (Local Multipoint Distribution Service) системы MMDS имеют большую дальность действия — до 20 с лишним километров — и более высокую пропускную способность. Их недостатками являются необходимость располагать узлы системы в зоне прямой видимости и относительно высокая стоимость пользовательского оборудования.

И наконец, несколько слов о спутниковой связи, привлекательность которой отнюдь не уменьшилась из-за коммерческого неуспеха некогда широко разрекламированной системы Iridium. В отличие от других типов радиодоступа услугами спутниковой связи можно пользоваться почти на всей территории планеты. Производители приемных систем цифрового спутникового телевидения разработали гибридные двунаправленные системы, использующие в качестве обратного канала связи

наземные телефонные линии. Такие решения подходят, пожалуй, лишь для домашних пользователей. Выбирайте двунаправленные спутниковые системы следующего поколения, которые получат широкое применение через год-полтора.

Глава 5. Беспроводные WAN-сети

Несмотря на существование нескольких конкурирующих стандартов сотовой связи, делающих глобальный роуминг трудно осуществимым или даже вообще невозможным, сотовые телефоны используются повсеместно. Отсюда можно сделать вывод, что следующим этапом в развитии сотовых сетей станет глобальный мобильный доступ к данным, включая возможность работать с беспроводными службами Web. Под воздействием телевизионной рекламы складывается впечатление, что такой доступ стал уже реален, но это не так. Дело в том, что существующая инфраструктура сотовых сетей плохо подходит для организации мобильного доступа к данным, кроме того, очень сомнительна польза большинства беспроводных приложений. Далеко не все владельцы сотовых телефонов хотят оплачивать по высоким повременным тарифам проверку расписания вылетов самолетов или операции с акциями.

Однако со временем для беспроводных WAN-сетей будут разработаны новые приложения и развернуты инфраструктуры следующего поколения. По данным компании Dataquest, объем рынка мобильных Интернет-устройств возрастет с 200 млн долл. в 1999 г. до 11 млрд долл. в 2005 г.

Сегодняшние сети второго поколения поддерживают максимальную скорость передачи данных 14,4 Кбит/с, которой хватает только для работы с простейшими текстовыми приложениями. К сожалению, созданию сетей третьего поколения мешает высокая стоимость соответствующего оборудования и частотных лицензий. Кроме того, в связной отрасли нет согласия относительно того, на каких технологиях должны базироваться эти сети. Пока же операторы пытаются «наложить» службы высокоскоростной передачи данных на существующие инфраструктуры речевой связи и при этом сталкиваются со значительными трудностями.

Самые мощные системы третьего поколения будут иметь пропускную способность 2 Мбит/с, большинство же разработок в данной области ориентированы на достижение скорости 384 Кбит/с. Это максимальные показатели, реальные же — окажутся гораздо ниже. Существенная ограниченность сетевой полосы пропускания сделает ее довольно

дорогой. Стоит отметить, что, несмотря на малые размеры экранов мобильных устройств, для реализации интерактивных видеоприложений потребуется разработка новых, более эффективных методов сжатия видеоизображения.

Хотя широкомасштабное строительство сетей третьего поколения вряд ли начнется раньше 2003 г., некоторые промежуточные решения по беспроводной передаче данных доступны пользователям уже сейчас. Растет популярность двустороннего обмена короткими сообщениями в рамках существующих низкоскоростных инфраструктур. Для того чтобы передавать значительные объемы информации с более высокими скоростями, можно воспользоваться услугами городских беспроводных сетей передачи данных, основанных на технологии расширения спектра сигнала по методу прямой последовательности.

Проанализировав положение дел с беспроводными WAN-сетями, можно сделать вывод, что вероятность широкого распространения высокоскоростных служб в ближайшие пять лет мала. Здесь уместно провести сравнение с рынками услуг широкополосного доступа на основе технологий DSL и кабельных модемов, которые, несмотря на острую нужду пользователей в таких услугах и наличие более четко сформулированных технических стандартов, развивались значительно медленнее, чем предсказывали многие аналитики. Пожалуй, время высокоскоростных беспроводных WAN-сетей наступит где-нибудь во второй половине начавшегося десятилетия.

Домашние сети Wi-Fi получают все большее распространение — и впервые опередили сети Ethernet по числу установок, утверждается в отчете о результатах исследования, проведенного в США.

Аналитическая фирма Parks Associates пришла к заключению, что 52% американских домовладений, в которых есть домашняя сеть, используют беспроводную технологию, тогда как на долю кабельных сетей Ethernet приходится 50% домовладений, а на долю сетей на основе силовой электропроводки — 5%. (В сумме эти цифры превышают 100%, так как в некоторых домах применяется комбинация из разных технологий.)

Часть 2. Высокая точность беспроводной передачи данных

Глава 1. Wi-Fi — что это такое?

Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity, которое можно дословно перевести как «высокая точность беспроводной передачи данных») в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам. Разработка этих стандартов ведется в рамках рабочей группы 802.11 Института инженеров по электротехнике и электронике (IEEE). Wi-Fi не является единственной технологией беспроводного доступа — специалисты IEEE и других учреждений разработали и продолжают работать над другими стандартами беспроводных коммуникаций, ориентированных на персональные сети (PWAN, для организации подключения в пределах, например, рабочего места сотрудника) или сети, масштаба города и региона (WWAN).

Количество точек беспроводного доступа в мире растет с каждым днем, обещая в недалеком будущем широкополосный вход в глобальную сеть откуда угодно и без особых проблем. Был бы под рукой компьютер с Wi-Fi-адаптером. Информационное издание JiWire опубликовало данные из которых следует, что в настоящее время насчитывается 56139 хот-спотов в 93 странах мира.

Абсолютное и неоспоримое лидерство по количеству точек доступа принадлежит США. Далее идут Англия, Германия, Франция и Япония. Однако, когда дошли до подсчета хот-спотов в отдельно взятом городе, оказалось, что лидером стал вовсе не один из американских мегаполисов. На первом месте оказался Лондон. Далее за ним идут Токио, Нью-Йорк, Париж, Сингапур, Берлин и Чикаго.

Первая коммерческая точка появилась в Санкт-Петербурге в 2003 г. Сейчас в городе открыт 58 хот-спот. Московский рынок опередил санкт-петербургский в 2004 — он насчитывает 67 точек доступа, что составляет 56% от общего числа по России. Доля других городов пока незначительна, в сумме она измеряется 4%. Однако, как отмечает бюллетень J'son & Partner, в Новосибирске, Нижнем Новгороде и Самаре растет число бесплатных хот-спотов. Лидерами Московского рынка названы компании «Моском» и «Таском» (13 и 17 коммерческих точек соответственно), за ними следуют eWi-Fi, Голден Телеком, Эквант, Wiland Ltd. и Вымпелком.

Wi-Fi предназначен для создания беспроводных локальных сетей (WLAN) и организации высокоскоростных беспроводных подключений к Интернету. В зависимости от конкретного стандарта сети Wi-Fi работают на частотах 2,4 ГГц или 5 ГГц и обеспечивают скорость передачи данных от 2 Мбит/с. Одна точка доступа может обеспечить охват в радиусе до 200 метров. Широкое распространение, помимо домашних и офисных сетей, Wi-Fi нашел в сфере организации публичного доступа в Интернет (хот-спотов) — с использованием этой технологии любой посетитель гостиницы, кафе, ресторана, бизнес-центра или аэровокзала (одним словом, заведения, в котором есть публичная точка доступа Wi-Fi) получает возможность мобильного подключения к Сети посредством своего ноутбука, КПК или телефона, поддерживающего стандарт беспроводного доступа.

Wi-Fi (читается «вай-фай») — это технология, которая позволяет разным устройствам, прежде всего компьютерам, взаимодействовать между собой без всяких проводов. Для того чтобы избавиться от них, надо установить hotspot (хот-спот, горячую точку, точку доступа) — передатчик, который ловит и передает сигнал в радиусе нескольких десятков метров. Если в этот передатчик воткнуть шнур с Интернетом, то Интернет, как бесцветный газ, повиснет в воздухе вокруг хот-спота. Сотрудники офиса, оборудованного Wi-Fi, не прикованы проводами к розеткам, а бродят со своими ноутбуками из кабинета в конференц-зал, оттуда — в столовую, оттуда — на балкон. По части удобства Wi-Fi будет почище мобильной связи.

За пределами офисов Wi-Fi тоже открывает массу перспектив — гулять по Интернету, валяясь на диване, проверять электронную почту, заходя в шанхайское кафе, купить нужную книжку в Интернет-магазине, занимаясь в библиотеке. Главное, чтобы поблизости находился хот-спот.

Почти все современные ноутбуки и карманные компьютеры так или иначе умеют работать в сетях Wi-Fi. Все больше и больше аэропортов, кафе и гостиниц в мире устанавливают у себя хот-споты, к которым

может подключиться любой желающий — за небольшие деньги или вообще бесплатно. Не за горами тот день, когда понятие «Интернет-кафе» станет бессмыслицей вроде «масла масляного» — Интернет будет в избытке в любом кафе.

Для подключения к Wi-Fi-сети можно помимо ноутбука использовать КПК, планшетный или даже персональный компьютер, лишь бы все они были оснащены беспроводными адаптерами. Если такого нет, то можно приобрести и установить адаптер дополнительно. Адаптер может быть в виде PCMCIA карточки преимущественно для мобильных ПК или в виде Compact Flesh карточки преимущественно для

Глава 2. Зачем нужен Wi-Fi?

Главное предназначение Wi-Fi — объединять компьютеры в локальную сеть. Раньше эта задача была непростой: сначала в компьютерном магазине надо было долго выбирать подходящие железячки, потом развинчивать компьютер и запихивать в него купленные детали, тянуть метры проводов, соединяя все со всем, и, наконец, убивать много часов, настраивая сеть. С Wi-Fi справится даже прекрасная бездельница.

Wi-Fi может связывать между собой не только компьютеры. Если у вас на ноутбуке хранится огромная коллекция музыкальных файлов, вы можете слушать их через колонки, которые находятся в другом конце дома; если в коллекции — кино, его можно транслировать на оборудованный Wi-Fi-проектор. Снаружи над входной дверью прикреплена камера наружного наблюдения? Выносите все провода на помойку и переходите на Wi-Fi-камеру — даже лежа в ванне, вы сможете следить за тем, не угнали ли там ваш небесно-голубой Ford Mustang.

Тенденция совершенно понятна. Оглянитесь вокруг: если вы видите какие-нибудь провода, значит, еще есть к чему стремиться.

В большинство современных ноутбуков и карманных компьютеров приемник и передатчик Wi-Fi уже встроены — например, он встроен во все ноутбуки, построенные на технологии Intel Centrino. Если встроенного Wi-Fi в компьютере нет, то придется купить недорогое устройство.

Поговаривают, что на старых компьютерах могут возникнуть сложности с подключением к беспроводной сети, но и это маловероятно. Чаще всего проблемы возникают из-за того, что ноутбук был настроен на работу в другой сети, скажем, в офисной. В таком случае не исключено,

что придется сначала отменить все старые настройки (например, настройки прокси-сервера).

Итак, вы заходите в кафе, заказываете кофе и включаете ноутбук. Если в ноутбуке есть адаптер Wi-Fi, то в правом нижнем (на ноутбуках Apple — в верхнем) углу экрана рядом с часами должна находиться иконка беспроводной сети. Если нажать на нее, появится список всех сетей Wi-Fi, которые ноутбук обнаружил в этом месте. Выбираете из списка нужную, нажимаете «Подключиться», и вы в Интернете. Иногда, особенно если сеть бесплатная, нужно поставить галочку, подтвердив, что вы осведомлены о недостаточной безопасности этого хот-спота.

Если услуга платная, подключиться не многим сложнее. Вместе с кофе придется заказать и столько-то часов Интернета: вам выдадут логин и пароль. Могут — на листочке бумаги (в гостинице), а могут — на карточке, похожей на карточку экспресс-оплаты мобильника. Пароль вас попросят ввести либо при нажатии кнопки «Подключиться», либо при попытке открыть какую-нибудь интернет-страницу. Единожды введя пароль, дальше вы сможете работать безо всяких препятствий.

Существует три способа организовать в квартире сеть с помощью Wi-Fi.

Способ №1

Если задача состоит в том, чтобы объединить всего два компьютера, то можно обойтись вообще без роутеров. Два Wi-Fi-адаптера могут работать друг с другом напрямую безо всяких центральных антенн. Этот способ годится только для двух компьютеров.

Способ №2

Если компьютеров больше, то понадобится точка доступа. Этим можно обойтись, если у вас есть компьютер, который вы готовы сделать сервером, то есть главным в сети. Для того чтобы сеть работала все время, сервер должен быть включен круглосуточно. Сервер может выполнять роль роутера и самостоятельно распределять Интернет-канал, но его настройка потребует некоторой квалификации, и если вы в себе не слишком уверены, лучше пригласить специально обученного человека.

Способ №3

Самый простой и универсальный. Точка доступа включается в роутер, роутер — в модем (впрочем, эти устройства могут быть объединены в два или даже в одно). Все! Теперь на каждом компьютере, в котором есть адаптер Wi-Fi, будет работать Интернет. Никакого сервера не нужно.

Любая компьютерная сеть — источник головной боли: чтобы обезопаситься от злоумышленников, приходится предпринимать кучу мер предосторожности. С Wi-Fi тоже надо быть начеку: ясно, что проникнуть в беспроводную сеть значительно проще, чем в обычную, — не нужно подключаться к проводам; достаточно оказаться в зоне приема сигнала. Так что если вы решили наладить у себя дома Wi-Fi, то имейте в виду следующее.

Сеть Wi-Fi может быть либо закрытой, либо открытой для всех желающих. Если у вас дома быстрый Интернет, вы уверены в своих администраторских силах и не чужды альтруизму, то сеть можно оставить и открытой. Это широкий жест. Постепенно на лужайке перед вашим домом станут собираться симпатичные молодые хакеры с ноутбуками. Ничего дурного в этом нет, и добрые люди по всему миру разрешают чужакам пользоваться своим Wi-Fi.

Если вы выберете путь филантропа, не забудьте поставить на все собственные компьютеры надежные операционные системы (если Windows — то либо 2000, либо XP) и нетривиальные пароли (не «a» и даже не «password», а какой-нибудь «3gH6j82Q»). Не помешает также иметь так называемый firewall, или брандмауэр, — программу, следящую за тем, чтобы никто незнакомый не пытался извне проникнуть в ваш компьютер. Хорошие роутеры (устройства, с помощью которых компьютеры объединяются в сеть) часто выпускаются со встроенным брандмауэром внутри, но чтобы грамотно его настроить, все равно придется несколько повозиться.

Как бы то ни было, лучше полностью закрыть сеть от несанкционированного доступа. Это можно сделать несколькими способами.

Способ №1

Запретить вашему роутеру передавать «идентификатор сети» (SSID) — аналог почтового индекса. Тогда сеть станет невидимой для посторонних. Это защитит от случайных прохожих, но не от серьезных хакеров.

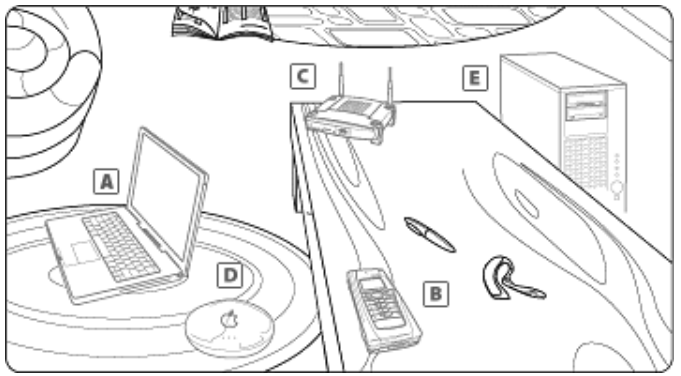
Способ №2

Для входа в сеть требовать специальный пароль. Такую возможность поддерживают почти все современные Wi-Fi-устройства.

Способ №3

Сконфигурировать роутер таким образом, чтобы он допускал подключения только с перечисленных вами вручную устройств. Другие компьютеры подключиться к сети не смогут в принципе.

Кроме того, возможна и другая опасность: хакеры решат перехватить информацию, которую вы пересылаете по сети Wi-Fi. Впрочем, вероятность этого бесконечно мала: по умолчанию при передаче данных с помощью Wi-Fi никакой шифровки не происходит. Если вы постоянно работаете с очень важными документами, то стоит подумать об использовании особой системы шифровки под названием VPN. Но если дело дошло до таких степеней защиты, лучше пригласить специально обученного человека.



Ноутбук

Если на ноутбуке есть наклейка Centrino, он может работать в сетях Wi-Fi — дополнительно ничего покупать не нужно. Если встроенного Wi-Fi в компьютере нет, то придется купить адаптер Wi-Fi. Это устройство размером с кредитку, как правило, вставляется в ноутбук сбоку в длинную дырку, похожую на щель в турникете при входе в метро.

КПК

В большинство современных карманных компьютеров приемник и передатчик Wi-Fi уже встроены.

Сетевой адаптер

Нужен каждому компьютеру, чтобы подключаться к сети. Для настольных компьютеров сетевые адаптеры бывают внутренние (вставляются внутрь компьютера) и внешние (подключаются к компьютеру через один из входов). Для ноутбуков и карманных компьютеров, если они изначально не поддерживают Wi-Fi, нужен внешний адаптер. Он подключается к ноутбуку либо через вход USB, либо через щель PCMCIA.

Роутер

Аналог электрического тройника, устройство, которое позволяет нескольким компьютерам подключаться к сети через один Интернет-канал. Чаще всего совмещен с беспроводной точкой доступа.

Точка доступа

Центральная антенна в беспроводной сети: она транслирует и принимает сигнал от всех компьютеров.

Глава 3. Хот-спот Wi-Fi —«горячая» точка мира телекоммуникаций

В последнее время в новостях все чаще стало встречаться загадочное слово «хот-спот» в сочетании с кофейнями, телефонией и ноутбуками. Что же такое хот-спот? Новое популярное блюдо американского фаст-фуда, чашка горячего кофе или нагретая солнцем телефонная будка? Попробуем разобраться.

Полтора года назад я уже говорил, что общедоступные беспроводные ЛВС, построенные по стандарту беспроводного Ethernet 802.11b (Wi-Fi), могут стать привлекательной альтернативой сотовым сетям третьего поколения 3G, которые по-прежнему буксуют. С тех пор технология Wi-Fi стала, пожалуй, одной из самых «горячих» точек мира телекоммуникаций.

Успех Wi-Fi объясняется тем, что эта технология уже проникла в десятки миллионов компьютеров, что позволило установить «смешные» цены на устройства Wi-Fi — вплоть до 30 долл. Скоро будет трудно встретить ноутбук без встроенного интерфейса Wi-Fi. Операторы поступят опрометчиво, если не обратят внимания на новый широкий рынок.

Общедоступные точки беспроводного доступа к Интернет по технологии Wi-Fi обычно организуются в аэропортах, отелях, конгресс-холлах, торговых центрах, кафе. По-английски эти точки доступа называются hot spot. В вольном переводе это означает «бойкое место». Не нужно быть пророком, чтобы предсказать: скоро слово «хот-спот» станет еще одним неологизмом в русском языке и его перестанут путать с хот-догом.

В США уже построено более 4 тыс. хот-спотов. Не прошло и двух лет, как бум Wi-Fi докатился до России. Несколько хот-спотов развернуты в московских отелях «Марриотт». О своих планах строительства хот-спотов в Москве также объявили компании «Вымпелком» и Art

Communications. Не отстает от Москвы и Санкт-Петербург — колыбель сотовой связи в России. Так, компания «Комсет» уже организовала в Северной столице 140 хот-спотов.

Большую активность в деле продвижения технологии Wi-Fi в России проявляет корпорация Intel, в марте с большим шумом объявившая о линии микропроцессорных продуктов Centrino, позволяющих экономически эффективно внедрять Wi-Fi в различные устройства.

Есть вопрос по поводу выгодности провайдерам предоставления большого объема трафика. Ведь не секрет, что скажем за «выделенку» пользователь вынужден платить примерно $50-90 в месяц за 500 Мб скаченной/принятой информации, а тут за несколько часов работы можно скачать гигабайт информации. На это специалисты отвечают следующее: «если у провайдера хорошо работает система биллинга и он своевременно выставляет клиентам счета за его потребление, то чем больше трафика будет потреблено, то тем большая сумма будет за него заплачена». Т.е. хот-спот при умелом маркетинге окупает себя.

Среди читателей наверняка есть предприниматели, которые с интересом смотрят на Wi-Fi-связь. Итак, что же нужно сделать для открытия беспроводной точки (хот-спота). Необходимо:

1. Провести изучение места

Важнейшие параметры, которые необходимо учитывать в первую очередь — это требуемая дальность действия сети, предполагаемое количество клиентских систем, подключенных к сети, и перспективы дальнейшего роста.

2. Выбрать стандарт для беспроводной сети

Напомним, в настоящее время существуют три отраслевых стандарта для беспроводной передачи данных, определенных Инженерным институтом электротехники и радиоэлектроники (IEEE): 802.11b, 802.11g и 802.11a.

3. Спланировать размещение компонентов сети

Если ваша компания невелика, то лучше охватить все предприятие беспроводной сетью. Например, устройство сетевого доступа по стандарту 802.11b имеет дальность действия до 100 м. Зоны действия базовых станций должны перекрывать друг друга без «белых пятен», чтобы исключить потерю связи с сотрудниками при переходе от одной точки доступа к другой. Если у вас крупная организация (например, компания, расположенная на нескольких этажах большого здания) то лучше разворачивать беспроводную постепенно.

4. Установить устройства беспроводного доступа

После того, как будет проложена широкополосная линия связи до вашего офиса, можно приступать к закупке и установке базовых станций. Большинство подобных устройств обладает сходными возможностями, поэтому единственно правильного решения в выборе поставщика нет. Убедитесь, что мобильные ПК настроены в соответствии с требованиями безопасности для беспроводных сетей.

5. Обеспечить безопасность сети

Защитить вашу беспроводную сеть не так уж сложно. Многие производители предлагают удобные в использовании и недорогие решения для этих целей. Кроме того, стандартами 802.11a и 802.11b поддерживается ряд мер безопасности, позволяющих вам повысить надежность и безопасность использования беспроводной сети в интересах бизнеса.

Как минимум, для защиты локальной беспроводной сети в малом и среднем бизнесе следует сменить идентификатор SSID (Service Set Identifier) вашего устройства доступа, который идентифицирует беспроводную сеть. Для доступа к сети клиентские ПК должны быть настроены на использование правильного SSID. К сожалению, применение идентификаторов SSID и паролей, установленных в системе по умолчанию, является распространенной практикой, что открывает хакерам доступ к компьютеру.

6. Расширить зону действия сети

С увеличением офисных площадей достаточно будет просто добавлять новые устройства беспроводного доступа. Такой план развития подойдет для любого предприятия. Работа в двух диапазонах включает в себя низкие частоты (от 5,15 до 5,35 ГГц).

По оценкам специалистов, «небольшой хот-спот, в котором планируется оказывать коммерческие услуги клиентам (т.е. сетевая инфраструктура плюс система биллинга), обойдется от 5 до 15 тысяч долларов США».

В настоящее время уже более половины всех выпускаемых ноутбуков и КПК имеют встроенную поддержку Wi-Fi, обычно стикер на корпусе устройства сообщает пользователю об этом. Кроме того, почти в любом компьютерном магазине можно приобрести различные адаптеры, позволяющие осуществлять подключение к Wi-Fi — они представляют собой либо PCMCIA-карты, либо внешние устройства, которые подключаются через USB. Подключение таких адаптеров не требует особы навыков и полностью регламентируется инструкцией производителя. При выборе адаптера надо обратить внимание на то, какой именно стандарт семейства IEEE 802.11 он поддерживает (в настоящее время это a, b и g),

обеспечивает ли он шифрование данных, какие типы соединения позволяет устанавливать (соединение с точкой доступа и равноправное — adhoc).

Для того чтобы подключиться к сети Wi-Fi, надо оказаться в зоне действия хот-спота. Затем следует установить связь между ноутбуком и точкой доступа — они определяют друг друга автоматически, после чего на корпусе или экране устройства появляется индикация беспроводной сети. После этого надо активировать доступ в Интернет. В большинстве случаев для этого достаточно просто запустить браузер и набрать в нем адрес какого-нибудь веб-сайта.

Глава 4. Как подключиться к Wi-Fi

В настоящее время уже более половины всех выпускаемых ноутбуков и КПК имеют встроенную поддержку Wi-Fi, обычно стикер на корпусе устройства сообщает пользователю об этом. Кроме того, почти в любом компьютерном магазине можно приобрести различные адаптеры, позволяющие осуществлять подключение к Wi-Fi — они представляют собой либо PCMCIA-карты, либо внешние устройства, которые подключаются через USB. Подключение таких адаптеров не требует особы навыков и полностью регламентируется инструкцией производителя. При выборе адаптера надо обратить внимание на то, какой именно стандарт семейства IEEE 802.11 он поддерживает (в настоящее время это a, b и g), обеспечивает ли он шифрование данных, какие типы соединения позволяет устанавливать (соединение с точкой доступа и равноправное -adhoc).

Для того чтобы подключиться к сети Wi-Fi, надо оказаться в зоне действия хот-спота. Затем следует установить связь между ноутбуком и точкой доступа — они определяют друг друга автоматически, после чего на корпусе или экране устройства появляется индикация беспроводной сети. После этого надо активировать доступ в Интернет. В большинстве случаев для этого достаточно просто запустить браузер и набрать в нем адрес какого-нибудь веб-сайта

Глава 5. Как платить за Wi-Fi

В некоторых случаях точки публичного беспроводного доступа могут работать на бесплатной основе (например, в режиме тестовой экс-

плуатации). Однако в большинстве хот-спотов за их пользование взимается плата. В зависимости от провайдера и заведения тарификация доступа может осуществляться на повременной основе или в из расчета за использованный трафик. В настоящее время разброс цен на пользование хот-спотами очень велик — от 90 рублей за час доступа, а также от 2 рублей за мегабайт.

Чаще всего доступ оплачивается с помощью предоплаченных карточек, которые продает оператор хот-спотов. Эти карты можно приобрести в офисах оператора, в заведениях, где есть хот-споты. В случае использования таких карт оплата доступа похожа на оплату услуг IP-телефонии — в тех заведениях, где есть хот-споты, обслуживаемые оператором, выпустившим карту, можно пользоваться доступом в Интернет до исчерпания лимита карты.

В некоторых случаях оплата использования хот-спота может осуществляться посредством мобильного телефона — пользователь отправляет SMS на определенный номер, получает код авторизации для подключения к хот-споту, оплата трафика или времени пользования точкой доступа списывается со счета у сотового оператора.

В гостиницах оплата за использование хот-спотов может включаться в счет за проживание.

Глава 6. Что такое беспроводная локальная сеть (WLAN)?

Сеть WLAN — вид локальной вычислительной сети (LAN), использующий для связи и передачи данных между узлами высокочастотные радиоволны, а не кабельные соединения. Это гибкая система передачи данных, которая применяется как расширение — или альтернатива — кабельной локальной сети внутри одного здания или в пределах определенной территории.

Каковы преимущества использования WLAN вместо проводной локальной сети?

- **Повышение производительности**. Сеть WLAN обеспечивает не привязанную к отдельным помещениям сеть и доступ в Интернет. Сеть WLAN дает пользователям возможность перемещаться по территории предприятия или организации, оставаясь подключенными к сети.

- **Простое и быстрое построение локальной сети**. Не нужно тянуть и укреплять кабели.
- **Гибкость установки**. Беспроводную сеть можно построить там, где нельзя протянуть кабели; технология WLAN облегчает временную установку сети и ее перемещение.
- **Снижение стоимости эксплуатации**. Беспроводные сети снижают стоимость установки, поскольку не требуются кабельные соединения. В результате достигается экономия, тем более значительная, чем чаще меняется окружение.
- **Масштабируемость**. Расширение и реконфигурация сети для WLAN не является сложной задачей: пользовательские устройства можно интегрировать в сеть, установив на них беспроводные сетевые адаптеры.
- **Совместимость**. Различные марки совместимых клиентских и сетевых устройств будут взаимодействовать между собой.

Трудна ли установка и администрирование сети WLAN?

Нет. Беспроводную локальную сеть строить проще, чем кабельную, администрирование же обоих типов сетей почти не отличается друг от друга. Клиентское решение сети WLAN построено на принципе Plug-and-Play, который предполагает, что компьютеры просто подключаются к одноранговой сети (peer-to-peer).

Какова дальность связи устройств WLAN?

Дальность действия радиочастот, особенно в помещениях, зависит от характеристик изделия (в том числе от мощности передатчика), конструкции приемника, помехозащищенности и пути прохождения сигнала. Взаимодействие радиоволн с обычными объектами здания, например со стенами, металлическими конструкциями и даже людьми, может повлиять на дальность распространения сигнала, и таким образом, изменить зону действия конкретной системы. Беспроводные сети используют радиочастоты, поскольку радиоволны внутри помещения проникают через стены и перекрытия. Диапазон или область охвата большинства систем WLAN достигает 160 м, в зависимости от количества и вида встреченных препятствий. С помощью дополнительных точек доступа можно расширить зону действия, и тем самым обеспечить свободу передвижения.

Надежны ли сети WLAN?

Да, сети WLAN исключительно надежны. Поскольку беспроводная технология уходит корнями в оборонную промышленность, обеспе-

чение безопасности беспроводных устройств предусматривалось с самого начала. Вот почему беспроводные сети обычно более надежны, чем кабельные. В сетях WLAN используется технология Direct Sequence Spread Spectrum (DSSS), которая отличается высокой устойчивостью к искажению данных, помехам, в том числе преднамеренным, и обнаружению. Кроме того, все пользователи беспроводной сети проходят аутентификацию по системному идентификатору, что предотвращает несанкционированный доступ к данным.

Для передачи особо уязвимых данных пользователи могут использовать режим Wired Equivalent Privacy (WEP), при котором сигнал шифруется дополнительным алгоритмом, а данные контролируются с помощью электронного ключа. Вообще говоря, в отдельных узлах перед включением в сетевой трафик должны приниматься свои меры безопасности. В сетях WLAN, работающих по спецификации 802.11b, для обеспечения более высокой надежности сети вместе с аутентификацией пользователя могут применять 40-битные и 128-битные алгоритмы шифрования. Перехват трафика, как умышленный, так и неумышленный, практически невозможен.

Что такое IEEE 802.11b?

IEEE 802.11b — выпущенная институтом Institute of Electrical and Electronic Engineers (IEEE) техническая спецификация, которая определяет функционирование беспроводных локальных вычислительных сетей, работающих в диапазоне 2,4 ГГц со скоростью 11 Мбит/с по протоколу Direct Sequence Spread Spectrum.

Какова пропускная способность сети WLAN 802.11b?

Сети WLAN 802.11b работают со скоростью до 11 Мбит в секунду. Для пользователей скорость работы сравнима со скоростью кабельной сети. Точно так же, как и в обычной сети, пропускная способность сети WLAN зависит от ее топологии, загрузки, расстояния до точки доступа и т.д. Как правило, заметной разницы в производительности беспроводной и кабельной сети нет.

Что такое точка доступа?

Точка доступа соединяет кабельную и беспроводную сеть и позволяет клиентам последней получить доступ к ресурсам кабельной сети. Каждая точка доступа расширяет общую вычислительную мощность системы. Пользователи могут перемещаться между точками доступа, не теряя соединения с сетью, — как и при подключении к сети с помощью сотового телефона. Другими словами, точка доступа — это программно-аппаратное устройство, которое выполняет роль концентратора для клиента беспроводной сети и обеспечивает подключение к кабельной сети.

Сколько пользователей может поддерживать одна система WLAN?

Количество пользователей практически неограниченно. Его можно увеличивать, просто устанавливая новые точки доступа. С помощью перекрывающихся точек доступа, настроенных на разные частоты (каналы), беспроводную сеть можно расширить за счет увеличения числа пользователей в одной зоне. Перекрывающихся каналов, которые не будут создавать взаимные помехи, одновременно может быть установлено не более трех; эти каналы втрое увеличат количество пользователей сети. Подобным образом можно расширять беспроводную сеть, устанавливая точки доступа в различных частях здания. Это увеличивает общее число пользователей и дает им возможность перемещаться по зданию или территории организации.

Сколько пользователей одновременно поддерживает одна точка доступа?

Количество пользователей в этом случае зависит, в первую очередь, от загруженности трафика. В сети WLAN полоса пропускания делится между пользователями так же, как в кабельной сети. Исходя из числа пользователей производительность сети зависит также от рода выполняемых пользователями задач.

Глава 7. Wi-Fi сеть в Московском метро: лето 2005 года

Пассажиры Московского метрополитена смогут уже летом 2005 года выходить в Интернет. Одна из известных российских телекоммуникационных компаний уже разместила в столичной подземке 40 так называемых хот-спотов (точек беспроводного доступа к Интернету) и до конца года доведет их число до 200-300.

Проект будет ориентирован, прежде всего, на «высокотехнологичных» пассажиров — владельцев смартфонов и карманных компьютеров. Эти аппараты уже оснащены технологией беспроводного доступа, а число их владельцев растет день от дня. Предполагается, что наиболее востребованными услугами будет электронная почта и веб-серфинг (навигация по сети). А люди, следящие за событиями в мире и стране, смогут подгружать последние новости прямо в пути, на остановках.

Технология беспроводного выхода в сеть из точек доступа в общественном транспорте имеет большие перспективы. Беспроводной Интернет уже получил широкое распространение в странах Европы и США.

На конец 2004 года только в Старом Свете насчитывалось 27 тысяч точек беспроводного публичного доступа, более 68% из которых расположены во Франции, Германии и Великобритании.

Чтобы успешно построить сеть Wi-Fi, нужно не только правильно выбрать оборудование для нее, но и тщательно спланировать саму сеть, уделив пристальное внимание мельчайшим деталям ее функционирования. Технология Wi-Fi продолжает развиваться. При этом изменяются как протоколы физического уровня, так и сама системная архитектура. Некоторые аналитики характеризуют данный процесс как «борьбу» между «тонкими» и «толстыми» точками доступа, однако опытные сетевые специалисты понимают, что при столь упрощенном подходе к анализу ситуации в индустрии беспроводных ЛВС (БЛВС) теряется понимание главного: предприятиям требуются системы Wi-Fi, работающие с высокой надежностью, имеющие масштабируемую производительность, многоуровневую защиту данных и централизованное управление. К тому же они должны быть недорогими в эксплуатации.

Глава 8. Wi-Fi сегодня и завтра

Несмотря на то, что организация Wi-Fi пока еще не приносит ощутимого дохода российским компаниям, и они ставят на него в долгосрочной перспективе, в этом сегменте рынка все же продолжают появляться новые игроки. В списке компаний предоставляющих Wi-Fi доступ в Интернет прибыло — российский альтернативный оператор «Комстар Объединенные Телесистемы» запустил в тестовую эксплуатацию публичную зону беспроводного доступа в Интернет в гостиничном комплексе «Пекин».

Ставшее притчей во языцех отношение владельцев беспроводных локальных сетей к их защищенности от проникновения извне, может повлечь за собой множество негативных последствий. Проблема с сохранностью информации внутренней, принадлежащей владельцам сети — лишь самое очевидное из них. Менее очевидно использование внутренних ресурсов сети и машин для выхода на ресурсы внешние, расположенные в Интернет. Проблема кажется надуманной, но — если есть возможность, то почему бы ею и не воспользоваться? Именно об этом говорилось в докладе Адриана Райта (Adrian Wright) на прошедшей в Лондоне конференции по компьютерной безопасности First International Security Users Conference.

Райт, один из руководителей британской компании Secoda Risk Management, описал предельно простой механизм использования беспроводных локалок. Злоумышленник, намеренный использовать чужую Wi-Fi сеть в качестве стартовой площадки, подъезжает на территорию, покрываемую радиопередающим оборудованием (т.н. точкой доступа) некой компании, подключается к сети и использует ее, к примеру, для спам-рассылки по десяткам миллионов адресов. После чего спокойно ретируется с места событий. Стоит ли игра свеч? Безусловно! Причин, по которым некто может захотеть воспользоваться чужой беспроводной локалкой, сразу несколько. Прежде всего: провайдеры, наконец-то, начали следить за действиями чересчур активных пользователей, блокируя или наказывая тех, кто использует их ресурсы для спорных с точки зрения закона действий (Россия, кстати, не исключение). Поэтому для спамера работа через чужой канал оказывается спокойней с точки зрения собственной безопасности. Кроме того, по словам Райта, при достаточно больших объемах рассылаемой почты, значителен и генерируемый трафик, поэтому работа через чужой канал обещает принести уже чисто экономическую выгоду. Но самое главное — отследить спамера в таком варианте представляется делом почти невозможным: если спамер и рекламодатель — разные лица, отыскать непосредственного виновника (а им будет именно спамер — обвинить размещающих рекламу человека или компанию куда сложнее) будет почти невозможно.

Впрочем, панику поднимать рано: как оказалось, ZDNet News, опубликовавшее отчет о выступлении Райта, слегка приукрасило реалии. На самом деле, Райт говорил лишь о потенциальной осуществимости такого механизма — прямых доказательств его использования на практике у исследователя нет. Но, как и всегда, это лишь вопрос времени — ведь ситуация с защищенностью беспроводных корпоративных сетей и в самом деле аховая. Из-за своей гибкости, дешевизны и удобства такие сети — одна из самых привлекательных компонент ИТ-инфраструктуры. Попросту говоря, штука модная — а как и всегда в таких случаях, о побочных эффектах задумываются немногие. В результате, по некоторым данным, до 80% корпоративных Wi-Fi локалок никак не защищены от вторжения. А те, кто беспокоится о защите входа, часто оставляют неприкрытой передаваемую информацию — не пытаясь использовать даже минимальный криптографический инструментарий.

Конечно, решения проблемы есть — но все они требуют от владельцев сети дополнительных и серьезных затрат. Так, можно использовать физические средства сигнализации о вторжении (пример — Intrusion Detection System от Netsec): устройства, установленные по периметру охраняемого здания, сигнализирующие о подключении извне. Однако здесь совершенно необходимо наличие службы безопасности,

способной распознавать информационные угрозы. Можно поступить иначе, ограничив объем данных и сервисов, доступных пользователям через беспроводное соединение (такой тактики придерживается, в частности, Deutsche Bank). Но и здесь свои проблемы, главная из которых — личная сознательность персонала, которому необходимо втолковать разницу между различными способами получения доступа к нужным данным.

Глава 9. Wi-Fi для всех

2004 стал годом повсеместного запуска услуг Wi-Fi в России — к такому выводу пришли прогнозисты компании J'son & Partner, специализирующейся на проведении исследований в области телекоммуникаций, медиа и информационных технологий. Согласно отчету, иллюстрирующему текущее состояние рынка беспроводных сетей, к концу 2007 году количество точек доступа в двух столицах может превысит 550.

На данный момент в России насчитывается 21 провайдер Wi-Fi (WISP), девять из них предоставляют услугу на коммерческой основе. Обычно с клиентов взимается почасовая оплата, которая составляет 6–10 долларов за час. Лишь 3 WISPa считают работу с Wi-Fi своим основным бизнесом, остальные пока рассматривают ее как возможное направление будущего развития компании, прощупывают рынок.

Большая часть российских пользователей Wi-Fi — студенты, они составляют 60% от общего числа (800–1000 человек в первом квартале 2004 г.). Такое положение вещей объясняется просто: в главных университетах страны открыто много бесплатных хот-спотов. Вторую категорию активных потребителей услуги представляют бизнесмены. По разным оценкам, в настоящий момент от 400 до 600 предпринимателей пользуются беспроводными сетями регулярно. Именно они приносят Wi-Fi провайдерам 70% реальных доходов.

Обычным местом предоставления доступа в интернет через Wi-Fi в России являются кафе и кофейни, которые ориентируются, в основном, на обеспеченных молодых людей — своих постоянных клиентов. Треть всех коммерческих хот-спотов расположены в отелях и аэропортах, их целевой аудиторией являются деловые люди, для которых удобство важнее цены. Так, общая сумма ежемесячных доходов от Wi-Fi в отелях по состоянию на март 2005 г. составила $150 000.

К сожалению, пока не во всех отелях постояльцы могут легко обнаружить информацию о возможности пользования Wi-Fi, осведомленность местного персонала, который мог бы ответить на вопросы об услуге, тоже пока оставляет желать лучшего. Сейчас, и это относится не только к гостиничному бизнесу, желающий воспользоваться Wi-Fi должен проявить большую настойчивость, специально спрашивая о наличии сервиса и способе его оплаты.

При этом ключевым фактором успеха хот-спота аналитики J'son & Partner считают именно инструктаж персонала, который должен быть проведен таким образом, чтобы служащие, например, отеля могли описать потенциальному клиенту предоставляемую услугу Wi-Fi. Одновременно специалисты указывают на необходимость проведения провайдерами активных рекламных кампаний, если те заинтересованы в привлечении большего числа платежеспособных пользователей.

Что касается развития Wi-Fi в мире, то здесь в течение 2005 года ожидается более чем 225-процентный рост числа хот-спотов, так что если их количество в конце 2004 доходило до 73 000, то к концу текущего года число точек доступа должно достичь 240 000. Лидирующее место на мировом рынке занимают на данный момент страны Азии, на долю которых приходится 49% хот-спотов. К концу второго квартала 2005 года 28% точек были открыты в США, так что количество европейских хот-спотов соответствовало 23%.

Глава 10. Безопасен ли Wi-Fi?

Защита беспроводных соединений обеспечивается использованием протоколов WPA и WEP, осуществляющих контроль за аутентификацией пользователей и кодированием сетевого трафика. Кроме шифрации трафика 40, 64 или даже 128 битным ключом, в беспроводных сетях возможен выбор полос частоты, в которых работают устройства передачи данных. В сетях WLAN используется особая технология Direct Sequence Spread Spectrum, обеспечивающая высокую устойчивость ко всем видам искажениям и помехам в радиоэфире. Разработчики ведут постоянную работу по совершенствованию защиты беспроводных сетей.

Глава 11. Взлом сетей Wi-Fi

Каждая беспроводная сеть имеет как минимум два ключевых компонента, базовую станцию (stations) и точку доступа (access points). Беспроводные сети могут функционировать в двух режимах: ad-hoc (peer-to-

peer) и infrastructure. В первом случае сетевые карточки напрямую общаются друг с другом, во втором случае при помощи точек доступа, в этом случае такие точки служат в качестве Ethernet мостов.

Клиент и точка перед передачей данных должны установить соединение. Как не трудно догадаться между точкой и клиентом может существовать всего три состояния:

- Аутентификация не пройдена и точка не опознана
- Аутентификация пройдена, но точка не опознана
- Аутентификация принята и точка присоединена

Обратно не трудно понять, что обмен данными может идти только в третьем случае. До установления соединения стороны обмениваются управляющими пакетами, точка доступа передает опознавательные сигналы с фиксированным интервалом, клиент, приняв такой пакет, начинает аутентификацию посылкой опознавательного фрейма, после авторизации клиент посылает пакет присоединения, а точка — пакет подтверждения присоединения беспроводного клиента к сети.

Механизмы безопасности

Стандарт 802.1 для беспроводных сетей предусматривает несколько механизмов обеспечения безопасности сети. В этом разделе мы рассмотрим пять основных, наиболее используемых.

Wired Equivalent Protocol

Wired Equivalent Protocol, или WEP, разработан был автором стандарта 802.1. Основная функция WEP — шифрование данных при передаче по радио и предотвращение неавторизованного доступа в беспроводную сеть. По умолчанию WEP отключен, однако его можно легко включить и в таком случае он начнет шифровать каждый исходящий пакет. Для шифрования WEP использует алгоритм RC4.

WEP 2

Представленный в 2001 году после обнаружения множества дырок в первой версии, WEP 2 имеет улучшенный механизм шифрования, и поддержку Cerberus V. Понятно, что полную поддержку такой системы еще не кто не осилил.

Open System Authentication

Система аутентификации, по умолчанию используемая в протоколе 802.11. Собственно системы как таковой нет — аутентификацию проходит любой, кто запрашивает. В случае OSA не помогает даже WEP,

так как в ходе экспериментов было выяснено, что пакет аутентификации посылается НЕ зашифрованным.

Access Control List

В протоколе 802.11 не описывается, но используется многими в качестве дополнения к стандартным методам. Основа такого метода — клиентский Ethernet MAC, уникальный для каждой карточки. Точка доступа ограничивает доступ к сети в соответствии со своим списком MAC адресов, есть клиент в списке и доступ разрешен, нет — значит, нет.

Closed Network Access Control

Тут не намного сложнее: либо администратор разрешает любому пользователю присоединяться к сети, либо в нее может войти только тот, кто знает ее имя, SSID. Сетевое имя в таком случае служит секретным ключом.

Атаки

По некоторым оценкам 95% сетей практически беззащитны и каждый из описываемых методов имеет 98% шанс на успех. Зачем можно использовать такую сеть? Ну, например, для получения бесплатного доступа в Интернет, изучения материалов, представленных в сети, да и просто для развлечения, ведь в отличие от стационарной сети поимка хакера в беспроводной среде — довольно не тривиальное дело.

Access Point Spoofing & MAC Sniffing

Список доступа вполне пригоден к использованию совместно с правильной идентификацией пользователей в этом самом списке. В случае же с MAC адресом Access Control List очень просто побороть, так как такой адрес просто изменить (беспроводные сетевые карты позволяют программно менять MAC адрес) и еще проще перехватить, так как он даже в случае с WEP передается в открытом виде. Таким образом, элементарно проникнуть в сеть, защищенную Access Control List и использовать все ее преимущества и ресурсы.

В случае наличия у вас в загашнике собственной точки доступа есть другая возможность: устанавливаете Access Point рядом с существующей сетью — если ваш сигнал сильнее оригинального, то клиент подключится именно к вам, а не к той сети, передав при этом не только MAC адрес, но и пароль и прочие данные.

WEP Attacks

Для объяснения всех атак сначала, думаю, необходимо рассказать о том, как же шифруются данные в WEP. Итак, вот весь план:

- Чистые данные проходят проверку целостности, и выдается контрольная сумма (integrity check value, ICV). В протоколе 802.11 для этого используется CRC-32.
- ICV добавляется в конец данных.
- Генерируется 24-битный вектор инициализации (IV) и за ним привязывается секретный ключ. Полученное значение является исходным для генерации псевдослучайного числа.
- Генератор случайных чисел выдает ключевую последовательность.
- Данные XOR'ятся с этой ключевой последовательностью.
- Вектор инициализации добавляется в конец и все это передается в эфир.

Plaintext атака

В таком взломе атакующий знает исходное послание и имеет копию зашифрованного ответа. Недостающее звено это ключ. Для его получения атакующий посылает цели небольшую часть данных и получает ответ, получив его, мы находим 24-битный вектор инициализации, используемый для генерирования ключа — нахождение ключа в таком случае всего лишь задача брутфорса.

Другой вариант — обычный XOR. Если у нас есть посланный plain text и его зашифрованный вариант, то мы просто XOR'им шифр и на выходе получаем ключ, который вместе с вектором дает возможность «грузить» пакеты в сеть без аутентификации на точке доступа.

Повторное использование шифра

Атакующий выцепляет из пакета ключевую последовательность. Так как алгоритм шифрования WEP на вектор отводит довольно мало места, атакующий может перехватывать ключевой поток, используя разные IV, создавая для себя их последовательность. Таким образом, хакер может расшифровывать сообщения, используя все тот же XOR, когда по сети пойдут зашифрованные данные при помощи сгенерированных ранее ключевых потоков их можно будет расшифровать.

Атака Fluhrer-Mantin-Shamir

Летом прошло года работник Cisco Scott Fluhrer, Itsik Mantin и Adi Shamir из научного института Израиля, обнаружили уязвимость в алгоритме Key Scheduling Algorithm (KSA) который работает в RC4. С ее помощью можно получить как 24-битный ключ WEP, так и 128-битный

ключ WEP 2. На всеобщее обозрение было представлено две программы — Air snort и WEPCrack.

Low-Hanging Fruit

Собственно как ясно из названия дело тут даже не в атаке, а в добыче халявы из незащищенных сетей. Большинство беспроводных сетей абсолютно не защищены, в них не требуется авторизации и даже не используют WEP, так что человек с беспроводной сетевой карточкой и сканером может легко подключиться к Access Point'у и использовать все ресурсы им предоставляемые. Отсюда и название — низко висящие фрукты, которые сорвать не составляет никакого труда...

Глава 12. Безопасность сетей

Итак, мы рассмотрели основные проблемы безопасности, настало время поговорить и о защите от хакеров. В этой главе вы узнаете об основных методах борьбы с незаконным проникновением:

Фильтрация MAC-адресов

В этом варианте администратор составляет список MAC адресов сетевых карт клиентов. В случае нескольких AP необходимо предусмотреть, чтобы MAC адрес клиента существовал на всех, дабы он мог беспрепятственно перемещаться между ними. Однако этот метод легко победить, так что в одиночку его использовать не рекомендуется.

WEP

Обеспечивает шифрование при передаче данных между клиентом и сервером, однако как я уже описывал, так же легко поддается взлому. Использовать его, тем не менее, можно и нужно, дабы не облегчать взломщику его задачу.

SSID (Network ID)

Первой попыткой обезопасить беспроводные сети была система Сетевых Идентификаторов или SSID. При попытке клиента подключиться к AP на него передается семизначный алфавитно-цифровой код, используя метку SSID мы можем быть уверены, что только знающие его клиенты будут присоединяться к нашей сети. При использовании WEP сетевой идентификатор при передаче шифруется, однако на конечном устройстве он хранится в виде plain-text'a, так что злоумышленник, имеющий доступ к девайсам сможет его прочесть.

Firewall

По ходу дела единственная вещь, которая может помочь от неавторизованного доступа. Доступ к сети должен осуществляться при помощи IPSec, secure shell или VPN и брандмауэр должен быть настроен на работу именно с этими безопасными соединениями — они и помогут избежать присутствия нежелательных «насекомых».

AccessPoints

Точку доступа надо настраивать на фильтрацию MAC адресов, кроме того, физически сам девайс необходимо изолировать от окружающих. Рекомендуется так же конфигурировать точку только по telnet, отрубив конфигурацию через браузер или SNMP.

Структура сети

Основы безопасности необходимо закладывать еще на стадии проектирования беспроводной сети. Вот несколько фишек, которые помогут «протянуть» правильную сеть:

- Защищайте свою сеть при помощи VPN или access control list
- Точка доступа не должна быть напрямую подсоединена к локальной сети, даже если WEP включен
- Точка доступа никогда не должна находиться позади брандмауэра
- Доступ клиентам беспроводной сети надо давать по secure shell, IPSec или виртуальные частные сети. Они обеспечивают приемлемый уровень безопасности.

Глава 13. Запуск Wi-Fi Комстар

«Комстар Объединенные Телесистемы», Fujitsu Siemens Computers, Intel и «РосБизнесКонсалтинг» объявляют о запуске нового проекта «Wi-Fi Комстар», направленного на создание сети точек беспроводного доступа и популяризацию мобильных Интернет-решений. Запуск проекта «Wi-Fi Комстар» связан с началом активного развития сетей беспроводной передачи данных, способствующих росту как потребительского сектора, так и корпоративного.

Суть проекта заключается в создании и накоплении критической массы хот-спотов, достаточной для охвата большинства общественных и

деловых центров Москвы и массового распространения технологии Wi-Fi. Стратегия развития проекта предполагает работу по нескольким направлениям: организация точек беспроводного доступа в публичных местах и использование беспроводной технологии в качестве альтернативы кабельных локальных сетей. Планы развития на 2005-2006 гг. включают открытие более 200 хот-спотов. Инвестиции в проект составят $3,3 млн.».

Для продвижения проекта предполагается использовать все возможные варианты сотрудничества с заказчиками: организация хот-спота как за счет оператора связи, так и владельца здания, работа с существующими клиентами по расширению имеющегося у них набора услуг связи, привлечение заказчиков, нуждающихся в организации защищенной локальной радиосети. Таким образом, «Комстар» получает возможность создать новую топологию сети, увеличить свое присутствие на территории Москвы и заметно упрочить положение в новом сегменте рынка. Основное поле для реализации этой бизнес-модели — гостиницы, деловые центры, любые площадки, имеющие отношение к бизнес-клиентам, реально приносящим более 70% доходов от Wi-Fi.

К работе над проектом привлечены крупнейшие мировые компании Fujitsu Siemens Computers, Intel и «РосБизнесКонсалтинг», участие которых в значительной степени расширяет возможности «Wi-Fi Комстар». С каждым днем повышается спрос на портативные устройства с поддержкой Wi-Fi, уже сейчас выпуск подобной техники составляет более 80% в общем объеме портативных устройств, что говорит о несомненной популярности Wi-Fi-решений в будущем.

Глава 14. Wi-Fi на практике

О технологии Intel Centrino для мобильных ПК с момента ее появления не писал разве что ленивый. Описывалась сама технология, подробно рассматривались ноутбуки на базе этой технологии, были представлены новости об открытии хот-спотов, но ни слова не было сказано о качестве работы в беспроводной сети. Попытаемся исправить сложившуюся ситуацию и описать свои ощущения от работы с беспроводным ноутбуком на форуме компании Intel, который завершился в общем-то недавно. В 2003 году корпорация Intel создала фонд с капиталом 150 миллионов долларов для инвестиций в компании, способствующие расширению и внедрению инфраструктуры и функциональных возможностей для беспроводного доступа.

Как работает ноутбук Centrino?

Радиоинтерфейс передачи данных типа IEEE 802.11b интегрирован в мобильные компьютеры, построенные по технологии Centrino и является их неотъемлемой составной частью. Благодаря этому ноутбук автоматически находит все близлежащие хот-споты (если таковые имеются) и запрашивает у пользователя пароль на подключение.

А в это время в Америке

В США, в отдаленных районах страны, затруднена прокладка проводов, поэтому беспроводная связь почти не имеет альтернативы. Чтобы доставить Интернет в сельскую местность, приходится расширять частотный спектр беспроводных устройств. Федеральная комиссия по Коммуникации США. 18 ноября этого года заявила, что решением проблемы будет 80 процентное повышение диапазона, который беспроводные сети смогут использовать для соединения компьютеров и других электронных устройств между собой.

Беспроводной широкополосный Интернет занимает на рынке все более и более прочные позиции. Но на сегодняшний день, существующих частот явно не достаточно, чтобы охватить широкополосным соединением все отдаленные и малозаселенные участки. Новые частоты находятся в 5 гигагерцовом диапазоне. Это намного выше, чем у коммерческих радио и телевизионных станций.

Глава 15.
Игра по беспроводной сети

Сегодня все больше игровых программ поддерживают многопользовательский режим. Сетевые игры дают ощутимые преимущества и быстро развиваются. Но прокладывать кабели по дому — занятие отнюдь не из легких. Предлагаю вам ознакомиться с возможным решением этой проблемы — беспроводной сетью.

Уже несколько лет важнейшие «игроки» продвигают на компьютерном рынке технологии беспроводных сетей. Если первоначально каждая компания желала выдвинуть свое решение, несовместимое с остальными, то сегодня «игроки» пришли к пониманию необходимости развития и совершенствования единого стандарта — WiFi. Но даже WiFi (Wireless Fidelity) неоднозначен. Его основой является технология 802.11b, которая работает в диапазоне 2,4 ГГц и имеет максимальную теоретическую пропускную способность 11 Мбит/с. Существует и другая технология, 802.11a, но она работает только в США. Телекоммуникации

в частотном диапазоне, близком к 5 ГГц, фактически запрещены в России и в Европе. Пропускная способность 802.11a выше — 54 Мбит/с, однако радиус действия сети намного меньше. Чтобы улучшить производительность 802.11b, некоторые производители анонсировали «ускоренную» версию, которая может достичь пропускной способности 22 Мбит/с. Такая технология получила название 802.11b+.

И, наконец, новый стандарт, в который заложена технология 802.11g, все еще находится в стадии доработки. Стандарт будет продолжать использовать частотный диапазон 2,4 ГГц, к тому же он, в свою очередь, совместим с 802.11b, что позволяет надеться на светлое будущее. Технология 802.11g обеспечивает максимальную теоретическую пропускную способность 54 Мбит/с, и обладает чуть уменьшенным радиусом действия по сравнению с 802.11b.

Радиус действия, скорость и оборудование

Поскольку Wi-Fi является беспроводным протоколом связи, он характеризуется радиусом действия. Все производители указывают максимальный теоретический радиус 150 метров. Но такое расстояние возможно лишь при отсутствии препятствий на пути распространения сигнала. Более того, на максимальном расстоянии вы не получите высокую скорость, поскольку она будет поэтапно уменьшаться до 1 Мбит/с. Чтобы связь при увеличении расстояния не прерывалась, WiFi предусматривает автоматическую подстройку скорости передачи в зависимости от условий связи.

Глава 16.
Wi-Fi в самолете: небо без проводов!

Компания Connexion, подразделение Boeing, продолжает расширять свою деятельность — хот-споты уже установлены на бортах авиакомпаний Lufthansa, Singapore Airlines, SAS, ANA и Japan Airlines.

Через три-четыре часа полета усталость дает о себе знать. К этому моменту вас уже наверняка покормили, вы прочитали очередную главу книги, пролистали журнал и даже успели посмотреть фильм, который никогда и не подумали бы посмотреть, будучи на земле. Однако что делать следующие два, три или даже десять часов полета?

Подразделение компании Boeing — Connexion желает, чтобы пассажиры навсегда забыли о скуке и продуктивно работали во время полета. Для этого Connexion обеспечивает пассажиров скоростным доступом в Интернет через спутник. Этот сервис Connexion разрабатывала в тече-

ние нескольких лет, так как после трагических событий 11 сентября в местных перевозках США и на международных рейсах произошла некоторая стагнация.

Эта служба уже работает на некоторых самолетах и маршрутах компаний Lufthansa, Singapore Airlines, SAS, ANA и Japan Airlines. Ожидается, что в течение этого года к ним присоединятся China Airlines, El Al и Korean Air. British Airways также высказала намерение присоединиться, но о сроках ничего не сообщила. Lufthansa использует сервис Connexion на рейсах между 13 городами Северной Америки и Германией, SAS — на всех авиарейсах в Сиэтл.

Connexion через партнерские компании предлагает как предварительную оплату за всю продолжительность перелета, так и оплату по времени. Если полет длится менее трех часов, то неограниченное использование Интернета обойдется вам в $14,95; от трех до шести — $19,95; более шести — $29,95. При повременной оплате Интернета первые полчаса будут стоить $9,95, после чего вы будете платить по 25 центов за каждую последующую минуту. Второй вариант интереснее использовать при продолжительных полетах, когда имеет смысл потратить $10 — $15, вместо $30.

Во время подключения к Сети появляется экран авторизации, напоминающий авторизацию в хот-спотах, на котором предлагается ввести данные кредитной карточки. Передача данных защищается SSL.

Принцип работы

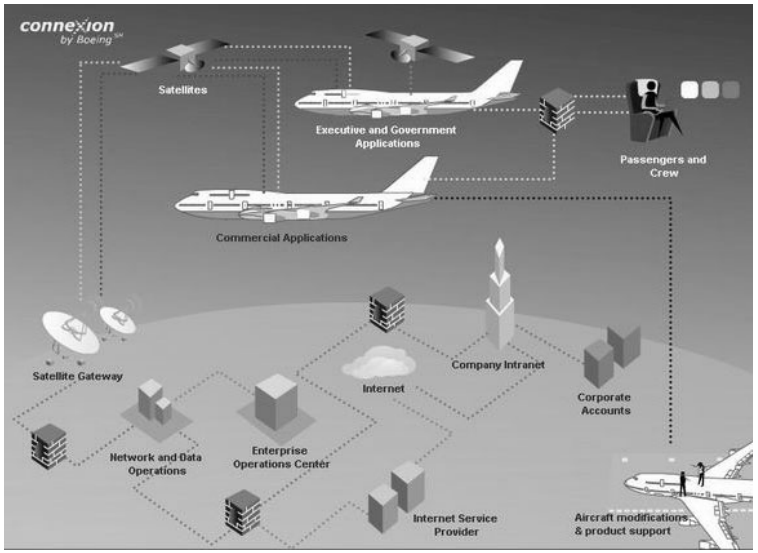
Connexion использует геостационарные спутники, работающие в диапазоне Ku, которые могут передавать данные с наземных станций на неподвижные и мобильные ресиверы, находящиеся на участках площадью в сотни квадратных километров. На спутниках установлено множество пар ретрансляторов, отдельно для приема и передачи, которые покрывают выбранный регион. Диапазон Ku занимает полосу частот от 10,7 до 12,75 ГГц, что позволяет обеспечивать высокую пропускную способность каналов.

На орбиту выведено несколько десятков Ku-спутников, которыми владеют различные компании всего мира. Boeing сотрудничает с несколькими спутниковыми операторами и при необходимости будет дополнять их количество.

В небе принято решение использовать частотный диапазон спутниковой связи, который позволяет обеспечить достаточную пропускную способность, чтобы пользователи смогли работать в Интернете из самолета так же, как на земле.

Вместо того чтобы заново изобретать велосипед, Connexion решила воспользоваться уже существующей технологией.

Было необходимо создать систему, которая сможет работать на самолете, летящем со скоростью около 1000 км/ч на любой широте и высоте полета, и которая позволила бы пользоваться Интернетом нескольким десяткам пассажиров одновременно.



Суть технологии Connexion заключается в использовании спутниковой антенны. Антенна должна служить проводником между самолетом и спутником. Она разработана с учетом того, чтобы наиболее эффективно передавать и принимать сигнал со спутника.

Чем более эффективной будет антенна, тем меньше услуга будет стоить Boeing, и тем большая пропускная способность будет обеспечиваться. Это позволяет постоянно следить за спутниками, которые находятся на высоте 37 тысяч километров над экватором и покрывают территорию до 75 градусов северной и южной широты. Следует отметить, что по ней проходит 99,2 процента авиаперелетов.

Доступ в Интернет обеспечивается на протяжении всего перелета. Однако некоторые пассажиры отмечают пропадание канала, хотя в целом связь остается стабильной. Впрочем, пропадания носят кратковременный характер.

Самонастраивающиеся антенны в самолетах связываются со спутниками, которые, в свою очередь, имеют постоянные соединения с наземными станциями. Boeing использует станции в Литлтоне (Littleton), Колорадо; Японии; Швейцарии и Москве. Пятая станция пока официально не была объявлена, но, как ожидается, она начнет работать уже в этом месяце.

Скорость соединения с самолетом составляет 5 Мбит/с для входящего трафика (земля-спутник-самолет) и 1 Мбит/с — для исходящего (самолет-спутник-земля). Дил уточнил, что можно расширить канал до 20 Мбит/с, но пока никому не требовалось более 5 Мбит/с.

Партнеры Connexion, в большинстве своем, предпочитают устанавливать в самолетах только сети Wi-Fi. Некоторые самолеты оборудованы Ethernet-портами, например часть бортов Lufthansa, но только для бизнес-класса и первого класса. (Там же обычно устанавливаются и розетки питания).

Конечно же, указанная полоса пропускания разделяется на всех пользователей самолета, а не дается каждому лично.

Не только для пассажиров

Как предполагается, Интернетом будут пользоваться, в первую очередь, пассажиры самолетов. Но представители Boeing сообщают, что соединение Connexion может использоваться для других нужд. Например, уже в этом году на самолетах Singapore Airlines должна появиться широковещательная передача видео. Сначала Connexion предложит четыре канала новостей и познавательных передач, но в дальнейшем появятся и другие, в частности, спортивные.

Ожидается, что живое вещание видео позволит развиться и телемедицине. Тогда доктор сможет удаленно общаться с пассажиром и дать какие-либо рекомендации по картинке видео и биометрическим показателям типа пульса и артериального давления. В итоге пассажиру будет оказана помощь еще до посадки. В принципе, уже сегодня экипаж самолета может советоваться с наземными медицинскими службами, но видео в реальном времени и биометрические данные облегчают эту задачу.

В будущем пилоты смогут более детально сообщать о проблемах в самолете, для решения которых требуется техническая поддержка, еще до приземления. Телеметрические системы смогут передавать состояние самолета и предупреждать возникновение неисправностей.

Boeing оптимистично относится к тому, что в будущем Wi-Fi будет работать в качестве магистральной сети самолета, предоставляя различные услуги. Технология Wi-Fi достаточно быстро развивается, так что

для такого самолета, как 787, Wi-Fi может стать не только магистралью для коммуникаций, но и магистралью развлечений.

Есть проблемы?

Ситуация Connexion выгладит оптимистичной, но не стоит забывать и о некоторых проблемах.

Ограничения диапазона Ku

Спутники, работающие с диапазоном Ku, направлены на определенные территории. То есть самолеты, находящиеся над одной территории, могут перегрузить полосу пропускания спутника. Если Connexion получит широкое признание, то компании наверняка придется арендовать гораздо больше ретрансляторов, либо придется столкнуться с нехваткой полосы пропускания в наиболее загруженных зонах. Конечно, можно вывести на орбиту дополнительные спутники, но это очень дорого.

Безопасность

Connexion не предоставляет никакого уровня защиты типа 802.1X или VPN. Пользователи должны заботиться о собственной безопасности самостоятельно. То есть, как и в случае с другими открытыми сетями, следует использовать защищенные сеансы связи. В частности, все протоколы типа POP, SMTP и IMAP для почты должны передаваться через шифрованное соединение или VPN.

Сервис VPN можно «купить», например, у HotSpotVPN.com, при этом начисляется только абонентская плата, без ограничения трафика. Все участники нашего тестирования сошлись в том, что VPN-соединения работали во время перелетов четко, без неожиданностей.

Что касается безопасности, Connexion не сообщает, как именно она обеспечивается. Судя по всему, здесь используются средства VLAN, которые позволяют разделить трафик пользователей, — достаточно распространенная практика в хот-спотах.

В небе голубом

Единственным конкурентом Boeing можно назвать компанию Tenzing, которая предлагает лишь низкоскоростную передачу данных на скорости от 64 до 128 кбит/с. Для связи используется инфраструктура AirFone на территории США и низкоскоростная сеть спутникового оператора третьего поколения Inmarsat над океаном и в других местах. После объединения в прошлом году Tenzing превратилась в компанию OnAir, которая частично принадлежит конкуренту Boeing — Airbus.

Сервис стоит дорого — за просмотр первых двух килобайт каждого сообщения придется заплатить от $10 до $20. Причем сервис ограничен у многих авиакомпаний только проверкой почты через web-интерфейс, когда подключение устанавливается через внутренний прокси-сервер самолета. Однако Inmarsat уже запустила первый из двух-трех спутников четвертого поколения, которые обеспечат скорость передачи данных 432 кбит/с в обоих направлениях на каждый канал, при этом на самолет могут выделяться 1, 2 или 4 канала одновременно. Поскольку авиационная электроника Inmarsat уже используется на тысячах самолетов, то решение Tenzing требует небольших вложений в оборудование, после чего связь уже можно будет использовать. Как ожидается, новая система начнет работать уже в конце этого года.

Inmarsat использует направленные ретрансляторы, которые позволяют формировать узкие лучи, сфокусированные на небольших территориях. Таким образом, можно направить луч в нужную точку. Однако на каждый спутник можно установить только нескольких сотен транспондеров. Поэтому Inmarsat придется постараться, чтобы обеспечить качественные услуги.

В своем проекте Connexion смогла объединить достаточно высокую скорость канала и простую реализацию, обеспечивая надежность, удивительно малые задержки и высокую стабильность канала.

Система постепенно распространяется на все большее количество рейсов основных авиакомпаний. За последние месяцы Connexion серьезно расширила круг своих клиентов и продолжает набирать темпы.

Если вы являетесь корпоративным пользователем и на вашем ноутбуке уже установлены необходимые службы доступа по коммутируемой сети, через хот-спот отеля или аэропорта, то не мешает обзавестись подпиской Connexion.

Connexion подписала прямые соглашения с несколькими корпорациями, в результате чего работники получают общий корпоративный вход и могут пользоваться Интернетом во время перелетов.

Довольно интересно, как быстро Boeing окупит миллиарды долларов, вложенные в этот проект. Впрочем, Connexion, наконец-то, перешла от разговоров к делу. Приятно, что вскоре небо тоже станет беспроводным!

Глава 17.
Будущее уже сегодня?!

Сейчас ведутся споры и разговоры: «готова ли Россия к Wi-Fi, к ноутбукам, к мобильной жизни вообще?». Конечно, большинство из нас не готовы покупать себе импортные мобильные ПК по ценам подержанных отечественных автомобилей. Беспроводная связь требует небольших вложений, но для ее развития нужны большие усилия. В общем ситуация сравнима с тем что было в 1994 году с сотовой связью. Мобильные телефоны тогда стоили приличных денег, связь была очень дорогой, зон покрытия было очень и очень мало. Но вот что мы имеем сейчас, думаю, рассказывать не надо.

Пока идут споры, новые технологии постепенно внедряются в нашу жизнь. Стандарты будут сменять друг друга и вполне возможно, что проводная связь уступит господство беспроводной. Точки Wi-FI перестанут быть точками и захватят все обитаемое пространство Земли. Выходить в Интернет можно будет с любого населенного пункта, а скорость будет ограничена лишь скоростью приемного устройства (винчестера, флэш-памяти и т.п.). Звучит фантастично, но все идет именно к этому.

Часть 3. Магистральные каналы связи

Глава 1. Плюсы-минусы оптоволокна

Прежде всего определимся с тем, что представляет собой Интернет: Это несколько огромных глобальных и региональных магистральных сетей связи, объединенных друг с другом. Основным физическим носителем таких сетей является оптоволокно, преимущества которого над медными кабелями давно известны: это и отсутствие побочного электромагнитного излучения, и невосприимчивость к электромагнитным помехам, и повышенная дальность передачи данных (от 70 до 300 км) благодаря минимальным потерям из-за рассеивания света и, конечно, повышенная пропускная способность. Наконец, в отличие от электрических цепей, для передачи данных по оптоволокну требуется всего один проводник. Недостатки оптического волокна, вызванные физическими свойствами самого материала, тоже известны: относительная хрупкость (невозможность сгиба оптического кабеля под прямым углом), трудность обнаружения места излома, а также необходимость использования специального оборудования для полировки концов кабеля.

Однако все эти недостатки — ничто по сравнению с потенциальными возможностями оптоволокна. Теоретическая пропускная способность этого носителя — 100 Тбит/с, но современные сети позволяют достичь только скорости в 1 Тбит/с, которая, впрочем, тоже впечатляет. На этой оптимистической ноте обычно и заканчивается описание магистральных сетей в «компьютерной прессе». О чем же умалчивают компьютерщики? О том, что прекрасно известно связистам. Дело в том, что в настоящее время используется только часть теоретически возможной полосы пропускания оптоволокна. В значительной степени это вызвано несовершенством технологии изготовления стеклянных волокон, в которых присутствуют ионы воды, поглощающие свет как синего, так и красного и инфракрасного спектров. Одним из первых производителей, предложивших решение этой проблемы, была компания Lucent Technologies, которая еще в 1998 году объявила о разработке оптоволокна, почти полностью очищенного от ионов воды. По утверждению разработчика, ширина полосы этого всеволнового носителя увеличена на 100 нм по сравнению с обычными одномодовыми световодами. В результате появляется возможность использовать для передачи данных ранее не задействованную область 1400 нм. Уже существуют опытные образцы с пропускной способностью более 10 Тбит/с, но широкое внедрение таких сетей пока не началось.

Так уж и быть, знаний в области физики или химии от певцов «мультимедийного завтра» никто и не требует, но разбираться в технологиях передачи данных они просто обязаны. Какие же технологии используются сегодня в магистральных сетях? В первую очередь это технология спектрального уплотнения WDM (Wavelength Division Multiplexing), позволяющая одновременно передавать по оптоволокну несколько сигналов с различной длиной волны. К примеру, при работе в области 1550 нм стандартом G.692 Международного союза электросвязи предусматривается до сорока каналов с шириной полосы 100 ГГц (около 0,8 нм) и нагрузкой на каждый канал в 2,5 или 10 Гбит/с. Работы по совершенствованию технологии WDM продолжаются: планируется довести ширину канала до 0,4 и даже 0,2 нм, а скорость передачи данных — до 160 Гбит/с.

Прекрасная технология, жить бы да радоваться. Однако специалисты знают, что у спектрального уплотнения есть один принципиальный недостаток: для усиления и коммутации оптический сигнал сперва преобразуется в электрический, а затем обратно в оптический. Этот рудимент прошлого усложняет и удорожает построение магистральных сетей, поэтому будущее — за полностью оптическими (или фотонными) сетями, которые в силу дороговизны и технологического несовершенства пока не получили распространения. Однако перспективные наработки в этой области, безусловно, имеются: уже сегодня при использовании усилителей на основе оптоволокна, легированного эрбием (EDFA), появляется возможность передавать данные по оптическим сетям на расстояние больше тысячи километров. Для маршрутизации сигналов с разной длиной волны в таких сетях применяются микроэлектромеханические системы коммутации (MEMS), состоящие из миниатюрных зеркал. В лабораторных условиях уже испытываются системы маршрутизации, вообще не имеющие механических частей, в частности маршрутизаторы на основе жидких кристаллов, однако пока они могут предоставить всего 16 портов, что вдвое меньше возможностей современных микрозеркальных систем. Поэтому воспевать фотонные сети пока рано.

В свое время огромным достижением считались синхронные оптоволоконные сети связи, которые строились телефонными компаниями для цифровой передачи голосовых данных. В Европе эти сети получи-

ли название SDH (Synchronous Digital Hierarchy — синхронная цифровая иерархия), а в Северной Америке — SONET (Synchronous Digital NETwork — синхронная цифровая сеть связи). Такие сети гарантируют обещанную пропускную способность, а также позволяют гибко изменять скорость передачи данных от 155 Мбит/с до 40 Гбит/с. Со временем в сети SDH проник и Интернет, однако эти сети в силу своей специфики не были оптимизированы для передачи данных и коммутации пакетов, поэтому работа над новыми стандартами, рассчитанными на взаимодействие с кабельными системами Ethernet и IP/MPLS, продолжается до сих пор. Всем известны достоинства технологии передачи данных Ethernet: дешевизна и простота построения сети. Оптимизация SDH под Ethernet (особенно под 10-гигабитный) теоретически означает огромную пропускную способность при минимальных затратах оператора и пользователя на оборудование. Если использовать 10-гигабитный Ethernet вместо применяемых сегодня в глобальных сетях интерфейсов Frame Relay или ATM, то скорость передачи данных в сетях SDH максимально приблизится к 10 Гбит/с. Такие решения представляются оптимальными, к примеру, для организации городских сетей на основе SDH. Но пока все реализованные проекты можно пересчитать по пальцам.

Если в локальных сетях технология Gigabit Ethernet практически вытеснила ATM (Asynchronous Transfer Mode — режим асинхронной передачи), то в магистральных сетях, в том числе и глобальных корпоративных, ATM, несмотря на дороговизну оборудования, остается одной из широко используемых технологий. Главным достоинством ATM является возможность коммутации каналов и пакетов в сочетании с постоянной заказной скоростью передачи данных и низким временем задержки. Тем не менее, производительность ATM серьезно тормозится из-за необходимости преобразования IP-пакетов в 53-байтные (53-октетные) ячейки ATM и обратно. Поэтому современное ATM-оборудование обзавелось поддержкой метода MPLS, созданного, для сопряжения протоколов IP и ATM.

Протокол IP, как и все в этом мире, имеет не только преимущества, среди которых быстродействие, дешевизна и постоянная готовность, но и такие недостатки, как использование сетевого протокола без установления соединения, низкая защищенность и отсутствие поддержки качества услуг (QoS). Открытый метод многоуровневой коммутации по меткам MPLS, разработанный в конце 90-х годов прошлого столетия, позволяет избавиться от многих недостатков IP. Присвоение «меток» потоку данных повышает производительность и упрощает маршрутизацию потоков, которая осуществляется не на основе анализа многоуровневой информации, а по «меткам» определенной длины. Кроме того, благодаря MPLS появляется возможность использования QoS (предусмотренного в ATM), что необходимо для создания виртуальных частных сетей (VPN). Технология MPLS оказалась настолько удачной, что действующие сети на ее основе уже появились и в России. К примеру, компания «ТрансТелеКом» с апреля 2004 года предоставляет услуги VPN на базе своей оптоволоконной магистрали с наложенной сетью IP/MPLS в девятнадцати регионах России, а телефонный оператор «Комстар» с января 2004 года строит собственную мультисервисную сеть на основе MPLS.

Глава 2. «Последняя миля»

Прогресс очевиден, но пожинать его плоды придется еще нескоро. Здесь все упирается в ограниченные возможности «последней мили», которая реализуется, как ни странно, по своего рода «обходным» технологиям. Практически полностью сошла на нет превозносимая еще лет пять назад теми же компьютерщиками технология ISDN (Integrated Service Digital Network — цифровая сеть с интеграцией служб), разработанная для доставки по обычным телефонным абонентским линиям оцифрованных голосовых сигналов и данных. Теоретическая пропускная способность сетей ISDN составляет всего 160 Кбит/с, а реальная — 144 Кбит/с (128 Кбит/с — полезный сигнал, 16 Кбит/с — синхронизация и кадрирование), а оборудование для таких сетей остается весьма дорогим. Поэтому, хотя ISDN еще используется в ряде стран (например, в Северной Америке и Германии) для доступа в Интернет, массовое признание давно получили более скоростные технологии, прежде всего xDSL (Digital Subscriber Line — цифровая абонентская линия).

xDSL также обеспечивает цифровую передачу данных по обычной телефонной линии, но при этом пропускная способность таких сетей существенно выше, чем у ISDN. Существует множество вариантов xDSL, из которых самый распространенный — ADSL (Asymmetric Digital Subscriber Line — асимметричная цифровая абонентская линия). Поскольку, как правило, пользователи получают больше информации, чем отправляют сами, асимметричная линия дает возможность повысить скорость входящего трафика за счет ограничения скорости исходящего. Максимальная скорость входящего трафика в сетях ADSL составляет 6,144 Мбит/с, а исходящего — 640 Кбит/с (из них 64 Кбит/с используется сетевым управляющим каналом). Однако и тут нас ждет подвох, да еще какой: максимальная скорость передачи данных в таких сетях достижима далеко не всегда. Ограничивающим фактором является качество самой телефонной абонентской линии, электрические характеристики которой нестабильны даже в самых развитых странах. Поэтому в ADSL-

модемах применяется адаптивная технология, гарантирующая лишь максимальную скорость доступа, возможную на используемой линии. В России, например, можно встретить ADSL-подключение со скоростью входящего трафика 32 Кбит/с, что нормально, пожалуй, только для аналогового модема. Тем не менее, ADSL довольно быстро распространяется по стране как технология доступа в Интернет с оптимальным соотношением цена/качество. Коммерческое предоставление услуг на основе ADSL началось еще в 2000 году компаниями «Вэб Плас» в Санкт-Петербурге, а также МГТС и «МТУ-Интел» («Точка.ру») — в Москве. Однако массовыми эти услуги так и не стали. По-видимому, операторы намеренно завышают цены и предлагают клиентам только дорогостоящие абонентские устройства от крупнейших брэндов, поскольку пока не в силах обслуживать десятки и сотни тысяч подписчиков.

Еще один вариант асимметричной xDSL — VDSL (Very-high bit rate Digital Subscriber Line — сверхвысокоскоростная цифровая абонентская линия) — обеспечивает при использовании одной витой пары скорость входящего потока от 12,9 до 52,8 Мбит/с, а исходящего — от 1,5 до 2,3 Мбит/с. Главный недостаток VDSL — малая дальность связи, не превышающая 1,5 км, поэтому для достижения заявленных скоростей требуются концентраторы абонентской линии (ONU — оптических сетевых блоков), которые по оптоволокну соединяют группы абонентов с телефонной станцией. В принципе VDSL можно считать экономически оправданной альтернативой более дорогостоящей оптоволоконной выделенной линии, но массовому пользователю она до сих пор недоступна.

Чтобы добавить толику позитива в наше пессимистичное повествование, упомяну о том, что в начале 2003 года были приняты стандарты ADSL второго поколения — ADSL2. Среди их самых больших достижений — возможность программного изменения объема служебной информации в передаваемых пакетах в диапазоне от 2 до 32 Кбит/с, что особенно актуально на линиях большой протяженности, где полоса пропускания сужается до 128 Кбит/с. Максимальная пропускная способность канала выросла до 12 Мбит/с для входящего трафика, а благодаря возможности передавать ADSL-данные в «голосовой» полосе максимальная скорость исходящего трафика повысилась почти до 900 Кбит/с. Первое оборудование для ADSL2 должно вот-вот появиться на рынке, а на очереди уже внедрение технологии ADSL2+, стандартом на которую предусмотрена скорость входящего трафика до 25 Мбит/с при дальности связи 1,5 км. Такая высокая скорость достигается благодаря повышению верхней границы рабочей частотной области с 1,1 до 2,2 МГц, однако с ростом протяженности линии скорость связи, разумеется, падает до более привычных значений.

Конечно, асимметричное подключение подходит далеко не всем: к примеру, для компании, открывшей своим клиентам доступ к каталогу, размещенному на внутреннем сервере, требуется большая скорость именно исходящего трафика. В этом случае можно использовать более дорогостоящую симметричную технологию SDSL (Symmetric Digital Subscriber Line — симметричная цифровая абонентская линия), которая обеспечивает максимальную скорость доступа до 2,048 Мбит/с (в зависимости от расстояния до узла связи и качества линии) и дальность соединения до 6 км. Более прогрессивная модификация симметричной линии — HDSL (High-Rate Digital Subscriber Line — высокоскоростная цифровая абонентская линия), позволяющая добиться скорости 1,544 Мбит/с в обоих направлениях. При этом для HDSL, в отличие от ADSL, необходимы уже две витые пары, но дальность связи ограничена 1,5 км, а требования к качеству кабельной системы существенно выше. Зато отказоустойчивость HDSL повышается за счет использования двух витых пар: при неполадках в одной из них связь не прерывается, просто скорость доступа падает вдвое.

К сожалению, несмотря на существование отраслевого стандарта HDSL, несовместимость HDSL-оборудования различных производителей стала притчей во языцех. Кроме того, неудачная схема распределения частотного диапазона не позволяла одновременно передавать по двум (!) витым парам данные и голосовой сигнал. Решить эти проблемы был призван стандарт G.921.2 (G.SHDSL), принятый Международным союзом электросвязи в феврале 2001 года. При сохранении всех достоинств HDSL полоса пропускания канала SHDSL при работе с одной витой парой была расширена до 2,3 Мбит/с. Кроме того, была обеспечена максимальная совместимость с широко распространенной технологией ASDL. Возможность симметричного подключения по одной витой паре — одно из главных достоинств SHDSL, при этом коммутаторы и модемы стали доступны по цене маленьким компаниям и даже некоторым индивидуальным пользователям.

Общего недостатка всех систем на основе телефонных линий — повышенной чувствительности к электромагнитным помехам — лишены решения на базе сетей кабельного телевидения (CATV — Community Antenna TeleVision — абонентского телевещания). Кабельное ТВ широко распространено в странах Северной Америки, где эти сети с успехом используются для широкополосного доступа в Интернет. Крупные российские города также имеют системы кабельного телевидения, поэтому несколько слов об особенностях этого типа подключения. Максимальная скорость получения данных по кабельному модему — 36 Мбит/с, однако чисто технически невозможно выделить каждому подключенному абоненту индивидуальную частоту несущей, поэтому здесь применяется

технология мультиплексирования с временным уплотнением, из-за которой реальная скорость значительно меньше теоретической, причем она меняется в зависимости от числа подключенных абонентов. Более того, поскольку сеть кабельного телевидения рассчитана на одностороннюю передачу данных от провайдера к абоненту, то для передачи исходящего трафика необходимо иметь, например, низкоскоростное коммутируемое подключение. Технология HFC (Hybrid Fiber Coax — гибридная оптоволоконно-коаксиальная система) обеспечивает двухстороннюю связь по каналам кабельного ТВ, однако для ее реализации требуется практически полная замена действующих кабельных систем и усилителей. Впрочем, несмотря ни на что, крупные негосударственные операторы связи, например «МТУ-Информ», проявляют интерес к предоставлению широкополосного доступа в Интернет по сетям кабельного телевидения, а «Комкор-ТВ» уже обеспечивает таким сервисом несколько московских микрорайонов.

Домовые сети — куда более дешевая и поэтому распространенная альтернатива скоростным кабельным сетям. Если еще года два назад домовые сети в России представляли собой полулегальные предприятия, основанные на подключении к одному выделенному каналу десятков и даже сотен абонентов, то сегодня государство пытается взять такие сети под свой контроль. Лучше всего это получается в Москве, где построена соответствующая инфраструктура: Московская волоконно-оптическая сеть (МВОС) имеет более десяти тысяч кабельных линий, а порядком устаревшие кабельные телевизионные сети «Мостелекома» проложены почти во всех домах города. Кроме того, домовые сети контролируются и крупными негосударственными компаниями (к примеру, «МТУ-Интел» и «РМ-телеком»), располагающими собственными магистральными линиями связи или предоставляющими услуги радиодоступа.

Как правило, домовые сети представляют собой обычную 10- или 100-мегабитную локальную сеть Ethernet, тем или иным способом подключенную к провайдеру. Соответственно скорость передачи данных зависит как от канала, так и от количества «сидящих» на нем клиентов. Крупные провайдеры, имеющие собственные магистральные линии, создают в каждом доме микрорайона узлы доступа на основе маршрутизаторов, которые подключаются к сети оптоволоконными каналами с пропускной способностью от 256 Кбит/с до 2 Мбит/с. Безусловно, эти скорости не позволяют многочисленным подписчикам одновременно пользоваться современными мультимедийными сетевыми сервисами, однако такие сети имеют право на жизнь в качестве недорогой альтернативы модемному коммутируемому соединению. Но, увы, широкополосным доступом такое решение не назовешь.

Спутниковые системы доступа в Интернет — чрезвычайно перспективная технология, однако, опять же, ее распространение ограничивается рядом факторов. Во-первых, полноценный симметричный спутниковый доступ пока чрезвычайно дорог даже для крупных организаций. Во-вторых, асимметричный доступ, при котором исходящий трафик передается через низкоскоростное, в том числе и коммутируемое соединение, не всегда экономически оправдан, особенно на фоне снижения цен на технологии ADSL и SHDSL. Операторы спутникового доступа предлагают различные типы подключения, которые предусматривают скорость входящего трафика от 64 Кбит/с (для индивидуальных клиентов) до 55 Мбит/с (для корпоративных клиентов). Как правило, спутниковый доступ имеет смысл использовать там, где принципиально невозможно кабельное подключение либо где необходим канал с очень высокой пропускной способностью.

Глава 3. «Последний дюйм»

Технологии организации «последнего дюйма» принципиально не слишком отличаются от рассмотренных выше решений: в основном это все те же «обходные» пути. К сожалению, для подавляющего большинства домашних пользователей «последний дюйм» пока выглядит как медная пара — обычный телефонный провод, используемый для коммутируемого подключения. При таком подключении даже по Москве средняя скорость входящего трафика не превышает 33 Кбит/с. В новостройках уже на этапе проектирования предусматриваются кабельные системы, подключаемые, как правило, к оптоволоконным каналам провайдера. В зданиях, не оснащенных кабельной разводкой, используются Ethernet-вариации на тему xDSL (в виде HomePNA) с доступом по телефонной проводке или по радиотрансляционной сети, технологии доступа через кабельное телевидение, по электросети, либо беспроводный радиодоступ на основе технологий Wi-Fi.

Стандартом HomePNA 2.0 (Home Phoneline Networking Alliance — Союз производителей оборудования для передачи данных по телефонным сетям) установлена скорость передачи данных до 10 Мбит/с при использовании частоты около 10 МГц. Этого уже хватает для передачи видео среднего качества, но совершенно недостаточно для видеоконференций в реальном времени. В стандарте HomePNA 3.0 планируется увеличить скорость доступа до 100 Мбит/с, что сопоставимо с обычными локальными сетями 100 Ethernet. При этом никакой дополнительной разводки не требуется, нужно лишь установить специальные сетевые

карты и коммутатор. Аналогичную технологию на основе HomePNA 2.0 продвигает на рынке Московская городская радиотрансляционная сеть (через Центральный телеграф), однако здесь используется проводная радиосеть, которая, в отличие от телефонной проводки, имеется в каждой квартире.

Интересное решение — передача информации через электропроводку. Технология PLC (PowerLine Communications — связь через электропроводку) предусматривает установку на местной подстанции специального оборудования, соединенного с сетями IP. Полезный сигнал абонент может выделить при помощи адаптера, подключаемого в обычную розетку, при этом пропускная способность сети достигает 14 Мбит/с. К сожалению, пока отсутствует стандарт подключения по PLC многоквартирных зданий: существующий американский стандарт HomePlug 1.0 не допускает подключения к одному трансформатору более 16 узлов-розеток. Кроме того, для передачи данных требуется сложный алгоритм модуляции, поскольку характеристики линии (затухание, искажения, уровень шума) сильно зависят от энергопотребления. Тем не менее, если для европейских стран PLC — скорее экзотика, в США на основе этой технологии строятся целые системы «умных домов», в которых по электросети передаются команды самой разной бытовой технике.

Одно из наиболее оптимальных и красивых решений проблемы «последнего дюйма» — использование беспроводного радиодоступа, для которого не нужны ни кабель, ни сложные алгоритмы модуляции сигнала. Базовый стандарт беспроводных локальных сетей (Wi-Fi) IEEE 802.11 был разработан еще в 1997 году, а самый распространенный в настоящее время IEEE 802.11b — в 1999 году. Оборудование стандарта 802.11b работает на частоте 2,4 ГГц и обеспечивает передачу данных со скоростью до 11 Мбит/с (в среднем — около 6 Мбит/с) на расстоянии до 300 метров. Более совершенный стандарт IEEE 802.11a предусматривает работу в частотном диапазоне 5 ГГц, а скорость передачи данных на расстоянии до 100 метров может достигать 54 Мбит/с. К сожалению, эти стандарты несовместимы друг с другом, а новый стандарт IEEE 802.11g (частотный диапазон 2,4 ГГц, максимальная пропускная способность — 54 Мбит/с) обратно совместим только с IEEE 802.11b. Интересно, что один из крупнейших производителей телекоммуникационного оборудования, компания Conexant, комплектует свои чипсеты для кабельных и xDSL-модемов контроллерами Wi-Fi фирмы Intersil, что вообще позволяет снять вопрос о базовой станции: достаточно иметь карточку доступа Wi-Fi в компьютере — и вы в Интернете. Кстати, технология Intel Centrino для ноутбуков нового поколения в обязательном порядке предусматривает установку в компьютер чипа Wi-Fi.

Глава 4.
Воздушные Замки

Наблюдать со стороны за тем, как развиваются события, занятие не всегда полезное, но неизменно увлекательное. В зависимости от предполагаемой значимости действа меняется и число участников, и, тем более, болельщиков, и просто зевак, а уж когда дело доходит до евангелистов и проповедников, становится ясно, что происходит нечто незаурядное.

Появление первых продуктов нового беспроводного стандарта передачи данных, 802.11a, стало, пожалуй, одним из наиболее заметных (и незаурядных) событий прошлого года.

Table 111—North American operating channels

Set	Number of channels	HR/DSSS channel numbers
1	3	1, 6, 11
2	6	1, 3, 5, 7, 9, 11

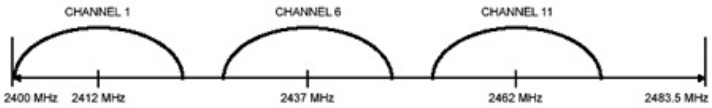


Figure 141—North American channel selection—non-overlapping

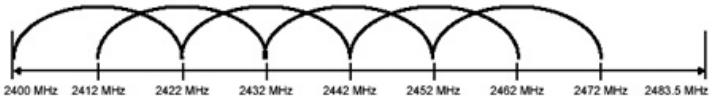


Figure 142—North American channel selection—overlapping

Впрочем, «новый» — понятие относительное, и слово это, если быть точным, относится здесь скорее не к стандарту, а к продуктам, его реализующим. Ведь спецификация .11a была принята в далеком уже 1999 году, и принятие ее прошло тогда практически незамеченным. Она хоть и обещала, в сравнении с 802.11b (далее термин Wi-Fi, обозначающий устройства стандарта 802.11b, сертифицированные консорциумом WECA),

впятеро большую скорость данных — до 54 Мбит/с (против максимальных для .11b 11 Мбит/с), но ценой несопоставимых вычислительных затрат и использования нового, пятигигагерцового частотного диапазона.

В силу перечисленных факторов, 802.11a (по аналогии с Wi-Fi, устройства этого стандарта, сертифицированные WECA, получили обозначение Wi-Fi5) засиделся на старте: основные силы были брошены на освоение и продвижение более привычного 802.11b, который стремительно, по сравнению с HomeRF и Bluetooth, набирал очки весь прошлый год.

HomeRF, скорее всего, через некоторое время просто сойдет со сцены — в силу отказа фирмы Intel от поддержки этого стандарта и его несовместимости с Wi-Fi (HomeRF и Bluetooth используют модуляцию со скачками по частоте [FHSS], а Wi-Fi — с размазыванием по спектру путем умножения на кодовую последовательность [DSSS]). А вот после того, как рабочая группа 802.15 по персональным сетям (Personal Area Network, PAN) комитета IEEE, приняла спецификацию, оговаривающую порядок совместной работы в эфире технологий Bluetooth и Wi-Fi (и освобождение перекрывающихся диапазонов частот), можно было бы предположить, что оба стандарта будут сосуществовать долго и счастливо. Добавим сюда и общее падение цен, которое делает затраты на инсталляцию Wi-Fi-сетей сравнимыми с расходами на СКС.

В общем, дела для Wi-Fi складывались бы как нельзя лучше, если б не появление еще более высокоскоростного беспроводного стандарта. Пятикратный перевес в скорости передачи данных при цене, сопоставимой с оборудованием предыдущего стандарта, — факт сам по себе достаточно примечательный, чтобы привлечь внимание к новой технологии.

Но ее проповедники на этом не останавливаются и пускают в ход заведомо ложные или, выражаясь мягче, не совсем честные аргументы. Например, сравнивая с Wi-Fi, утверждают, что последняя допускает использование лишь трех неперекрывающихся частотных диапазонов — в отличие от Wi-Fi5, у которой таких диапазонов двенадцать, и тут же делают выводы, что у Wi-Fi могут возникнуть трудности с частотным планированием, тогда как у Wi-Fi5, наоборот, все просто замечательно.

Так вот, неперекрывающихся диапазонов у Wi-Fi действительно всего лишь три, зато перекрывающихся — аж тринадцать. Перекрытие рабочих диапазонов становится возможным вследствие широкополосных принципов передачи данных в 802.11 и корреляционных методов приема. В зависимости от национальных особенностей регулирования частотного спектра число диапазонов, правда, меняется: так, например, в США их 11, а в России — столько, сколько сочтет нужным выделить местный Госсвязьнадзор.

А у Wi-Fi5, наоборот, три поддиапазона, с максимальными мощностями излучения 10, 50 и 200 мВт и четырьмя рабочими частотами в каждом из них (итого, действительно, двенадцать).

В зависимости от мощности передатчика, очевидно, будет меняться и радиус соты. Соответственно, частотное планирование может превратиться в запутанную и неочевидную задачу, при решении которой не обойтись без специализированного ПО. А может быть, и наоборот, позволит размещать соты с большей мощностью в местах с наименьшей плотностью абонентов. Притом оставив, при регулярном покрытии, лишь четыре доступных частотных диапазона.

Далее: признавая меньшую дальность нового стандарта, его апологеты тут же пускаются во все тяжкие: да, на открытом пространстве дальность передачи будет меньше почти в два раза, но зато в реальных условиях, в помещениях, по расчетам наших теоретиков, разницы не будет — ну или почти не будет.

Меньшая дальность стандарта обусловлена тем, что используемый метод модуляции OFDM (Orthogonal Frequency Division Multiplex — модуляция с ортогональным разделением каналов по частоте) делит рабочую полосу частот (20 МГц) на 52 канала передачи данных и, в свою очередь, использует в каждом из них модуляцию QAM, как известно, далеко не самую эффективную по соотношению сигнал/шум, и вдобавок проигрывает в мощности излучения. Свою лепту вносят и особенности распространения радиоволн 5-гигагерцового диапазона. К слову, в отличие от DMT (Discrete Multi Tone), очень похожего метода модуляции, нашедшего применение в стандарте ADSL и использующего в каждом из частотных канальцев оптимальный для фактического соотношения сиг-

нал/шум метод модуляции и, таким образом, обеспечивающего максимально достижимую скорость передачи данных в заданной полосе частот, OFDM стрижет всех под одну гребенку: метод модуляции один на все каналы, и при наличии узкополосных помех приходится либо жертвовать отдельными каналами, либо — во всех, разом, менять метод модуляции и, соответственно, уменьшать общую скорость передачи данных.

Как бы то ни было, стандарт 802.11a очень благожелательно был встречен рынком, о производстве чипсетов или о планах по их производству уже заявили, по крайней мере, восемь компаний (в то время как чипсеты для Wi-Fi производят лишь три компании — Intersil, Agere и Texas Instruments; хотя не исключено, что список уже не полон), а первые карточки этого стандарта, Harmony 802.11a компании Proxim, были даже отмечены наградой «Best of Show» в номинации беспроводного оборудования на недавней выставке «Comdex».

Уже в декабре «Гармонии» добрались до Москвы: пара таких карточек, вместе образующих набор FastWireless Networking Kit.

Несколько слов о карточках. «Гармонии» основаны на чипсете AR5000 компании Atheros Communications и в турборежиме могут использовать сразу два частотных диапазона, обеспечивая двухкратную, в сравнении со стандартом, скорость передачи данных — то есть, в пределе, до 108 Мбит/с. Карточки, входящие в комплект, позволяют строить только одноранговые, ad-hoc-сети.

Идущий в комплекте с карточками софт содержал драйверы для любых операционных систем, за исключением Windows XP. Попытка установить ПО через программу инсталляции (setup.exe) под Windows XP закончилась неудачей. Но тем не менее, драйверы были успешно «скушаны» этой операционной системой через процедуру установки нового оборудования, правда, с некоторыми странностями. Так, я некоторое время с удовольствием наблюдал забавную картину: по неработающему беспроводному интерфейсу (Wireless connection unavailable) со скоростью 1,9 Мбайт/с бегали данные. Причем эта скорость обеспечивалась, даже несмотря на высокие потери в канале (доходящие до 10-25 %) и работу «планировщика качества обслуживания» (QoS Sheduler). И еще одна загадка: после отключения планировщика потерь пакетов стало значительно меньше.

В дальнейшем, во избежание таких вот непонятностей, эксперименты на ноутбуке проводились под Windows 98, для определения скорости передачи данных использовался протокол FTP и установленный на десктопе FTP-сервер.

Максимальная достигнутая скорость — 2,3 Мбайт/с — на расстояниях до шести метров (или почти 20 Мбит/с — вчетверо больше, чем у Wi-Fi). Правда, в режиме Turbo скорость увеличилась, к сожалению, не в два раза, — до 3,3 Мбайт/с, или 26,4 Мбит/с! Однако увеличение скорости передачи данных почему-то привело к потере чувствительности. Либо не справляется математика и переходит на более простые алгоритмы модуляции, либо одно из двух...

А теперь о странностях, позволяющих предположить некоторую «сырость» софта, входящего в комплект поставки. Скорость передачи данных, отображаемая на встроенном индикаторе, менялась в очень широких пределах — до 50 процентов от среднего значения, причем от отсчета к отсчету, перманентно. Создавалось ощущение, что драйвер никак не может определиться с выбором оптимальной скорости, хотя видимых источников излучения этого диапазона в квартире обнаружено не было, да и не могло их быть. Разве что шальной радар с расположенного неподалеку «Внукова» или ЗРК СС-300...

Еще один минус: после потери связи, вызванной разнесением адаптеров на относительно большое расстояние, скорость передачи данных не вернулась к прежним значениям, а встроенный индикатор застыл на отметке 24/12 Мбит/с. Вывести карточки из клинча не удалось даже совмещением антенн обоих адаптеров!

И наконец, капитальная стена толщиной около 40 см (по опыту, весьма и весьма твердая) оказалась для 802.11a и вовсе непреодолимым препятствием...

Поэтому в небольшой городской квартире, изобилующей стенками и капиталками, связь возможна в пределах максимум десяти-пятнадцати метров, при этом существуют зоны, где связь отсутствует вовсе.

Впрочем, сложившаяся ситуация могла объясняться и сыростью драйверов, и неудачным расположением одной из карточек — десктоп по квартире особенно не подвигаешь, с точкой доступа свободы было бы значительно больше.

А вот оборудование стандарта Wi-Fi, выпестованное Agere, на удивление, показывало чудеса стабильности: при фиксированном положении приемника и передатчика скорость передачи данных менялась лишь в третьем знаке, в пределах нескольких процентов. Максимальная дальность передачи, в отсутствие прямой видимости и капитальных стен, достигала 30 метров. Капитальная стена, ставшая для «Гармоний» непреодолимым препятствием, осталась почти незамеченной — скорость передачи данных по FTP упала с максимальных для комплекта 595 Кбайт/с до 590 Кбайт/с! Видимо, радиоволны нашли более короткую дорогу.

Диапазон частот, ГГц	Макс. вых. мощность, мВт*
5,15 - 5,25	10
5,25 - 5,35	50
5,725 - 5,825	200

Гораздо нагляднее и интерфейс прикладных программ, предоставляющий информацию и о соотношении сигнал/шум на обоих концах линии, и о запасе по мощности, и о скорости передачи данных.

Часть 4. Путеводитель по стандартам на беспроводные ЛВС

Глава 1. Тенденции рынка

Сегодня беспроводные ЛВС можно встретить в офисах компаний, в университетах, жилых домах и в общественных местах, включая аэропорты, гостиницы и рестораны. Некоторые некоммерческие организации даже пытаются охватить ими целые городские районы и на их основе предоставить пользователям бесплатный доступ в Интернет. Все ведущие производители блокнотных ПК предлагают беспроводные интерфейсы для своих продуктов. Столь высокий уровень популярности этих сетей объясняется тем, что они стали стабильными в работе, хорошо известными (сетевым специалистам и пользователям) и недорогими. Использование оборудования для беспроводных ЛВС — это неплохой вариант построения компьютерной сети.

Специалисты в области сотовой связи уже давно «дразнят» нас ее потенциальными возможностями по обеспечению высокоскоростного доступа к данным в любое время и в любом месте (где бы ни находился пользователь), но, видя все более широкое распространение беспроводных ЛВС, можно предположить, что быстрее такой доступ будет реализован на основе последних. Вас беспокоит, что пропускной способности этих сетей не хватит для нормальной работы ваших приложений? Если скорости передачи 11 Мбит/с не достаточно для этого, то скоро на рынке появятся беспроводные средства с пропускной способностью до 54 Мбит/с, по цене ненамного дороже выпускаемого сейчас оборудования для беспроводных ЛВС.

При всей своей привлекательности внедрение беспроводных ЛВС ставит перед менеджерами по ИТ сложные проблемы. Одна из них заключается в том, как развернуть сеть сегодня, чтобы можно было легко

модернизировать ее завтра. Другая проблема связана с обеспечением высокого уровня защиты данных. Межсетевой экран стоимостью несколько тысяч долларов может оказаться полностью скомпрометирован при наличии одной неправильно сконфигурированной точки доступа (даже если она находится за кирпичной стеной здания). Кроме того, как это ни странно, но беспроводные ЛВС могут стать жертвой своего же собственного успеха: средства, основанные на разных беспроводных технологиях, включая Bluetooth, способны создавать сильные взаимные помехи. Имеются также проблемы с IP-адресацией, которые делают невозможным роуминг между установленными в разных подсетях точками доступа без использования специального связующего ПО.

К счастью, большинство названных проблем имеют решения. Кроме того, многие недостатки сегодняшних сетей будут преодолены в новых стандартах. Беспроводные ЛВС хорошо работают уже сейчас, но со временем станут работать еще лучше. Однако, чтобы успешно использовать эти сети, нужно знать присущие им ограничения и перспективы их развития.

Нет никакого сомнения в том, что сегодня рынок беспроводных ЛВС испытывает самый настоящий бум. По данным компании IDC, в прошлом году мировой объем продаж оборудования для беспроводных ЛВС вырос на 80% и составил около 1 млрд долл., предполагается, что к концу 2005 г. он достигнет 3,2 млрд долл. Традиционно самым большим спросом эти сети пользуются на вертикальных рынках — в лечебных учреждениях, на больших складах и т. д., поскольку медицинские, складские и другие специализированные приложения позволяют быстро окупить значительные затраты на приобретение радиооборудования и развертывание сети. Однако с прошлого года беспроводные ЛВС стали довольно популярными и на горизонтальных рынках — их используют теперь компании самого разного профиля, службы эксплуатации жилых зданий и образовательные учреждения.

Самые большие средства затрачивают на строительство беспроводной инфраструктуры те компании, которые работают в сфере высоких технологий и/или имеют большое число сотрудников, оснащенных блокнотными ПК. Например, корпорация Microsoft развернула у себя около 2 тыс. точек доступа, обслуживающих примерно 10 тыс. пользователей. Многие компании устанавливают точки доступа в комнатах для переговоров, в конференц-залах, кафетериях и учебных классах. Для небольшой фирмы беспроводная ЛВС привлекательна тем, что ее можно развернуть в арендуемом недорого помещении, где отсутствует структурированная кабельная система, а затем, когда фирма станет крупнее, можно будет легко переместить эту сеть в новый офис. Пользователи домашних ПК все чаще прибегают к беспроводным ЛВС для совместного

использования (с членами своей семьи, а иногда и с соседями) периферийного оборудования и широкополосных каналов доступа в Интернет.

Благодаря усилиям компаний MobileStar Network и Wayport, лидирующих на рынке услуг сетей доступа, основанных на технологии беспроводных ЛВС, число последних растет в аэропортах, отелях, конгресс-центрах и крупных магазинах. Людей весьма привлекает возможность использовать (для удаленного доступа к данным) свой блокнотный или карманный ПК с беспроводным интерфейсом и на работе, и дома, и в поездке.

Хотя большинство крупных беспроводных ЛВС начали работать совсем недавно, многие рыночные аналитики уже утверждают, что они гораздо лучше подходят для организации широкополосных соединений общего пользования, например в аэропортах, чем сети третьего поколения (3G), которые получат широкое распространение только через несколько лет. Благодаря более низкой стоимости оборудования и его работе в нелицензируемом (в США и ряде других стран) частотном диапазоне передача данных по беспроводным ЛВС может быть в десять и более раз дешевле, чем по сотовым сетям. Сегодня перед операторами сотовой связи стоит дилемма: использовать технологии беспроводных ЛВС наряду с технологией сотовой связи или попытаться конкурировать с первыми.

Некоторые европейские операторы сотовой связи, в том числе финская фирма Sonera и шведская компания Telia, уже предоставляют своим абонентам дополнительные услуги на базе средств беспроводных ЛВС, но операторы Северной Америки пока еще не готовы идти по этому пути. Вы можете спросить, почему операторы тратят десятки миллиардов долларов на развертывание сотовых сетей 3G, если сегодняшние технологии сотовой связи в сочетании с технологиями беспроводных ЛВС способны предоставить пользователям примерно тот же сервис, но при гораздо меньших капиталовложениях? Дело в том, что в настоящее время поддержка технологий беспроводных ЛВС не входит в генеральные планы развития сетей большинства операторов, и, чтобы включить ее в эти планы, им придется не только проделать огромную техническую работу, но и пересмотреть свое отношение к рынку беспроводных услуг вообще.

Оборудование для беспроводных ЛВС становится все более привлекательным по ценам. Сегодня сетевой радиоадаптер PC Card стоит дешевле 100 долл., а всего несколько лет назад подобная плата стоила около 500 долл. (при этом ее пропускная способность была меньше). Совсем недавно точки доступа покупали примерно за 1500 долл.; сейчас беспроводные шлюзы с функциями маршрутизатора и межсетевого эк-

рана, предназначенные для небольших и домашних офисов, продаются по цене около 200 долл. Впрочем, точка доступа с поддержкой роуминга, расширенными функциями защиты данных, большой дальностью действия и мощными средствами управления стоит дороже.

Еще одна положительная характеристика сегодняшних устройств для беспроводных ЛВС — взаимная функциональная совместимость оборудования разных производителей. Благодаря сертификации продуктов на соответствие требованиям спецификации Wi-Fi (Wireless Fidelity), проводимой ассоциацией производителей WECA (Wireless Ethernet Compatibility Alliance), большинство представленных на рынке беспроводных адаптеров и точек доступа совместимы между собой, но проблема взаимодействия точек доступа разных производителей в рамках одной сети еще не решена.

Сильным стимулом развития рынка беспроводных ЛВС, о котором специалисты почему-то упоминают довольно редко, является совместимость этих сетей с предназначенными для традиционных ЛВС сетевыми ОС и приложениями (например, Lotus Notes и Microsoft Exchange). Когда возникает необходимость в организации доступа к приложениям через мобильные телефоны, то по причинам низкой скорости передачи данных по радиоканалам сотовых сетей, значительной задержки сигнала в этих сетях и высокой стоимости пользования ими необходимо либо тщательно конфигурировать приложения, либо применять беспроводное связующее ПО, либо обращаться к услугам поставщика беспроводных приложений (ASP). Скорее всего, вам придется модифицировать свое приложение, приспосабливая его к работе через сотовую инфраструктуру. Что же касается беспроводных ЛВС, то благодаря их высокой пропускной способности и низкой стоимости пользования ими предприятия могут задействовать почти все свои существующие сетевые приложения без каких-либо изменений.

Однако необходимо сделать ряд предупреждений. Если вы хотите осуществлять доступ к частной интрасети по беспроводной ЛВС общего пользования, то с целью защиты передаваемого трафика от перехвата следует задействовать ПО для работы в виртуальной частной сети (VPN). Если же вы хотите сохранять свой IP-адрес при переходе от одной подсети к другой или же поддерживать установленные сеансы связи при кратковременном выходе из зоны действия сети, используйте беспроводное связующее ПО, подобное поставляемому компанией NetMotion Wireless. Вообще говоря, все эти трудности незначительны по сравнению с преимуществами широкополосного мобильного доступа.

Новым приложением, которое может стать значительной движущей силой развития рынка беспроводных ЛВС, является распространение видеопрограмм в жилых домах. Сегодня для приема цифрового ТВ-сигнала каждый телевизор необходимо оборудовать специальной приставкой, что довольно дорого. Дешевле задействовать одну приставку, принимающую цифровой ТВ-сигнал из кабельной сети или со спутника, и беспроводную ЛВС, транслирующую видеоинформацию всем телевизорам в доме. Это станет возможным после введения новых стандартов на беспроводные ЛВС, определяющих необходимые (для такой трансляции) скорости передачи данных и механизмы обеспечения качества обслуживания.

В настоящее время на рынке большим успехом пользуются 11-Мбит/с беспроводные ЛВС стандарта IEEE 802.11b. Они обеспечивают достаточно высокие для нормальной работы большинства приложений скорости передачи данных, несмотря на то, что их реальная пропускная способность составляет всего около 6 Мбит/с и с ростом числа абонентов снижается гораздо быстрее, чем производительность проводной сети.

Ethernet (из-за менее эффективного протокола доступа клиентских станций к среде передачи данных). Поскольку сети стандарта IEEE 802.11b (изначально предназначенные для предприятий) применяются теперь и в домах, судьба ориентированной на домашние сети спецификации HomeRF стала весьма неопределенной (особенно если учесть, что корпорация Intel, в прошлом один из крупнейших сторонников этой спецификации, сегодня поддерживает стандарт IEEE 802.11b).

Специалисты должны тщательно отслеживать процесс создания новых стандартов. Стандарт IEEE 802.11b сыграл роль катализатора развития индустрии беспроводных ЛВС. Но широкое применение последних выявило серьезные недостатки в их системе информационной безопасности, которые сегодня устраняются только с помощью фирменных решений. Следите за появлением стандартных решений в этой области и старайтесь спроектировать свою сеть таким образом, чтобы со временем можно было легко перейти на новые и улучшенные технологии.

Производители и органы стандартизации совершенствуют беспроводные ЛВС по трем основным направлениям: увеличение скорости передачи данных, повышение степени информационной безопасности и реализация эффективно работающих механизмов обеспечения QoS. В идеале хотелось бы видеть один новый стандарт, охватывающий все эти улучшения. Причем желательно было бы иметь возможность обновлять ПО сетевого оборудования для поддержания нового стандарта. Но наш мир далеко не идеален, поэтому прогресс в деле развития беспроводных ЛВС по основным направлениям осуществляется с разной скоростью, приводя к появлению отдельных стандартов.

Что касается увеличения скорости передачи данных, то здесь имеются значительные успехи. Стандартом IEEE 802.11a (который начали разрабатывать раньше, чем уже ставший популярным стандарт IEEE 802.11b) определен новый физический уровень, обеспечивающий скорость передачи данных до 54 Мбит/с. Хотя реальная пропускная способность сетей этого стандарта вряд ли будет превышать 25—30 Мбит/с, но такая скорость в пять раз больше реальной скорости передачи данных в нынешних беспроводных ЛВС стандарта IEEE 802.11b. Таким образом, будущий процесс внедрения на предприятиях оборудования стандарта IEEE 802.11a можно сравнить с процессом перехода от технологии Ethernet к технологии Fast Ethernet в проводных ЛВС.

Стандартом IEEE 802.11a предусмотрено использование передовой радиотехнологии, получившей название «ортогональное частотное мультиплексирование» (Orthogonal Frequency Division Multiplexing — OFDM). Согласно этой технологии вместо последовательной передачи информации по одному высокоскоростному каналу осуществляется параллельная передача потоков данных по многочисленным отдельным поднесущим. В результате получается один широкополосный и помехоустойчивый канал с высокой пропускной способностью. Многие новейшие радиосистемы, включая широкомасштабные сети фиксированной и мобильной связи, основаны на этой технологии.

Кроме того, в зависимости от качества и уровня принимаемого радиосигнала, OFDM-устройства могут динамически задействовать разные методы модуляции, обеспечивая тем самым либо высокую скорость передачи данных на небольшие расстояния, либо низкоскоростную, но надежную связь на большие дистанции. Стоит также отметить, что оборудование стандарта IEEE 802.11b работает в перегруженном диапазоне частот 2,4 ГГц, а стандартом IEEE 802.11a предусмотрено использование более свободного диапазона 5 ГГц, в котором в США для нелицензируемой работы оборудования выделена более широкая полоса частот, примерно в три раза шире, чем та, которую используют в диапазоне 2,4 ГГц (300 МГц по сравнению с 83 МГц). Однако со временем и частотный диапазон 5 ГГц может стать сильно загруженным и несвободным от взаимных помех, создаваемых оборудованием.

Переход на эту технологию связан с решением ряда сложных проблем. Прежде всего остается неизвестной дальность связи (между радиоадаптером и точкой доступа) в помещении, на которую можно рассчитывать при развертывании беспроводных ЛВС стандарта IEEE 802.11a. Согласно законам физики, дальность связи в открытом пространстве уменьшается с ростом рабочей частоты, но в помещении помимо этого на нее влияют поглощение и отражение радиоволн. Кроме того, дальность связи зависит от мощности излучаемого радиосигнала и вида его

модуляции. Поэтому очень трудно заранее определить этот параметр для любой радиотехнологии.

По данным компании Mobilian, производящей компоненты оборудования стандартов IEEE 802.11a и IEEE 802.11b, для радиопокрытия одной и той же территории потребуется примерно в четыре раза больше точек доступа стандарта IEEE 802.11a, чем точек доступа стандарта IEEE 802.11b. Однако проведенные компанией Atheros испытания обоих типов оборудования в офисной среде показали другие результаты. Специалисты компании Atheros утверждают, что, если точки доступа размещены очень близко друг к другу (на расстоянии 18—24 м), то наложить сеть стандарта IEEE 802.11a на сеть стандарта IEEE 802.11b совсем несложно. Оборудование стандарта IEEE 802.11a обеспечивает передачу данных с максимальной скоростью 54 Мбит/с на расстояние около 15 м. При дальности связи 30 или 60 м скорость передачи падает до 36 или 6 Мбит/с соответственно. Помните, что реальная скорость передачи данных составляет примерно половину указанных здесь максимальных значений.

Хотя с увеличением дальности (при использовании любого оборудования) скорость передачи данных снижается, согласно информации, полученной от компании Atheros и других фирм-производителей, в сетях стандарта IEEE 802.11a она всегда остается на более высоком уровне, чем в сетях стандарта IEEE 802.11b. Однако до тех пор пока оборудование стандарта IEEE 802.11a не поступит в продажу, и не будут проведены его дополнительные испытания, наложение сети стандарта IEEE 802.11a на сеть стандарта IEEE 802.11b останется сложной задачей, которую вряд ли можно решить только заменой радиоадаптера в двухслотовой точке доступа.

Кроме того, существует проблема с обратной совместимостью нового оборудования. Сети стандартов IEEE 802.11a и IEEE 802.11b работают в разных частотных диапазонах, и большинство радиоадаптеров стандарта IEEE 802.11a, которые первыми появятся на рынке, будут поддерживать только этот стандарт. Двухрежимные радиоадаптеры (IEEE 802.11a/b) тоже поступят в продажу, но первое время они будут стоить дороже однорежимных, поскольку для поддержания каждого из рабочих режимов в них будут использоваться отдельные микросхемы. Первые инсталляции оборудования стандарта IEEE 802.11a будут иметь небольшое радиопокрытие по сравнению с зонами действия сетей стандарта IEEE 802.11b, что сделает невыгодной модернизацию ПК для большинства пользователей.

Стоит отметить, что ведущие производители оборудования стандарта IEEE 802.11b не торопятся с выпуском устройств стандарта IEEE 802.11a. Первыми производителями этих устройств станут в основном

небольшие компании, стремящиеся упрочить свое положение на рынке. И все же переход индустрии беспроводных ЛВС на новые высокопроизводительные технологии неизбежен, поскольку они обеспечивают не только более высокие скорости передачи данных, но и поддержку большего числа пользователей. Последнее особенно важно, поскольку беспроводные ЛВС становятся все более популярными и число их пользователей быстро растет.

Стандарт IEEE 802.11a — это не единственная высокоскоростная альтернатива стандарту IEEE 802.11b. Европейский институт стандартов электросвязи (European Telecommunications Standards Institute — ETSI) разработал высокоскоростной беспроводной стандарт HiperLAN/2, являющийся прямым конкурентом стандарту IEEE 802.11a. Эти стандарты имеют очень похожие спецификации на протоколы физического уровня, предусматривающие работу оборудования в частотном диапазоне 5 ГГц и использование технологии OFDM, но отличаются протоколами более высоких уровней. Если стандарт IEEE 802.11a базируется на протоколе CSMA (Carrier Sense Multiple Access), то в стандарте HiperLAN/2 предусмотрено централизованное управление доступом мобильных станций к радиоканалу с динамическим выделением им тайм-слотов. Этот детерминистический подход (аналогичный используемому в технологии Token Ring) более сложен в реализации, но зато обеспечивает необходимые уровни QoS (сегодня в стандарте IEEE 802.11a соответствующие механизмы отсутствуют) и облегчает интеграцию сетей HiperLAN/2 с сетями ATM. Однако в плане поддержания IP-приложений возможности обеих стандартов сопоставимы.

Придется ли нам стать свидетелями жесткой конкуренции между ними? Возможно, но стандарт IEEE 802.11a имеет определенную «фору»: его поддерживают больше компаний — производителей компонентов для беспроводных устройств и первые основанные на нем продукты для конечных пользователей должны появиться на рынке раньше, чем появится оборудование стандарта HiperLAN/2. Кроме того, недалек тот день, когда сети стандартов IEEE 802.11 начнут поддерживать механизмы QoS. Однако европейские регулирующие органы, отвечающие за электромагнитную совместимость систем связи, отдают предпочтение стандарту HiperLAN/2. В настоящее время, чтобы усилить позиции стандарта IEEE 802.11a, институт IEEE разрабатывает спецификацию IEEE 802.11h, в которой будут определены механизмы использования частот для оборудования этого стандарта.

Ситуация со стандартами очень непроста для понимания, поскольку институт IEEE разрабатывает еще один высокоскоростной стандарт — IEEE 802.11g — на беспроводные ЛВС, передающие данные на скоростях 20 Мбит/с и выше. Скорее всего он тоже будет основан на технологии OFDM. Хотя стандартом IEEE 802.11g не предусмотрена обратная совместимость с оборудованием стандарта IEEE 802.11b, в нем определено использование того же самого диапазона частот, в котором работает названное оборудование. Можно предположить, что производители выпустят радиоадаптеры, поддерживающие сразу оба стандарта — и IEEE 802.11b, и IEEE 802.11g, что должно упростить модернизацию сетей. Однако если вскоре начнутся широкомасштабные поставки оборудования стандарта IEEE 802.11a, то не исключено, что более медленный стандарт IEEE 802.11g окажется запоздалым и никому не нужным.

Пока непонятно, что будут делать производители для обеспечения пользователям возможности модернизации своих точек доступа с целью поддержания более высоких скоростей передачи данных. Очевидно, что точки доступа, оснащенные съемными радиоадаптерами (например, формата PC Card), будет модернизировать легче, чем точки доступа с интегрированными радиоадаптерами. Точки доступа с двумя слотами для радиоадаптеров смогут поддерживать стандарты IEEE 802.11a и IEEE 802.11b одновременно, но при этом не исключены проблемы с радиопокрытием (из-за разной дальности действия соответствующих радиотехнологий). Альтернативным подходом является наложение сети стандарта IEEE 802.11a (или IEEE 802.11g) на сеть стандарта IEEE 802.11b и независимое использование обеих сетей. Вероятно, данный подход несложно реализовать, но он неэффективен с точки зрения использования сетевой инфраструктуры. Если вы все же планируете сделать это, то заранее позаботьтесь о том, чтобы в сетевой инфраструктуре для каждой точки доступа имелось по два порта Ethernet (второй потребуется для подключения новой, высокоскоростной точки доступа).

Глава 3. Беспроводные сети. Взлом и защита

Многие пользователи и специалисты в первую очередь обращают внимание на скоростные возможности новых стандартов и технологий, но не менее важны и новые методы обеспечения информационной безопасности, призванные сделать нашу жизнь спокойнее. Используемый сегодня в сетях стандарта IEEE 802.11 метод обеспечения информационной безопасности, получивший название WEP (Wired Equivalent Privacy), основан на алгоритме шифрования RC4 с 40-битовым или 128-битовым ключом. К сожалению, этот метод имеет серьезные недостатки, которые позволяют раскрыть передаваемую информацию, и предполагает распределение ключей шифрования вручную.

Решить эти проблемы призвана новая система сетевой безопасности, разработанная институтом IEEE и описанная в стандарте IEEE 802.11x. Она ориентирована на все виды сетей доступа (проводные и беспроводные), соответствующие стандартам IEEE. В ней предусмотрены подсистемы аутентификации, шифрования и распределения ключей шифрования. Система, о которой идет речь, предназначена для совместной работы с существующими средствами защиты данных, поддерживающими стандарты EAP (Extensible Authentication Protocol) и RADIUS (Remote Access Dial-in User Service).

Еще один новый стандарт, IEEE 802.11i, определяет специфические для беспроводных сетей, включая инфраструктуры стандартов IEEE 802.11b и IEEE 802.11a, защитные функции. Учитывая сильную поддержку новых стандартов обеспечения информационной безопасности со стороны таких крупных компаний, как Cisco Systems и Microsoft, можно предположить, что соответствующие этим стандартам сетевые продукты появятся в начале следующего года.

Стоит отметить, что ОС Microsoft Windows XP поддерживает стандарты IEEE 802.11x и EAP. Благодаря этому, пройдя единую процедуру аутентификации, пользователь получает возможность работать как в беспроводной, так и в инфраструктурной сети. Чтобы воспользоваться преимуществами новых методов защиты данных, необходимо проделать определенную работу по интеграции проводной сети с беспроводной. Должно пройти еще некое время, прежде чем большинство производителей начнут поддерживать новые стандарты сетевой безопасности. Кроме того, могут возникнуть проблемы с совместимостью решений от разных производителей.

Обеспечить необходимые уровни качества обслуживания трафика в беспроводных сетях призван другой новый стандарт — IEEE 802.11e.

В нем определены асинхронная и контролируемая по времени передачи данных. Последняя нужна для пересылки аудио- и видеоинформации. Кроме того, для разных видов потоков данных предусмотрена возможность использования разных методов передачи. Например, для пересылки чувствительного к задержкам видеопотока вместо механизма повторной передачи пакетов можно задействовать метод упреждающей коррекции ошибок. Одновременная поддержка в оборудовании стандартов IEEE 802.11e и IEEE 802.11a позволит получить примерно такой же набор рабочих характеристик и функциональных возможностей, какой предусмотрен стандартом HiperLAN/2.

Необходимые для качественной передачи аудио- и видеоинформации механизмы обеспечения QoS беспроводной ЛВС должны быть интегрированы с соответствующими механизмами инфраструктурной

сети, а на это потребуется некоторое время. Возможно, до появления корпоративных приложений, использующих механизмы QoS для беспроводных ЛВС, пройдут годы. Гораздо быстрее интегрированные (предназначенные для передачи речи, видео и данных) беспроводные ЛВС появятся в жилых домах. Однако не стоит откладывать развертывание беспроводной ЛВС, ожидая появление продуктов с новыми функциями. Возможностей сегодняшних устройств вполне хватает для нормальной работы большинства приложений. Предварительно обсудив с представителями фирмы-производителя ее планы по модернизации выпускаемого оборудования, смело разворачивайте у себя беспроводную ЛВС, функциональность которой вы со временем сможете улучшить.

Предлагаемые методы защиты

Маскировка сети

Если отключить широковещательную передачу узлом доступа «маячковых» сигналов с идентификатором сети, то теоретически такая сеть становится «скрытой». Пользователь, находясь в зоне доступа «скрытой» сети, не получает «маячковых» сигналов от узла доступа. Следовательно, не может определить идентификатор сети. А если у него нет идентификатора, то и подключиться к сети он тоже не может. О надежности такого способа маскировки позднее, а пока для подключения к «скрытой» сети пользователю необходимо ввести значение сетевого идентификатора вручную.

Шифрование передаваемых данных

Реализованный в протоколе 801.11 метод — WEP. Это симметричный способ шифрования, когда для кодирования и декодирования данных используется один и тот же кодирующий ключ, состоящий из двух частей. Одна часть — секретный ключ, хранится у получателя и отправителя. Вторая — вектор инициализации — генерируется случайным образом в системе отправителя. На основании этих двух значений вычисляется псевдоуникальный кодирующий ключ.

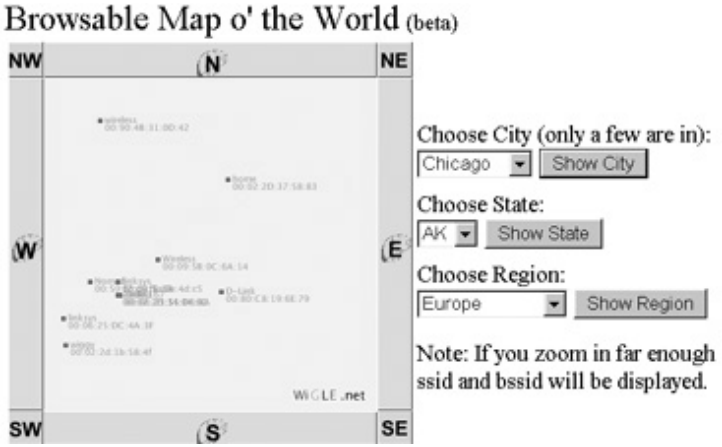
Данные между сетевыми системами передаются в виде пакетов. Структурно, каждый пакет состоит из двух частей — заголовка и тела. В заголовке хранится служебная информация, в частности, идентификатор сети, аппаратные адреса получателя и отправителя. В теле передаются данные и значение контрольной суммы передаваемых данных (ICV), используемое получателем для проверки целостности данных.

Для каждого нового сетевого пакета применяется новый кодирующий ключ. Причем, кодируется только тело пакета. В заголовок добавляется значение вектора инициализации соответствующего данному паке-

ту кодирующего ключа. Содержание заголовка не кодируется и передается в открытом виде.

Если используемый системой генератор случайных чисел достаточно качественен в статистическом отношении, то проведенная операция шифрования обеспечивает шумоподобный характер передаваемых данных, что в теории, без знания секретного ключа, делает возможность декодирования перехваченного сообщения очень длительным процессом даже при современной вычислительной технике.

При расшифровке пакета получателем программа кодирования инициализируется секретным ключом и извлеченным из полученного пакета значением вектора инициализации. После расшифровки тела сетевого пакета, система вычисляет контрольную сумму полученных данных и сравнивает со значением контрольной суммы, переданной отправителем в этом же пакете. При положительном результате данные начинают обрабатываться, и отправителю передается подтверждение удачного приема. В противном случае, отправитель повторно осуществляет передачу.



Контроль доступа

Сетевой доступ к какому-либо беспроводному устройству можно избирательно контролировать, используя список контроля доступа. Там указываются аппаратные адреса сетевых устройств, связь с которыми разрешена. Соответственно, любая сетевая активность устройств с аппаратными адресами, не внесенными в список, будет проигнорирована. Данный вид защиты основан на том, что аппаратный адрес — это уникальный идентификатор устройства, присваиваемый производителем.

Теоретически, двух сетевых устройств с одинаковым аппаратным адресом быть не может. Следовательно, на основании этой характеристики сетевого устройства можно однозначно идентифицировать его владельца.

В стандартах рассматриваемых беспроводных сетей были изначально заложены механизмы идентификации клиентов (по аппаратным адресам), защиты (WEP) и контроля целостности передаваемых данных. Исходя из предоставленных разработчиками технологии средств, в теории, беспроводная сеть должна быть наиболее защищена при работе в режиме инфраструктуры (когда весь трафик клиентов проходит через узел доступа) с включенным WEP-кодированием и фильтрацией аппаратных адресов беспроводных клиентов.

Методики нападения

Главным преимуществом беспроводных сетей (равно как и их ахиллесовой пятой) является доступность физической среды передачи данных — радиоэфира. И если для площадок общественного доступа к сетевым ресурсам (hot spots) такая возможность это благо, то для домашних или локальных сетей доступность за пределами ограниченной территории, определенной стенами офиса или квартиры, совершенно излишня. Пространственно зона доступа одного узла представляет собой сферу, радиус которой определен максимальным удалением от центра с сохранением устойчивого качества работы беспроводных клиентов. На практике, реальная пространственная зона доступа далека от геометрически красивой фигуры из-за поглощения окружающей физической средой радиосигнала. Говоря нормальным языком, при одинаковом оборудовании размеры зон доступа в кирпичных и панельных зданиях с железобетонными перекрытиями будут различаться. Надо быть готовым, что, настроив офисную беспроводную сеть, можно не только обеспечить подключение из любой точки офиса, но и из таких неожиданных мест, как чердак, автостоянка или здание напротив. Если для защиты от вторжения при прокладке кабельных сетей можно было использовать экранированную витую пару, то в качестве аналогичного решения для физического ограничения пространственной зоны доступа беспроводной сети придется использовать экран из заземленной металлизированной сетки, натянутой по границам зоны доступа. Можно представить, что укладка такого экрана даже в случае небольшой офисной сети будет нелегким и недешевым удовольствием.

Также следует заметить, что максимальное расстояние от клиента до точки доступа напрямую зависит от используемого оборудования. Так, при работе с направленной антенной для адаптера DWL-520 удалось установить подключение к офисной сети с расстояния порядка 450 мет-

ров, тогда как со встроенной антенной максимальное удаление было около 80 метров.

Прослушивание (Sniffing)

Сбор информации об атакуемом объекте — это необходимый этап при подготовке атаки. К сожалению администраторов и владельцев беспроводной сети, пассивное прослушивание и анализ передаваемой информации может предоставить сторонним наблюдателям достаточно данных для успешного проникновения в сеть. И предусмотренные разработчиками методы защиты не смогут этому помешать.

Для сбора информации достаточно войти в зону покрытия сети, и, воспользовавшись рабочей станцией с беспроводным сетевым интерфейсом, подключить программный анализатор сетевого трафика (например, Kismet или Ethereal). Если WEP-кодирование не включено (обычная заводская настройка оборудования), наблюдатель видит в открытом виде все данные, передаваемые в сети. Если WEP-кодирование все-таки включено, то, следует заметить, кодируются только данные, передаваемые в сетевом пакете, а заголовок пакета передается в открытом виде. Из анализа заголовка можно извлечь информацию об идентификаторе сети, аппаратных адресах узлов доступа и клиентов сети, а также значение вектора инициализации, используемое получателем для дешифровки полученных данных.

Как можно себе представить, прослушивание и анализ перехваченных сетевых пакетов делает попытки сокрытия беспроводной сети несостоятельными за счет отключения широковещательной передачи узлами доступа «маячковых» сигналов.

Подделка аппаратного адреса (MAC spoofing)

Использование механизма идентификации клиентов по аппаратным адресам сетевых интерфейсов для доступа к сетевым ресурсам — не самая лучшая идея. Перехватив и проанализировав сетевой трафик, можно за короткое время получить список аппаратных адресов всех активных клиентов. Задача же изменения аппаратного адреса своего сетевого интерфейса давно решена. Под «линуксоподобными» операционными системами достаточно воспользоваться стандартной сетевой утилитой ifconfig, а для Windows-систем надо трудиться несколько больше, переставляя драйвер сетевого интерфейса или устанавливая дополнительную утилиту.

Взлом криптозащиты

Дьявол прячется в деталях. Стандарт 802.11 предусматривает две длины ключей — 40 бит и 104 бита. При длине ключа в 104 бита декодирование данных прямым перебором становится довольно утомительным занятием даже при работе новейшей вычислительной техники. На первый взгляд, реализованный в WEP-механизм криптозащиты должен быть устойчив ко взлому. Но обратите внимание на следующий факт: обе стороны (отправитель и получатель) должны обладать секретным ключом, используемым вместе с вектором инициализации для кодирования и декодирования информации. А в стандарте 802.11b не оговорен механизм обмена ключей между сторонами. В результате, при интенсивном обмене данными, реальна ситуация повторного использования значений векторов инициализации с одним и тем же секретным ключом. Особенность реализованного алгоритма криптозащиты приводит к тому, что, имея два сетевых пакета, зашифрованных одним кодирующим ключом, можно не только расшифровать данные, но и вычислить секретный ключ. Это позволяет не только декодировать всю перехваченную информацию, но и имитировать активность одной из сторон.

Тонкость работы с алгоритмом кодирования, реализованном в WEP, в том, что нельзя допускать повторного использования кодирующих ключей. И этот момент был упущен при разработке стандарта.

Посредник (Man-In-The-Middle)

Данный вид атаки использует функцию роуминга клиентов в беспроводных сетях. Злоумышленник на своей рабочей станции имитирует узел доступа с более мощным сигналом, чем реальный узел доступа. Клиент беспроводной сети автоматически переключается на новый узел доступа, передавая на него весь свой трафик. В свою очередь, злоумышленник передает этот трафик реальному узлу доступа под видом клиентской рабочей станции. Таким образом, система злоумышленника включается в обмен данными между клиентом и узлом доступа как посредник, что и дало название данному виду атаки — Man-In-The-Middle. Эта атака опасна тем, что позволяет взламывать защищенные соединения (VPN), устанавливаемые по беспроводной сети, вызывая принудительную реавторизацию VPN-клиента. В результате злоумышленник получает авторизационные данные скомпрометированного им клиента.

Отказ в обслуживании

Сама среда передачи данных предоставляет возможность силовой атаки на беспроводные сети. Цель подобного нападения — снижение производительности сети или ухудшение качества сетевого обслуживания вплоть до полного паралича сети. Атаки подобного вида называются DoS (Denial of Service) или DDoS (Distributed DoS). В процессе нападения злоумышленник передает трафик, объем которого превышает возможности пропускной способности сетевого оборудования. Или сетевые

пакеты со специально нарушенной внутренней структурой. Или имитируя команды узла доступа, вызывает отключение клиентов и т.д. и т.п. Злоумышленник может избирательно атаковать как отдельную рабочую станцию или точку доступа, так и всех клиентов сети. DoS-атака может быть и непреднамеренной. Например, вызванная включением радиопередающего оборудования, работающего на той же частоте, что и беспроводная сеть.

Возможно, DoS-атака не так изящна как проникновение в сеть со взломом криптозащиты, зато убийственно эффективна. С учетом того, что нельзя избирательно ограничивать доступ к физической среде передачи данных в беспроводных сетях — радиоволнам, вероятно, придется смириться с существованием еще одной ахиллесовой пяты данной технологии.

Сетевой взлом клиентов беспроводной сети

Тема локализации и устранения уязвимости программного обеспечения непосредственно не относится к вопросу безопасности беспроводных сетей, но является достаточно важной, чтобы кратко упомянуть о ней. Тем более что, получив доступ в сеть, злоумышленник вполне может атаковать клиентов сети для получения доступа к их ресурсам.

Проверка надежности разнообразного программного обеспечения на нескольких десятках клиентских машин с разными операционными системами весьма нетривиальная задача даже для опытного специалиста. Удобным инструментом, позволяющим отчасти автоматизировать и ускорить процедуру проверки надежности защиты компьютерных систем, является сканер безопасности. По результатам исследования систем, сканер формирует отчет с описанием обнаруженных явных и потенциальных уязвимостей, их анализом и рекомендациями по устранению. К самым известным в данной области можно отнести такие программные сканеры как: ISS (Internet Security Scanner), Retina, Nessus.

Аудит

Провести аудит защиты беспроводной сети и убедиться в ее недостаточности можно при помощи свободно распространяемых программ AirSnort или Wellenreiter. У них сходный принцип действия. Они позволяют определять рабочий канал беспроводной сети, ее идентификатор и аппаратные адреса активных сетевых клиентов, а также взломать WEP-защиту. Из всех этих задач взлом криптозащиты — наиболее длительное занятие, требующее несколько часов; для сбора остальных данных достаточно минуты. Для определения секретных ключей, в среднем, необходимо перехватить и проанализировать порядка 8–10 миллионов зашифрованных сетевых пакетов (это примерно 6 часов работы при средней загрузке узла доступа). После перехвата пакета, зашифрованного уже использованным кодирующим ключом, восстановить секретный ключ — секундное дело.

В том, что взлом беспроводных сетей превратился в народное развлечение, можно убедиться, заглянув на ресурсы WiFinder и Wingle, где собрана информация о беспроводных сетях с указанием их точного географического положения и технических характеристик. Карты сетей, представленные этими ресурсами, чем-то неуловимо напоминают дорожный список отелей и ресторанов для путешественников. Кстати, из владельцев российских сетей указаны только отели «Мариотт».

Выводы и рекомендации

Проанализировав приведенные выше данные о методиках злоумышленников, можно убедиться, что предусмотренных в технологии беспроводных сетей средств недостаточно для адекватной защиты. Скрытая сеть легко находится, аппаратные адреса имитируются, а WEP-защита взламывается. Это не означает, что следует отказываться от использования беспроводных сетей, просто следует учитывать, что на данный момент это потенциально опасная среда передачи данных. Из этого вывода сразу следуют общие рекомендации по защите. Рекомендуемые методики непосредственно не связаны с беспроводными сетями и были давно отработаны в другой потенциально опасной среде — в Интернете:

- для авторизации пользователей можно использовать технологию RADIUS (Remote Authentication Dial-In User Service);
- уменьшение риска сетевого взлома на серверах и рабочих станциях достигается использованием программных брандмауэров (firewall);
- идентифицировать активность злоумышленников лучше на ранней стадии; для этого служат сетевые системы обнаружения вторжения и системы-ловушки;
- для защиты передаваемой информации от несанкционированного доступа лучше отказаться от потенциально небезопасных прикладных протоколов, передающих данные в открытом виде (FTP, TELNET, SMTP и т.д.), заменив их криптозащищенными аналогами или использовать криптозащиту на сетевом уровне — VPN, IPSEC;
- а с DoS-атакой, как уже было замечено выше, придется смириться.

Глава 4.
Настоящее и будущее

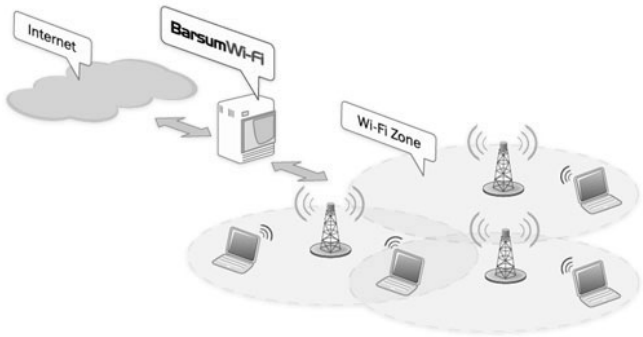
Неудивительно, что разработчиков стандарта 802.11 не удовлетворила низкая практическая надежность механизмов защиты беспроводных сетей. Следствием этой неудовлетворенности стала призванная заменить WEP криптозащита WPA, базирующаяся на временном протоколе целостности ключей (TKIP), задача которого — не допустить повторного использования кодирующих ключей. WPA обеспечивает обратную совместимость с WEP, что позволяет использовать ее на той же аппаратной базе. Но TKIP рассматривается всего лишь как временная мера. Более криптоустойчивые методы защиты (например, AES) требуют уже другого аппаратного обеспечения, что должно привести к полной замене существующего оборудования беспроводной локальной сети.

Беспроводные сети имеют хорошую потенциальную возможность стать настолько же распространенным сервисом, как и сотовая телефонная связь. Достигнуто многое, но самое главное, что существуют возможности дальнейшей эволюции и совершенствования беспроводных технологий передачи данных. Не стоит только забывать, что до окончательной оптимизации технологий, как с точки зрения максимальной производительности сетей, так и вопросов безопасности, еще далеко. И, пожалуй, не стоит облегчать задачу взломщикам, пренебрегая пока немногими и еще несовершенными средствами безопасности.

Глава 5.
Что такое Barsum Wi-Fi?

Barsum Wi-Fi — это универсальная программная платформа для развертывания Wi-Fi зоны с использованием любых точек доступа любых производителей. Основные функции Barsum Wi-Fi — контроль доступа в сеть и биллинг, однако платформа включает в себя все необходимые сервисные функции для полноценного функционирования хот-спота, такие как генерация PIN-кодов для карточек доступа, гибкая схема тарификации, припейд/постпейд оплата, интеграция с PMS или другими биллинговыми системами и т.д.

Barsum Wi-Fi является идеальным stand-alone решением для организации коммерческой услуги доступа в Интернет на отдельно взятом объекте, а также может стать компонентом программного комплекса Интернет-оператора, отвечающим за учет и управление беспроводными сетями на объектах клиентов.



Программный комплекс Barsum Wi-Fi является компонентом Автоматизированной Системы Расчетов «Барсум Оператор» (сертификат соответствия ССС № ОС/1-СТ-344) и предназначен для решения задач организации биллинга и авторизации клиентов в широкополосных сетях беспроводного доступа стандарта IEEE 802.11x (Wi-Fi).

Основные возможности Barsum Wi-Fi:

- авторизация клиента при подключении к беспроводной сети Wi-Fi;
- контроль доступа клиента к сети на основании установленных для него расчетных схем и тарифных планов;
- генерация кодов доступа с проверкой уникальности;
- создание и управление тарифными планами;
- тарификация клиентов в реальном времени;
- администрирование и разграничение прав доступа к управлению системой;
- учет чистого времени клиента, проведенного в сети INTERNET (учет времени между операциями login/logout);
- печать отчетов о проданных и сгенерированных картах;
- доступ и учет для проводных Ethernet-сетей.

Преимущества Barsum Wi-Fi:

- удобные средства управления и администрирования системы;

- работа по дебетовой и кредитной схемам оплаты;
- мониторинг и отчетность по работе системы;
- интегрируемость — возможность взаимодействия с внешними программными системами (PMS в гостиницах, системы биллинга сторонних производителей и т.д.);
- модульность — может поставляться с дополнительными модулями, позволяющими расширять спектр предоставляемых услуг;
- применен широкий опыт создания и внедрения систем тарификации традиционной телефонии;
- оперативная техническая поддержка.

Функциональные возможности Barsum Wi-Fi

Система доступа:

- для доступа в Интернет посредством Wi-Fi клиенту достаточно открыть окно браузера, после чего ему будет предложено ввести PIN-код доступа
- с использованием предоплатных карт с PIN-кодом, доступ к сети Wi-Fi возможен в любой момент. Клиент может воспользоваться услугами сети Wi-Fi по своему желанию и без участия оператора
- для прохождения процесса авторизации клиенту не нужно устанавливать на своем компьютере никаких дополнительных приложений и настроек. Весь процесс авторизации клиента происходит через WEB-интерфейс
- после прохождения процесса авторизации клиент получает полный доступ в Интернет и может пользоваться всеми необходимыми сервисами, включая VPN-соединения
- возможность ограничения доступа клиента к сети Интернет в зависимости от объема трафика, продолжительности сеанса работы, стоимости трафика, срока действия PIN-кода
- также можно использовать совмещенные схемы ограничения доступа (одновременное ограничение по объему трафика и по времени и т.д.)

- каждому клиенту выдается уникальный PIN-код, который используется только один раз для активации услуги доступа и не может быть использован повторно
- встроенный DHCP-сервер
- встроенный WEB-сервер
- встроенный сервер авторизации
- существует две схемы предоставления PIN-кода клиентам:
- предварительная генерация PIN-кодов с последующей передачей/продажей клиентам карточек, содержащих PIN-код
- генерация PIN-кода в момент обращения клиента к оператору с распечаткой PIN-конверта. При этом возможно использование «post-paid» тарификации с последующим выставлением счета клиенту (схема, как правило, используемая в гостиницах для предоставления доступа к сети Интернет постояльцам гостиницы)

Система тарификации:

- тарификация услуг в режиме реального времени
- тарификация по времени и/или объему трафика
- поддержка нескольких тарифных таблиц
- зависимость тарифа от времени суток, типа дня, даты, направления трафика
- учет налогов
- мультивалютность
- администрирование и работа с системой
- разграничение прав пользователей
- использование логинов и паролей для авторизации пользователей в системе
- разграничение доступа к интерфейсам системы (просмотр, редактирование данных, запрет доступа)
- разграничение доступа к данным системы (возможность скрывать те или иные данные для различных пользователей)

- управление системой посредством пользовательских GUI-интерфейсов
- отображение информации о состоянии карт доступа в режиме реального времени
- логирование системных событий (активация пользователями PIN-кода, прохождение пользователями авторизации и т.д.)
- логирование действий пользователей системы с привязкой всех действий ко времени и имени пользователя
- автоматический журнал ошибок
- учет дилеров карт доступа (справочник дилеров, привязка карт к дилерам)
- управление процессами сбора статистики и тарификации (настройка периода времени сбора статистики с коммутационного устройства, настройка периода тарификации, настройка периода обмена данными через PMS во внешние информационные системы автоматизации гостиничного бизнеса)
- автоматизация процесса резервного копирования базы данных

Отчетность:

- встроенный генератор отчетов

Взаимодействие с гостиничными PMS

Наличие модуля интеграции с PMS позволяет оператору гостиничной системы, пользуясь единым интерфейсом гостиничной системы, предоставлять PIN-коды для доступа в Интернет постояльцам гостиницы и производить расчет за услуги доступа в общем счете клиента.

Принцип работы

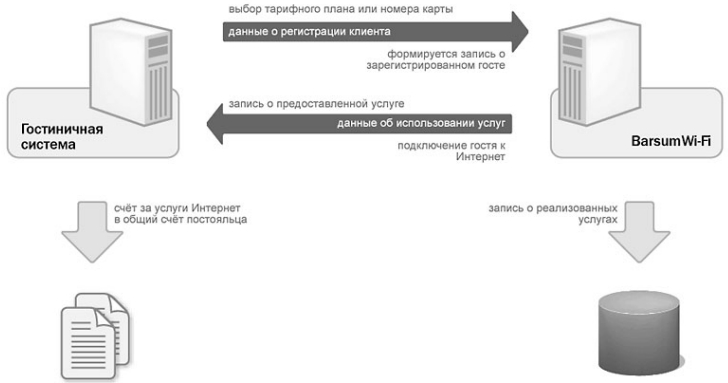
Производится регистрация гостя в гостиничной системе. При регистрации клиента указывается «Группа ограничений» карты, присутствующая в Barsum Wi-Fi. Либо указывается номер непроданного PIN-кода, существующего в системе Barsum Wi-Fi. Для клиента распечатывается PIN-конверт.

Гостиничная система передает данные модулю Barsum Wi-Fi PMS о регистрации клиента.

Модуль Barsum Wi-Fi PMS помечает указанный PIN-код как проданный, либо создает новую карту в случае, если при регистрации клиента была указана группа ограничений. В системе Barsum Wi-Fi появляется запись о зарегистрированном госте.

После активации карты клиентом вся стоимость за трафик передается в гостиничную систему.

При выписке клиента в гостиничной системе выставляется счет, который включает в себя стоимость использованных услуг Интернет. В системе Barsum Wi-Fi приписанная карта к клиенту помечается как израсходованная.



Прием платежей по банковским-картам и Интернет-платежей

Данный модуль позволяет, при заключении дополнительного соглашения с ASSIST, продавать услуги доступа владельцам пластиковых банковских карт (VISA, MASTER и т.д.).

Переход к платежной системе осуществляется в случае, если при попытке подключения абонента он нажал соответствующую кнопку в появившемся окне, где ему предлагается ввести имеющийся или купить PIN-код для доступа.

По факту успешной оплаты в платежной системе, в модуль Barsum Wi-Fi передаются данные об оплате определенного тарифного плана, после чего для пользователя генерируется и выдается новый PIN-код с соответствующим тарифным планом.

Глава 6.
Локальная сеть в мобильном офисе

Прежде чем говорить о мобильной сети в офисе, давайте представим сотрудников этого офиса и сферу их деятельности. Кому требуется мобильность и оперативность получения информации? Первыми, по известной причине, приходят на ум журналисты.

Следующими будут работники торговой сферы. Этот термин не сводится к тетушкам в халатах в залах супермаркетов, хотя высокотехнологичные решения существуют и для них. Речь идет обо всех, чья работа заключается в продаже и покупке товаров. Именно им нужна горячая информация, причем не только в тот момент, когда они сидят за дисплеем в офисе, но и за его пределами.

Ранее все технологии обработки и передачи информации в этом секторе сводились к использованию телефона, калькулятора да изредка факсимильного аппарата. Во времена становления капитализма на обломках Союза ССР чуть ли не каждый третий наш соотечественник попробовал себя в роли торговца — от челнока до брокера на товарно-сырьевой бирже. Но если работа первых сводилась к немудрящему отовариванию в одном месте и распродаже в другом, то брокерам, а проще говоря, посредникам, приходилось шевелить мозгами на порядок интенсивнее. Это хорошо описано в анекдоте той поры. Первый брокер сообщал второму, что срочно требуется вагон сахара. Второй отвечал ему: «О'кей, найдем, но в обмен на цистерну топлива». Первый убегал искать цистерну топлива, второй же отправлялся на поиски вагона сахара. Скорее всего, и то, и другое успешно находилось и продавалось. Но для этого нужно было совершить не менее сотни телефонных звонков и около десятка встреч. Словом, найти пресловутый вагон или цистерну было довольно непросто, а уж каким образом за нее рассчитывались — вопрос отдельный. В эпоху вынужденного бартера цепочка из трех-четырех обменов считалась нормальной практикой. И добивался успеха тот, кто раньше узнавал о предложениях сахара или топлива, а также вариантов бартера, то есть владел информацией и оказывался в нужном месте быстрее, иначе говоря, обладал мобильностью.

Сегодня торговать чем бы то ни было значительно проще, чем на заре девяностых. Интернет стал доступен каждому, и на скоростях гораздо больших, чем подключение к BBS тогдашних бирж через модем по протоколу MNP-5. С мобильностью тоже все устаканилось — сейчас имеется выбор из нескольких вариантов доступа к информации «в походных условиях». Это тандем из ноутбука и мобильного телефона, связка мобильник-КПК, смартфон для тех, кто предпочитает интегрированные решения, либо GPRS-модули для лэптопов и наладонников. И уже не редкостью стали совещания в торговых фирмах, где перед сотрудниками лежат не пухлые ежедневники, а гораздо более изящные карманные компьютеры или гордо открытые экраны ноутбуков. И все эти устройства связаны друг с другом, то есть представляют собой мобильный офис, объединенный в незримую сеть.

Каким же образом осуществляется связь составляющих мобильного офиса? Оставим в стороне кабели и провода, так как мобильным такой офис назвать трудно. Тогда нам останется только два варианта: радиоинтерфейсы Wi-Fi и Bluetooth. Последний, правда, малопригоден для организации компьютерной сети, но может использоваться как шлюз к проводным сетям Ethernet. Что же касается Wi-Fi, это целый класс решений для беспроводных локальных сетей (WLAN), обеспечивающий разные скорость и дальность передачи информации.

Как выше было сказано что, по классификации IEEE (Institute of Electrical and Electronics Engineers, Inc.), определяющего стандарты в области электротехники, беспроводные сети описываются семейством стандартов 802.11, лидирующим из которых стал 802.11a (хотя возник он уже после 802.11b). Он обеспечивает скорость передачи данных до 54 Мбит/с в диапазонах 5,15–5,35 ГГц и 5,725–5,85 ГГц. К сожалению, в России первый диапазон относится к категории «для правительственного использования», поэтому использование такой аппаратуры может вызвать некоторые неприятности. Вторую полосу частот использует для своих нужд российская армия, поэтому и здесь можно столкнуться с лицензионными ограничениями. Впрочем, эти вопросы решаемы, да и радиус действия адаптеров связи 802.11a не превышает пары десятков метров.

Второй по популярности протокол беспроводной связи носит имя 802.11b, кстати, именно его и назвали впервые Wi-Fi. Устройства этого стандарта ведут передачу на частотах около 2,4 ГГц. В большинстве стран Европы и Северной Америки вещание в этом диапазоне (называемом ISM — Industrial, Scientific, Medical) не требует лицензирования. Дальность передачи стандарта «b» составляет 100 метров, но скорость ограничена 11 мегабитами в секунду. Зато в придачу к большему радиусу действия пользователь получает повышенную помехозащищенность. А уж для обмена информацией бизнес-характера 11 Мбит/с хватит за глаза. Следует только учитывать, что в этом диапазоне довольно сильно шумят и микроволновые печи, столь популярные в офисах, так что во время подготовки к трапезе можно ожидать снижения пропускной способности WLAN-сети на базе 802.11b.

Последний, принятый IEEE в июне 2003 г., стандарт беспроводной связи именуется 802.11g и также, как и 802.11a, обеспечивает обмен данными на скорости до 54 Мбит/с в диапазоне 2,4 ГГц. Одно из главных преимуществ нового протокола в том, что соединение, установленное с его помощью, обладает повышенной устойчивостью. К тому же этот стандарт обратно совместим со своим предшественником 802.11b. Таким образом, если в вашем мобильном офисе уже есть устройства, работающие по протоколу 802.11b, можно без опаски приобретать новое оборудование стандарта 802.11g. Адаптеры и точки доступа такой смешанной сети будут прекрасно понимать друг друга. Радиус действия устройств 802.11g на скорости 54 Мбит/с составляет 15 метров, обеспечивается качественная связь даже при отсутствии прямой видимости между устройствами.

Мобильная сеть с использованием протоколов 802.11x сегодня строится достаточно просто. На рынке имеется масса адаптеров, коммутаторов и точек беспроводного доступа самых разных производителей. Владелец ноутбука может воспользоваться адаптером формата PCMCIA (PC Card), Secure Digital и даже USB. Существуют и варианты подключения Wi-Fi адаптеров к обычным портам Ethernet, такие устройства, например, выпускает компания Buffalo. Правда, габариты и масса этих адаптеров не позволяют назвать их мобильными. Гораздо удобнее в использовании карты расширения для ноутбуков.

В последнее время производители начинают встраивать оборудование Wi-Fi в мобильные компьютеры, а кое-кто даже делает это ключевым элементом маркетинговой политики. Так, в начале года пионер IT-инноваций, корпорация Intel, вывела на рынок мобильную платформу Centrino.

Краеугольный «камень» этой архитектуры — процессор, известный ранее под кодовым названием Banias, а также чипсет Intel 855 с интегрированным видеоконтроллером Intel Extreme Graphics 2 (опционально) и адаптер WLAN Intel PRO/Wireless 2100 (протокол 802.11b). Все компоненты Centrino подобраны таким образом, чтобы максимально увеличить продолжительность автономной работы ноутбука. Так, центральный процессор, благодаря технологиям Intel SpeedStep и Mobile Voltage Positioning, может работать на разных частотах и напряжениях. Разумный шаг, особенно в свете того обстоятельства, что беспроводная связь изрядно увеличивает энергоаппетиты ноутбуков. Контроллер WLAN тоже интеллектуализирован в плане энергосбережения — технология Intelligent Scanning Technology снижает энергопотребление путем управления частотой сканирования при поиске точек доступа. Пользователь может выбрать один из пяти режимов энергопотребления беспроводного адаптера, что позволяет ему самостоятельно установить соотношение между энергопотреблением и производительностью при питании ноутбука от батарей.

Все перечисленные технологии опосредованно влияют, причем положительным образом, на габариты и вес ноутбука, так что решения на платформе Centrino будут неплохим выбором для мобильного офиса. Стоимость ноутбука с логотипом Centrino от известного производителя приближается к двум тысячам долларов. За эти деньги пользователь получает систему на процессоре Pentium-M с частотой 1,3 ГГц с мегабайтом кэша, 14-дюймовый экран, отдельный, либо интегрированный видеоадаптер, 128 Мбайт памяти, оптический накопитель, винчестер на 20 Мбайт — то есть полноценный компьютер, производительности которого хватит на работу со всеми офисными приложениями. Известный российский производитель, компания DVM Group, предлагает Centrino-ноутбуки серии Roverbook Nautilus; компании iRu и Bliss также отметились в этом секторе своими линейками Stilo и 50xx соответственно.

Счастливым обладателям КПК беспроводная связь доступна посредством адаптеров с интерфейсами CompactFlash, Secure Digital и PCMCIA. Правда, разъемами последнего типа оборудована небольшая часть наладонников, и стоят адаптеры к ним порядка 80 «зеленых». Покупать их могут и те, чьи КПК имеют «жакет» расширения с PCMCIA-разъемом. Но лучше приобрести WLAN-карту в формате CompactFlash, так как это самые компактные карты расширения мобильных устройств. Стоимость таких беспроводных адаптеров не превышает ста долларов.

Кстати, компания SanDisk недавно анонсировала новые продукты — серия флэш-карт Connect предоставляет пользователям как беспроводную связь стандарта 802.11b, так и дополнительную память объемом 128, либо 256 Мбайт. Первые стоят около $130, вторые, более емкие — в районе 150 долларов США. Это решение интересно тем, что позволяет не жертвовать памятью ради связи и наоборот. Впрочем, если ваш наладонник бизнес-класса выпущен недавно, вполне возможно, что он уже оборудован адаптером беспроводной связи. Например, адаптерами WLAN стандарта 802.11b оснащены КПК Toshiba e740 и iPAQ H5450. Другие производители тоже расширяют функциональность своих изделий в плане беспроводной коммуникабельности.

Итак, все сотрудники мобильного офиса обзавелись портативными или карманными компьютерами с возможностью подключения к беспроводной сети. Уже сейчас можно начинать совместную работу, но надо учесть некоторые ограничения. Так, максимальное число участников сети, при котором возможна устойчивая связь, равняется восьми и превышать это количество не рекомендуется. Компьютеры с беспроводными адаптерами могут связываться друг с другом в режиме «ad hoc». Это

соединение типа «точка-точка» (peer-to-peer) и его особенность в том, что отдельные абоненты сети могут устанавливать связь даже на расстояниях, превышающих радиус действия их Wi-Fi адаптеров. Если между компьютерами, находящимися далеко друг от друга, поместить еще одного абонента беспроводной сети, связь будет возможна при его посредничестве. Но если он выйдет за пределы досягаемости одного из адаптеров, связь между удаленными компьютерами прервется. Так что этот вариант применим лишь в случае компактного расположения абонентов и небольшом их количестве. К тому же, в данном случае невозможно организовать доступ пользователей к ресурсам проводной сети Ethernet. А если кому-то из сотрудников понадобится распечатать прайс-лист или деловое предложение, придется приобретать беспроводной принт-сервер (такие выпускает, например, компания Linksys) — это коробочка с парой антенн, подключаемая к обычному принтеру.

Мобильный офис с большей площадью и населенностью придется оборудовать так называемой «точкой доступа» (Wireless Access Point или сокр. WAP или AP). Это устройство исполняет функции коммутатора и/или маршрутизатора, а также способствует увеличению дальности действия беспроводной сети до 200 метров. Как правило, точка доступа располагается высоко на стене или даже на потолке офиса.

К преимуществам использования точки доступа можно отнести еще и отсутствие коллизий, часто возникающих при связи «ad hoc», и повышенную степень защиты передаваемых данных. Точка доступа в силу своей стационарности может быть подключена к локальной сети офиса, что обеспечит связь настольных ПК и мобильных компьютеров.

Наконец, точек доступа может быть несколько, и это позволит значительно расширить площади, охватываемые беспроводной сетью.

Приобрести точки беспроводного доступа стандарта 802.11b производства компаний D-Link, Lantech, Compex можно не дороже ста долларов. Устройства, поддерживающие больше одного протокола и носящие логотипы известных производителей, стоят от 120 долларов и выше.

Часто кроме коммутации радиопакетов эти изделия предоставляют возможность подключения к линиям xDSL и снабжены разными интерфейсами, в том числе и USB 2.0. Это делает возможным подключение, например, к стационарному серверу сети, который будет выполнять дополнительные задачи по обеспечению сетевой безопасности.

Глава 7. «Двенадцать обезьян»

Поиск беспроводных сетей с открытым доступом превратился в своеобразный спорт и получил название «warchalking». Корень «war» заимствован из термина «wardialing», означающего тотальный перебор телефонных номеров интернет-провайдеров на предмет обнаружения дармового доступа в глобальную сеть. «Chalk» же с английского переводится как «мел», и целиком термин «warchalking» означает оставление пометок мелом в местах, где возможен вход в беспроводную сеть без ведома ее хозяев (помните культовый фильм «Двенадцать обезьян»?). Энтузиасты warchalking'а рыскают по улицам с Wi-Fi наладонником, либо разъезжают на машине с ноутбуком, сканируя эфир в поисках WLAN-трафика. Обнаружив таковой, охотник определяет параметры беспроводной сети и рисует на ближайшей стене значок, характеризующий данную сеть. Знающий эти обозначения сразу поймет, что в этом месте можно подключиться к сети и как это сделать.

Открытые зоны беспроводного доступа (hot spots) сегодня развертываются во всем мире. С их помощью странствующие коммивояжеры могут за некоторые деньги пользоваться Интернетом и работать с электронной почтой без подключения проводов. И здесь лидером выступает корпорация Intel, активно расширяющая сеть зон доступа в отелях, аэропортах, кафе и прочих местах общественного пользования. Французские связисты используют инфраструктуру парижского метрополитена, чтобы покрыть невидимой сетью практически весь город. В Канаде и США для этого уже применяется существующая сеть таксофонов, подобное решение намеревается внедрить и крупный китайский оператор связи Chunghwa Telecom. Нет сомнения, что это направление провайдерского бизнеса будет расширяться, так что при покупке нового мобильного компьютера следует озаботиться приобретением Wi-Fi адаптера или выбрать ноутбук на платформе Centrino.

Глава 8. Любопытно?

В послевоенном обустройстве Ирака будут принимать участие не только нефтедобывающие компании. Большую работу предстоит проделать и в области развития информационных технологий. Существует мнение, что при создании телекоммуникационной инфраструктуры нового Ирака будет целесообразнее сразу внедрять беспроводную передачу данных. Таким образом пропускается этап прокладки дорогих информа-

ционных магистралей. Примеры внедрения технологий Wi-Fi в странах третьего мира уже существуют. В частности, в Бутане беспроводная связь соединяет две деревеньки, одна из которых находится в горах, а вторая на равнине. Проект недорогой связи деревень спонсировала государственная телефонная компания Бутана. Таким образом обеспечена телефонная связь и даже подключение к Интернету. Посредством Wi-Fi Интернет добрался и до вершины Эвереста. В апреле 2003 г. вьючные яки доставили наверх оборудование для Интернет-кафе, из которого альпинисты смогут выходить на связь по электронной почте и телефону.

Кроме горных условий радиосвязь удобна и на морских просторах. Индонезия выбирает Wi-Fi для связи с островами, из которых преимущественно и состоит это государство. Прокладка подводного кабеля обошлась бы несравнимо дороже, а воинствующие сепаратисты, пираты и акулы значительно затрудняли бы обслуживание каналов. В Ирландии также ведутся работы по развитию беспроводной сети, которая охватит удаленные населенные пункты. А в индейских резервациях Калифорнии беспроводным образом интернетизируются школы и полицейские участки. Университет Калифорнии в Сан-Диего и компания Hewlett-Packard на собственные средства устанавливают оборудование Wi-Fi в восемнадцати резервациях округа Сан-Диего.

Итак, можно с уверенностью констатировать, что беспроводные сети стандартов 802.11 являются практически единственным на сегодня решением, пригодным для организации мобильного офиса. Широкая поддержка этих стандартов изготовителями компьютеров и сетевого оборудования дает повод надеяться, что конкуренция вскоре приведет к значительному снижению цен на беспроводные решения. Этому будет способствовать и то, что все больше производителей элементной базы объявляют о создании одночиповых контроллеров WLAN. Устройства на их основе станут как дешевле, так и компактнее, а заодно и будут потреблять меньше энергии. Вырастет и скорость передачи данных — уже есть чипы и антенны, обеспечивающие пропускную способность до 108 Мбит/с. Сейчас эта скорость доступна некоторым адаптерам 802.11g благодаря объединению двух частотных каналов, при этом максимальная скорость передачи (54 Мбит/с) увеличивается вдвое.

Глава 9. Альтернативы

Из альтернативных протоколу 802.11 способов построения беспроводной сети можно упомянуть разве что интерфейс Bluetooth да инфракрасную связь. Применение первого ограничено вследствие низкой

пропускной способности, которая не превышает 700 Кбит/с, да и радиус действия Bluetooth-связи в большинстве случаев составляет максимум 10 метров. Следует помнить и о том, что аппаратная часть технологии до сих пор остается несколько дороже оборудования для сетей Wi-Fi. Но «синезубые» устройства — как адаптеры для КПК и ноутбуков, так и точки доступа — выпускаются и продаются. Последние обойдутся в 120–150 долларов и позволят подключать до семи абонентов. Цены же на адаптеры стандарта Bluetooth 1.1 опустились в последнее время до отметки в 40 долларов.

Для инфракрасных сетей существует масса вариантов реализации, да и внедрение такой сети обойдется дешевле, так как почти все КПК и ноутбуки уже имеют инфракрасные порты. Здесь необязательна точная направленность приемника на передатчик, допустимые углы отклонения — 15–75 градусов; может приниматься и отраженный сигнал. К сожалению, дальность связи ИК-адаптеров не превышает 4 метров, так что «посотрудничать» с коллегой удастся, только сидя за одним с ним столом. Скорость инфракрасной связи может достигать 4 Мбит/с. Устройства для организации инфракрасной сети выпускает, например, компания Clarinet Systems. Кстати, в ассортименте компании (и не только ее одной) есть коммутатор, позволяющий подключать несколько КПК или лэптопов, оборудованных ИК-портами, к беспроводной сети стандарта 802.11b. Инфракрасные приемопередатчики стоят около $30–40, но принцип действия ограничивает их применение стенами одной комнаты. К тому же, невысокая скорость мало кого устроит на сегодняшний день. Использовать их можно разве что в качестве «шлюза» локальной сети для подключения наладонников, оборудованных ИК-портом.

Прочитав вышеизложенное, читатель может подумать, что сеть для мобильного офиса — благодать, доступная только топ-менеджерам, использующим связь для отслеживания котировок акций на бирже, проведения видеоконференций и прочей фантастики. Но на самом деле это еще и удобное средство для автоматизации многих бизнес-процессов. Представим себе склад, где хранятся тысячи наименований товара. Процесс передачи товара в торговый зал или филиал компании сопровождается регистрацией этого события в базе данных, осуществляемых путем ручного набора его индекса или артикула. Если номенклатура товаров достаточно обширна, недолго ошибиться и потерять товар, а затем и часть заработной платы. А если бы кладовщик и экспедитор имели при себе КПК со сканером штрих-кодов и доступом к беспроводной сети предприятия, процедура могла бы значительно ускориться. Кто стоял в очереди на оптовых складах, должен меня понять. Здесь скорость и точность обработки напрямую связаны с оборотом денежных средств, так что сеть Wi-Fi на складе оправдает себя очень быстро.

Торговый зал — еще один кандидат на автоматизацию. Очень часто встречается ситуация, когда менеджер не может рассказать о преимуществах одного высокотехнологичного товара перед другим или просто дать ему исчерпывающие характеристики. КПК с тем же сканером штрих-кодов очень помог бы ему в этом случае. Отослать распознанный артикул товара на сервер БД предприятия и получить описание товара (из той же базы данных, что представлена на веб-сайте компании) можно за несколько секунд. Эффективно и эффектно — мнение потрясенного покупателя о «продвинутом магазине» будет однозначно положительным. А вслед за ним вашу торговую точку обязательно посетят и его знакомые, с которыми он не замедлит поделиться впечатлениями.

Получить информацию о товаре можно не только путем сканирования штрих-кода. Можно использовать электронные метки — миниатюрные радиочипы, прикрепленные на каждую единицу товара. Сейчас ведутся активные разработки в этом направлении, чему способствует и поддержка маркетологов, намеревающихся таким образом заодно изучать покупателей. Кстати, радиочипы более эффективно, чем магнитные ярлыки, предупреждают хищение товара.

Резюмируя сказанное, заключу — беспроводные технологии могут найти место практически в любой области торгового бизнеса. Находится ли бизнесмен в кабинете, летит ли на деловую встречу, осматривает ли склады — быстрая и надежная связь всегда пригодится ему и его работникам. И реальным вариантом ее обеспечения сегодня являются беспроводные сети Wi-Fi.

Часть 5. Windows XP SP2: настройка беспроводной сети и брандмауэра

Глава 1. Что нового в SP2?

Как и предполагалось, новые функции SP2, в первую очередь, затрагивают наиболее актуальные сегодня направления: безопасность системы и беспроводную связь.

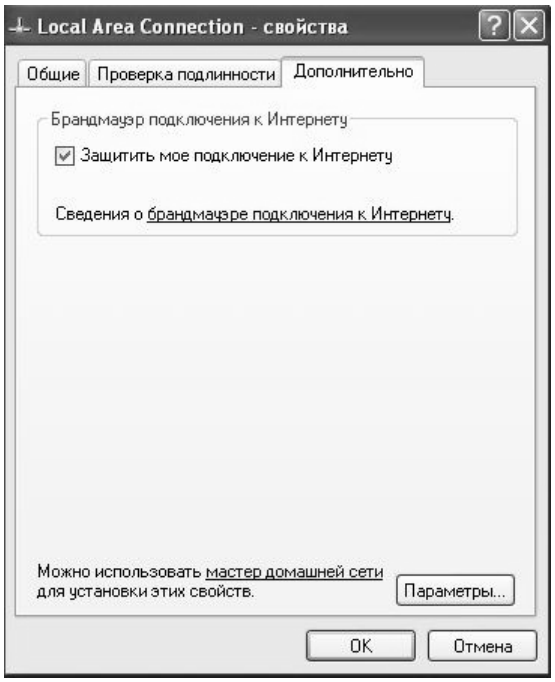
Новый межсетевой экран Windows

В Windows XP SP2 появился новый межсетевой экран (Windows Firewall), заменивший Internet Connection Firewall (ICF) в Windows XP с SP1 и в «чистой» установке. Межсетевой экран запрещает пришедший из Интернета трафик, пропуская:

- информацию, которая пришла в ответ на запрос с вашего ПК;
- информацию, соответствующую правилам заданных фильтров.

В SP2 брандмауэр был усовершенствован. Впрочем, напомню, что в системах на ядре NT5 (Windows 2000, XP) уже присутствует неплохой брандмауэр, доступный через Windows IP Security Policy (**Локальная политика безопасности ⇨ Политика безопасности IP**).

В Windows XP с SP1 и в «чистом» варианте брандмауэр ICF по умолчанию был отключен для всех соединений. Включить его можно было с помощью Мастера при создании нового подключения к Интернету, или через закладку «**Дополнительно**» в свойствах соединения. При этом допускалось пропускание трафика снаружи по фильтрам портов TCP или UDP.



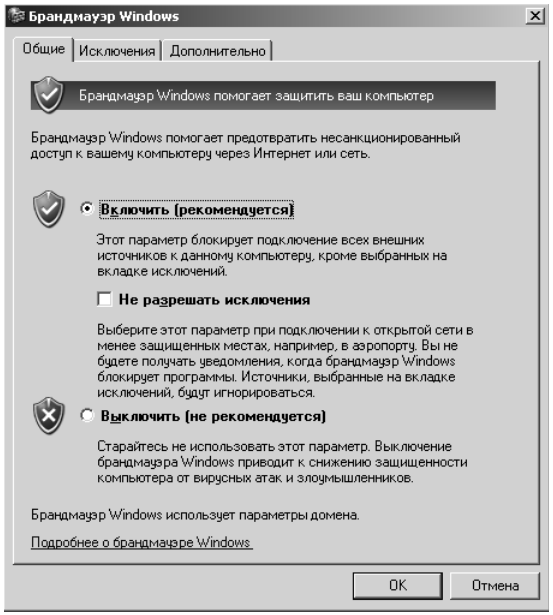
В Windows XP SP2 произошло много изменений, в том числе:

- система защищена с самого начала работы;
- брандмауэр используется по умолчанию для всех соединений;
- настройки едины для всех соединений (хотя можно выбирать соединения, на которые будут действовать правила);
- разрешение пропускания трафика как по портам, так и по программам;
- разрешение пропускания трафика по диапазонам IP-адресов;
- встроенная поддержка IP шестой версии;
- новые возможности конфигурации через утилиту netsh или групповую политику.

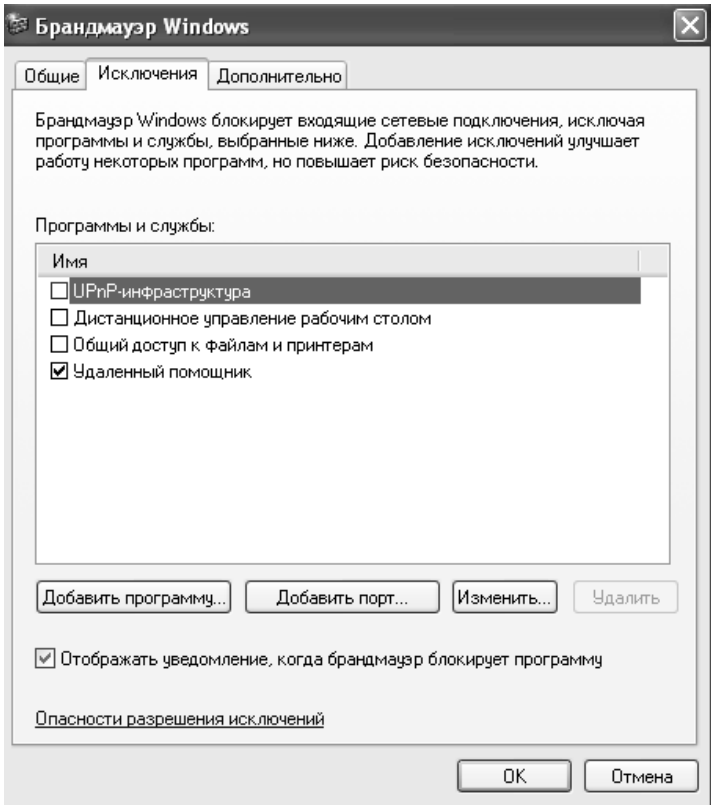
Глава 2.
Настройка межсетевого экрана Windows

Для перехода к настройке брандмауэра Windows можно воспользоваться значком панели управления «**Центр обеспечения безопасности**», нажав который, вы запустите интерфейс управления. В нижней части «**Настройки параметров безопасности**» выберите «**Брандмауэр Windows**». (***Примечание:*** если в «**Панели управления**» у вас включен классический вид, то просто выберите значок «**Брандмауэр Windows**»). На первой странице можно включить/выключить брандмауэр, а также задействовать параметр «**Не разрешать исключения**», что удобно использовать при подключении к сетям, надежность которых не гарантирована. Скажем, когда вы работаете в публичном хот-споте. При этом настройки на закладке «**Исключения**» игнорируются.

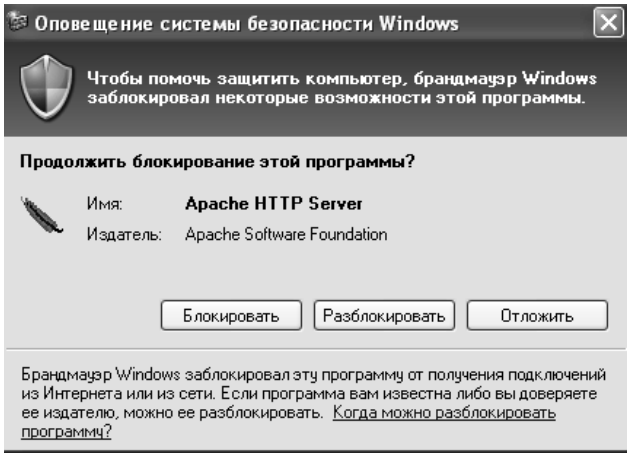
Приведу типичный сценарий: в локальной сети вашей организации вы отдали папку на вашем ноутбуке в общий доступ (установили исключение «**Общий доступ к файлам и принтерам**»). Затем вы уезжаете в командировку — и подключаетесь к гостевой сети, чтобы почитать почту. В этом случае и следует устанавливать галочку «**Не разрешать исключения**», чтобы к вашей папке никто не получил доступ.



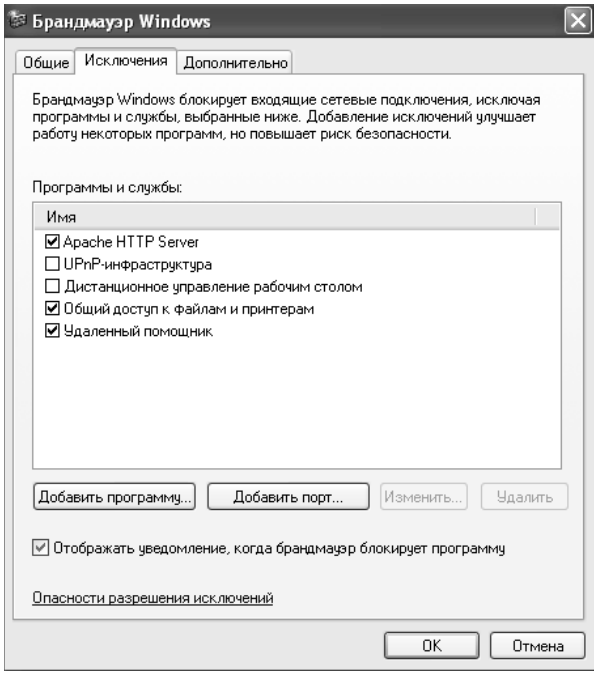
Если вы используете Интернет только для просмотра web-страниц или чтения почты, то исключения вам не потребуются вообще. Они нужны в том случае, если на вашем компьютере работают какие-либо специальные или серверные программы (ftp-сервер, www-сервер), или вы желаете предоставить доступ к своим папкам в сеть. Чтобы настроить исключения, необходимо перейти на закладку «**Исключения**». Здесь уже присутствует несколько служб по умолчанию. Отметим, что закладка «**Дополнительно**» позволяет указывать исключения отдельно по соединениям. На закладке «**Исключения**» указываются исключения, которые будут действовать для всех соединений.



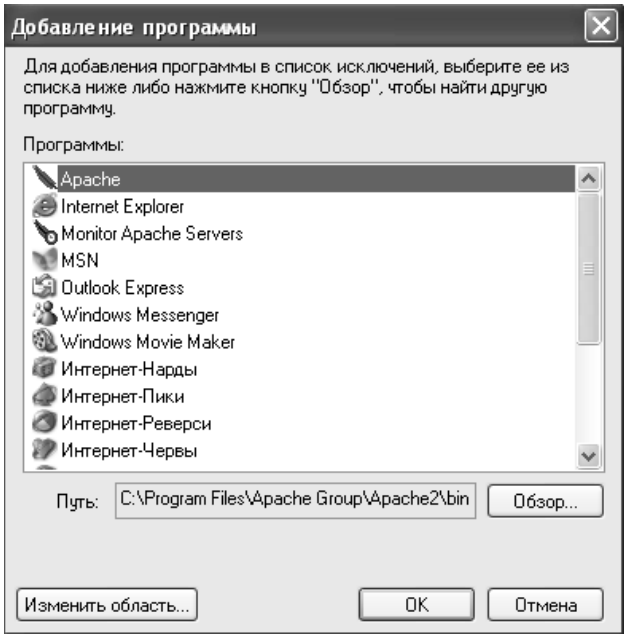
В принципе, во время установки программы Windows XP сама предупредит вас, что для нее следует добавить исключение.

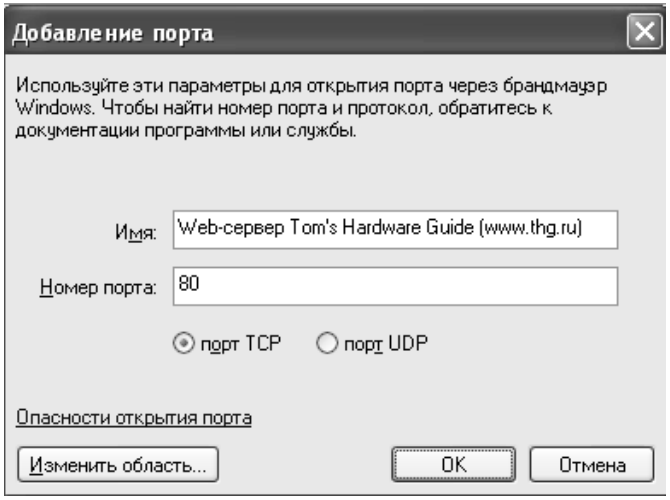


Если вы нажмете клавишу «**Разблокировать**», то для данной программы (web-сервера Apache) будет добавлено исключение.



Исключения можно добавлять и вручную. Для этого следует воспользоваться клавишами «**Добавить программу**» или «**Добавить порт**».



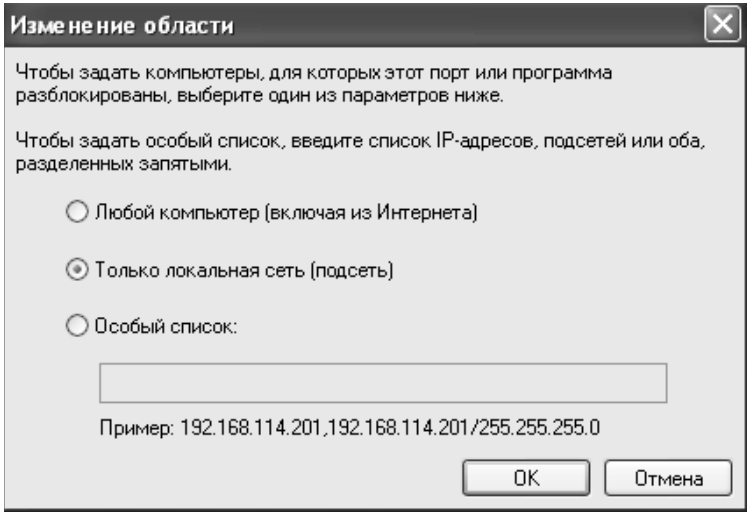


Для добавления исключения вы можете использовать либо программу, либо порт — подойдет любой из этих способов. Пользуйтесь тем, который вам удобнее.

Обратите внимание, что для каждого исключения можно задать область действия:

- любой компьютер (включая из Интернета);
- только локальная сеть (подсеть);
- особый список.

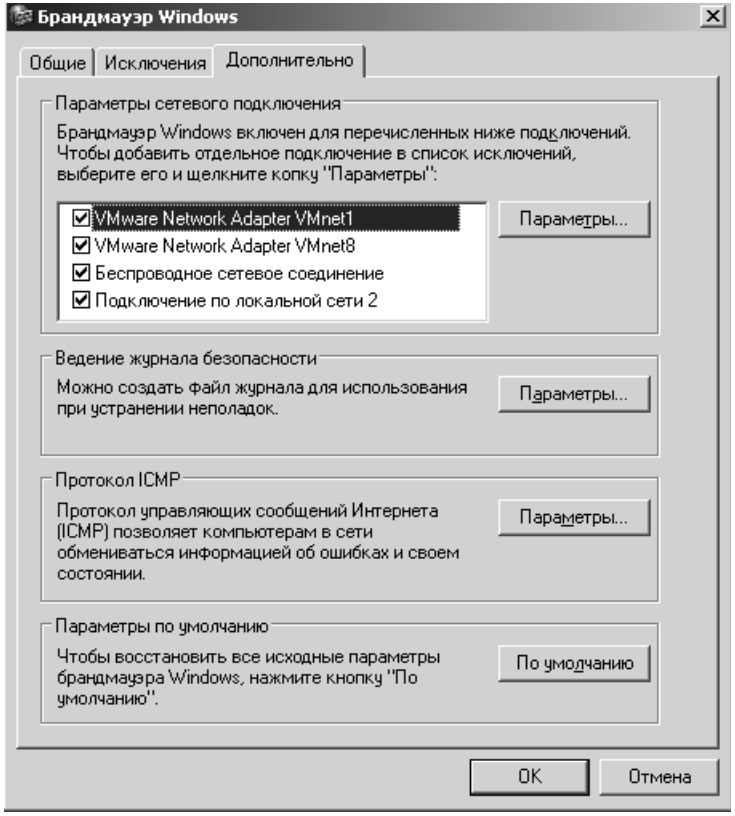
Последний вариант позволяет задать список IP-адресов (включая маску), для которых будет действовать исключение. Следует отметить, что тот же «Общий доступ к файлам и принтерам» Windows по умолчанию ограничивается только локальной сетью. Так что хакеры из Интернета к вам не проберутся.



Изменить область можно при добавлении исключения (клавиша «**Изменить область**») или позже, выбрав исключение и нажав клавишу «**Изменить**», а затем «**Изменить область**».

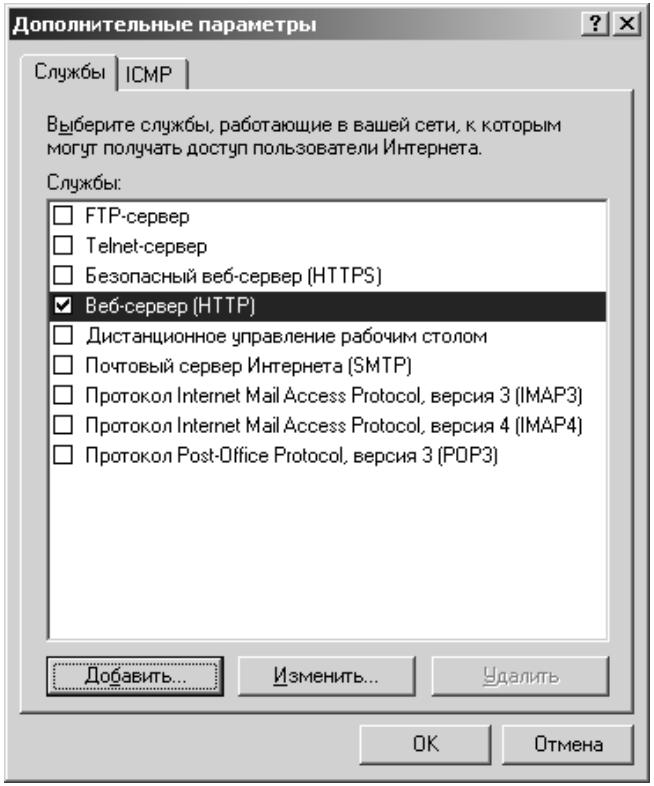
В нижней части закладки исключений находится флажок «**Отображать уведомление, когда брандмауэр блокирует программу**». Если вы желаете, чтобы соответствующее окно с сообщением появлялось при каждом таком случае, то флажок следует установить, если же не хотите отвлекаться, — убрать.

Последняя закладка настроек брандмауэра «**Дополнительно**» бывает очень полезна. Начнем с того, что брандмауэр можно включать или выключать для определенного сетевого соединения.



Скажем, вы можете полностью отключить брандмауэр для локальной сети (просто убрав галочку) и оставить его для беспроводной сети или подключения к Интернету. Впрочем, лучше так не делать — воспользуйтесь исключениями.

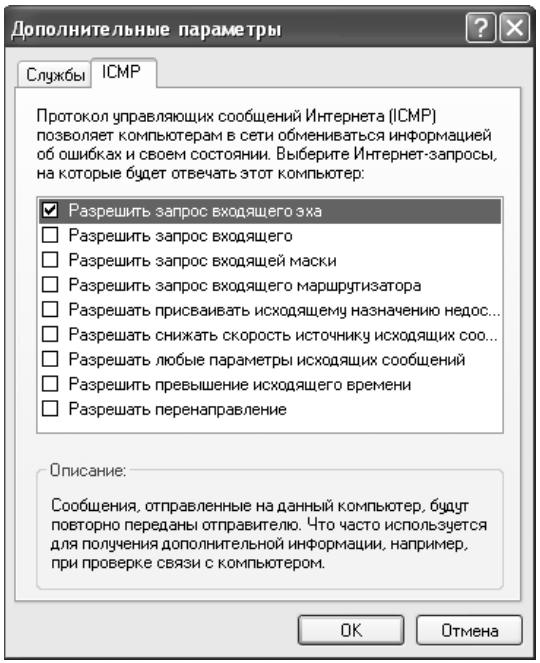
На закладке «**Дополнительно**» можно настроить брандмауэр отдельно для каждого подключения. Например, тот же web-сервер Apache можно использовать для обслуживания только клиентов локальной сети. Для этого удалите исключение (закладка «**Исключения**»), а затем на закладке «**Дополнительно**» выберите нужное сетевое соединение (скажем, локальную сеть) и нажмите клавишу «**Параметры**».



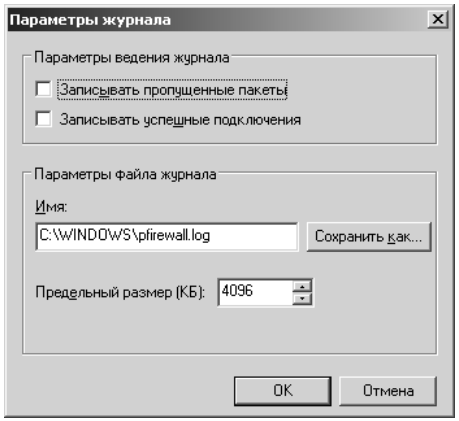
В данном примере достаточно указать службу «**Веб-сервер (HTTP)**». После этого клиенты локальной сети смогут подключаться к вашему web-серверу. Также вы можете добавить и свою службу (клавиша «**Добавить**»), но для этого необходимо знать ее рабочий порт. Отметим, что добавить исключения по приложению здесь не получится — эта функция работает только для общих исключений (закладка «**Исключения**»).

Здесь же, в окне «**Дополнительные параметры**» можно регулировать работу протокола ICMP для каждого соединения (закладка «**ICMP**»).

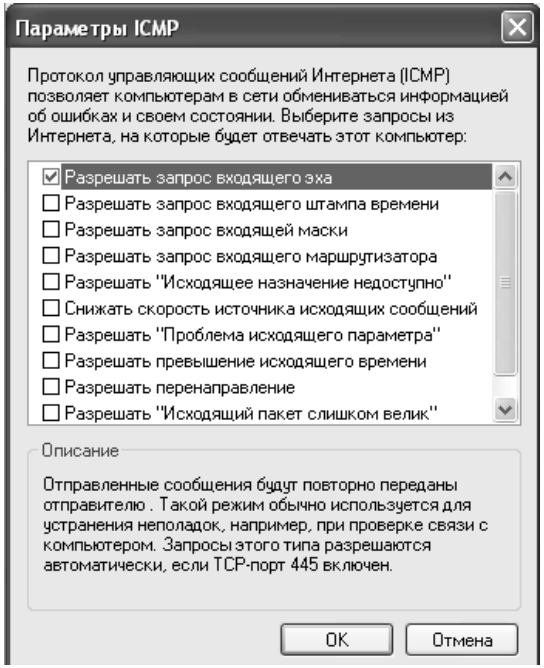
Мы рекомендуем указывать галочку «**Разрешить запрос входящего эха**», чтобы вы могли проверять работу сети командой «ping» с других компьютеров на ваш. Впрочем, ICMP можно настроить и для всех подключений сразу.



Следующей на закладке «**Дополнительно**» идет область «**Ведение журнала безопасности**». Клавиша «**Параметры**» позволяет задать название файла журнала, размер и параметры записей. Включив ведение журнала, вы сможете отслеживать работу брандмауэра.



Область «**Протокол ICMP**» на закладке «**Дополнительно**» позволяет установить параметры ICMP сразу для всех соединений.



Опять же, мы рекомендуем указывать галочку «**Разрешить запрос входящего эха**», чтобы вы могли проверять работу сети командой «ping» с других компьютеров на ваш.

Наконец, последний пункт «**Восстановить умолчания**» на странице «Дополнительно» позволяет вернуть все параметры к исходным.

Глава 3. Беспроводные сети в Windows XP SP2

В SP2 Microsoft улучшила работу с беспроводными сетями, внеся следующие изменения.

- **Встроенная поддержка WPA**. Если ранее для этого требовалось скачать дополнение, то теперь все необходимые параметры задаются на закладке свойств

соединения. Естественно, для этого адаптер и драйвер должны поддерживать WPA.

- **Служба простой настройки беспроводной сети**. Это обновление позволяет автоматизировать и упростить настройку беспроводных соединений, что облегчит подключение к хот-спотам.
- **Мастер настройки беспроводной сети**. Он позволяет выполнить пошаговую настройку беспроводной сети и сохранить конфигурацию на USB-брелок, который в дальнейшем можно будет использовать для настройки других систем.
- **Журналирование службы Wireless Zero Configuration**. Служба отвечает за обнаружение и подключение к предпочтительным беспроводным сетям, поэтому ее журналы помогут разобраться в возможных проблемах установки соединения.
- **Восстановление беспроводного соединения**. Для того чтобы воспользоваться восстановлением, достаточно щелкнуть правой кнопкой мыши по ярлычку соответствующего соединения и в контекстном меню выбрать «**Восстановить**». На самом деле, выполнится лишь отключение и повторное включение соединения.

Изменилось поведение при использовании аутентификации 802.1x. При автоматическом отключении беспроводного клиента, когда аутентификация не проходит, 802.1x автоматически отключается при ручном задании ключа шифрования.

Существенным изменениям подверглось и окно беспроводных сетевых соединений.

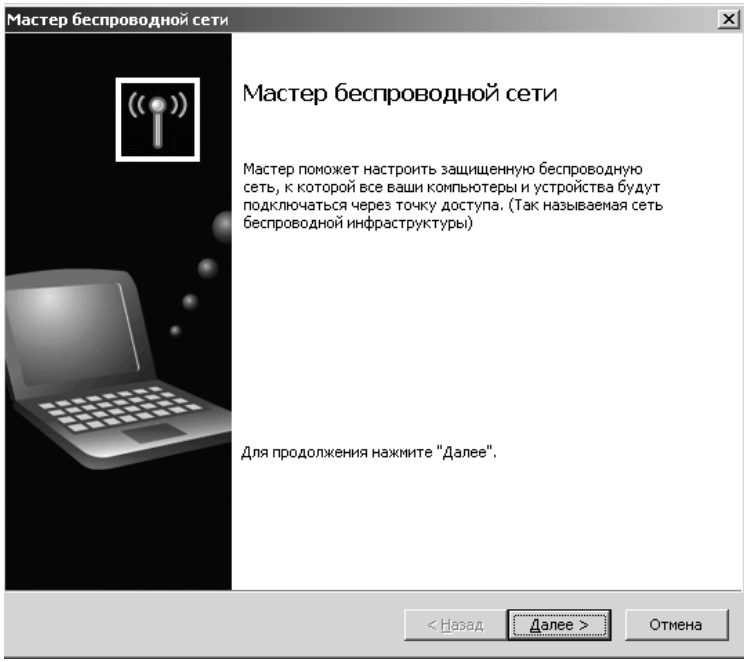
Глава 4. Доступные сети

Здесь, как и раньше, отображается список всех доступных сетей, причем для просмотра доступны такие параметры, как имя сети, тип сети (Ad-Hoc или Infrastructure). Из новинок следует отметить появление уровня сигнала (индикатор в правой части окна доступной сети), защиты сети, статуса (для подключенной сети отображается специальный значок) и предпочтительной сети.

Теперь можно одной клавишей запускать поиск доступных сетей, установку беспроводных сетей, изменять порядок предпочтений, просматривать свойства беспроводных соединений.

Процесс подключения теперь отображается и виден пользователю. Если подключение удалось, и доступ оказался разрешен, то следующим этапом будет получение сетевого адреса. Если адрес получить не удалось, то есть сервер DHCP недоступен, то адаптеру будет автоматически присвоен адрес из диапазона 169.254.0.0/16, что отобразится на статусе соединения (предупреждение со знаком восклицания). То есть уже с первого взгляда становится понятен статус соединения: подключено, отключено, ограничено или соединение устанавливается.

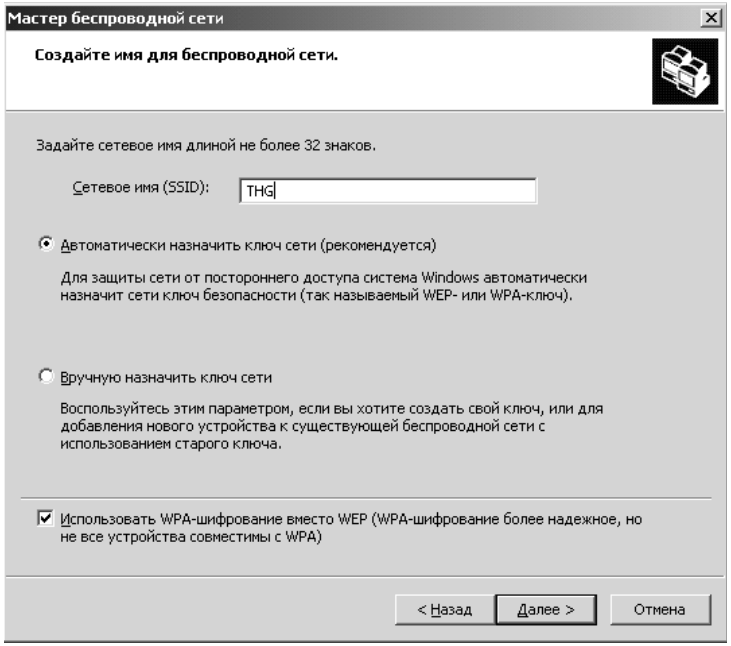
Глава 5. Устанавливаем беспроводную сеть



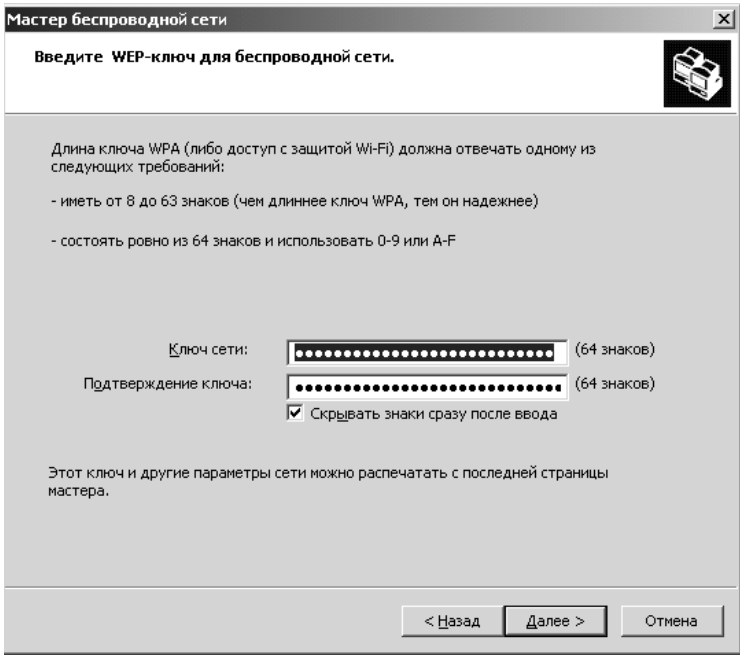
Настройка беспроводной сети также значительно упростилась. Начнем с создания беспроводной сети. Сначала нужно зайти в «**Сетевое**

окружение» и выбрать пункт «**Установить беспроводную домашнюю сеть или сеть малого офиса**», после чего запустится Мастер установки сети. Можно пойти и другим путем: **Пуск ⇨ Все программы ⇨ Стандартные ⇨ Связь ⇨ Мастер настройки беспроводной сети**. Следует отметить, что Мастер позволяет настраивать только сети с использованием точки доступа (режим **Infrastructure**). Если вы планируете развернуть сеть AdHoc (без точки доступа, на базе только беспроводных карт), то придется воспользоваться ручной настройкой.

Следующий экран предлагает задать имя SSID, которое должно быть единым для всей сети, определить способ назначения ключей шифрования и выбрать непосредственно способ шифрования (WEP или WPA — с помощью галочки в нижней части окна). Позволим себе в очередной раз напомнить, что защита WEP не слишком надежна, хотя для домашней сети ее будет достаточно. Если есть возможность, лучше использовать WPA (если адаптер и драйвер поддерживают его — обратитесь к документации).

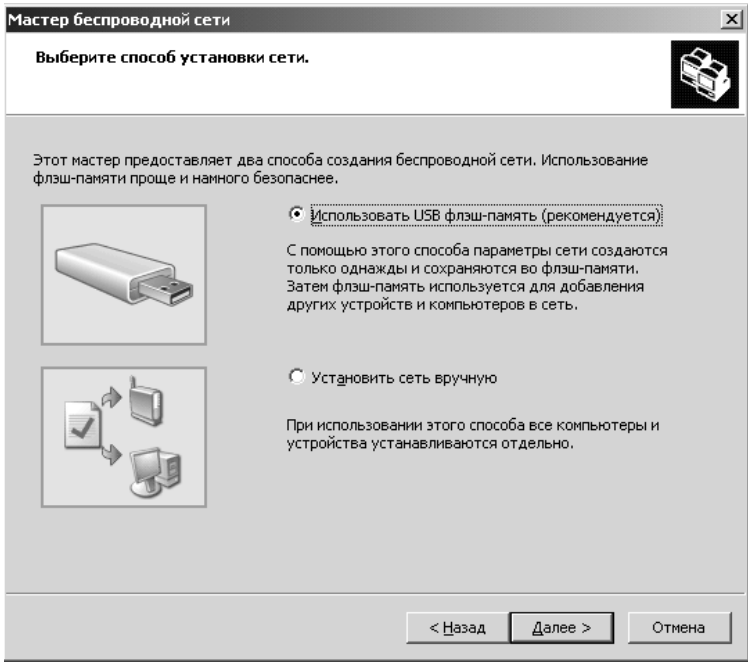


Ключи шифрования можно либо назначить автоматически, либо указать собственные. При выборе собственных появится следующее окно с предложением ввода ключей.

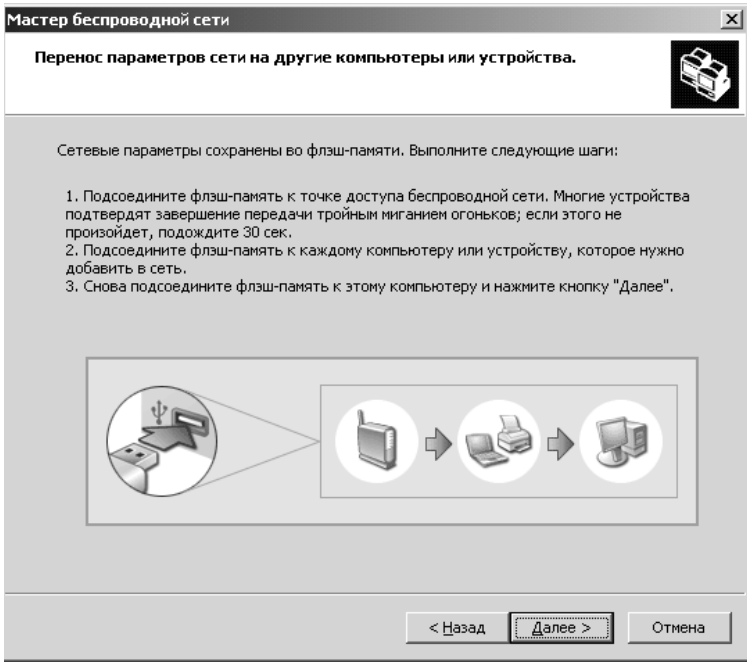


При автоматической генерации этот шаг будет пропущен.

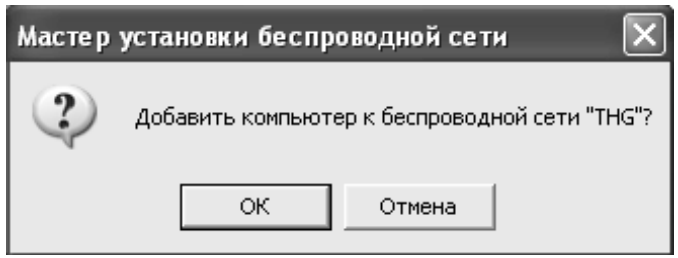
После назначения всех необходимых параметров переходим к следующему экрану. Вам будет предложено либо использовать флэш-брелок, либо настроить сеть вручную.



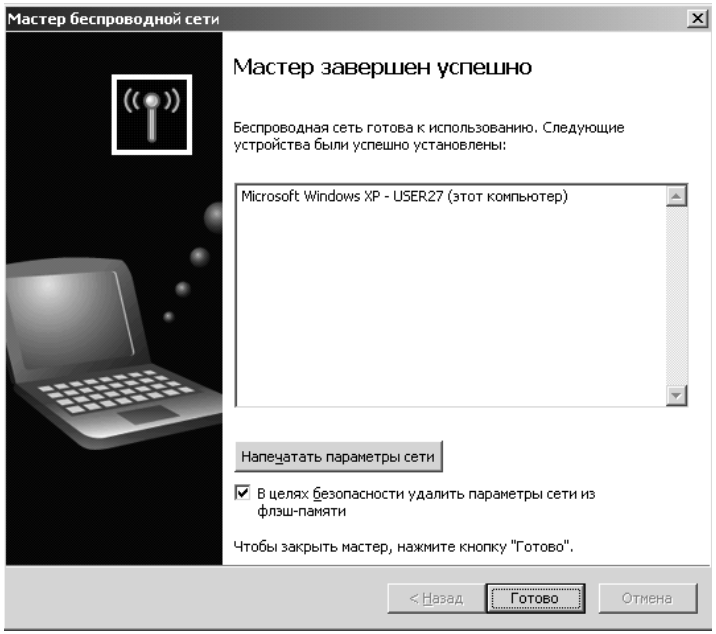
Первый способ позволяет легко переносить конфигурацию на другие компьютеры беспроводной сети. Для этого достаточно провести процедуру настройки лишь однажды, сохранив при этом все параметры на брелок. Кстати, если точка доступа не поддерживает ввод информации с USB-брелоков, то ее придется настроить вручную.



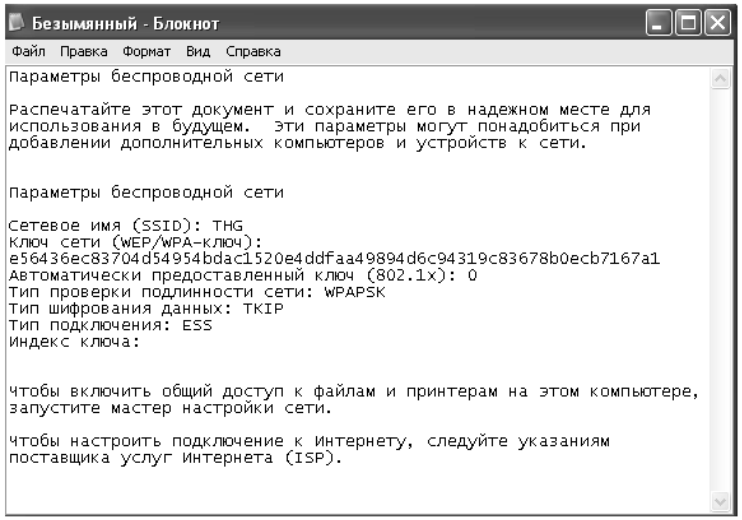
Теперь, следуя инструкции, необходимо отсоединить брелок и подключить его ко всем компьютерам, которые необходимо добавить в сеть.



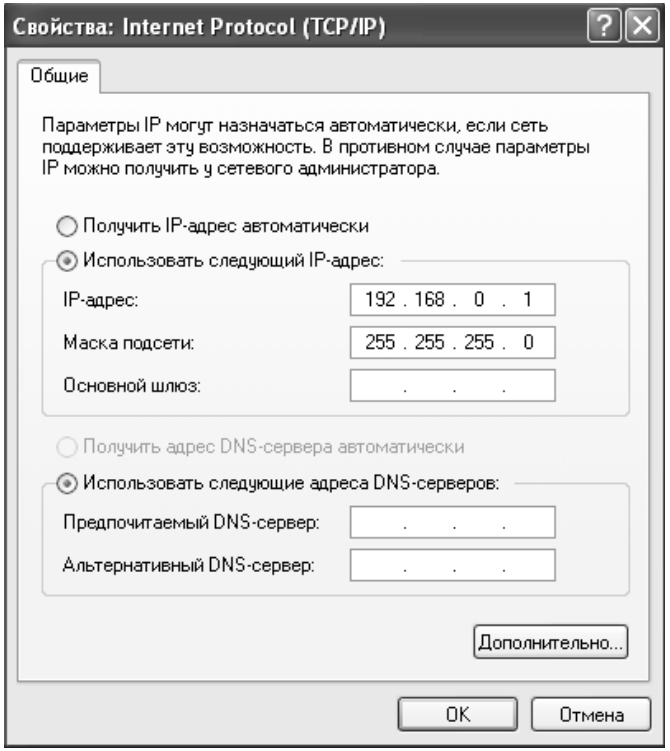
Когда вы подключите брелок к другому компьютеру, то появится приглашение добавить его в вашу беспроводную сеть. Если приглашения не появилось, запустите вручную с брелока файл setupSNK.exe. После того, как вы обойдете с брелоком все компьютеры, вставьте его обратно в первый и завершите работу Мастера.



После этого не забудьте распечатать параметры сети.



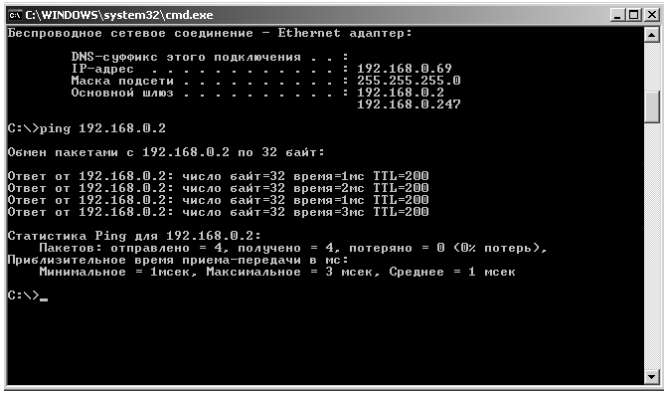
Сейчас вы можете подключаться к установленной беспроводной сети. Но для работы необходимо еще и ввести IP-адреса на каждом компьютере. Для этого следует выбрать сеть 192.168.x.y, где x — номер вашей сети (от 0 до 255), а y — номер компьютера в сети (от 1 до 254). В вашей сети все компьютеры должны иметь одинаковый номер сети и разный номер компьютера. Скажем, 192.168.0.1, 192.168.0.2 и т.д. IP-адрес задается в свойствах соединения (найдите значок соединения, нажмите на нем правую клавишу мыши и выберите «**Свойства**»). Затем на закладке «**Общие**» выберите протокол «**Internet Protocol (TCP/IP)**» и нажмите клавишу «**Свойства**». В появившемся окне выберите «**Использовать следующий IP-адрес**». В качестве маски укажите 255.255.255.0.



Выполните процедуру ввода IP-адреса на всех компьютерах.

Для проверки соединения можно воспользоваться утилитой ping. Для этого нужно запустить командную строку (**Пуск ⇨ Выполнить**) набрать в ней «**cmd**», подтвердить ввод. В командной строке наберите «**ping**»

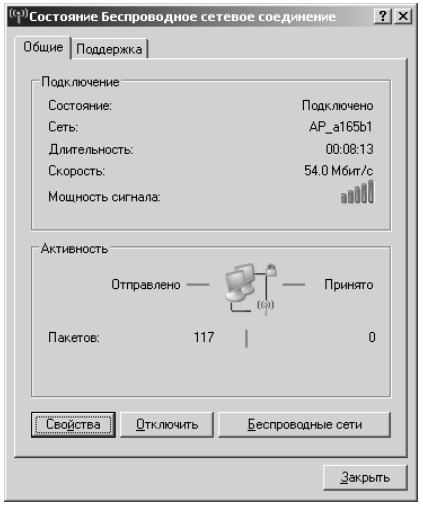
и укажите IP-адрес другого компьютера (к примеру, 192.168.0.2). Кстати, у вас может быть отключена поддержка исключения ICMP — тогда ping-ответа вы не получите.



Если связь есть, то вы получите ping-ответы, как показано на иллюстрации.

Поздравляю, ваша сеть настроена.

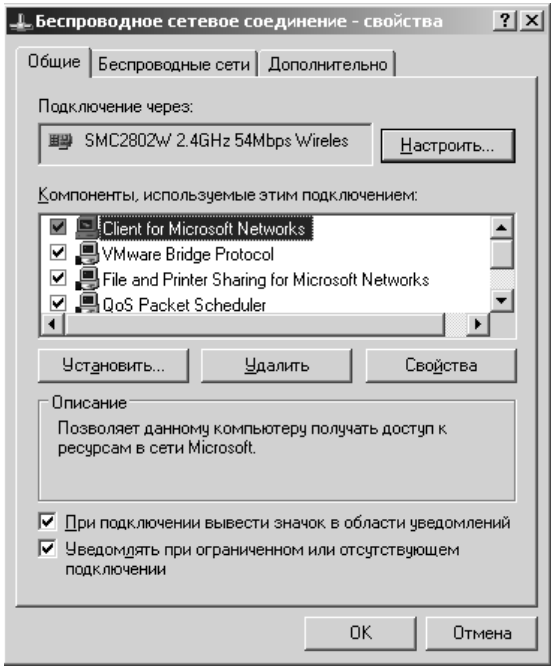
Информацию о работе беспроводной сети вы можете получить в окне состояния соединения. Для этого нажмите правой клавишей мыши на значок соединения и выберите «**Состояние**».



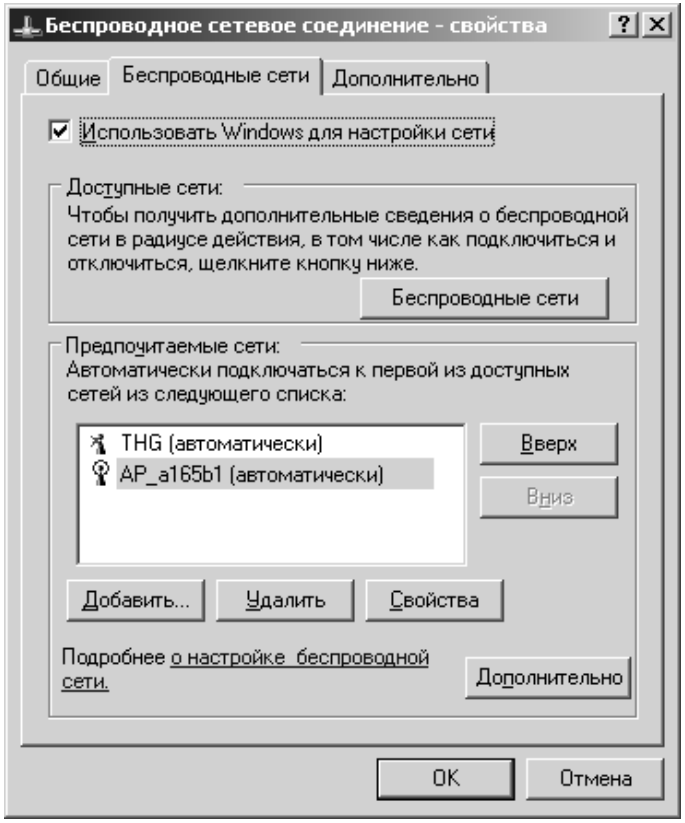
В окне состояния соединения отображается состояние соединения (подключено, отключено или подключение ограничено или отсутствует), имя сети, то есть SSID, продолжительность соединения, скорость соединения и мощность сигнала. Если у иконки соединения виден знак восклицания, это означает, что соединение ограничено или отсутствует, то есть системе не удалось получить IP-адрес. Замок говорит о защите соединения.

Глава 6. Настройка беспроводной сети без точки доступа (режим AdHoc)

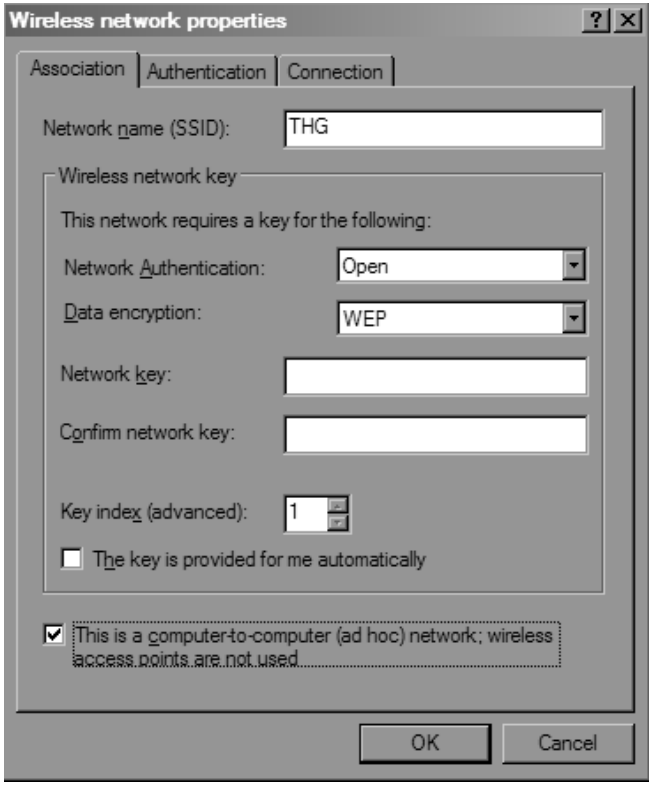
К сожалению, Мастер настройки беспроводной сети не позволяет создавать сеть AdHoc — то есть сеть без точки доступа, только между адаптерами. Чтобы ее настроить, нажмите правой клавишей мыши на значок беспроводного адаптера (соединения) и выберите «**Состояние**» (Status). Затем перейдите в окно «**Свойства**» (Properties).



В этом окне выберите закладку «**Беспроводные сети**» (Wireless Networks).



Нажмите клавишу «**Добавить**» (Add).



В появившемся окне следует указать имя вашей сети (например, «THG»), а также ключ шифрования WEP или WPA (если поддерживается адаптерами). Снимите галочку автоматической генерации ключа и наберите его вручную. Также в нижней части окна поставьте галочку, указывающую на сеть AdHoc. Затем укажите для адаптера IP-адрес.

После того, как вы создали беспроводную сеть на одном компьютере, вам следует добавить к ней остальные компьютеры. Это сделать еще проще. В окне «**Состояние**» (Status) беспроводных соединений других компьютеров нажмите клавишу «**Беспроводные сети**» (View Wireless Networks). Там вы должны увидеть только что настроенную сеть, к которой легко сможете подключиться. При этом необходимо будет ввести ключ WEP (или WPA), а также указать IP-адрес.

Изменения, пришедшие со вторым пакетом обновления (Service Pack 2) для Windows XP затронули беспроводные сети и брандмауэр. Но-

вый Мастер установки позволяет последовательно задать все необходимые параметры для подключения к выбранной сети, а возможность сохранения конфигурации на флэш-брелок позволяет облегчить настройку других беспроводных станций, что очень удобно в крупной сети.

Новый межсетевой экран обладает не только хорошей гибкостью, но и достаточно удобным интерфейсом, что немаловажно для массового использования продукта. Сейчас можно разрешать доступ не только по портам, но и по приложениям.

Глава 7. Детектор беспроводных сетей PCTEL: ищем точки доступа

Детектор не так прост, как может показаться с первого взгляда. На самом деле он определяет только точки доступа, не обращая внимания на адаптеры в режиме AdHoc. Я также пытался определить точки доступа в режиме моста WDS, но все усилия оказались бесполезны, чего нельзя сказать о режиме повторителя. Детектор успешно обнаружил точку доступа, работающую повторителем WDS, но терял ее при переключении в режим моста.

Беспроводные клиенты в режиме бездействия не влияют на работу устройства. Сначала отключал беспроводной адаптер при работе детектора. Позже выяснилось, что он никак не реагирует на беспроводной адаптер, даже когда он подключен к WRT54GS, но не передает данные! Также детектор никак не реагирует на встроенный адаптер Bluetooth H2210 iPAQ, находящийся в режиме поиска других устройств.

Если вы относите себя к мобильным пользователям, которым часто бывает необходимо определить наличие беспроводной сети, то это детектор — именно то, что нужно.

Часть 6. Руководство по решению проблем: настройка моста/повторителя WDS

Глава 1. Технология WDS

Термин WDS расшифровывается как «беспроводная система распределения» (Wireless Distribution System), которая поддерживается все большим количеством точек доступа 802.11. Проще говоря, она позволяет точкам доступа устанавливать беспроводное соединение между собой, вместо того, чтобы использовать проводные Ethernet-каналы.

Соединения WDS основываются на MAC-адресах и используют специальный тип кадров, в которых задействованы все четыре поля для MAC-адресов, определенные стандартом 802.11, вместо трех при обычной передаче данных между точкой доступа и клиентом.

Использование четырех полей MAC-адресов в кадре — единственное, что реализовано в стандартах 802.11, но этого оказалось достаточно для реализации функций моста в точках доступа уровня предприятия, то есть в дорогих моделях 802.11b, появившихся еще в конце 90-х годов прошлого века. Те решения работали на уровне доступа к среде передачи данных (MAC), а технология была разработана компанией Choice Microsystems.

Точки доступа с функцией беспроводного моста оставались весьма дорогими примерно до осени 2002 года, когда беспроводные мосты перешли в разряд массовых устройств. Известная многим компания D-Link была первой, кто снизил цену устройств подобного класса, выпустив бесплатное обновление прошивки к своей точке доступа DWL-900AP+.

Благодаря этому обновлению, на рынке появился первый недорогой продукт, поддерживающий функции моста и повторителя. Другие

компании вслед за D-Link тоже выпустили подобные обновления, а также представили беспроводные мосты в виде самостоятельных устройств, например, Linksys WET11.

Хотя в этих устройствах уже использовалась технология WDS, о ней ничего не упоминалось. Такое положение сохранялось до тех пор, пока на рынке не стали появляться продукты 802.11g на базе чипсета Broadcom, что произошло в начале 2003 года. Именно тогда термин WDS и начал широко использоваться. Broadcom включила поддержку WDS в программное обеспечение, и вскоре точки доступа стандарта 802.11g с поддержкой WDS набрали популярность.

WDS может использоваться для реализации двух режимов беспроводных соединений между точками доступа:

- режим беспроводного моста — позволяет точкам доступа работать только с другими точками доступа, но не с клиентскими адаптерами
- режим беспроводного повторителя — позволяет точкам доступа работать как с другими точками доступа, так и с клиентскими адаптерами

Недостатки WDS

Пропускная способность такого беспроводного соединения уменьшается примерно вдвое для каждого такого соединения, или «хопа». Это связано с тем, что при передаче и приеме всеми устройствами используется один канал, по которому данные передаются в проводную сеть.

Динамически распределенные и обмененные ключи не поддерживаются в соединениях WDS. Это означает, что WPA и другие технологии, использующие динамическое распределение ключей, несовместимы с WDS. Могут применяться только статические ключи WEP. Это также распространяется и на всех клиентов, подключенных через точки доступа WDS.

Глава 2. Совместимость реализаций WDS

Как уже упоминалось, единой спецификации WDS пока нет, хотя ситуация может вскоре измениться, если исследовательская группа IEEE, сформированная в начале этого года, получит статус «рабочей группы» (task group). А пока забота о совместимости различных моделей

целиком лежит на производителях оборудования, которые не прилагают никаких усилий, чтобы пользователи могли строить сети из оборудования различных моделей.

В итоге, производители указывают в документации, что режим моста и повторителя будет работать только с оборудованием этой же компании. И даже если прямого указания на проблему совместной работы режима WDS не будет, получить консультацию по вопросу совместимости устройства одного производителя с устройством другого будет практически невозможно!

К счастью, многие продукты 802.11g с поддержкой WDS выполнены на базе чипсетов от Broadcom, которая имеет стандарт де-факто в отношении реализации WDS в своем оборудовании. Но производители оборудования используют различные интерфейсы.

Поэтому нельзя гарантировать, что устройства с функцией беспроводного моста/повторителя WDS, выпущенные различными производителями, будут работать вместе! В некоторых случаях вам может не удастся установить соединение, даже если оба устройства выпущены одним производителем! Это может быть связано с тем, что они могут быть произведены различными OEM/ODM.

К счастью, со временем, после выпуска обновленных прошивок, шансы на успешную совместную работу продуктов WDS от разных производителей только возрастают. Тогда основным препятствием становится разная терминология, используемая разработчиками интерфейсов для мостов/повторителей. Один из примеров борьбы с подобной путаницей разобран ниже.

Примечание: Не хотелось бы повторяться, но снова отметим: продукты WDS от различных производителей не обязательно будут работать вместе. Поэтому лучше всего (и проще, с точки зрения работы с техподдержкой) использовать одинаковые модели устройств WDS от одного производителя. Если обойтись одной моделью не получается, то следует остановиться на нескольких моделях одного производителя. Вероятность того, что они будут работать вместе, достаточно велика.

Глава 3.
Шаги к успешной реализации WDS

Перед тем, как перейти к настройке, необходимо провести подготовительную работу, чтобы в дальнейшем не возникло проблем.

Ниже приведены три обязательных и два дополнительных шага, через которые рекомендуется пройти.

- Убедитесь, что беспроводные клиенты могут подключаться и передавать данные через все точки доступа. Подобную проверку достаточно просто сделать, если подключить точки доступа к сети через Ethernet-порты. Тогда можно будет гарантировать работу беспроводной сети.
- Задайте для каждой точки доступа постоянный IP-адрес. Вообще, такое решение достаточно удобно при настройке сетевого оборудования. Присваивая статические IP-адреса, вы избавляетесь еще от одного потенциального препятствия при решении проблем связи. Убедитесь, что присвоенные адреса исключены из диапазона DHCP-сервера, иначе вы рискуете оказаться в ситуации, когда в сети будет два одинаковых адреса, а в этом мало приятного!
- Установите на всех точках доступа один и тот же (свободный) канал. Поскольку все точки доступа в сети WDS передают данные между собой, они должны использовать один канал. Для сетей 802.11b и 11g мы рекомендуем использовать 1, 6 или 11 каналы. В любом случае, необходимо убедиться, что канал не используют соседние сети.
- Задайте различные SSID для точек доступа. Точки доступа WDS устанавливают соединения на основании MAC-адресов, поэтому смогут работать независимо от того, какие идентификаторы SSID заданы. С другой стороны, беспроводные клиенты при подключении используют SSID. С технической точки зрения, каждая точка доступа в сети WDS является частью одной зоны обслуживания (ESS) и должна иметь один и тот же SSID.

Алгоритмы роуминга большинства беспроводных клиентов между точками доступа реализованы таким образом, что клиенты не переключаются с одной точки доступа на другую, пока есть хоть какое-то соединение, пусть даже в ущерб скорости работы. Эта особенность становится неприятной, когда вы добавили повторители к вашей WLAN, а ноутбук отказывается с ними работать!

Присвоив различные SSID точкам доступа, вы сможете видеть каждую из них, даже используя стандартную утилиту WinXP «Zero Config», которая не отображает точки доступа с одинаковыми SSID. Кроме этого, клиенты сети без труда смогут переключаться на любую точку доступа, даже не зная ее MAC-адрес.

Задайте статические IP-адреса для беспроводных клиентов. Но иногда динамическое получение нового IP-адреса требует достаточно много времени. Указав параметры IP для беспроводных клиентов статически (в том числе адрес шлюза и сервера DNS), вы снизите вероятность возникновения ошибок при переключении клиента от одной точки доступа к другой. Кроме того, так можно обойти проблемы передачи запросов DHCP через мостовые подключения, которые существуют у некоторых маршрутизаторов.

В дополнение ко всему написанному выше необходимо решить вопрос с размещением точек доступа. Точно так же, как у любого другого беспроводного сетевого оборудования, скорость соединений WDS зависит от силы сигнала. В связи с тем, что каждый мост WDS снижает скорость работы примерно вдвое, не стоит снижать ее еще из-за расположения точек доступа слишком далеко друг от друга.

Чтобы выбрать удачные места для установки придется попробовать различные варианты, но не думайте, что установив устройство на границе существующей сети, вы получите быстрый канал! Компромиссом здесь будет установка повторителя там, где скорость соединения (отображаемая утилитой) составляет 5,5 Мбит/с или выше для 11b и 24 Мбит/с или выше для 11a и 11g, то есть, примерно, на половине максимального расстояния.

Закончив с приготовлениями, необходимо записать MAC-адреса устройств и можно приступать!

Глава 4. Сбор MAC-адресов

Как было сказано выше, соединения WDS работают на основе физических адресов. Некоторые модели позволяют использовать режим, не требующий указания MAC-адресов каждого члена сети, но я рекомендую его не использовать, а указать MAC-адреса. Такое решение обезопасит мост (и LAN), запретив «анонимное» подключение точек доступа к мосту. Кроме того, вероятно, такое решение имеет больше шансов на успех, особенно при использовании оборудования различных производителей.

Если вы используете утилиту WinXP Wireless Zero Configuration, то, вероятно, знаете, что она отображает только SSID точек доступа, находящихся в радиусе действия. Единственный MAC-адрес, который можно увидеть с ее помощью, принадлежит адаптеру, а не точке доступа.

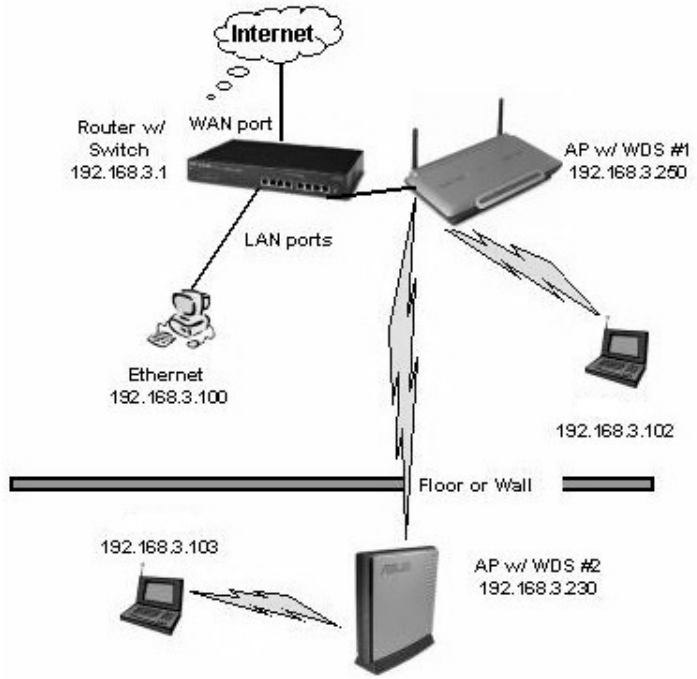
Самый простой способ узнать MAC-адреса точек доступа сети — воспользоваться утилитой, которая поставляется в комплекте с адаптером. Среди закладок с различными параметрами непременно можно встретить и список доступных точек доступа и их MAC-адреса.

Совет: в целях повышения уровня безопасности не стоит использовать простые SSID, подобные указанным на примере!

Если клиентская утилита не позволяет просматривать MAC-адреса, то можно воспользоваться интерфейсом администрирования точки доступа. Здесь стоит обратить внимание на тот момент, что некоторые модели отображают два MAC-адреса: для проводного и беспроводного интерфейсов. Если в вашем случае дело так и обстоит, то убедитесь, что записали именно MAC-адрес беспроводного интерфейса.

Пример 1: сеть с одним повторителем

На рисунке показана схема простой сети с одним повторителем и одним «хопом», которая может использоваться для увеличения радиуса действия беспроводной сети.



В этом примере использованы точки доступа 802.11g на чипах Broadcom — Belkin F5D7130 и ASUS WL300g. Хотя обе точки доступа имели схожее устройство, включая беспроводной сетевой процессор Broadcom BCM4702, ниже показано, что их интерфейсы значительно различаются в части настройки WDS.

Начнем с настройки WDS на точке доступа, подключенной к LAN. На рисунке выше показан экран настройки беспроводного моста для точки доступа.

Кстати, начать следует с подключения обеих точек доступа к проводной сети — и лишь затем осуществлять их настройку. Не стоит усложнять ситуацию, смешивая проводные и беспроводные соединения.

Верхний флажок включает мост WDS, который, кстати, отключен по умолчанию. Затем нужно «**Разрешить подключение только указанных точек доступа**» (Enable ONLY specific Access Points to connect), что делается для запрета анонимных подключений WDS. Необходимо также указать MAC-адреса тех точек доступа, которые смогут подключиться — в данном случае это адрес точки доступа ASUS.

Флажок «**Запретить подключение беспроводных клиентов**» (Disable ability for Wireless CLIENTS to connect) оставьте неотмеченным, поскольку наш сценарий настройки WDS подразумевает расширение беспроводной сети, то есть использование функции повторителя. Если флажок все же поставить, то Belkin больше не сможет работать в качестве точки доступа, и не сможет подключать к себе беспроводных клиентов. Вместо этого, она будет работать мостом между другими точками доступа и проводной сетью.

Проверка соединения WDS

Как проверить, работает ли соединение WDS? Если обе точки доступа подключены к коммутатору, то индикаторы **Link** (Соединение) и **Activity** (Передача) на вашем коммутаторе и обеих точках доступа будут активно мигать. Не пугайтесь, все нормально, это говорит о наличии двойного соединения (два MAC-адреса соответствуют одному IP-адресу) между точками доступа по проводному Ethernet и WDS.

Как только вы отключите кабель Ethernet от удаленной точки доступа (в нашем примере ASUS WL300g), мигание прекратится. Сейчас можно оставить точки доступа, запустить командную строку (сеанс MS-DOS) и отправить запрос ping на IP-адрес удаленной точки доступа. Если соединение WDS работает, то вы получите серию эхо-ответов на запрос ping. Соединение WDS работает!

Теперь пора задействовать ноутбук с беспроводным адаптером. Убедитесь, что в списке доступных сетей видны имена обеих точек доступа, попробуйте подключиться к каждой из них по очереди. (Теперь понятно, для чего нужно задавать различные SSID?)

Если все работает, то можно выключить удаленную точку доступа и установить ее в желаемое место. Затем подключить питание, подождать, пока она загрузится, и повторить тесты. Поздравляем! Вы только что увеличили радиус действия вашей беспроводной сети!

При проведении тестирования, ноутбук с адаптером NETGEAR WG511T 11g CardBus был размещен таким образом, чтобы уровень сигнала был максимальным (по данным утилиты WinXP Wireless Zero Config). Затем подключались к точкам доступа и проводили замеры. Верхняя кривая отображает пропускную способность через «корневую» точку доступа Belkin; нижняя — через ASUS WL300g и Belkin.

Даже с учетом того, что пропускная способность снизилась примерно на ожидаемые 50%, среднее значение около 8 Мбит/с через обе точки доступа все равно почти в два раза выше, чем у простого соединения 802.11b.

Возможные неисправности

Если при отправке запроса ping вы получаете превышение интервала ожидания, то повторите запрос через некоторое время. Замечено, что некоторые модели маршрутизаторов достаточно долго (вплоть до одной минуты) после загрузки не устанавливают соединение.

Если связи нет, то еще раз убедитесь в правильных настройках обеих точек доступа. В частности, проверьте, что у точек доступа указаны MAC-адреса противоположных концов соединения WDS. Также убедитесь в корректности указания самих адресов. Беспокоиться о том, что ноль может быть буковой «O» и наоборот, не нужно: в MAC-адресах используются только цифры и буквы от A до F.

Затем попробуйте включить/выключить питание точек доступа. Выключите обе, затем включите подсоединенную к LAN, подождите, пока она будет готова к работе. Затем включите другую и подождите, пока она также будет готова к работе. Теперь можно снова выполнить запрос ping, только убедитесь, что прошло достаточно времени.

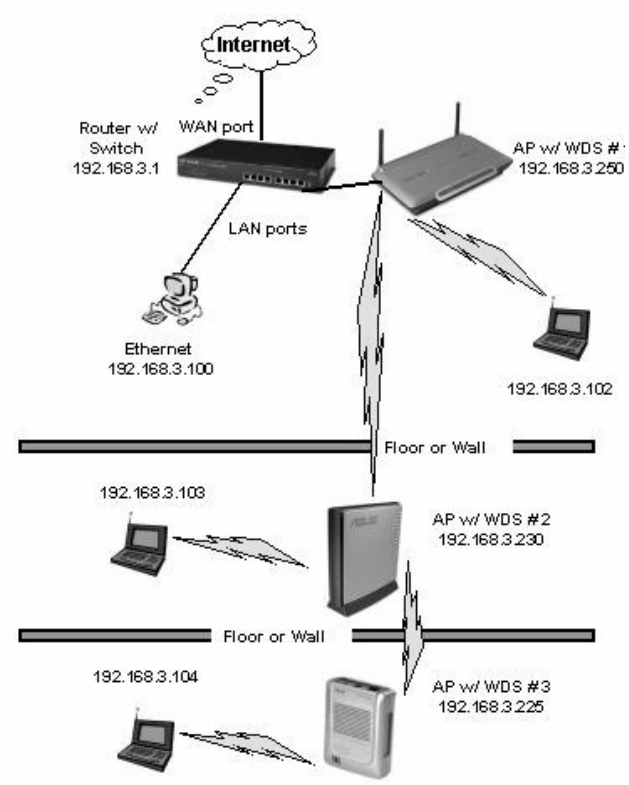
Если ничего, из указанного выше не помогло, и вы используете точки доступа разных производителей, то, возможно, вы столкнулись с несовместимыми продуктами. В этом случае единственное, что может помочь, — это использование другой модели точки доступа.

Наибольшие шансы на успех имеет конфигурация из двух точек доступа одной модели.

Пример 2: тестирование повторителя на два «хопа»

Бывают ситуации, когда для увеличения зоны покрытия нужно сделать цепочку из повторителей. Недостатки этого способа очевидны: низкая скорость подключения конечных станций к удаленным повторителям и меньшая стабильность соединения из-за дополнительного моста.

Однако, при использовании оборудования 802.11g, максимальная скорость работы станций, подключенных даже ко второму повторителю, будет не хуже скорости оборудования 11b. В большинстве случаев этого будет достаточно.



Немного разнообразим оборудование и в качестве третьей точки доступа возьмем ASUS WL330. Возьмем точку доступа 11b, чтобы показать вариант при совместном использовании оборудования 11g и 11b в режиме WDS. Кроме того, интересно узнать, как будет работать WDS с устройствами, построенными на разных чипсетах.

Хотя WL330 использует чипсет для точек доступа Marvell Libertas 802.11b, а не решение Broadcom, в нашем случае проблем не возникло. Возможно, помогло и то, что для моста WDS были использовали два продукта от ASUS.

Однако, при использовании оборудования 802.11g, максимальная скорость работы станций, подключенных даже ко второму повторителю, будет не хуже скорости оборудования 11b. В большинстве случаев этого будет достаточно.

Хотя оба устройства изготовлены ASUS, разница между настройками WDS у WL300g и WL330 видна с первого взгляда. У обеих есть режим «только-ТД», но 330 поддерживает только смешанный режим (Hybrid), то есть режим повторителя WDS. Таким образом, вам не удастся использовать ее в качестве только моста.

С другой стороны, у 330 нет раздельных опций «**Подключаться к точкам доступа в списке удаленных мостов?**» (Connect to APs in Remote Bridge List?) и «**Разрешить анонимное подключение?**» (Allow Anonymous?). Вместо них при выборе активного режима смешанной сети (Hybris-Active) появляется список MAC-адресов WDS, а при выборе пассивного режима (Hybrid-Passive) список отсутствует. Так как нам нужно было задать MAC-адрес точки доступа, выбран активный режим и указан MAC-адрес WL300g.

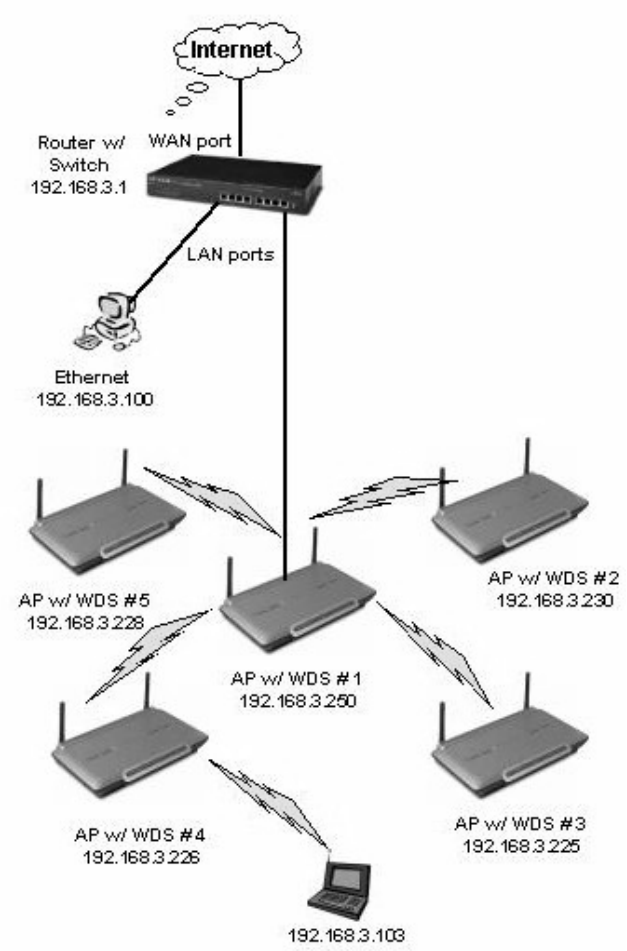
Среднее значение пропускной способности составляет 1,8 Мбит/с для клиента, подключенного к последней в WDS цепочке WL330 (нижний график). Результат, на первый взгляд, кажется низким, однако, если задуматься, он не так уж и плох.

В качестве последнего звена цепочки WDS было использовано устройство 11b, пропускная способность которого, в лучшем случае, может достигать 5–6 Мбит/с. Соответственно, должно было получиться 2,5–3 Мбит/с.

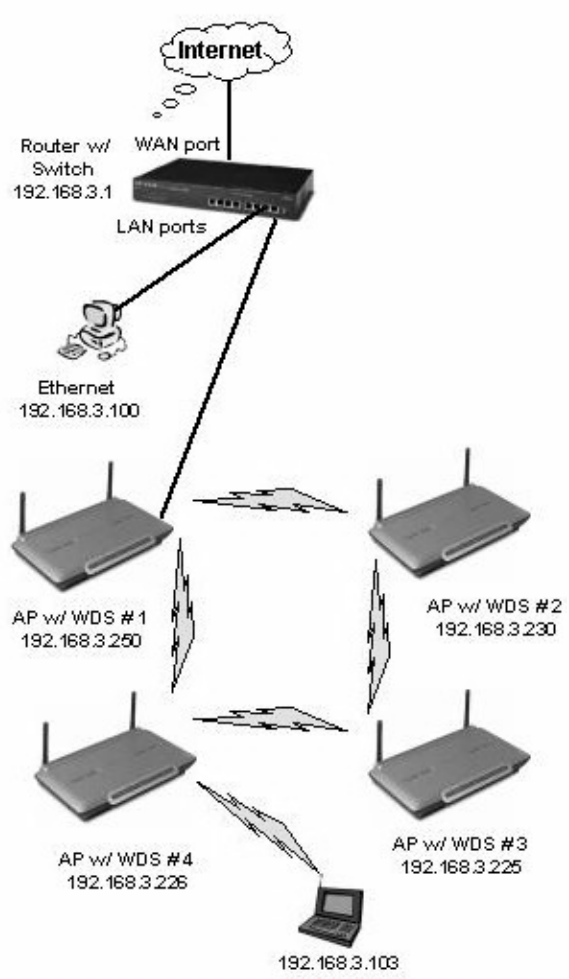
С учетом того, что для WL330 был доступен канал 8 Мбит/с, то расчетный результат получается как раз на уровне 1,8 Мбит/с.

Глава 5.
Звезды и кольца

Существует еще два способа настройки соединений точек доступа WDS — топология «**Звезда**» (Star), в которой одна точка доступа устанавливает канал с каждой из четырех удаленных точек доступа, каждая из которых имеет канал до «корневой» (подключенной к LAN) точки доступа.



Такая конфигурация предпочтительнее цепочки, рассмотренной во втором примере, она позволяет создать большую зону охвата сети с одним промежуточным беспроводным каналом до каждого повторителя. Однако ее основной недостаток в том, что подключение удаленных точек доступа к LAN зависит от работы «корневой» точки доступа. Для создания минимальной конфигурации типа «Звезда» требуется три точки доступа.



Хотя такая конфигурация также имеет единую точку отказа, она все же более надежна. Если одна из точек доступа, кроме #1, станет неисправной, соединение остальных с проводным сегментом LAN не нарушится. Эту конфигурацию не следует использовать, если вы не уверены, что все используемые точки доступа поддерживают алгоритм и протокол spanning tree. Если устройства не поддерживают spanning tree, то скорость сети резко снизится из-за широковещательных штормов broadcast storms.

Технология WDS предназначена для улучшения совместимости беспроводных мостов и повторителей, но она не обеспечивает ее так, как хотелось бы.

Часть 7. Когда беспроводные сети мешают друг другу

Глава 1. В чем суть проблемы?

Беспроводные сети прекрасны, но только если работают! Сегодня все большее число пользователей таких сетей встречаются с серьезной проблемой, когда даже после настройки своей WLAN (беспроводной сети), поддержание ее работоспособности и высокой производительности является сложной, а иногда и неразрешимой задачей. Иногда проблема кроется в сбойном оборудовании и его неправильной настройке, но все чаще приходится сталкиваться с проблемой работы сетей, связанной с ростом их популярности. И, как следствие, со все более широким распространением беспроводного сетевого оборудования.

Эта глава посвящена проблемам, которые могут возникнуть в расположенных близко друг к другу беспроводных сетях. Я также предоставлю готовые решения для избавления от большинства возникающих проблем, и даже расскажу, как сохранить драгоценное время и нервы при поиске проблем.

Итак, как определить, что проблема вызвана соседней беспроводной сетью, а не неисправностями оборудования? Для этого вам поможет следующий тест:

- окно просмотра доступных беспроводных сетей WinXP показывает наличие беспроводных сетей, отличных от вашей, при этом таких сетей может быть несколько;
- соединение с точкой доступа периодически разрывается, даже если вы находитесь рядом с ней;
- производительность вашей беспроводной сети постоянно снижается в одно и то же время... обычно после обеда и вечером;

- у вашего соседа тоже есть подобные проблемы с его беспроводной сетью;
- вы живете в общежитии, многоквартирном доме, или по соседству со зданием, в котором располагается множеством различных офисов, а также провайдеров широкополосного доступа в Интернет.

Причинами основных проблем, существующих у нескольких тесно расположенных беспроводных сетей, являются:

- большое число пользователей пытаются одновременно использовать один канал;
- радиочастотные помехи от соседних беспроводных сетей.

Первая проблема является результатом ограничения емкости сети, или недостаточной суммарной пропускной способности. Другими словами, в этом случае множество систем пытаются одновременно использовать один канал (то есть частотный диапазон) в одном месте. «Высокая плотность» — термин субъективный, но если сеть располагается в многоквартирном доме или общежитии, то он как нельзя лучше описывает ситуацию. Даже если сеть создана в отдельном коттедже, но расстояние до соседей относительно невелико (при этом ваша клиентская утилита показывает имена/SSID соседских сетей), то этот случай также можно отнести к данной категории!

Сети стандарта 802.11b предоставляют среднюю полезную пропускную способность около 5 Мбит/с. Даже этой пропускной способности может быть достаточно для большого числа пользователей, но только в том случае, если им нужны лишь кратковременные передачи данных, например в случае использования таких сервисов, как web, email, ICQ и им подобных. Но если учесть, что средняя скорость выделенной линии составляет 1-2 Мбит/с, то одновременное скачивание файлов, передача видео или web-конференции у нескольких клиентов могут быстро нагрузить существующую беспроводную сеть.

При переходе на сеть стандарта 802.11g полезная пропускная способность, конечно же, увеличивается, но не до тех 54 Мбит/с, о которых гласят рекламные надписи на коробках и корпусах устройств. Данное тестирование показывает, что полезная пропускная способность такого оборудования с клиентами WinXP составляет около 25 Мбит/с. При использовании Win98 средняя скорость может еще снизиться примерно до 20 Мбит/с, а работа в совместном режиме с клиентами 802.11b, подключенными к сети 11g, еще снизит полезную скорость до 12 Мбит/с.

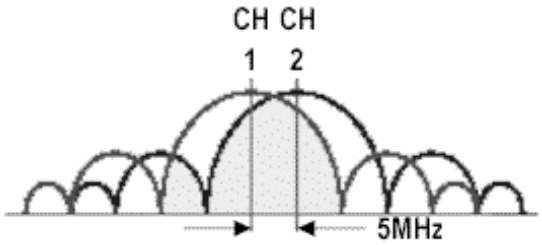
Вторая проблема попадает в категорию радиочастотных помех. Хотя традиционными источниками помех для беспроводных сетей являлись только беспроводные телефоны, работающие в диапазоне 2,4 ГГц, и микроволновые печи, в последнее время к этой категории оборудования все чаще можно отнести и само беспроводное оборудование, которое зачастую является источником помех.

При любой передаче данных приходится иметь дело с двумя составляющими: полезным сигналом, несущим информацию, и шумом, то есть всем остальным. Поэтому при разработке радиоприемников инженеры затрачивают свои усилия на увеличение чувствительности к полезному сигналу и уменьшению чувствительности к шуму.

До тех пор, пока оборудование 802.11b/g получает сигнал достаточного уровня, работает механизм управления сетью Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), являющийся частью беспроводного протокола. Сходный метод предотвращения коллизий также используется и в проводном Ethernet — в один момент времени только одно устройство может передавать данные, чтобы они были успешно доставлены до адресата.

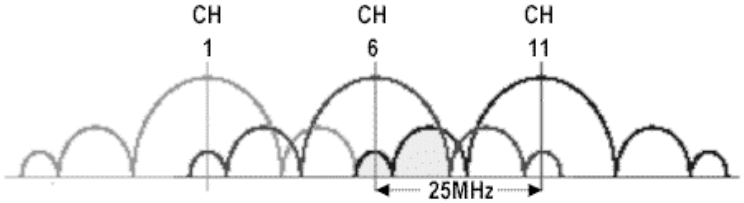
Однако когда полученный сигнал не удается распознать, даже если он пришел от разрешенного устройства, сигнал определяется как шум. Беспроводное сетевое оборудование проделывает огромную работу для того, чтобы отличить сигнал от шума, однако не все продукты одинаково успешно с этим справляются.

Если вы используете оборудование стандартов 802.11b или 802.11g, то, вероятно, знаете, что частотный диапазон, выделенный под это оборудование, разбит на 11 каналов. Менее известен тот факт, что только три из них могут использоваться одновременно.



Обратите внимание, что главный лепесток содержит большую часть энергии сигнала. Так как главные лепестки сигнала первого и второго каналов оказываются значительно перекрытыми, это очень нега-

тивно скажется на качестве связи обоих каналов. Отметим, что описанный эффект относится к любым двум соседним каналам, а не только к первому и второму.



Однако сигнал каждого из каналов не исчезает за границами выделенных частотных диапазонов по 22 МГц, и, как видно, «независимые» каналы все равно перекрываются. Но сейчас ситуация более благоприятна: желтая зона, обозначающая сигнал одиннадцатого канала, находится не меньше, чем на 30 дБ ниже пиковой мощности главного лепестка шестого канала (это 1/1000). Для большинства моделей такого значения вполне достаточно для отделения сигнала выбранного канала от шума.

Перекрывающиеся каналы — это не единственный источник помех в беспроводных сетях. Позже я покажу, что некоторые технологии, которые вы, вероятно, используете в вашей сети, чтобы снизить воздействие соседних сетей, на самом деле могут принести вам больше вреда, чем пользы.

Таким образом, для того чтобы избавиться от помех в вашей сети, нужно решить проблемы не только с микроволновыми печами и радиотелефонами, работающими в том же диапазоне, но и с другими беспроводными сетями.

Глава 2. Меняем каналы

Рассмотрев, как все это работает, можно перейти к решению проблем. В простейшем случае достаточно просто сменить канал, на котором работает точка доступа. К сожалению, утилита Windows XP Wireless Zero Configuration не позволяет узнавать каналы соседних сетей, поэтому вам лучше воспользоваться клиентскими утилитами, идущими в комплекте с адаптерами.

Ниже показана достаточно удобная утилита, которая идет в комплекте с адаптером ASUS WL-100g CardBus. Она не только отображает

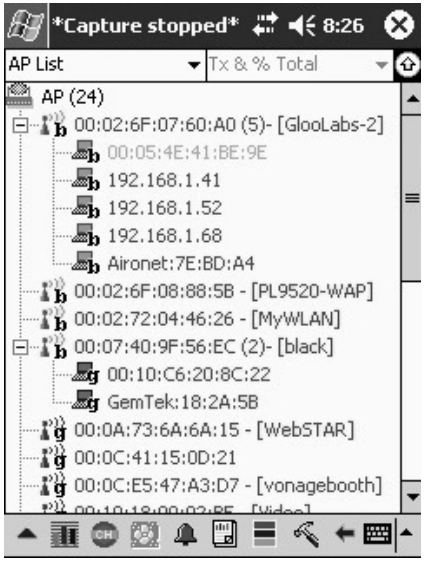
SSID и каналы соседних точек доступа, но также их MAC-адреса и уровни сигналов, что весьма удобно!

Как только стало известно, какие каналы заняты, необходимо выбрать тот из трех каналов (1, 6 или 11), который используется меньшим числом соседних точек доступа, у которого самый низкий уровень сигнала и который менее нагружен, — если выполняются все три условия, то вам повезло!

Изменить используемый канал достаточно просто, но для этого нужно открыть экран администрирования точки доступа или маршрутизатора (как это сделать, всегда можно узнать в документации к ТД или маршрутизатору).

Вероятно, вы захотите изменить оба эти параметра, но как и для чего нужно изменять SSID, мы рассмотрим немного позже. После указания желаемых параметров, не забудьте применить или сохранить их (кнопка «**Apply**» или «**Save**», в зависимости от продукта), чтобы они начали использоваться.

Кстати, хотя клиентские утилиты позволяют узнать количество точек доступа и определить занимаемые ими каналы, они не позволяют определить их загруженность — количество подключенных к точке доступа беспроводных клиентов. Для этого прекрасно подойдет весьма удобный инструмент — AirMagnet.



Показан один из вариантов просмотра доступного беспроводного сетевого оборудования средствами AirMagnet. При таком древовидном типе отображения показываются точки доступа (значки в виде вышек) и подключенные к ним клиенты (значки в виде ноутбуков). Как видно, в нашем примере множество точек доступа вообще не имеют клиентов, и чтобы узнать используемые ими каналы, достаточно лишь сделать пару щелчков мышью (или стилусом — на КПК).

К сожалению, AirMagnet и другие средства анализа беспроводных сетей не нацелены на простых пользователей, поэтому и стоимость их соответствующая — от $3000 и выше. Если вы дружите с Linux, то можете попробовать Kismet, но в этом случае придется самостоятельно считать точки доступа и их уровни сигналов, чтобы определить какой канал нужно использовать.

Примечание: даже не пытайтесь менять номер канала на клиенте. Канал сети, работающей в режиме **Infrastructure** (использующей точку доступа или маршрутизатор), указывается на центральном устройстве, а не на клиенте.

Одна из сетей не такая как все остальные

Определение неиспользуемого канала поможет решить большинство проблем, связанных с близким расположением соседних беспроводных сетей. Но, если это не помогло (или ничего не получилось), то остается жестко «привязать» компьютер к ТД.

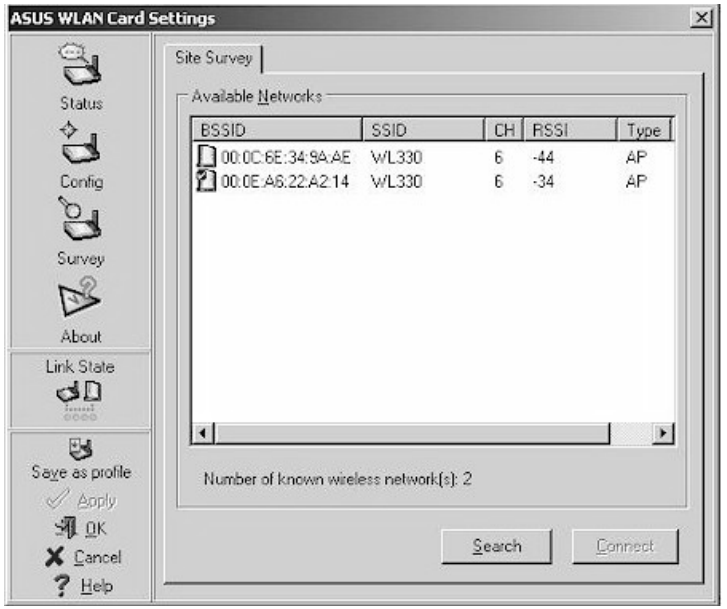
Попытки упростить создание беспроводных подключений настолько, насколько это возможно, привели к появлению некоторых странностей в работе ПО. Например, утилита WinXP Wireless Zero Configuration в своем поведении, по меньшей мере, не постоянна. Если один раз вы успешно подключились к беспроводной сети с определенным именем (SSID), она автоматически определяет ее как «предпочитаемую сеть» и подключается к ней всякий раз, когда обнаруживает ее сигнал.

Эта удобная функция становится проблемой в том случае, если вы перемещаетесь по зонам действия различных точек доступа с одинаковым именем, но принадлежащих разным сетям! Клиент считает, что точки доступа с одинаковым именем (SSID) принадлежат к одинаковой сети (на самом деле, беспроводные сети с несколькими точками доступа так и настраиваются). Компьютер не может определить, принадлежит ли другая точка доступа с таким же SSID к той сети, в который вы работали прежде, или нет, поэтому вполне возможна ситуация, когда он будет пытаться подключиться к той ТД, у которой будет сильнее сигнал, — хотя она принадлежит другой сети.

Конечно, в том случае, если в другой сети используется шифрование WEP/WPA или ограничение доступа по MAC-адресам, то подключение не установится. В этом случае вы увидите, как подключение разорвалось, затем (возможно) восстановилось с вашей ТД (хотя, возможно, вам придется самостоятельно проводить повторный поиск сетей и устанавливать подключение). На первый взгляд может показаться, что сеть начала сходить с ума, на самом же деле адаптер лишь делает свою работу, пытаясь поддерживать лучшее соединение.

Усугубляет эту проблему и то, что просмотр доступных сетей средствами стандартной утилиты XP Zero Config не показывает различные точки доступа с одним и тем же именем (SSID). Поэтому, для того чтобы узнать, с какой точкой доступа вы работаете в данный момент, стандартные средства не помогут — нужно использовать утилиты, которые поставляются в комплекте с клиентскими адаптерами.

В качестве примера, обратимся к утилите для адаптера ASUS WL100g. Ниже наглядно видно, что эта утилита отображает все обнаруженные точки доступа даже в том случае, если они используют один SSID.



К сожалению, эта утилита не позволяет подключаться к той точке доступа, к которой вы хотите. Наши эксперименты показали, что под-

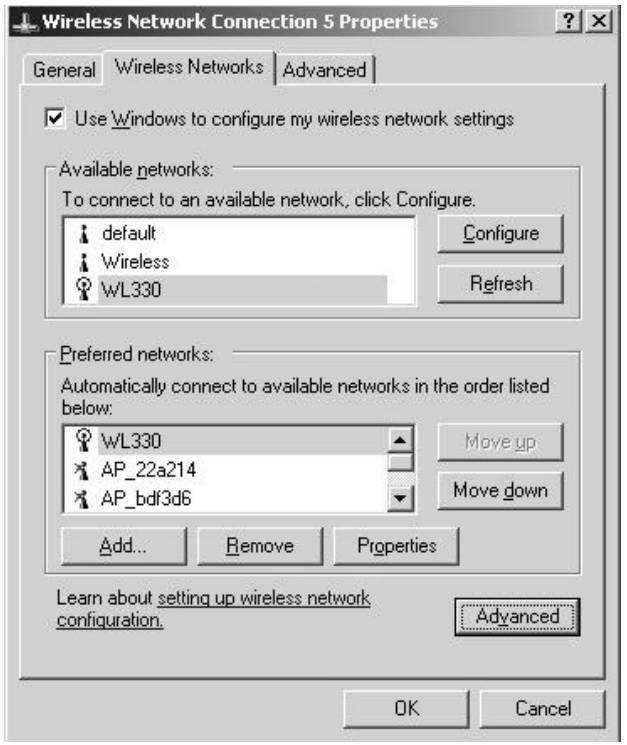
ключение устанавливается с той точкой доступа, сигнал от которой более сильный (на момент поиска точек доступа). К сожалению, в большинстве случаев правила подключения жестко прописаны в драйвере адаптера и не позволяют пользователю выбирать ТД самостоятельно.

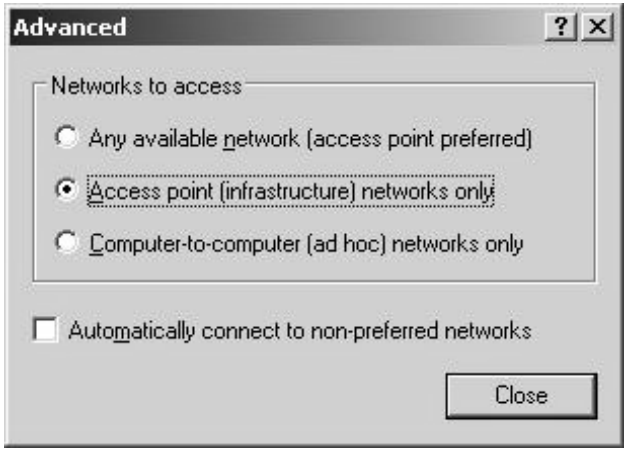
Глава 3. Как заставить адаптер не менять точку доступа

К счастью, есть два способа, которые позволяют удерживать подключение беспроводных клиентов к той точке доступа, к которой нужно. Первый — сменить SSID сети на другой, отличный от используемого соседними сетями. Стоит остановить выбор на оригинальном имени, которое никак не соотносится с названием или расположением. В имени могут использоваться буквы, цифры и символы подчеркивания — использование пробелов недопустимо.

Второй способ — если вы используете WinXP — заключается в очистке списка предпочитаемых сетей (**Preferred Network**). Убедитесь, что подключение к другим сетям запрещено. Значок адаптера можно увидеть в окне **Сетевые Подключения** (Network Connections) (**Start ⇨ Settings ⇨ Network Connections**).

В верхней части окна отображаются доступные сети или те сети, которые обнаружены в данный момент, в нижней части окна показан список предпочитаемых сетей. Нужно удалить из него все сети, кроме вашей. Затем, нажав кнопку **Дополнительно** (Advanced), в появившемся окне, следует убрать флажок из пункта **Автоматически подключаться...** (Automatically connect to non-preferred networks).





В результате карта не будет пытаться подключаться к сетям Ad Hoc (вряд ли они будут по соседству) — но что более важно, карта не будет автоматически пытаться соединиться с новыми беспроводными сетями, появляющимися в зоне действия.

Помните, если беспроводный клиент переместился в зону действия других сетей, то при возвращении снова необходимо очистить список предпочитаемых сетей.

Если вы не используете WinXP, или применяете клиентскую утилиту адаптера, не забудьте проверить наличие подобного пункта и, по возможности, сделать то же самое. Некоторые утилиты используют профили подключения, в которых сохраняются настройки подключения к различным беспроводным сетям, — при этом профили выбираются только вручную. В этом случае вам не нужно очищать список предпочитаемых сетей, но, возможно, потребуется удаление ненужных профилей, если они автоматически создадутся при обнаружении новых сетей.

Глава 4. Возможности поиска

Если найти свободный канал не удалось, и проблемы продолжают говорить о себе даже после блокирования ассоциаций клиентов к чужим точкам доступа, то пора подумать о том, как защитить сеть от радиопомех. Сначала важно разобраться в сути проблемы, а уже затем начать реализовывать какое-либо решение. При этом вам нужно знать уровень сигнала и параметры соседних сетей.

Что ж, придется провести «разведку боем» (на английском эту процедуру называют site survey). На самом деле, этот процесс представляет собой прогулку по исследуемой территории с любым устройством, позволяющим измерять и записывать уровень сигнала. Для этого можно использовать, например, ноутбук с беспроводным сетевым адаптером, если его клиентское приложение способно отображать все доступные точки доступа, используемые ими каналы и уровень сигнала. При этом абсолютно не важно, в каких единицах измеряется уровень сигнала: проценты, dBm или каких-то других. Также не особо важно, что именно измеряется: уровень сигнала, его качество, или и то, и другое. Внимание здесь следует обращать на изменение измеряемых характеристик. Еще немаловажно и то, насколько быстро реагирует утилита на произошедшие изменения, — естественно, лучшим вариантом является отображение значений в реальном времени, а еще лучше, если строится график уровня сигнала.

Если используемая клиентская утилита не имеет каких-то функций, то существует пара решений, способных помочь и в этой ситуации, но, к сожалению, они оба, вероятно, потребуют приобретения нового адаптера. На самом деле, это не так страшно — стоимость на адаптеры стандарта 802.11b уже снизилась, примерно, до $50. Первое решение — NetStumbler — представляет собой прекрасный инструмент для просмотра соседних беспроводных сетей. Он позволяет создавать графики уровней сигнала и шума. Существуют версии как для Windows, так и для PocketPC. Для работы ему требуется адаптер на базе чипа Lucent (Agere Systems) Hermes — например, ORiNOCO 802.11b. Полный список поддерживаемых адаптеров приведен в документации к NetStumbler.

Можно воспользоваться и коммерческой утилитой. К примеру, решение, поставляющееся с адаптерами ASUS WL-100 и WL-100g, показало себя достаточно хорошо.

Как только инструмент для измерения оказался у вас в руках, нужно воспользоваться им в проблемных местоположениях. Поскольку все проблемы, связанные с одинаковыми SSID, уже были решены (не так ли?), можно приступить к определению каналов и уровней сигналов соседних точек доступа. Наибольшее количество проблем обычно доставляют те точки доступа, которые используют тот же канал, и уровень сигнала которых выше или равен уровню вашей точки доступа.

Как только вы узнали окружение, в котором приходится работать точке доступа, можно переходить к изменению ситуации. Подходящее решение этой проблемы — улучшение производительности беспроводной сети, но суть такова: лучше постараться уменьшить влияние соседней WLAN, а не пытаться усилить свой собственный сигнал, создавая, тем самым, проблемы кому-то еще. В большинстве случаев помогает небольшой алюминиевый экран, разумное использование направленных антенн или просто перемещение точки доступа в другое место.

Помните, что увеличить характеристики передачи можно даже в том случае, если возможности подключения внешних антенн нет.

Переход к 802.11a

Иногда стоит задуматься о переходе на оборудование, использующее другой частотный диапазон. Если все усилия по избавлению оборудования 802.11b/g от помех не привели к успеху, то, может, стоит задуматься о приобретении оборудования 802.11a? Вопреки распространенному мнению, сегодняшние продукты 802.11a имеют сопоставимую или более высокую скорость работы по сравнению с решениями 802.11b и g.

В силу того, что они работают в менее загруженном (пока) диапазоне 5 ГГц, все проблемы, связанные с соседними сетями 11b и g, просто исчезнут.

Если вы решите пойти этим путем, то не стоит брать однодиапозонное оборудование (только-11a). Все такие модели построены на чипах первого поколения и имеют меньший радиус действия.

По этой причине стоит приобретать только двухдиапазонные двухрежимные (11a / 11b) или двухдиапазонные трехрежимные (11a/b/g) решения. Многие продукты 11a сегодня снизились в цене, так что обратите внимание и на этот вариант.

Социальная инженерия

К сожалению, не все проблемы можно решить в одиночку. Суть проблемы может заключаться в недостаточном взаимодействии пользователей, создающих беспроводные сети. Так, если на относительно небольшой площади сконцентрировано несколько беспроводных сетей, то наиболее эффективным будет использование описанных выше приемов сообща.

Возможно, вы будете удивлены тем, с какой охотой люди будут сотрудничать с вами во благо решения общей проблемы, — особенно если им не придется сильно утруждать себя. Соберитесь с пользователями соседних сетей: вероятнее всего, если у проблемы есть у вашей сети, то они есть и у других.

Как только удалость собрать все заинтересованные стороны вместе, осталось разработать и принять схему распределения каналов. Если в сети всего три точки доступа, то можно считать, что задача решена. Если точек доступа больше, то придется приложить усилия для создания приемлемой схемы распределения каналов между точками доступа.

Для этого необходимо нарисовать схему расположения точек доступа с максимально возможной точностью. При наличии схемы распределить каналы будет гораздо проще. Точки доступа, использующие один канал, должны быть расположены так, чтобы их взаимное влияние было минимальным. То есть на практике это означает, что нужно использовать один канал на максимально удаленных друг от друга точках доступа. Но в некоторых случаях расстояние не играет решающей роли. Например, при размещении точек доступа в здании, следует учитывать стены здания, экраны и прочие преграды, ослабляющие сигнал. В многоэтажных зданиях следует учитывать три измерения — радиоволны распространяются во всех направлениях.

Когда каналы уже распределены, необходимо для каждой точки доступа указать уникальное имя SSID. Хотя с точки зрения распределения каналов все ТД принадлежат одной WLAN, пользователям нужны разные сети с точки зрения работы. Уникальные SSID нужны для того, чтобы беспроводные клиенты не переключались с одной ТД на другую, когда это не нужно.

Кроме того, если соседи не знакомы с такими возможностями, как шифрование WEP/WPA, фильтрация MAC-адресов и другими функциями безопасности беспроводных сетей, то помогите им их настроить. Проблема снижения пропускной способности при использовании шифрования WEP в сегодняшнем оборудовании решена, поэтому если вы не хотите, чтобы любой желающий мог свободно «гулять» по вашей сети, то мы настоятельно рекомендуем использовать эту возможность.

Что не решит проблему

При возникновении подобных проблем в беспроводной сети пользователи испытывают практически все, что только могут придумать. Некоторые такие «решения» не только не помогут, но способны даже навредить не только собственной, но и соседним сетям. Рассмотрим наиболее яркие примеры.

Включение WEP/Использование аутентификации

Конечно, методы шифрования, такие как WEP и WPA, а также использование методов аутентификации 802.1x, не разрешат подключиться к вашей сети всем желающим. Но пытаться они могут сколько угодно. Подобные попытки подключения, особенно если количество «чужих» машин велико, могут существенно снизить скорость работы всей сети, что наиболее заметно в медленных сетях 802.11b.

С другой стороны, шифрование, на самом деле, ничего не делает с радиосигналом, поскольку при шифровании лишь изменяются передаваемые данные.

Мы рекомендуем использовать шифрование WPA (или WEP, если WPA не доступно) только для усиления безопасности — оно никак не решает проблему большого количества одновременно работающих устройств на небольшой территории.

Отключение широковещания SSID

Хотя отключение широковещания SSID вашей сети не помешает попыткам ваших клиентов подключиться к другим сетям, чужие клиенты будут оставаться в пределах своих сетей. Но и здесь не мешает сменить

SSID, установленный по умолчанию, — если соседский ноутбук успел заметить вашу сеть и сохранить ее в списке предпочитаемых сетей, то он будет продолжать искать ее при установке подключения.

Выбор режима только-11g

Обладатели беспроводного оборудования стандарта 802.11g могут изменять еще и некоторые параметры, которые различаются в разных продуктах. Некоторые ТД стандарта 11g позволяют отключать механизм «защиты» 802.11b, который отвечает за взаимодействие медленных клиентов 11b с быстрыми точками доступа 11g. Отключение этого механизма схоже с включением WEP или WPA, когда радиосигнал (и помехи) никуда не исчезают. Однако отключение механизма защиты может создать даже больше проблем для сети, чем включение WEP или WPA.

Вообще, пропускная способность зависит от множества факторов, но отключение механизма защиты отключает также взаимодействие между оборудованием 11b и 11g. При этом появляются коллизии и возрастает вероятность того, что данные придется передавать заново, что снижает пропускную способность сети.

Усиление сигнала

Как я говорил выше улучшение производительности беспроводной сети, усиление сигнала решает, в лучшем случае, половину проблем, оно лишь помогает клиенту «лучше слышать» передаваемые точкой доступа данные. Прибегать к подобной мере следует только в крайнем случае, когда ничего другое уже не помогает.

Использование Super-G

Super-G использует достаточно противоречивую технологию объединения каналов, которая может, в ряде случаев, стать причиной проблем в соседних сетях. Отнесем использование Super-G к той же категории, что и усиление сигнала, — то есть это не панацея, и может причинить дополнительные проблемы вместо того, чтобы решить существующие.

Протокол 802.11, являющийся основой используемых сегодня беспроводных сетей, позволяет работать в одной сети десяткам, если не сотням станций одновременно. И здесь нужно стараться работать совместно, а не пытаться конкурировать друг с другом.

В любом случае, чтобы добиться успешной работы нескольких беспроводных сетей, расположенных вблизи друг от друга, не следует бояться экспериментировать.

Глава 5.
Выбираем КПК для Wi-Fi

Новое развлечение энтузиастов хайтека — поиск беспроводных сетей с открытым доступом (так называемых хот-спотов). Для этого вида досуга существует два названия — war-chalking и war-driving. Последнее подразумевает катание на автомобиле с ноутбуком, оснащенным оборудованием Wi-Fi в поисках зоны, где возможно подключение к чьей-то локальной сети, а то и выход через нее в интернет. Термин War-chalking теперь, стало быть, характеризует пешие прогулки. А прогуливаясь на своих двоих, для поиска WLAN-сетей гораздо удобнее пользоваться карманным компьютером.

Наладонник будет удобен и в другом случае — при посещении заведений, где организован беспроводной доступ в сеть. По данным Cnews-WiFi, на пространстве СНГ функционирует более трех сотен хот-спотов. Более сотни из них расположены в Москве, 70 с лишним — в Санкт-Петербурге, остальные рассеяны по крупным городам бывшего СССР. Примечательно, что значительная часть хот-спотов, как правило, в предприятиях общепита, предоставляет бесплатный доступ в сеть. Сегодня это стало дополнительным способом привлечения посетителей в кафе и рестораны. А также — в клубы, рестораны и казино. И снова повторим — карманный компьютер в этих местах окажется удобнее ноутбука.

Итак, нам предстоит выбрать КПК, одним из назначений которого будет вход в беспроводные сети. Рассмотрим только те модели, что уже имеют встроенный WLAN-адаптер, иначе список кандидатов окажется слишком велик. Согласитесь, наладонник с врожденной способностью к Wi-Fi гораздо удобнее в обращении, да и слот расширения не будет занят. К тому же, КПК, спроектированный с прицелом на использование в беспроводных сетях, будет заведомо более надежен, чем связка из машинки попроще и карты сторонних производителей. Также исключим из обзора наладонники дороже 600 долларов — в верхнем ценовом диапазоне сомнительных моделей почти не бывает, да и критерии выбора там, скорее, эстетические. На что же стоит обратить внимание?

Подавляющее большинство наладонников оснащается модулями Wi-Fi стандарта 802.11b. Они обеспечивают скорость связи до 11 Мбит/с (на деле выходит около шести) и дальность на расстоянии до 100 метров. Параметры для тех, кто практикует war-chalking, вполне подходящие. Но не это главное. Находясь в движении, вы будете оторваны от сети электроснабжения и придется полагаться только на аккумулятор. Поэтому одним из основных критериев должно стать время автономной работы кар-

манного компьютера. На это влияет множество факторов — частота процессора, тип и объем памяти, яркость подсветки экрана и наличие других отъедающих энергию компонентов. А устройства беспроводной связи — одни из самых охочих до энергии.

Второй важный критерий — приспособленность КПК для работы в Интернете. Тут сразу намечается некий водораздел, имя которому — Unicode. Наладонники на платформе Pocket PC и Windows Mobile выглядят с этой точки зрения более предпочтительными, так как поддержка Unicode встроена в ОС этих машин. Но если вы готовы терпеть неудобства или серфить исключительно по англоязычным сайтам, никто не заставляет вас отказываться от платформы Palm. Особенно если вы всем сердцем любите эти заслуживающие уважения КПК.

Наличие аппаратной клавиатуры не выглядит решающим фактором. В процессе веб-серфинга чаще придется пользоваться стилом для кликанья ссылок. А для общения по ICQ сгодится и виртуальная клавиатура. Заодно получите полезный навык — формулировать мысли ясно и коротко. Удобство серфинга более зависит от разрешения экрана — но тут надо помнить, что большой экран означает большие потребности в энергии. И преимущества высокого разрешения нивелируются укороченным временем работы.

Среди карманных компьютеров на базе Windows Mobile можно выделить следующие WLAN-устройства:

HP iPAQ hx2415

Наладонник HP iPAQ hx2415 типичен для рассматриваемой категории. Этот карманный компьютер позиционируется как модель среднего уровня. Но при этом он построен на базе процессора Intel с частотой 520 МГц. Объем памяти не назовешь большим — по 64 Мб ОЗУ и ПЗУ, зато поддерживаются два слота расширения — CompactFlash и SD/MMC. Наладонник оснащен всеми возможными интерфейсами — Bluetooth, WiFi, IrDA, USB. Может использоваться как флэш-накопитель, для чего доступно 20 Мб ОЗУ. На энергообеспеченность благотворно влияет возможность замены аккумулятора (по умолчанию — 1440 мАч). Можно прикупить дополнительный, емкостью 2880 мАч.

iPAQ rx3715

Интересным представляется аппарат от той же HP — «мультимедийный» iPAQ rx3715. Мультимедийность выражается в наличии фотокамеры с матрицей в 1,2 мегапикселя и усиленного ИК-порта. Последний полезен для дистанционного управления развлекательной техникой. Максимальное разрешение фото — 1280 x 960 точек, есть возможность записи видеороликов. Ради этого пришлось ограничиться одним слотом для карт расширения — SD/MMC/SDIO. Комбинация камеры и WLAN-возможностей открывает такие возможности, как например, ведение сетевого репортажа. «Оператор» КПК может вести съемку на клубном концерте и оперативно выкладывать фото и видео-ролики в Интернет. Если ему это позволит аккумулятор наладонника. Производитель заявляет, что среднее время работы от одной зарядки — около семи часов. Но похоже, что это время работы в режиме неторопливого чтения без подсветки. Ведь кроме Wi-Fi и усиленного ИК-порта здесь присутствуют адаптер Bluetooth и порт USB. Не будем забывать про фотокамеру. Все это хозяйство поддерживает сменный аккумулятор на 1440 мАч. Возможно, сказывается невысокая частота процессора — 400 МГц.

Fujitsu-Siemens Pocket LOOX 710

Выгодной покупкой для охоты на хот-споты можно счесть наладонник Fujitsu-Siemens Pocket LOOX 710. Имея не самый быстрый процессор (Intel XScale с частотой 416 МГц) и минимальный объем памяти (64/64 Мб ОЗУ/ПЗУ), «семьсот десятый» компенсирует это аккумулятором на 1640 мАч и 12 часами работы. И это при том, что на борту имеются Bluetooth-модуль и USB-хост, значительно расширяющий возможности устройства. Других излишеств нет, да и не нужно — масса КПК уже достигает 180 граммов.

Dell Axim X50v

Чуть больше стоит, но гораздо более впечатляюще выглядит Dell Axim X50v. В его основе — самый скоростной из существующих процессор — Intel Bulverde 624 с частотой МГц. Экран имеет VGA -разрешение (480 x 640 точек), управляется видеоакселератором Intel 2700G с 16 Мб собственной памяти. В КПК встроены все возможные интерфейсы, размер флэш-диска составляет 92 Мб. Заплатить за это пришлось «лишним весом» — 175 г. Батарею, видимо, утяжелить не решились, и поэтому владелец ограничен емкостью в 1100 мАч. А ведь VGA-экран явно требует большего. К счастью, аккумулятор поддается замене.

Tungsten C

Единственный прибор с поддержкой WiFi от PalmOne — Tungsten C с аппаратной клавиатурой. Памяти традиционно немного, зато имеется непривычно высокочастотный для Palm процессор XScale 400 МГц. Адаптер Bluetoooth и слот CompactFlash отсутствуют. Ёмкость несменного аккумулятора восполняется достаточной для Palm емкостью — 1500 мАч. Это позволяет добиться восьми часов работы от одной зарядки. Как водится, большее, чем у Pocket PC разрешение экрана — 320 x 320 пикселей.

Sony Clie PEG-UX50

Ряд Palm-клавиатурников продолжает трансформер Sony Clie PEG-UX50. Вы получите аппарат с встроенным фотоаппаратом и большим экраном (480 x 320 точек) под управлением графического акселератора. Наладонник умеет делать снимки с VGA-разрешением и записывать и видео (MPEG4, 30 fps, 160x112 пикселей). Присутствует контроллер Bluetooth. Остальные параметры интереса не вызывают. Разве

что частота процессора, которая может снижаться до восьми мегагерц в целях продления работы. Сообщается, что электронной книгой КПК работает неделю, плеером — 16 часов, а беспроводную связь может поддерживать в течение 4-5 часов.

Clie PEG-TJ37

Самый недорогой из WLAN-наладонников Sony — модель Clie PEG-TJ37. Даже в бюджетный КПК японские инженеры втиснули VGA-камеру и mp3-плеер. На этом прелести заканчиваются. Пользователю доступно всего 23 Мб памяти, Bluetooth-связь не реализована, аккумулятор обеспечивает в седнем пять часов работы.

RoverPC P7

Наконец, помянем КПК от российского производителя. RoverPC P7 выглядит вполне на уровне средних наладонников от зарубежных

компаний. Конфигурация типична, отмечу лишь полный набор интерфейсов (Bluetooth, IrDA, USB). Имеется флэш-диск на 32 Мб, два слота карт расширения.

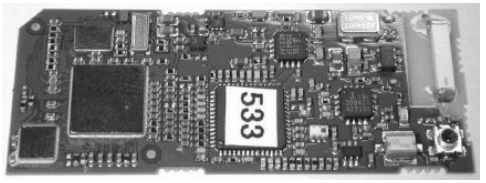
Глава 6. Оснащаем КПК: беспроводная карта SanDisk SD Wi-Fi в формате Secure Digital

Карта SanDisk SD WiFi впечатляет своим технологическим совершенством — полнофункциональный клиентский адаптер 802.11b имеет размер всего с две почтовые марки. Но внешний вид — далеко не все. Посмотрим, так ли впечатлит производительность адаптера, как его размер.

SanDisk доставил немало радости сообществу Pocket PC, выпустив в августе долгожданную карту Wi-Fi SD.

Внутреннее строение

Карта SD Wi-Fi является перемаркированным эталонным дизайном SyChip WLAN SD6060, чьи внутренности показаны ниже. Как видим, перед нами великолепный продукт инженерной мысли.



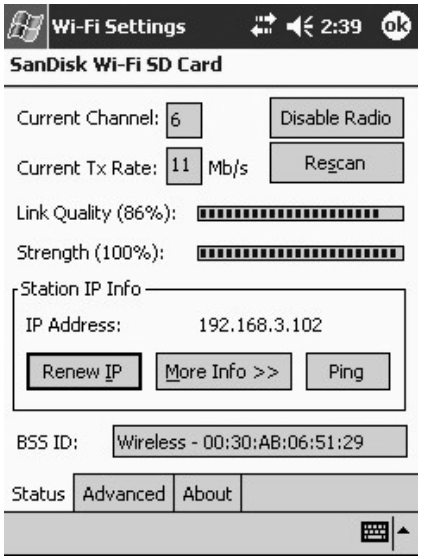
Чтобы использовать это маленькое чудо, вам понадобится КПК с PocketPC 2002, 2003 или CE.net.

Карта содержит все элементы, характерные для беспроводных адаптеров PC Card и CF, и построена на базе двухчипового дизайна радиочасти BB/MAC.

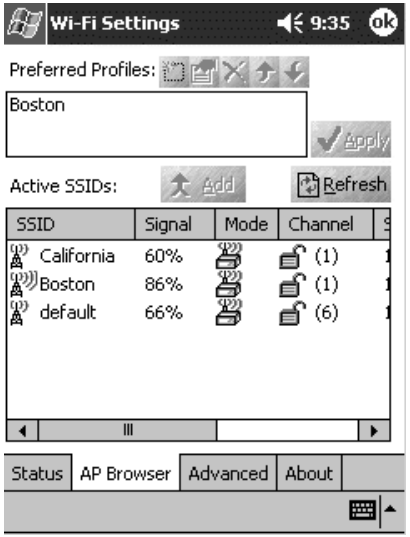
Карта имеет крошечный индикатор на своей поверхности, который мигает, когда карта не ассоциирована с сетью, и горит непрерывно после ассоциации.

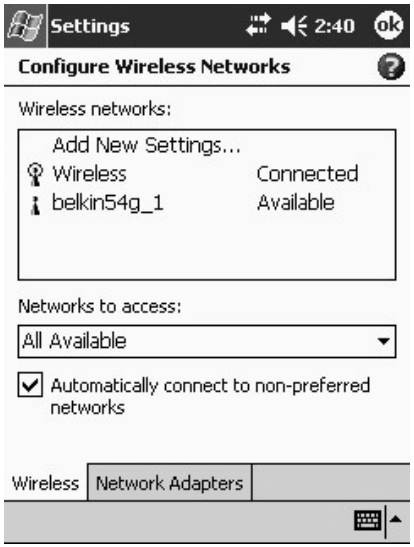
Управление и настройка

SanDisk поставляет с картой хорошую клиентскую утилиту, однако встроенная в Pocket PC 2003 нулевая конфигурация отключает функцию просмотра доступных точек доступа и возможность добавлять/изменять свойства подключения.



Клиентский браузер точек доступа SanDisk намного лучше, чем вариант от Microsoft, поскольку он отображает статус WEP, рекламируемые скорости подключения, канал и MAC-адрес точки доступа.





Чтобы вы не терять время в поисках способа настройки этого маленького «зверя» под Pocket PC 2003, учтите, что большинство настроек вынесено в утилиту Zero Config, которую можно вызвать двойным нажатием на значок **Connectivity** в верхней части экрана **Today**. Затем перейдите на закладку **Настройки** (Settings), выберите закладку **Расширенные** (Advanced), затем нажмите на клавишу **Сетевая карта** (Network Card). Настройки WEP выводятся после выбора нужного значка беспроводной сети и перехода на закладку **Аутентификация** (Authentication).

Производительность

Первая плохая новость — проблемы при попытке ассоциировать SD Wi-Fi с двумя точками доступа 802.11g на базе Broadcom (ASUS WL-300g и Belkin F5D7130). Карта видела обе сети, но подключиться не смогла.

Полагаю, проблема здесь заключается в драйвере карты, поскольку защита 802.11b была активирована на точках доступа, и даже переключили одну из них в режим объявления только — 802.11b скоростей передачи. У нас не возникло проблем с подключением карты к точке доступа NETGEAR ME102 802.11b.

Но самая плохая новость заключается в том, что другие обозреватели пользователи — карта ужасно «тормозит».

Хорошая новость заключается в том, что производительность карты незначительно зависит от расстояния, и радиус действия сравним с другими картами 802.11b, протестированными нами. Крохотная антенна не ограничивает радиус действия или пропускную способность карты, как теоретизировали некоторые товарищи.

Наконец, при включении WEP не происходит заметного падения пропускной способности. И подобно другим продуктам 802.11b, карта SD Wi-Fi не поддерживает шифрование Wi-Fi Protected вообще.

Карту SanDisk SD Wi-Fi можно признать достижением технической мысли.

Но огорчает — крайне низкая пропускная способность и продолжающееся отсутствие обещанных драйверов под Palm OS. В общем, на данный момент у карты SD Wi-Fi есть, что улучшать. Пока что можно рекомендовать приобретать КПК со встроенными беспроводными картами, или докупать карты CF.

Глава 7.
«Железо» Wi-Fi

Беспроводные мосты

Беспроводные мосты предназначены для работы в качестве корневого узла радиосети, ретранслятора и удаленного узла и поддерживают типовые мостовые функции. Существуют различные варианты оборудования, основанные на поддержке стандартов IEEE 802.11a/b/g (Cisco Systems, Inc., Zyxel), и, кроме того, с успехом применяются устройства, использующие фирменный стандарт (Proxim Corp.). Некоторые из этих устройств, кроме мостовых функций, поддерживают функции точек доступа с реализацией технологии Wi-Fi. Существуют модели, выполненные в уличном всепогодном варианте со встроенными антеннами.

Беспроводные точки доступа

Беспроводные точки доступа предназначены для быстрого развертывания и организации с минимальными затратами беспроводных локальных сетей с поддержкой функций Wi-Fi в офисах, гостиницах, кафе, аэропортах и ж/д вокзалах, т.е. наиболее подходят для создания узлов «hotspot». Точки доступа Wi-Fi обеспечивают поддержу различных стандартов IEEE 802.11a/b/g и дают возможность высокоэффективного соединения на скорости до 54 Мбит/сек. на полосах частот 2.4 и 5 ГГц. В некоторых устройствах возможна комбинация двухдиаппазонных стандартов для более гибкого построения офисных радиосетей. В различных сериях реализовано оборудование с возможностью использования как встроенных, так и внешних антенн.

Клиентские беспроводные адаптеры

Беспроводные клиентские адаптеры обеспечивают поддержку стандартов IEEE 802.11a/b/g. Существуют варианты адаптеров, которые работают с поддержкой одного, двух или трех стандартов одновременно. Беспроводные адаптеры стандартов IEEE 802.11a/b/g — это Wi-Fi совместимые устройства, комбинирующее возможности беспроводных сетей с работой, безопасностью и управляемостью, необходимыми в различных видах коммерческой деятельности.

PCI-адаптеры обеспечивают беспроводное подключение к сети стационарных компьютеров с PCI-интерфейсами. В большинстве случаев, существует возможность наращивания кабеля и установки необходимой антенны для лучшего приема радиосигнала.

Клиентские PCMCIA-адаптеры обеспечивают беспроводное подключение к сети мобильных компьютеров со слотом расширения PCMCIA.

USB-адаптеры позволяют быстро подключить к беспроводной сети любой настольный или мобильный компьютер с USB-интерфейсом.

Как выбрать беспроводной сетевой адаптер

Когда-нибудь все компьютеры будут иметь встроенные интерфейсы для беспроводных сетей, но пока еще эти интерфейсы продаются преимущественно в виде добавочных (к ПК) устройств. При развертывании корпоративной беспроводной ЛВС почти всегда компьютеры оснащаются беспроводными сетевыми адаптерами, стоят они недорого, но при схожих ценах имеют конкурентные различия. Сегодня самыми распространенными являются беспроводные сетевые адаптеры стандарта 802.11b (Wi-Fi), но спрос на устройства стандартов 802.11a и 802.11g и мультистандартные платы растет.

Многие компании (особенно те, которые ориентированы на рынок оборудования для индивидуальных потребителей и небольших офисов) покупают поставляемую ими продукцию у OEM-производителей. Они выпускают устройства (программно-аппаратные платформы), на которые (по заказу) наносятся логотипы конкретных поставщиков. Последние нередко снабжают купленную ими платформу усовершенствованными драйверами и утилитами (инсталляционными и клиентскими) собственной разработки.

Все начинается с набора микросхем

Наборы микросхем для беспроводных сетевых адаптеров производят всего несколько компаний. Каждый адаптер состоит из высокоскоростного радиомодема, обеспечивающего прием и передачу сигналов, и процессора, отвечающего за сетевые функции, включая формирование кадров и реализацию алгоритма доступа к среде передачи на MAC-уровне.

Раньше OEM-производители беспроводного оборудования, как правило, использовали в своих платформах микросхемы разных фирм, но сейчас они все больше ориентируются на интегрированные наборы микросхем. Фирмы Atheros Communications, Broadcom, Intersil и другие производители полупроводниковых компонентов для беспроводных систем конкурируют между собой, что приводит к расширению функциональности компонентов и их удешевлению. Производители наборов микросхем разрабатывают базовые аппаратно-программные решения и продают их OEM-производителям оборудования.

С точки зрения развития техники производители наборов микросхем и OEM-производители беспроводного оборудования играют гораздо более важную роль, чем поставщики этого оборудования. Дело в том, что все основные функции адаптера, как правило, реализуются аппаратно. Можно расширить его функциональность с помощью ПО, но тогда он наверняка будет работать медленно. Так, например, в недалеком прошлом в некоторых платах стандарта 802.11 функция WEP-шифрования была реализована программно и при включении ее пропускная способность такой платы значительно уменьшалась. Кроме того, радиотехниче-

ские характеристики адаптера, в том числе чувствительность радиоприемного тракта, в основном определяются параметрами аппаратного обеспечения.

Некоторые производители микросхем утверждают, что по сравнению с продукцией конкурентов их изделия обеспечивают большую дальность связи или потребляют меньше электроэнергии, но по мере развития рынка устройства для беспроводных ЛВС по своим техническим характеристикам становятся все более похожими друг на друга. Чтобы выделить свои продукты на фоне оборудования конкурентов, производители нередко реализуют в них фирменные функции. Так, в некоторых устройствах стандарта 802.11a реализован турборежим, обеспечивающий удвоение скорости передачи данных путем объединения двух радиоканалов.

Новой тенденцией в сетевой индустрии является производство мультистандартных беспроводных сетевых адаптеров. Первые продукты этой категории поддерживали стандарты 802.11a и 802.11b. Новейшие же платы совместимы со стандартами 802.11a, 802.11b и 802.11g. Мультистандартные устройства характеризуются большей гибкостью применения, но за это пользователям приходится платить и более высокую цену. Так, один крупный Интернет-магазин предлагает обычный (стандарта 802.11b) адаптер Orinoco Gold фирмы Proxim за 60 долл., а мультистандартную (802.11a/b/g) плату этой же фирмы — уже за 99 долл.

Хост-интерфейсы

Самые распространенные адаптеры для беспроводных ЛВС имеют формфактор PC Card Type II. Для подключения к ПК они оснащены либо 16-разрядным хост-интерфейсом PCMCIA, который можно сравнить со старой компьютерной шиной ISA, либо 32-разрядным хост-интерфейсом CardBus, являющимся аналогом шины PCI. Для нормальной работы 11-Мбит/с адаптера стандарта 802.11b вполне достаточно пропускной способности 16-разрядного интерфейса, но платы стандартов 802.11a и 802.11b, работающие быстрее, должны иметь интерфейс CardBus — многие ноутбуки оснащены им. Не следует думать, что если мобильное вычислительное устройство новое, то оно обязательно оборудовано слотом CardBus. Например, блок расширения PC Card для популярных карманных компьютеров HP iPaq поддерживает только 16-разрядные платы PCMCIA.

Большая часть недавно выпущенных ноутбуков оснащена встроенным 32-битовным хост-интерфейсом mini-PCI. Обычно слот mini-PCI находится под крышкой на нижней панели ноутбука. Очень часто беспроводные сетевые адаптеры mini-PCI предустанавливаются производи-

телями на свои машины. Если в вашем ноутбуке такой адаптер отсутствует, вы можете купить и инсталлировать его сами.

Стационарный ПК подключается к беспроводной ЛВС с помощью либо беспроводного сетевого PCI-адаптера, либо беспроводного интерфейса USB. Для установки PCI-адаптера нужны определенные навыки, и здесь стоит отметить, что если системный блок ПК располагается под столом, то там же оказывается и антенна этого адаптера — согласитесь, не лучшее место для нее с точки зрения обеспечения надежной радиосвязи. Беспроводной интерфейс USB инсталлировать гораздо удобнее, к тому же его можно разместить так, чтобы ничто не мешало приему и передаче радиосигналов. Впрочем, в случае применения этого интерфейса может наблюдаться некоторое снижение скорости передачи данных по сравнению с таковой у PCI-адаптера.

ПО — это очень важно

Выбирая беспроводной сетевой адаптер, обращайте внимание не только на характеристики его аппаратной части, но и на функциональность прилагаемого ПО — она должна соответствовать вашим требованиям. Если все компьютеры вашей компании работают под управлениям ОС Windows XP, вам нужен только соответствующий драйвер, поскольку в этой ОС уже имеются средства настройки беспроводной связи и контроля доступа. Многим другим организациям могут потребоваться драйверы для разных ОС и гибкие клиентские утилиты.

Клиентские утилиты, поставляемые с адаптерами для беспроводных ЛВС, позволят вам сконфигурировать все параметры их работы. С помощью этих утилит можно управлять функциями защиты данных, регулировать излучаемую мощность адаптера и осуществлять другие настроечные операции. Если вы пользуетесь несколькими беспроводными ЛВС (например, офисной и домашней), то для вас весьма полезной окажется имеющаяся в клиентских утилитах возможность создавать и сохранять именованные профили настройки адаптера, необходимые для работы в этих сетях. Во многих клиентских утилитах есть функции обследования места установки сети (site survey) и поиска неисправностей в ней.

Пропускная способность и дальность

Реальная пропускная способность хорошего беспроводного сетевого адаптера должна составлять 50—60% своего теоретического максимального значения. Иными словами, выбирая адаптеры стандарта 802.11b, ищите такие, которые в сети с одной рабочей станцией принимают и передают данные с максимальной скоростью около 6 Мбит/с. Ес-

ли же вам нужны адаптеры стандарта 802.11a или 802.11g, покупайте те из них, которые в аналогичной простейшей сети имеют пропускную способность не ниже 27 Мбит/с. В обычных беспроводных ЛВС, где клиентские станции конкурируют между собой за доступ к радиоканалу, скорость передачи может быть ниже.

Помимо пропускной способности, очень важной характеристикой оборудования для беспроводных ЛВС является дальность действия. К сожалению, определить ее, руководствуясь приведенными в описаниях устройств техническими характеристиками, довольно трудно. Дальность действия беспроводного устройства зависит от уровня выходной мощности его передающего тракта, чувствительности радиоприемного тракта, коэффициента усиления антенны и способности работать в условиях многолучевого распространения радиосигналов и сильных помех.

Для создания беспроводной ЛВС в жилом доме или складском помещении следует использовать оборудование с большой дальностью действия. Напротив, в крупных компаниях, где для повышения пропускной способности каждой клиентской станции нужны малые размеры сот беспроводной ЛВС, большая дальность действия беспроводных устройств является их недостатком, поскольку приводит к возникновению помех в соседних сотах. В самых лучших продуктах имеется функция динамического регулирования уровня выходной мощности.

Заглядывая вперед

В будущем развитие беспроводных сетевых адаптеров продолжится, продолжится и снижение цен на них. Скорее всего, усилится тенденция к созданию мультистандартных устройств, и в скором времени на рынке появятся платы, поддерживающие не только стандарты на беспроводные ЛВС, но и спецификации на территориально распределенные беспроводные сети GPRS и CDMA2000 1xRTT и обеспечивающие прозрачный роуминг между ними.

Очень кстати был бы технологический прорыв в плане снижения энергопотребления адаптеров. Пользователям нужны более экономичные интерфейсы, и их появление будет способствовать широкому применению в беспроводных ЛВС компактных устройств (например, карманных ПК и мобильных телефонов) с аккумуляторами небольшой емкости.

Сетевой адаптер LANTECH Wireless PCMCIA 8800-510

Lantech Computer Company — успешно развивающаяся тайваньская фирма, предлагающая широкий спектр сетевого оборудования. Компания образовалась в 1986 г., отделившись от первого официального дистрибутора Novell в Тайване, и стала пионером рынка сетевого оборудования страны. Тогда же была принята стратегия компании Lantech по предложению заказчику высокотехнологичного оборудования при минимальных ценах и организованы программы обучения для сотрудников других молодых компьютерных фирм.

Lantech Computer Company заметно выделяется среди других азиатских производителей, прежде всего, широким спектром предлагаемого оборудования и, что особенно важно, качеством своей продукции.

Компания предлагает различное оборудование от обычных сетевых адаптеров и до серьезных управляемых устройств с высокой плотностью портов Gigabit Ethernet.

Важно отметить, что наличие «тяжелого» оборудования в спектре предлагаемых продуктов не является традиционным для азиатской компании и лишний раз доказывает большие возможности развития Lantech Computer Company.

Все оборудование проходит строгий многоуровневый контроль качества, в результате чего статистика отказов значительно меньше одного процента от общего объема.

Надежность оборудования подтверждается трех-пятилетней гарантией. Сертификат ISO-9001 Lantech Computer Company получила в 1996 г.

Особое внимание в компании уделяется научным исследованиям и новейшим разработкам.

Опираясь на 14-летний опыт работы, Lantech Computer Company четко отслеживает тенденции рынка и предлагает оборудование, в высшей степени отвечающее современным требованиям. Прежде всего, компания акцентирует внимание на бурно развивающихся рынках SOHO, рынках сетей для рабочих групп и департаментов, а также сетей филиалов крупных компаний.

Компания Lantech очень внимательно относится к своим заказчикам и наряду с высоким качеством своей продукции предлагает хорошо развитую инфраструктуру информационной и технической поддержки, благодаря чему 80% клиентов компании осуществляют повторные закупки оборудования.

Сетевой адаптер D-Link AirPlus DWL-650+

D-Link DWL-650 — 11 мегабитный беспроводной PC Card Type-II адаптер, совместимый со стандартом IEEE 802.11b.

Устройство предназначено для работы в домашних сетях и небольших офисах, в диапазоне 2.4 ГГц используя метод с прямой последовательностью сигналов (DSSS), по которому передача сигнала осуществляется сразу на нескольких частотах, что обеспечивает гарантированную доставку. Разработан для использования в слотах с напряжением 3.3 или 5.0 В.

Средством обеспечения безопасности является поддержка 64/128 шифрования по протоколу WEP (Wired Equivalent Privacy).

DWL-650 может работать как в режимах «постоянная» (Infrastructure Network) (с использованием точки доступа), так и «временная» сеть (Ad Hoc) (два адаптера связанны между собой). В режиме «постоянной» сети DWL-650 можно использовать для организации доступа сети к широкополосному шлюзу или DSL/кабельному модему с выходом на Интернет.

DWL-650 может передавать данные со скоростью 11, 5.5, 2 или 1 Мегабит в секунду на канал. Режимы передачи данных устанавливаются вручную и могут быть выбраны из Auto Select 1 или 2 мегабит, Fixed 1 мегабит, Fixed 11 мегабит, Fixed 2 Mbps, Fixed 5.5 Mbps и Fully Auto. Адаптер обеспечивает мобильность и прозрачный роуминг между точками доступа в сеть. Дальность передачи составляет до 100 метров внутри и до 300 метров вне помещений.

Адаптер поставляется с внешней несъемной всенаправленной антенной и индикаторами работы сети, наличия электропитания, связи и активности.

Устройство совместимо с Windows 98, ME, 2000, XP и NT 4.0.

Сетевой адаптер D-Link DWL-120

D-Link DWL-120 — это адаптер стандарта IEEE 802.11b на шину USB для беспроводных сетей со скоростью передачи до 11 Мбит/сек. Он работает на частоте 2.4 ГГц и предназанчен для домашнего или офисного применения. Карточка использует 40-bit WEP кодирование (с возможностью дальнейшего апгрейда до 128-битного) для безопасного подключения к сети.

Адаптер DWL-120 может работать в двух режимах: точка — к — точке (два адаптера связываются между собой не используя при этом никаких дополнительных устройств) и режим инфраструктуры (для доступа в сеть используется точка доступа). В режиме инфраструктуры мобильные пользователи могут через точку доступа подключаться с Интернет и другим сетевым ресурсам.

Адаптер DWL-120 может передавать и принимать данные со скоростью 11, 5.5, 2 или 1 Мбит/сек на канал. Скорость работы может быть выбрана вручную либо в автоматическом режиме. Применяя этот адаптер, пользователь становится по-настоящему мобильным. Он может пе-

ремещаться между точками доступа от ячейки к ячейки. Вне здания зона покрытия одной точки доступа составляет от 100 до 300 метров.

Адаптер DWL-120 поставляется со внешней малогабаритной антенной и оснащен одним светодиодным индикатором, дающим информацию о наличии питания и соединения. В комплекте поставляются драйверы для MS Windows 98, ME, 2000.

Сетевой адаптер Allied Telesyn AT-WCL007

Компания Allied Telesyn предлагает ряд дополнительных модулей и аксессуаров для своих коммутаторов. Они способны облегчить установку оборудования Allied Telesyn и существенно расширить его функциональные возможности.

Сетевой адаптер D-Link AirPro DWL-AB650

D-Link AirPro DWL-AB650 — это высокопроизводительный двухдиапазонный адаптер для ноутбуков с интерфейсом PC Card. Адаптер позволяет подключиться к сети, работающей как на частоте 5 ГГц, так и на частоте 2, 4 ГГц предоставляя вам доступ к сетям 802.11a и 802.11b. Скорость передачи адаптера — до 11 Мбит/с для стандарта 802.11b и до 54 Мбит/с для стандарта 802.11a. Обеспечивая поддержку промышленного

стандарта, надежную безопасную передачу данных и гибкую поддержку частот, этот адаптер предоставляет по настоящему быстрый и безопасный мобильный доступ к сети.

Точка доступа D-Link AirPlus DWL-900AP+

DWL-900AP — беспроводная точка доступа 11Mbps D-Link.

Данное устройство соединяет беспроводных клиентов в законченную инфраструктуру (клиент-сервер). По мере роста количества беспроводных пользователей, можно добавлять точки доступа для улучшения производительности сети.

DWL-900AP также поддерживает бриджинг «точка — точка», т.е. может работать с другой точкой доступа DWL-900AP, что позволяет расширить зону покрытия. DWL-900AP можно настроить для работы в качестве абонентского устройства.

С помощью встроенного 10Base-T RJ-45 порта, точку доступа можно подключить к стационарной сети Ethernet. Это позволяет прозрачно общаться клиентам беспроводной сети и сети Ethernet.

Можно также подключить к 10Base-T порту Интернет сервер. С помощью этого Интернет сервера беспроводные пользователи могут использовать один выход в Интернет через Dial-Up, кабельный или ADSL модем. Таким образом можно экономить средства и предоставлять всем беспроводным пользователям выход в Интернет.

Съемная антенна с разъемом SMA позволяет подключить внешнюю антенну для улучшения качества связи.

Сетевой адаптер LANTECH Wireless USB 8800-550

Точка доступа/маршрутизатор D-Link AirPlus DI-614+

Маршрутизатор D-Link AirPlus DI-614+. Имеет четыре порта 10/100Base-T (витая пара). Встроенный DHCP сервер автоматически присваивает IP-адреса беспроводным клиентам, которые получают доступ к локальным сетевым ресурсам. Управление настройками роутера осуществляется через интуитивно понятный web-интерфейс. Поддерживаются: аутентификация MAC-адреса, Network Address Translation (NAT), IPSec, L2TP и PPTP. D-Link AirPlus DI-614+ имеет две съемные ненаправленные антенны. Как особое достижение преподносится возможность работы с фильтрами блокировки. Заблокировать можно все: URL — блокируются доменные имена содержащие заданное слово; домены; IP-адреса.

Сетевой адаптер D-Link AirPro DWL-AB520

AirPro DWL-AB520 — адаптер PCI для настольных компьютеров, поддерживающий стандарты беспроводных сетей 802.11b и 802.11a.

DWL-AB520 позволяет планировать будущий рост сети или немедленно развернуть беспроводную сеть. Дополнительные каналы с высокой полосой пропускания, доступные со стандартом 802.11a, предоставляют пользователям надежный способ передачи больших объемов данных намного быстрее, чем было возможно со стандартом 802.11b.

Сетевой адаптер AVAYA Wireless USB Client gold

Avaya — бывшее подразделение Корпоративных сетей связи компании Lucent Technologies, является ведущим поставщиком коммуникационных систем для предприятий, включая частные компании, правительственные структуры и другие организации. Компания стала полностью самостоятельной 30 сентября 2000 года, объединив в своем продуктовом портфеле хорошо известное и превосходно зарекомендовавшее себя оборудование — телекоммуникационный сервер DEFINITY, линейку коммутаторов для локальных сетей Cajun, структурированные кабельные системы SYSTIMAX.

Выделение Avaya из состава Lucent позволило новой компании сосредоточить все силы и средства на основных направлениях бизнеса, достичь высочайшего уровня сотрудничества с клиентами и бизнес-партнерами. Став независимой, Avaya расширила спектр своих предложений: по мере становления электронного бизнеса Avaya становится первым глобальным поставщиком коммуникационных решений для предприятий, работающих на этом быстро меняющемся рынке.

В то же время Avaya сохраняет лидерство в мире по продажам систем обработки сообщений и структурированных кабельных систем, занимает лидирующие позиции США по операторским центрам и системам голосовой связи для предприятий.

Точка доступа D-Link AirPro DWL-6000AP

Точка доступа DWL-6000AP способна работать в беспроводных сетях стандартов 802.11a, и 802.11b. DWL-6000AP работает на 11 неперекрывающихся каналах и является идеальным устройством для работы в сети, включающей устройства обоих стандартов. DWL-6000AP создана с использованием новейших технологий и с учетом последних разработок. Она построена на контроллере 802.11b от Texas Instruments, использующего фирменную технологию Digital Signal Processing, и чипсета от Atheros для 802.11a.

Преимущество новейшей двухдиапазонной технологии 2, 4Ггц и 5Ггц, состоит в возможности организовывать сети общего доступа в публичных местах (образовательных заведениях и пр.). Устройство незаменимо для беспроводных сетей в аэропортах, кафе, универмагов, университетов и мест с большой концентрацией людей.

DWL-6000AP также может выполнять роль моста между сетями 802.11a и 802.11b, или связывать их с традиционными, «проводными» сетями, для чего в устройстве есть встроенный порт 10/100 Ethernet.

Часть 8. Руководство «сетевика»: Wi-Fi Protected Access (WPA)

Глава 1. Все зависит от элементов в уравнении

WPA представляет собой подмножество технологий из грядущего стандарта 802.11i, который комитет Wi-Fi Alliance называет WPA2. Комитет Wi-Fi Alliance посвятил WPA целый раздел сайта для продвижения нового стандарта в жизнь. Так что если вам нужна подробная информация из первых рук, то вы знаете, где ее найти.

Достаточно полезным документом можно назвать презентацию для средств массовой информации, показанную на последней выставке Networld+Interop в апреле. Презентация дает как подноготную WPA, так и информацию о составляющих элементах технологии.

Там же дается простое «уравнение» расчета WPA:

```
WPA = 802.1X + EAP + TKIP + MIC
```

То есть WPA является суммой нескольких элементов.

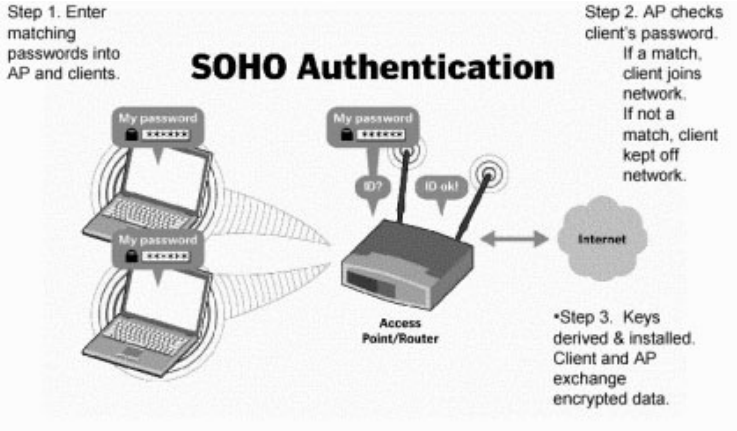
Глава 2. Аутентификация пользователя

Стандарт WPA использует 802.1x и Расширенный протокол аутентификации (Extensible Authentication Protocol, EAP) в качестве основы для механизма аутентификации. Аутентификация требует, чтобы пользователь предъявил свидетельства/мандат (credentials) того, что ему позволено получать доступ в сеть. Для этого права пользователя проверяются по базе данных зарегистрированных пользователей. Для работы в сети пользователь должен обязательно пройти через механизм аутентификации.

База данных и система проверки в больших сетях обычно принадлежат специальному серверу — чаще всего RADIUS. Однако, поскольку

применение WPA подразумевается всеми категориями пользователей беспроводных сетей, стандарт имеет упрощенный режим, который не требует использования сложных механизмов.

Этот режим называется Pre-Shared Key (WPA-PSK) — при его использовании необходимо ввести один пароль на каждый узел беспроводной сети (точки доступа, беспроводные маршрутизаторы, клиентские адаптеры, мосты). До тех пор, пока пароли совпадают, клиенту будет разрешен доступ в сеть.



Глава 3. Шифрование

Несмотря на то, что предшественник WPA, протокол WEP, не имел каких-либо механизмов аутентификации вообще, ненадежность WEP заключается в криптографической слабости алгоритма шифрования. Как указано в этом прекрасно написанном документе от RSA Security, ключевая проблема WEP кроется в слишком похожих ключах для различных пакетов данных.

Части TKIP, MIC и 802.1X уравнения WPA играют свою роль в усилении шифрования данных сетей с WPA. В следующей выдержке из документации Wi-Fi Alliance WPA дан хороший обзор того, как они работают вместе: TKIP увеличивает размер ключа с 40 до 128 бит и заменяет один статический ключ WEP ключами, которые автоматически создаются и распространяются сервером аутентификации. TKIP использует иерархию ключей и методологию управления ключами, которая убирает

предсказуемость, использовавшеюся взломщиками для снятия защиты ключа WEP.

Для этого TKIP усиливает структуру 802.1X/ EAP. Сервер аутентификации, после принятия мандата пользователя (credential), использует 802.1X для создания уникального основного ключа (двустороннего) для данного сеанса связи. TKIP передает этот ключ клиенту и точке доступа, затем настраивает иерархию ключей и систему управления, используя двусторонний ключ для динамического создания ключей шифрования данных, которые используются для шифрования каждого пакета данных, которые передаются по беспроводной сети во время сеанса пользователя. Иерархия ключей TKIP заменяет один статический ключ WEP на примерно 500 миллиардов возможных ключей, которые будут использоваться для шифрования данного пакета данных.

Проверка целостности сообщений (Message Integrity Check, MIC) предназначена для предотвращения захвата пакетов данных, изменения их содержимого и повторной пересылки. MIC построена на базе мощной математической функции, которую применяют отправитель и получатель, а затем сравнивают результат. Если он не совпадает, то данные считаются ложными и пакет отбрасывается.

С помощью значительного увеличения размера ключей и числа используемых ключей, а также создания механизма проверки целостности, TKIP преумножает сложность декодирования данных в беспроводной сети. TKIP значительно увеличивает силу и сложность беспроводного шифрования, делая процесс вторжения в беспроводную сеть намного более сложным, если не невозможным вообще.

Важно отметить, что механизмы шифрования, используемые для WPA и WPA-PSK, являются одинаковыми. Единственное отличие WPA-PSK заключается в том, что там аутентификация производится по какому-либо паролю, а не по мандату пользователя. Некоторые наверняка заметят, что подход с использованием пароля делает WPA-PSK уязвимой для атаки методом подбора, и в чем-то они будут правы. Но мы хотели бы отметить, что WPA-PSK снимает путаницу с ключами WEP, заменяя их целостной и четкой системой на основе цифробуквенного пароля. И наверняка подобная система пойдет дальше WEP, поскольку она настолько проста, что люди будут использовать ее на самом деле.

После того, как вы узнали теорию о работе WPA, давайте перейдем к практике.

Глава 4.
От теории к практике

Модернизация: 11g впереди всех

Итак, вас привлекает WPA, и вы желаете внести поддержку этого стандарта в свою беспроводную сеть как можно быстрее! С чего начать?

Будь вы «корпоративным» или домашним пользователем, вам необходимо пройти три шага:

- Узнать, поддерживает ли ваша точка доступа или беспроводный маршрутизатор WPA, либо к ним появилось соответствующее обновление прошивки.
- Узнать, поддерживает ли ваши клиентские адаптеры WPA, либо к ним появились новые драйверы.
- Понять, нужно ли вам покупать дополнительное приложение поддержки для вашего беспроводного клиента.

Шаги 1 и 2 кажутся простыми, однако для их реализации продукты должны пройти всю эволюционную цепочку. Поскольку большинство производителей сетевого оборудования для OEM и ODM находится на Тайване, эти компании должны первоначально получить и внедрить код от производителей беспроводных чипов, а уже затем выпустить драйверы и прошивки для своих продуктов.

Задача отнюдь не мизерная, учитывая, что сегодня по данным Wi-Fi Alliance существует более 700 сертифицированных продуктов, не говоря о сотнях несертифицированных решений. Обновления сначала необходимо выслать компаниям-производителям сетевого оборудования, которые проведут тестирование и (будем надеяться) при успешной работе выложат драйвер для скачивания.

По всей видимости, первыми обновление прошивки получат продукты на базе 802.11g. Вряд ли производители будут медлить с выпуском этих продуктов, поскольку они заинтересованы в появлении на полках магазинов последних версий устройств со своей торговой маркой. Однако нам показался удивительным тот факт, что продукты на базе Broadcom, похоже, первыми получат обновление WPA, несмотря на то, что Intersil уже выпустила код WPA своим клиентам в январе для чипсета 11b PRISM 2.5 и в марте для чипсетов 11g GT и 11a/b/g Duette.

Модернизация: 11b и прочее...

Если первые предложения можно считать каким-либо показателем, то владельцам продуктов 802.11b и a/b следует набраться терпения и ждать появления обновлений WPA. Известно что, на данный момент единственными устройствами 11b с обновлением до WPA являются Cisco 802.11b Aironet 1100 и 11a/b Aironet 1200, клиентская карта Linksys WPC11 Ver3 и линейка 3Com AP8000

Создаем VPN-соединение: маршрутизаторы SMC7004 FW и SMC7004WFW

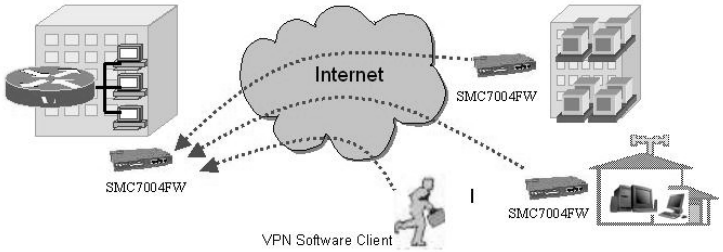
У многих компаний существует необходимость объединения нескольких территориально разделенных локальных сетей своих подразделений или подключения удаленных пользователей. Если использовать для этого публичную сеть, например Интернет, то неизбежно придется прибегнуть к технологиям безопасной передачи данных типа VPN.

У многих компаний существует необходимость объединения нескольких территориально разделенных локальных сетей своих подразделений или подключения удаленных пользователей. При компактном расположении, конечно, возможно использование собственных или арендованных каналов связи или телефонных линий. Но, вполне очевидно, что оба эти решения будут достаточно дорогими, если расстояние, на котором необходимо установить соединение между сетями или между клиентом и сетью, велико, например, если вам, находясь на том же IDF в России, нужно получить доступ к своей локальной сети, расположенной в Калифорнии. При использовании телефонной сети вам придется оплачивать огромные счета за международные телефонные разговоры, а скорость телефонного подключения будет, к тому же, довольно низкой. А для объединения двух офисов, находящихся на разных континентах, при помощи собственного кабеля вам потребуется огромная сумма.

Одним из способов снижения затрат на передачу данных являются технологии «Виртуальных частных сетей», или VPN (Virtual Private Network). Технологии VPN позволяют использовать общедоступные сети в качестве надежного и недорогого транспорта для ваших данных, обеспечивая при этом их защиту. В случае использования VPN все затраты сводятся к оплате доступа к Интернету, что существенно дешевле междугородных и международных звонков, и, естественно, дешевле организации физического канала. Подключившись к Интернету, вы устанавливаете соединение с удаленным шлюзом VPN и используете полученный канал для обмена данными.

Одной из существующих проблем в данном случае является то, что данные передаются по общим сетям и могут быть перехвачены злоумышленниками, поэтому особое внимание уделяется безопасности таких каналов. Естественно, при разработке технологии VPN были предприняты меры для надежной защиты трафика, как от просмотра, так и от подмены.

При установлении VPN-соединения создается так называемый туннель, или логический путь, по которому передаются данные. Конечно же, данные не передаются по туннелю в открытом виде, ибо любые данные, передаваемые по общей сети, можно перехватить. Для того чтобы защитить информацию от попадания к злоумышленнику, используется шифрование — при отправке исходные данные зашифровываются, а затем передаются. При достижении конечной точки соединения происходит обратный процесс, и вновь появляется исходный пакет в первоначальном виде. Таким образом, в публичную сеть данные в незашифрованном виде не передаются.



VPN-соединение с удаленной машиной представляет собой обычное соединение «точка-точка», поэтому все промежуточные сетевые устройства, через которые проходит туннель, для конечного пользователя не заметны.

Вариант реализации на базе маршрутизаторов SMC

Компания SMC Networks, производитель уже достаточно хорошо знакомого нашему читателю оборудования для сетей, производит достаточно много. Давайте обратимся именно к тем возможностям сетевого оборудования, которые становятся все актуальнее с каждым днем, а именно, к возможностям создания защищенных туннелей VPN.

VPN на базе PPTP

PPTP (Point-to-Point Tunneling Protocol) — один из протоколов, используемых для создания виртуальных частных сетей (VPN) на основе сетей TCP/IP. Этот протокол был разработан в результате совместных трудов компаний Microsoft, Ascend Communications, 3Com/Primary Access, US Robotics и ECI-Telematics, которые ставили перед собой целью разработку стандартного протокола защищенного канала. Однако стоит отметить, что PPTP в качестве стандарта так и не был принят, что, в свою очередь, связано с параллельной разработкой другими компаниями во главе с Cisco подобного протокола, носившего название L2F (Layer Two Forwarding). L2F тоже постигла участь PPTP — он не был принят. Но был создан протокол L2TP (Layer Two Tunneling Protocol), объединивший в себе PPTP и L2F. Однако PPTP, благодаря стараниям компании Microsoft, получил достаточно широкое распространение. Отметим, что операционные системы компании Microsoft имеют встроенный клиент PPTP, настройка которого не вызывает никаких сложностей. Данный протокол позволяет создавать виртуальные частные сети на основе общедоступных сетей TCP/IP, например Интернета. PPTP осуществляет туннелирование, инкапсулируя данные протокола IP внутри дейтаграмм PPP. Таким образом, пользователи могут запускать программы, работающие с конкретными сетевыми протоколами через установленное соединение. Туннельные серверы выполняют все необходимое для обеспечения защиты передаваемых данных, обеспечивая безопасную их передачу.

VPN на базе IPSec

IPSec (Internet Protocol Security) — еще один протокол, или даже система стандартов, направленная на установление и поддержание защищенного канала для передачи данных. IPSec предусматривает аутентификацию при установлении канала, шифрование передаваемых данных и распространение секретных ключей, необходимых для работы протоколов аутентификации и шифрования. Средства IPSec реализуют защиту содержимого пакетов IP, а также защиту от сетевых атак путем фильтрации пакетов и использования только надежных соединений. В разработке принимали активное участие такие компании, как Microsoft и Cisco Systems.

Для аутентификации источника данных и для обеспечения целостности пакетов здесь используется протокол AH (Authentication Header). Также шифрование, аутентификация и целостность передаваемых данных обеспечиваются средствами протокола ESP (Encapsulation Security Payload). Протокол IKE (Internet Key Exchange) используется для определения способа инициализации защищенного канала, кроме того,

IKE определяет процедуры обмена и управления секретными ключами соединения.

Шифрование в IPSec может обеспечиваться любым алгоритмом симметричного шифрования.

Из ограничений IPSec можно отметить, что он работает только в том случае, если передача данных на сетевом уровне обеспечивается средствами протокола IP, то есть в случае использования другого протокола сетевого уровня, например IPX, воспользоваться средствами IPSec будет невозможно. Конечно, это уже не актуально в связи с повсеместным распространением IP сегодня. Кроме того, всегда есть возможность совместного использования шифрования IPSec с тунеллированием L2TP.

У IPSec возможны два режима работы: транспортный (для передачи пакета по сети используется оригинальный заголовок) и туннельный (исходный пакет помещается в новый пакет, в теле которого он и передается по сети).

Данный протокол позволяет создавать многопротокольные виртуальные частные сети на основе общедоступных TCP/IP-сетей, например Интернета. PPTP осуществляет туннелирование, инкапсулируя данные протоколов IP и IPX внутри дейтаграмм PPP. Таким образом, пользователи могут запускать программы, работающие с конкретными сетевыми протоколами через установленное соединение. Туннельные серверы выполняют все необходимое для обеспечения защиты передаваемых данных, обеспечивая безопасную их передачу.

Глава 5. Различное оборудование

Существуют многочисленные конфигурации беспроводных сетей, предусматривающие использование различного оборудования. В случае с настольным компьютером вы можете использовать внешний Wi-Fi модуль, подключающийся по интерфейсу USB. Модули очень просты в установке. Если же у вас ноутбук — то приобретите Wi-Fi карту в PCMCIA-формате. Для улучшения связи при работе нескольких пользователей или когда вам нужно подключить беспроводную сеть к кабельной сети, лучшим вариантом станет использование точки доступа. Функционально она аналогична сетевому коммутатору или концентратору.

Trust предлагает комплект для начинающих пользователей UN110W, содержащий USB модуль и PCMCIA-карту.

Belkin имеет богатый ассортимент Wi-Fi оборудования, включающий PCMCIA-карты и беспроводные интернет-маршрутизаторы.

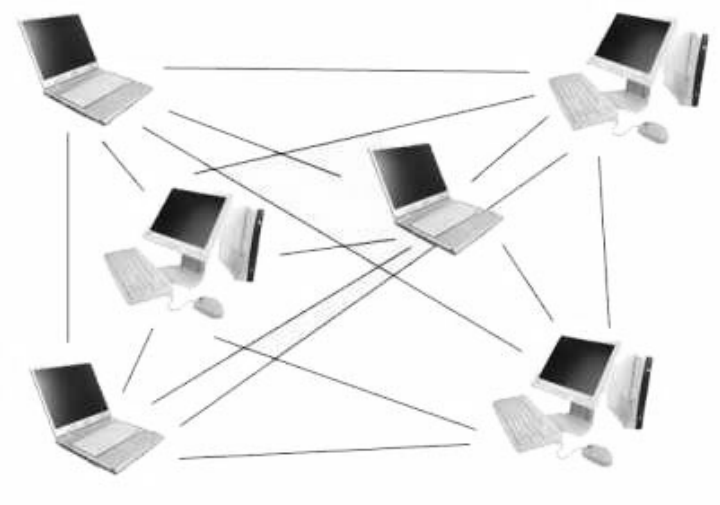
Компания 3Com предлагает точку доступа AP 8000.

Два режима работы

Как и в кабельной сети, беспроводная сеть имеет два режима работы.

Режим Ad Hoc

Данный режим предусматривает соединение карт клиентов по принципу «точка-точка» (point-to-point, P2P). В этом режиме каждый компьютер может связываться с любым другим компьютером в сети. Такой режим работы называется Ad Hoc, он обладает как своими преимуществами, так и недостатками.



Основное преимущество — быстрая и дешевая установка. Все, что вам нужно для организации такой сети, — оснастить каждую станцию (настольный компьютер или ноутбук) своей беспроводной карточкой или Wi-Fi модулем. Как только вы завершите конфигурацию, все станции смогут связываться друг с другом. Второе преимущество заключается в возможности располагать компьютеры на значительном расстоянии друг от друга — в результате мы получаем увеличенную зону действия сети. Если компьютер A удален от компьютера C на 300 метров, вы можете установить между ними компьютер B, и все три компьютера смогут связываться между собой. Обратной стороной медали является то, что компьютер B не будет работать, если связь между A и C прервется. Режим Ad Hoc рекомендуется для сетей, содержащих не более восьми машин. Подобная конфигурация обеспечит достаточную пропускную способность для всех типов игр.

Режим точки доступа

Если в вашей сети располагается больше восьми компьютеров, и все они находятся в ограниченном пространстве, скажем, в 200 квадратных метров, вам потребуется точка доступа. Она позволит вам осуществлять несколько функций, например, централизовать связь между всеми компьютерами, то есть работать как концентратор, или соединить вашу проводную и беспроводную сеть.

Кроме того, в проводной и беспроводной сети точка доступа может работать как Интернет-маршрутизатор, то есть раздавать по сети со-

единение с Интернетом. Обычно такая опция ограничена использованием широкополосного подключения к Интернету, типа кабельного или ADSL. Беспроводные маршрутизаторы выпускаются в различных версиях. Например, существует беспроводный маршрутизатор с портом Ethernet. Однако подобные устройства отличаются от автономных маршрутизаторов, которые управляют USB модемом по ADSL линии, так что для подобных соединений вам понадобится беспроводный маршрутизатор с встроенным ADSL модемом. Что касается России, то здесь необходимо выбирать модель с модемным или ISDN соединением. В любом случае маршрутизатор работает как точка доступа в сети WiFi.

Глава 6. Беспроводные маршрутизаторы

Связующее звено

Совсем не сложно описать идеальную точку доступа WLAN с встроенным маршрутизатором (по совместительству являющимся DSL или кабельным модемом) — просто возьмите лучшее от продуктов Lancom, Netgear и Samsung. На практике, однако, идеал не так легко достижим. Точка доступа Netgear обеспечивает максимальную пропускную способность, в то время как продукцию Samsung легче всего конфигурировать.

Netgear FM-144P ближе всего подходит к званию идеального продукта «все в одном». Он показывает высокую среднюю пропускную способность в 497 кбайт/с (измеряется при хорошей связи без шифровки данных), устройство легко в управлении и имеет несколько полезных функций. Netgear включает в себя сервер печати, равно как и 4-портовый коммутатор.

Идеальная комбинация: DSL/кабельный модем и WLAN

Если вы желаете установить высокоскоростное соединение с Интернетом, то вам понадобится кабельный или DSL модем. В зависимости от вашего места жительства, вы можете выбрать любой из двух вариантов. DSL зависит от расстояния до телефонной станции, в то время как кабельный модем — от расстояния до центра кабельного телевидения, который предоставляет эту услугу. Если кабельный модем в большинстве случаев обеспечивает большую скорость и производительность по сравнению с DSL, на практике он может оказаться не столь хорошим, поскольку кабельный модем использует принцип разделяемой пропускной способности, в то время как DSL предусматривает персональное выделенное соединение. Именно эти две технологии доминируют на рынке высокоскоростного доступа в Интернет в Северной Америке. В Европе все по-другому, там более популярны ISDN и DSL. Возможность раздавать ваше соединение с Интернетом на другие компьютеры зависит не только маршрутизатора, но и от провайдера. Некоторые провайдеры не позволяют использовать подобные продукты. Перед выбором таких устройств для подключения к вашему DSL/кабельному модему, лучше проверить ваш договор с провайдером на предмет разрешения их использования. Если вы желаете подключиться по DSL или кабельному модему в США, то вам могут помочь ресурсы типа http://www.2wire.com или http://www.dslreports.com.

Если вам нужно разделять ваше DSL/кабельное соединение с Интернетом между несколькими компьютерами, то вам понадобится DSL/кабельный маршрутизатор. Это устройство скорее не является полноценным маршрутизатором, который обеспечивает прямой доступ в Интернет нескольким компьютерам. DSL/кабельный маршрутизатор использует трансляцию адресов NAT для обеспечения одновременного доступа нескольких компьютеров в Интернет.

Важно заметить, что несмотря на весь маркетинг, эти устройства не являются настоящими брандмауэрами, скорее это нечто большее, чем коробка с NAT. Настоящие брандмауэры обеспечивают большую гибкость и функциональность, нежели стандартные NAT маршрутизаторы. И хотя NAT маршрутизаторы гарантируют вполне приемлемую защиту, им не хватает возможности определения атак, фильтрации содержания и различных опций по отчетам, которые мы видим в соответствующих продуктах уровня корпорации. (Впрочем, подобное утверждение тоже не постоянно — появляются новые NAT маршрутизаторы, обладающие все большим набором функций, унаследованных из корпоративного рынка). Если вы желаете составить себе более полное впечатление о различиях, то можете посетить сайт Sonic Wall . В зависимости от ваших потребностей, в большинстве случае вам хватит простейшего NAT, он действительно обеспечивает дополнительный уровень защиты, но не стоит на него всецело полагаться. Впрочем, даже небольшая защита лучше, чем никакая, поэтому рекомендую использовать NAT маршрутизаторы даже для подключения одного компьютера к Интернету.

Прокладка кабельной Ethernet сети для подсоединения компьютеров к DSL/кабельному маршрутизатору довольно трудоемка, да и отнимает много времени. Для многих покупателей DSL/кабельных маршрутизаторов подобные усилия излишни, но в зависимости от ваших потребностей и от числа компьютеров, стандартное кабельное решение бывает эффективнее. К примеру, если вы часто играете по сети, то про-

водной вариант даст вам большую пропускную способность, которая явно не станет лишней. Многие пользователи выбирают смесь проводных и беспроводных решений для своих домашних сетей, но все, опять же, зависит от ваших задач. В описанной выше ситуации, или если у вас уже есть проводной DSL/кабельный маршрутизатор, вам будет лучше докупить беспроводную точку доступа. Точка доступа обеспечивает вас беспроводным подключением к вашей проводной сети. Но при этом вы идете на определенные жертвы: у точки доступа, в отличие от беспроводного маршрутизатора, нет функции трансляции сетевых адресов. Впрочем, все зависит от конкретной ситуации — строите ли вы новую сеть или модернизируете старую, — вам могут понадобиться различные устройства.

Беспроводные LAN (WLAN) часто оказываются идеальным решением, они дают гибкость, которую другим путем вы не получите. Стандарт 802.11b обеспечивает теоретическую пропускную способность 11 Мбит/с, и отнюдь не ограничивает пропускную способность DSL/кабельного маршрутизатора в 768 кбит/с. Конечно, такая пропускная способность не идет ни в какое сравнение со 100 Мбит/с Ethernet, особенно если вы будете копировать большое количество данных на файл-сервер, подключенный к точке доступа WLAN. Однако новые продукты, только начинающие появляться на полках магазинов, предлагают большее. Сегодня стандартом де-факто для беспроводных сетей стал 802.11b, и если вам нужна обратная совместимость, вам нужно приобрести двойную a/b точку доступа или дождаться выпуска 802.11g, который будет поддерживать 802.11b, равно как и обеспечивать 54 Мбит/с 802.11g (заявленные 72 Мбит/с по стандарту 802.11a можно скорее отнести к области фантастики, нежели реальности). Однако 802.11g пока еще только на горизонте. Неизвестно, когда он появится, однако он наверняка станет самым лучшим из всех беспроводных решений, и его действительно стоит подождать. Но не будем заглядывать в будущее.

Некоторые производители уже предлагают 802.11a продукты (равно как и выходят на шаг вперед, анонсировав комбинацию A/B), но они являются более дорогими по сравнению с 802.11b и работают на других частотах.

Устройства с 802.11b существуют на рынке уже долгое время. На сегодняшний момент для достижения высокой пропускной способности 802.11a вам необходимо находиться на близком расстоянии от точки доступа и соблюдать условие прямой видимости, без всяких препятствий типа стен или дверей. Так что для максимального отношения цена/производительность и для будущей совместимости лучше вам сделать свой выбор именно на 802.11b.

Комбинация DSL/кабельный маршрутизатор и беспроводная точка доступа — вариант очень и очень неплохой. Мало того, что при этом вам не нужно соединять маршрутизатор и точку доступа кабелем, подобное интегрированное решение будет экономить ваши средства.

Безопасность

Почему же мы до сих пор слышим много нареканий по поводу безопасности беспроводных соединений?

Вопросы безопасности постоянно возникают вокруг стандарта 802.11b. Они действительно имеют под собой почву, но в конечном итоге безопасность зависит от пользователя. Беспроводные сети следует устанавливать с учетом тех же условий безопасности, которые используются для создания защищенных локальных сетей и dial-up доступа.

Изначально в стандарте IEEE 802.11 предусматривалась реализация протокола безопасности WEP (Wired Equivalent Privacy). С самого начала целью внедрения WEP было достижение того же уровня безопасности, который обеспечивается в традиционной проводной локальной сети. Ваша традиционная проводная локальная сеть уже обладает некоторыми механизмами защиты — вы можете контролировать точки доступа в нее внутри здания. Однако беспроводные сигналы способны проникать сквозь стены, так что обычные физические границы здесь не работают. Для обеспечения уровня физических ограничений обычной проводной сети в стандарт 802.11 было добавлено шифрование WEP.

Однако самая большая опасность беспроводных сетей состоит в том, что пользователи часто предпочитают не использовать вообще никакой защиты. В беспроводных сетях необходимо применять WEP, являющийся первой линией защиты. Однако многие пользователи работают открыто без всякой защиты, что подобно раскрытой двери в квартиру — «заходи, кто хочешь, бери, что хочешь». Во многих случаях WEP отпугнет потенциального взломщика, но если ваши данные вам дороги, то вам придется обратиться к более надежным и безопасным решениям.

Специалисты THG выдвигают семь рекомендаций:

- Регулярно проверяйте сайт поставщика насчет появления обновлений для ваших беспроводных устройств. Применяйте обновления, обновляйте прошивку вашего устройства. Не следует считать, что купленное устройство обладает самой свежей прошивкой.
- Включите WEP и повысьте его безопасность с помощью изменения ключа по умолчанию. Затем регулярно меняйте ключ WEP. Никогда не работайте с беспроводной точкой

доступа или беспроводным маршрутизатором без использования WEP. Конечно, если вам важны данные, передающиеся по вашей сети.

- Защита дисков и папок на вашем компьютере с помощью паролей сможет добавить еще один уровень безопасности.
- Измените SSID по умолчанию на что-нибудь иное.
- Используйте сеансовые ключи, если ваш продукт их поддерживает.
- Используйте фильтрацию по MAC-адресам, если ваш продукт поддерживает такую возможность. Блокировка маршрутизатора на работу только с определенными MAC-адресами дополняет защиту от несанкционированного доступа.
- Используйте VPN. Хотя для этого может потребоваться VPN сервер (или устройство, работающее как VPN сервер), VPN клиент уже включен в состав Windows 98SE, Windows 2000 и Windows XP.
- Помните, если данные в вашей сети требуют более высокого уровня защиты, то вам следует внедрить дополнительные меры безопасности типа доступа на основе RADIUS или Kerberos, шифровки информации, защиты паролей, аутентификации пользователя, VPN, SSL и брандмауэра. Вы можете интегрировать решение 802.11b в большинство других проверенных и безопасных решений.

Знакомимся с устройствами

Для успешного подключения к DSL сети в большинстве случаев вам необходим DSL/кабельный маршрутизатор, поддерживающий PPPoE (протокол точка-точка по Ethernet). Ни одно из рассмотренных устройств не имеет каких-либо проблем с подключением. Они соединяются за несколько секунд. В дополнение к PPPoE, некоторые маршрутизаторы также могли работать с другими протоколами типа PPTP (туннельный протокол точка-точка), поддержка которого требуется для некоторых DSL/кабельных провайдеров.

Важным фактором при оценке производительности WLAN является измерение дальности. Я находил максимальную дистанцию (точка-точка) между точкой доступа и устройством, при котором происходила устойчивая передача данных. Каждое тестируемое устройство подключалось в другой комнате, и между точкой доступа и устройством находилось, по крайней мере, две стены и дверь.

Поскольку планировка каждого дома или офиса индивидуальна, полученные данные по расстояниям будут не всегда соответствовать действительности. Однако поскольку тестировались все беспроводные маршрутизаторы в равных условиях, то можно считать сравнение достоверным.

Методика тестирования

Я постарался создать тестовое окружение для беспроводной точки доступа WLAN максимально близко к типичному офисному окружению. Точка доступа подключалась через 10/100 Мбит/с коммутатор HP к DHCP и файловому серверу, на котором работал Red Hat Linux 7.3. При передаче данных использовался стек протоколов TCP/IP. Клиентом был ноутбук Dell Inspirion 2650 с Windows XP. Что касается беспроводной PC Card, то использовалась модель того же производителя, чья точка доступа проходила тестирование.

Для оценки дружественности к пользователю беспроводных точек доступа, сначала конфигурировась точка доступа по интерфейсу WLAN. Если процедура конфигурации требовала Ethernet или подключения к последовательному порту, то соответственно эргономика снижалась. Особое внимание было уделено дружественности самой процедуры настройки.

Как только установка была закончена, далее начиналась провека максимальной пропускной способности при передаче данных. Для этого копировался (при идеальных беспроводных условиях) 100 Мб файл и 520 Мб каталог, содержащий несколько тысяч отдельных файлов на файловый сервер. Тест проводился три раза в обоих направлениях — от ноутбука на сервер и наоборот. Одна серия тестов была проведена с включенным WEP (Wired-Equivalent-Privacy) шифрованием и одна — с выключенным. Все протестированные продукты поддерживали максимальный уровень шифрования — 128 бит.

Важный тестовый критерий — дальность работы и функциональность

Чтобы проверить дальность, нужно поместить точку доступа в одно и то же место, а затем передвигать клиента за поле действия WLAN. При тестировании использовался тот же 100 Мб файл для проверки стабильности связи с шифрованием и без него.

Не менее важна и функциональность. Сколько существует способов конфигурации точки доступа (веб-браузер, собственные программы); имеет ли устройство порт для внешней антенны или для коммутатора и т.д.

Глава 7. Беспроводные устройства: как сделать правильный выбор

Вроде одно и то же, да не совсем

В условиях жесткого ограничения ресурсов создатели каждой из платформ умудрились вместить в нее огромное число функций и каждая из них имеет полнофункциональную среду ОС, обладающую такими характеристиками, как мультизадачность, управление памятью и полный набор средств для разработки сторонних приложений. Все платформы обеспечивают безопасность, главным образом используя средства VPN, и поддерживают самые распространенные технологии беспроводных сетей, в частности IrDA и Bluetooth (для личного использования) и CDMA 2000 1X и GSM/GPRS (в глобальных сетях). При этом многие из них поддерживают беспроводные сети Wi-Fi.

Все платформы снабжены встроенными средствами органайзера и работают с наиболее популярными системами обмена сообщениями — SMS и MMS. Каждая из платформ работает с ведущими почтовыми системами, например с Microsoft Exchange, Lotus Notes, и с протоколами Интернет IMAP и POP3. У всех у них имеются отвечающие условиям компактного отображения браузеры WML (Wireless Markup Language) и HTML, и все они способны обеспечить сетевое взаимодействие по TCP/IP. И наконец, ведущие поставщики ПО, например IBM и Oracle, уже переносят свои корпоративные приложения на каждую из этих платформ.

Различия между платформами, а иногда и продуктами внутри семейства диктуются тем, как предполагается использовать соответствующее устройство — преимущественно в качестве телефона или же портативного компьютера. Мало вероятно, чтобы комбинированный агрегат «телефон-КПК» столь же хорошо справлялся с конкретной задачей, как и соответствующее специализированное устройство. Кроме того, каждая из платформ имеет уникальный пользовательский интерфейс и реализует свой подход к обеспечению безопасности. Так, компания RIM разработала собственную модель сквозного обеспечения безопасности, PalmSource и Symbian используют VPN-средства третьих фирм, а Microsoft включила в список поддерживаемых протоколов PPTP и L2TP/IPsec VPN.

И хотя поддержку Java обеспечивают все платформы, но фирма Symbian предлагает еще и программные интерфейсы MIDP 2.0 и Personal

Java 1.1.1a. Как и следовало ожидать, платформы Microsoft, предоставляют наиболее сильную поддержку для .Net, хотя пользователям доступны и средства от третьих фирм, если они хотят работать в средах программирования Microsoft — OLE, .Net и Visual Basic. Различия наблюдаются и в браузерах, в части форматирования и представления сложных страниц, в результате для просмотра некоего контента одно устройство может оказаться значительно удобнее, чем его конкуренты.

Еще одна отличительная черта — поддерживаемые беспроводные сети. Ранее существовала тенденция, согласно которой карманные ПК поддерживали Wi-Fi или сотовую связь, а смартфоны — сотовую связь, но сейчас все большее число смартфонов поддерживают и Wi-Fi.

Что же касается тенденций в пользовательских предпочтениях платформ, то, по результатам опросов наших читателей, при оценочной шкале от 1 до 7 взвешенная средняя оценка для всех платформ составила от 3 до 5 без явных победителей и проигравших. Если расставить их по порядку от большего к меньшему, то список предпочтений будет выглядеть так: Microsoft Pocket PC, Palm OS, RIM Blackberry, Linux, Microsoft SmartPhone и Symbian. Большинство читателей предпочитают КПК.

Относительно характеристик, которые корпоративный пользователь считает самыми важными, можно сказать, что превыше всего ценится система безопасности.

Фавориты

Этот рынок просто еще «не дозрел», чтобы объявить единственного победителя. Нас отделяют годы от того времени, когда какая-либо из платформ станет по-настоящему «массовой». Хотя все они реализованы на хорошем уровне, но в долгосрочной перспективе вряд ли стоит ожидать, что рынок будет поддерживать более одной-двух из них.

Телефонные коммуникации: Symbian. В платформе Symbian основной упор сделан на сильные функции телефонии и на интеграцию их с обработкой данных. Учитывая, что главная «движущая сила» этой платформы — компания Nokia является ведущим производителем мобильных телефонов в мире, неудивительно, что самые продаваемые смартфоны базируются на Symbian. Лицензиаты Symbian поставляют по всему миру большой ассортимент разнообразных устройств, включая телефоны с обычной тастатурой и вводом данных с помощью пера, а также телефоны, снабженные стандартной алфавитно-цифровой клавиатурой Qwerty.

Электронная почта: RIM. Платформа RIM доказывает, что для успеха в сфере мобильных беспроводных коммуникаций модель настоль-

ной системы не годится. Тут необходимо полностью переосмыслить сам процесс работы людей с данными, с чем RIM справилась просто превосходно.

Мобильная передача данных: Microsoft и PalmSource. Для мобильной передачи общецелевых данных компания PalmSource разработала самый лучший на данный момент КПК с функциями телефона — Treo 600. Он может использовать огромную базу инсталлированных приложений Palm, которая практически гарантирует, что найдется «готовое к употреблению» приложение, подходящее для ваших нужд. Со своей стороны Microsoft обеспечивает самую мощную и гибкую операционную среду — Windows Mobile и сильную поддержку корпоративных пользователей, особенно тех, чья рабочая среда базируется на продукции этой компании. Кроме того, ОС от Microsoft обладает самыми сильными сетевыми средствами. Palm и Microsoft перенесли «поле битвы» на рынок мобильных телефонов, где им придется отныне соперничать и с Symbian.

Все платформы Linux

Самая последняя версия этой ОС для встроенных систем, т.е. для КПК и телефонов, имеет номер 2.6. Это мощная ОС с расширенными средствами обеспечения производительности в реальном времени, гибким вводом-выводом и поддержкой микроконтроллеров и больших объемов памяти. Хотя доля Linux на этом рынке пока ничтожно мала, со временем эта ОС может стать на нем основной, особенно когда аппаратные платформы нарастят свою вычислительную мощь и если ей окажут предпочтение поставщики мобильных телефонов. Пока же одним из немногих производителей, поставляющих смартфоны на базе Linux, является компания Motorola. Карманный компьютер Zaurus PDA фирмы Sharp также использует Linux, однако для беспроводной связи ему требуется модем.

Когда Linux завоюет большую долю серверного рынка, мобильные Linux-устройства смогут обеспечить «бесшовный» доступ к серверным данным и более комфортную среду разработки для самих организаций и независимых поставщиков ПО. Кто станет движущей силой данного рынка — поставщики мобильных телефонов, такие, как Motorola, или поставщики Linux, вроде Red Hat, — покажет время.

Microsoft

Уже не один год Microsoft, используя платформу Windows CE, ведет планомерное наступление на рынок КПК, медленно оттесняя с завоеванных позиций Palm. Сейчас Windows CE разделилась на две базовые версии: Pocket PC для КПК, и Windows SmartPhone для мобильных телефонов высокого класса. Обе они являются составной частью того, что Microsoft называет Windows Mobile. Pocket PC, в свою очередь, подразделяется еще на две версии — для обычных КПК и для КПК с функциями мобильного телефона. Последняя именуется Pocket PC Phone Edition.

Что касается устройств, поддерживающих платформу Microsoft, то здесь доминирует компания Hewlett-Packard (HP) со своей линией продуктов iPAQ. HP поставляет также Wi-Fi и Bluetooth-версии, но собственно телефонов в ее линии пока нет. В число поставщиков устройств, работающих под управлением Pocket PC Phone Edition, входят компании Audiovox, Hitachi и Samsung.

Другая платформа Microsoft — Windows SmartPhone пока не получила широкой поддержки со стороны производителей телефонов, но некоторые модели с этой ОС уже начинают поставляться на рынок в значительных объемах, как, например, MPx200, распространением которой занимается AT&T Wireless. Этот телефон обладает почти теми же средствами, что и Pocket PC, но предполагается, что человек сможет работать с ним одной рукой, и для ввода данных в нем используется телефонная тастатура, а не перо.

Для всех платформ, входящих в серию Windows Mobile, Microsoft обеспечивает мощные средства разработки и обещает пользователям тесную интеграцию со своими информационными системами. Хотя число сторонних поставщиков для них меньше, чем для Palm, Microsoft упоминает о тысячах внутренних корпоративных приложений, созданных самими компаниями для ее мобильных платформ. Если и вы захотите разработать такое приложение, Microsoft предлагает вам на выбор три подхода: Embedded Visual C++; разработка в среде .Net Compact Framework — «мобильной» версии платформы .Net и, наконец, инструментарий для web-разработки. Кроме того, можно воспользоваться версией J2ME языка Java с программным интерфейсом MIDP1.0. Платформа Windows Mobile поддерживает почтовые протоколы Microsoft и стандартные почтовые протоколы. Поддержка служб обмена сообщениями включает EMS, SMS, MMS, IM и WAP поверх SMS. Имеется также доволно удобный браузер.

Windows Mobile поддерживает множество протоколов беспроводных сетей, включая CDMA 1X, GPRS, Wi-Fi, IR и Bluetooth. С изначальной поддержкой IPsec, L2TP и IPPTP, а также с 13 независимыми поставщиками продуктов VPN-предложение от Microsoft сильнее, чем у любого из ее конкурентов.

Но, хотя платформа Pocket PC хорошо подходит для КПК, в индустрии средств беспроводной связи испытывают некоторые опасения по поводу доминирования Microsoft в этой области. Этим и объясняется,

почему Nokia, Sony Ericsson и Siemens объединились в использовании платформы Symbian для смартфонов. Впрочем, невзирая на все сопротивление телефоны под управлением Windows SmartPhone уже появились на рынке и на подходе их новые модели.

PalmSource

Хотя родоначальником концепции планшетных компьютеров является не компания Palm, а Apple с ее разработкой Newton, именно Palm сделала ее успешной и по-прежнему доминирует на этом рынке. Сейчас компания поделена на две — PalmSource, которая занимается поставкой ОС, и PalmOne, отвечающая за устройства.

Несмотря на резкий первоначальный рост, рынок КПК сейчас замер на уровне примерно 10 млн устройств в год, и Palm, как и все прочие поставщики, сосредоточила свои усилия на беспроводных платформах, в том числе на тех из них, которые поддерживают Wi-Fi, например Tungsten T, и сотовую связь, в частности Treo 300, 400 и 600. Линия Treo была разработана компанией Handspring, которую Palm недавно приобрела. Любопытно, что когда-то ее основали «перебежчики» из Palm. И хотя уровень продаж Treo 300 и 400 не слишком впечатляющий, похоже, что эти устройства смогут составить серьезную конкуренцию своим аналогам на рынке смартфонов. Особую силу позициям Palm придает огромное число приложений, доступных для ее платформы. Кроме того, у нее много преданных сторонников среди пользователей КПК, которые и при выборе беспроводной платформы будут тяготеть к продукции Palm.

Palm заявляет о более 20 тыс. наименований ПО для своей платформы. Это больше, чем у любой другой мобильной платформы. Звучит правдоподобно, принимая во внимание давнюю успешную историю карманных компьютеров Palm. Однако все же стоит заблаговременно узнать, предлагаются ли сейчас нужные вам приложения. Кроме того, написанные для предыдущих версий ОС приложения не всегда работают под новыми ее версиями. В этом случае вам помогут разнообразные средства разработки Palm, включая языки C, C++, подходы с использованием экранных форм, средств Java (J2ME и MIDP 1.0) и Visual Basic.

Платформа Palm поддерживает все основные протоколы электронной почты и обмена сообщениями и снабжена отвечающим всем требованиям браузером. Шестнадцать производителей оборудования поставляют 46 различных устройств Palm, но лишь часть из них широкодоступны. Три отдельных VPN-решения предлагаются сторонними компаниями. Беспроводная поддержка включает в себя CDMA 2000 1X, GPRS/EDGE, UMTS/WCDMA, Wi-Fi, IR и Bluetooth.

В модели Treo 600 используется Palm OS 5. И компания уже объявила о том, что готова следующая версия ее ОС, получившая название Cobalt. Она полностью переписана и обеспечивает такие возможности, как мультизадачность, многопоточность, защита памяти, поддержка больших объемов памяти и больших экранов, средства безопасности, соответствующие промышленному стандарту, плюс связующие среды framework для коммуникаций и мультимедиа, способные справляться со множеством соединений одновременно. PalmSource также выпустила усовершенствованную версию OS 5 под названием Garnet, снабженную стандартной поддержкой широкого диапазона разрешений экрана, динамичной областью ввода данных, усовершенствованными средствами сетевых коммуникаций и Bluetooth. Судя по всему, на рынке будут предложены обе версии данной ОС, причем Cobalt рассчитано на продукты более высокого класса, а Garnet — на устройства массового рынка и обе они могут использоваться в сетях беспроводной связи.

Research In Motion

Самым успешным поставщиком средств для беспроводной доставки данных стала компания RIM со своей линией продуктов Blackberry. Когда-то это были всего лишь технические «игрушки» размером с пейджер, теперь же RIM предлагает устройства размером с КПК, с цветными экранами и функциональностью мобильных телефонов. Секрет популярности продуктов компании RIM заключается в том, что она предлагает полнофункциональную систему обмена сообщениями, включающую устройство, ставшее пионером среди мини-клавиатур (типа thumb keyboard), управление электропитанием, позволяющее получать сообщения без необходимости держать устройство постоянно включенным, хороший почтовый клиент и шлюз к корпоративным почтовым системам. В результате получилась простая в работе мобильная почтовая система, обеспечивающая автоматическую доставку сообщений электронной почты пользователям методом «выталкивания» (push). В качестве альтернативы можно использовать и механизмы опроса почтового сервера, они хоть и работают, но не так удобны.

RIM перечислила 125 сторонних поставщиков приложений, входящих в ее программу ISV Alliance (Альянс независимых поставщиков ПО). Это несколько меньше, чем у конкурентов, ведь компания только недавно открыла свою платформу для приложений третьих фирм. Опции разработки включают Java, браузерный подход и C++, причем средства разработки предлагают пять поставщиков. Самая сильная составляющая платформы RIM — электронная почта, снабженная поддержкой всех основных почтовых протоколов. Браузер поддерживает HTML и WML, что позволяет использовать его как клиент для приложений, разработанных

на языках C++ и Java. Компания RIM выпускает 15 версий своего устройства.

Что касается безопасности, то здесь вместо поддержки стандартных VPN-служб RIM предлагает свою собственную сквозную модель безопасности, требующую добавления в корпоративную среду сервера Blackberry.

В число поддерживаемых беспроводных сетей входят как традиционные пакетные сети (DataTAC и Mobitex), так и новые сотовые (CDMA 1X, GSM/GPRS, Nextel IDEN).

Остается вопрос: насколько удачной окажется эволюция платформы RIM от служб обмена сообщениями к общецелевым приложениям беспроводных сетей? Страхуя свои ставки, RIM проводит лицензирование Blackberry, чтобы и другие беспроводные платформы смогли получать доступ к ее почтовым шлюзам. Так, например, устройства Sony Ericsson P900 Symbian скоро будут предлагать Blackberry-клиент. И это вполне разумно с учетом того, что RIM невзирая на все свои успехи имеет всего один миллион подписчиков.

Symbian

Последний «тяжеловес» на рынке беспроводных платформ — Symbian, это совместное предприятие Psion, Nokia, Sony Ericsson, Siemens и Samsung. Symbian появилась как ответ на идею, что сложность ПО следующего поколения требует общих усилий основных поставщиков мобильных телефонов. Смартфоны, базирующиеся на платформе Symbian, поставляют сейчас все перечисленные партнеры, а также Sendo и Motorola. Телефоны Symbian доминируют на этом рынке частично из-за того внимания, которое уделяют их функциональности лицензиаты Symbian, но в большей степени все-таки благодаря позиции, занимаемой на рынке главными лицензиатами.

Устройства Symbian отличаются разнообразием форм, включая устройства со стандартной телефонной тастатурой или с пером и сенсорной панелью, а некоторые из них даже с полнофункциональной клавиатурой. Размеры дисплеев также самые разные. Symbian предлагает производителям телефонов лицензии на версию ОС, носящую название UIQ, тогда как Nokia занимается лицензированием другой версии, с названием Series 60. В свою очередь, производители телефонов тоже расширяют возможности своих продуктов.

Специалисты Symbian перечисляют более 2 тыс. предлагаемых коммерческих приложений, многие из которых предназначены для бизнеса. Разработчики могут работать на C++, Java J2ME с MIDP 2.0,

Personal Java 1.1.1a, Visual Basic или WAP. Средства разработки поставляют девять компаний. Поддерживаемые почтовые протоколы включают POP3, IMAP4, SMTP и MHTML, а службы обмена сообщениями — EMS, MMS, SMS и факс. Поддержка браузеров в платформе обеспечивается за счет сторонних решений и архитектуры подключаемых браузерных модулей (plug-in). Теперь что касается оборудования: 5 поставщиков предлагают 15 различных устройств. Поддержку VPN обеспечивает клиент от фирмы Certicom. Поддержка беспроводной связи включает Bluetooth, IrDA, CDMA 1X, GPRS, EDGE и WCDMA.

Недавно Nokia приобрела долю Psion в Symbian и теперь владеет контрольным пакетом акций, тогда как Motorola покинула ряды Symbian. У платформы Symbian есть свои технические преимущества, но только время покажет, сумеет ли она преуспеть в качестве ОС для смартфонов, предлагаемых множеством поставщиков, или же превратится в платформу, где доминирует Nokia. Symbian еще предстоит побороться за пользователя в США, где ее конкуренты уже получили достаточную известность.

Приложения

Wi-Fi на службе оператора

Публичные Wi-Fi-сети становятся все более популярной услугой. Однако при внедрении таких услуг в операторских сетях возникает ряд проблем, и прежде всего проблема биллинга. Каковы же пути их решения?

Пожалуй, беспроводные технологии сегодня являются самой актуальной темой. Местные операторы связи уже сделали первые шаги в направлении развертывания систем Wi-Fi. Интересно, что в России это были сотовые компании, а в Украине развертыванием публичных сетей Wi-Fi занялся национальный телекоммуникационный оператор Укртелеком.

Однако темпы внедрения подобных решений не очень высоки по сравнению с использованием услуг GPRS, MMS, сетей третьего поколения, которые уже получили распространение в мобильной сфере. Попрежнему популярным остается «технологический» подход к внедрению новых услуг: 11 Мбит/с — хорошо, а 54 Мбит/с — еще лучше. При этом маркетинговый аспект, то есть то, как предложить абоненту новые услуги, часто отходит на второй план. Услуги на базе технологий семейства WLAN занимают различные рыночные ниши. WLAN — это и беспроводной удлинитель для дома, позволяющий в любое время в любом месте через ноутбук работать с Интернетом; и последняя миля для доступа к интернету в масштабах микрорайона или коттеджного поселка; и беспроводной офис, в пределах которого сотрудники могут перемещаться, не теряя связи с интране-том и интернетом. Отдельную нишу со своими особенностями и характеристиками занимают приложения WLAN для телекоммуникационных операторов, в первую очередь сотовых.

Согласно данным отчета, подготовленного исследовательской компанией Analysys Research, сегодня насчитывается от 10 до 20 тыс. активных пользователей WLAN, большая часть которых приходится на США. Однако уже к 2006 году, по прогнозу Analysys, только в Европе услуги публичных WLAN привлекут более 20 млн. человек, что принесет операторам этих сетей доход в размере 3 млрд. евро.

Основным фактором, определяющим развитие рынка беспроводных сетей, по мнению специалистов Analysys, является широкое распространение технических платформ на основе стандарта IEEE 802.11b. С одной стороны, стремительно растет число мобильных устройств (карманных компьютеров, телефонов, ноутбуков), продаваемых со встроенными средствами беспроводного доступа, а с другой — более 100 тысяч компаний по всему миру уже используют технологии WLAN при создании корпоративных сетей.

Авторы отчета, однако, заявляют, что операторам публичных беспроводных сетей предстоит решить целый ряд проблем, в частности, связанных с расширением зоны покрытия. Опыт США показывает, что европейским операторам следует заключать соглашения о роуминге как можно раньше, поскольку это позволит уменьшить общие расходы на развертывание точек доступа в публичных местах: к 2006 году планируется охватить беспроводной сетью около 90 тысяч публичных мест. С другой стороны, Analysys отмечает, что WLAN представляют собой реальную угрозу операторам 2,5/3С-сетей сотовой связи.

По оценкам компании, к 2006 году до 10% владельцев мобильных телефонов будут также пользоваться услугами операторов публичных WLAN, что чревато соответственно 10%-ным снижением трафика данных по GSM-каналам. GSM-операторам может помешать и другой аспект: компания Sharp, например, намерена предложить сервис Интернет-телефонии с использованием своих КПК Zaurus. Связь будет предоставляться на базе 300 WLAN-сетей оператора NTT Communications Corp. Абоненты получат возможность совершать неограниченное число звонков, но при этом должны будут платить абонентскую плату и оплачивать использование WLAN-сетей (в общей сложности — около $20 в месяц).

Зачастую данные, говорящие о степени внедрения публичных WLAN, касаются в основном исключительно количественных показателей развития инфраструктуры — установлены новые тысячи базовых станций, охвачены новые рестораны, кафе, бизнес-центры, подключены бензозаправки; непрерывно сообщается также о росте количества ноутбуков с поддержкой WLAN. Hot-spot устанавливают уже даже в поездах и самолетах.

При этом большинство аналитиков и экспертов оценивают потенциал Wi-Fi-услуг очень высоко. Однако для операторов ключевым является вопрос получения дополнительных доходов от WLAN, причем в недалекой перспективе.

Причины и следствия

Технологии беспроводного локального доступа к Интернету известны давно, но долгое время их использование ограничивалось пределами офисов, а главным их преимуществом считалась мобильность персонала и включение в сеть гостевых посетителей. Что же подвигло телекоммуникационных операторов на стремительное развертывание сетей Wi-Fi? Конечно же, проникновение Интернет-технологий во все сферы жизни, а также успехи и вызванные ими новые проблемы передачи данных в сетях сотовых операторов. Одной из современных задач является доступ к Интернет-ресурсам как из дома и офиса, так и из любой точки.

Для решения этой задачи используются самые различные технологии: ADSL, LMDS, GPRS, UMTS. GPRS долгое время считалась универсальным решением, и оборудование GPRS было внедрено практически во всех сотовых сетях. Однако первые результаты были достаточно скромными. Последующий анализ ошибок, допущенных при внедрении GPRS, позволил скорректировать их использование, и услуги на базе данной технологии обрели большую популярность.

Теперь сети перегружены трафиком передачи данных. Беспроводной мобильный доступ к Интернету становится все более и более распространенным, и совершенно очевидно, что только с помощью GPRS проблему увеличения пропускной способности сетей не решить. Причем те абоненты, которые достаточно часто работают с системами пакетной передачи данных, могут подтвердить, что характер трафика можно определить очень четко. Места, в которых концентрируется трафик передачи данных, очевидны, как очевидны и временные закономерности возникновения пиков трафика и их перемещения по различным зонам сети.

На основе этого можно сделать следующие выводы:

- очень часто доступ к Интернету требуется в строго определенных местах;
- обычно в этих местах необходимы именно высокоскоростные приложения;
- для многих пользователей услуги GPRS востребованы именно из-за возможности глобального покрытия и доступности в любом месте — на даче, в дороге, в офисе партнеров, то есть там, где фактически невозможно применить другую технологию доступа к Интернету.

В связи с этим возникла идея использовать WLAN для разгрузки GPRS-сетей и предоставления комбинированных услуг. Но уже на начальном этапе возникли проблемы, и первые установленные базовые станции отнюдь не были перегружены трафиком. Почему так происходит? Первая проблема — это отсутствие пользовательского оборудования у большинства абонентов.

Есть и другие трудности, и в первую очередь, это ошибки, допускаемые при позиционировании hot-spot. Несмотря на первые успехи GPRS, одного анализа трафика сетей пакетной передачи явно не достаточно. При принятии решения о развертывании WLAN часто действует простая бизнес-логика: абонентам просто необходим доступ к Интернету. Напрашивается вывод — базы WLAN нужно устанавливать во всех местах, где наблюдается скопление абонентов. Подобный принцип является верным, однако следует учитывать целый ряд факторов, которые могут повлиять на поведение будущих абонентов.

Во-первых, в отличие от спроса на GPRS-услуги, спрос на WLAN формируется не только благодаря пользователям мобильного Интернета, но и благодаря владельцам портативных компьютеров, которых гораздо меньше.

Во-вторых, пользователи еще не достаточно информированы о достоинствах WLAN, не уверены в их информационной безопасности и из-за незначительной распространенности hot-spot сомневаются в их доступности там, где они могут понадобиться.

В-третьих, существует определенная конкуренция со стороны более традиционных способов передачи данных — как проводных, так и мобильных.

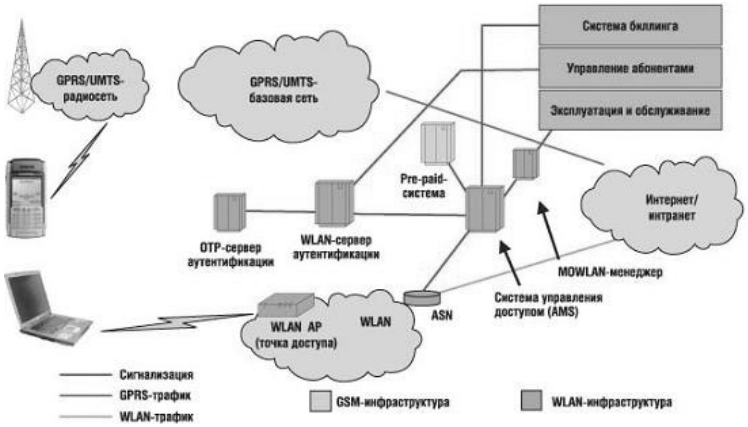
Таким образом, можно сделать следующие выводы:

- отдельные островки WLAN большой роли не сыграют. Для потенциальных пользователей интересны сети, покрывающие всю страну;
- сети должны работать под единой торговой маркой, обеспечивая пользователю качество услуг, безопасность, гибкую оплату и возможность пользоваться единым счетом в разных городах;
- необходимо развертывать WLAN в хорошо продуманных местах, причем в этом случае принципиально важны и анализ трафика GPRS, и проработка бизнес-модели, и маркетинговые исследования.

Подход, основанный исключительно на принципе привлечения максимального количества абонентов, может в ряде случаев не работать. Понятно, что для организации «последней мили» для одного микрайона не нужно строить сеть в масштабах страны. Но WLAN-сети, построенные на перечисленных принципах, более конкурентоспособны и могут занять свою рыночную нишу как для местных абонентов, так и для тех, кто пользуется услугами роуминга. Это огромный потенциал для сотовых и национальных телекоммуникационных операторов. Кроме того, у этих компаний есть хорошо узнаваемый бренд и налаженная система сбыта, а также отработанная модель партнерских отношений, что создает для подобных фирм дополнительные конкурентные преимущества при развертывании нового бизнеса.

Комплексный подход — важнейший аспект в построении WLAN-сети, ведь для конечного пользователя важен целый ряд характеристик: простота, надежность, удобство, гибкость расчетов с оператором и др.

В свою очередь, оператор сотовой сети, внедряя вторую систему радиодоступа, стремится минимизировать свои инвестиции и уменьшить затраты на эксплуатацию системы. Не каждая система WLAN удовлетворяет вышеуказанным требованиям.



Аспекты внедрения

Итак, какие же ключевые моменты нужно учитывать при внедрении WLAN-системы в дополнение к сотовой сети GSM, ведь совершенно очевидно, что во многом системы GSM и WLAN являются взаимопроникающими?

Несомненно, вопросы тарификации и удобства оплаты для конечного пользователя должны быть на первом месте. Желательно иметь один счет для всех услуг, предоставляемых сотовым оператором. Как следствие, необходима тесная интеграция с системой биллинга и, безусловно, pre-paid-системой сотового оператора. В противном случае pre-paid-абоненты могут остаться без дополнительных услуг (WLAN).

Особое внимание необходимо уделить удобству работы со счетом. Так, наиболее перспективным является использование web-интерфейса для проверки и пополнения (например, с помощью кредитной карты) баланса, просмотра статистики. Также можно создать pre-paid-счет через этот интерфейс и устанавливать дату окончания срока действия счета. Такой подход, реализованный в системе WLAN, будет максимально удобным и для абонента, и для персонала абонентских служб оператора.

Удобство аутентификации пользователей также является немаловажным фактором для абонентов, а надежность и гибкость этой системы принципиально важны для операторов. Рассмотрим возможные варианты аутентификации.

Аутентификация по статическому паролю является наиболее простым, широко применяемым, но неудобным методом, основанным на web-аутентификации. При необходимости использования услуг WLAN абоненту в качестве первой страницы предлагается web-страница с формой, в которой нужно указать свой пароль и имя пользователя. Эту информацию абонент может получить, купив карту, где указан единовременный пароль и имя.

Недостатком такого решения являются связанные с этими картами дополнительные затраты, которые не нужны ни оператору (печать, распространение, дополнительная система тарификации по картам), ни пользователю (покупка, сохранение данных).

Метод аутентификации по статическому паролю характерен для автономных систем с минимальной степенью интеграции с инфраструктурой сотового оператора и вряд ли устроит сотовых гигантов, однако может вполне подойти традиционным телекоммуникационным операторам.

Следующий метод — WLAN-аутентификация с использованием SIM-карты. Приведенная ниже схема достаточно наглядно иллюстрирует схему взаимодействия отдельных узлов сети GSM и WLAN. При попадании в зону работы базовой станции WLAN-запрос на аутентификацию направляется на абонентский ноутбук, который должен иметь SIM-адаптер, и вся информация, необходимая для аутентификации пользователя, считы-вается с его SIM-карты.

Несомненным преимуществом в этом случае является упрощение модели аутентификации, а недостатком — усложнение процедуры: возникает необходимость в SIM-адаптере, в который надо устанавливать персональную SIM-карту или отдельную SIM-карту только для услуги WLAN. Такой метод устроит сотового оператора, ибо подразумевает интеграцию с сетью GSM и получение информации об абоненте с его SIM-карты, что упрощает универсальную тарификацию для услуг GSM и WLAN.

Пожалуй, наиболее прогрессивной является аутентификация с помощью одноразового пароля (One Time Password). Кроме того, что этот тип аутентификации использует преимущества SIM-карт, при этом еще и не требуется никаких манипуляций с самой картой, и она продолжает оставаться в сотовом телефоне.

Если нужно воспользоваться услугами WLAN, абонент прежде всего должен заполнить web-форму, указав в ней номер своего мобильного телефона. По этому номеру система проверит, открыты ли подобные услуги для абонента, доступен ли счет, а затем вышлет абоненту одноразовый пароль с помощью SMS-сообщения.

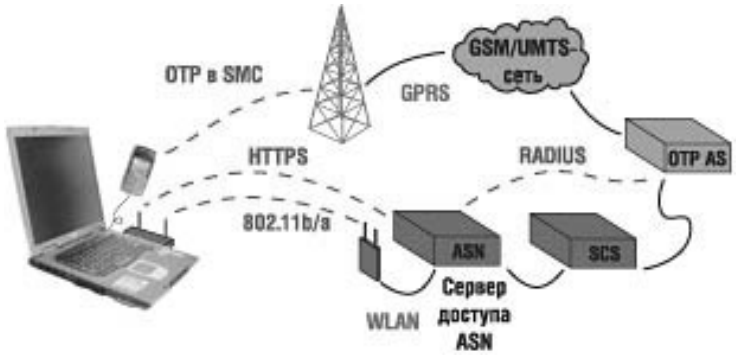
В качестве имени для входа можно использовать номер мобильного телефона. Гарантией правильности получения этого пароля является наличие у абонента указанного GSM-телефона, другой же абонент данный SMS получить не может в принципе. Таким образом, преимущества такого метода вполне очевидны.

А теперь рассмотрим особенности внедрения WLAN-систем в сетях сотовых операторов на конкретных примерах.

Внедрение услуг на базе технологии WLAN с SIM-аутентификацией позволит оператору предоставлять высокоскоростной удаленный доступ к Интернет-ресурсам и корпоративным сетям большому количеству абонентов одновременно, при этом для проверки абонентов будет использоваться информация, хранящаяся в GSM-подписке.

Для работы в данной сети абоненту необходимо иметь ноутбук, SIM-карту, PCMCIA WLAN-адаптер и SIM-адаптер (устройство для чтения SIM-карт в PCMCIA или в USB-исполнении). Беспроводные сети стандарта IEEE802.11Ь строятся на основе базовых станций оператора, подключаемых в его транспортную сеть. Радиус покрытия одной точки доступа составляет около 100 метров и может масштабироваться за счет установки дополнительных точек доступа. Одна точка доступа может одновременно поддерживать несколько десятков активных пользователей и обеспечивает скорость передачи информации для конечного абонента до 11 Мбит/с.

Также компания Ericsson и датский оператор мобильной связи TDC Mobil подписали контракт на развертывание WLAN-системы в сети оператора мобильной связи. Система позволит улучшить качество услуги GPRS и UMTS компании TDC Mobil, обеспечив широкую полосу пропускания в стратегически важных общественных точках доступа. Пользователи переносных и карманных компьютеров получат защищенный мобильный доступ к необходимым ресурсам со скоростью проводных локальных сетей. К тому же, система обеспечивает таким пользователям доступ к Интернету и корпоративным сетям. Для работы может использоваться любой переносной или карманный компьютер, укомплектованный платой WLAN и одним из популярных Интернет-браузеров. Корпоративным пользователям предоставляются VPN-каналы и сетевые экраны для защиты данных. Безопасность доступа к WLAN-услуге для всех пользователей обеспечивается механизмом предоставления одноразового пароля с помощью SIM-карты мобильного терминала.



Советы оператору

Итак, при внедрении систем WLAN сотовому оператору прежде всего необходимо тщательно проработать бизнес-стратегию и опреде-

лить ту целевую группу, которой будут предложены услуги WLAN. Как следствие, необходимо охватывать именно те точки, где система будет максимально востребована.

Не менее важна проработка стратегии внедрения и развертывания сети, и один из возможных вариантов — привлечение третьих компаний не столько для выполнения монтажных работ, сколько для поиска и организации партнерских отношений с владельцами hot-spot. Также очень важно выбрать максимально гибкую и надежную систему WLAN, способную интегрироваться с существующей сотовой сетевой инфраструктурой и обеспечивающую простоту и удобство для конечного пользователя.

Наличие такой функции, как автоматическое обновление абонентских данных, поможет снизить затраты на содержание полноценной системы радиодоступа WLAN. В этом случае запись о новом пользователе возникает в базе данных системы WLAN с момента первой сессии. Это значительно упрощает работу абонентских отделов.

Весьма необходимой для системы WLAN является функция управления типами услуг. В системе WLAN необходимо иметь несколько классов услуг, у каждой из которых будут собственные права доступа, ограничения по полосе пропускания, набор дополнительных услуг. С помощью заполнения web-страницы абонент может сам выбирать тот или иной класс обслуживания. Таким образом, оператор свободен и в выборе схемы тарификации для разного класса услуг.

Принимая во внимание в будущем внедрение UMTS, не последнюю роль будет играть совместимость с сетями третьего поколения, включая работу с U-SIM. Принципиальное значение имеет также поддержка роуминга, но это, пожалуй, очевидная вещь.

Возможности технологии Bluetooth

Технология Bluetooth предназначена для организации беспроводных персональных сетей.

В настоящее время средства Bluetooth встраиваются в сотовые телефоны, карманные ПК, беспроводные точки доступа, телефонные гарнитуры, клавиатуры, мыши, принтеры и даже цифровые ручки (digital pens). Однако, несмотря на доступность, до сих пор эта технология не получила широкого применения. Вероятно, данная ситуация вскоре изменится, поскольку поддержка Bluetooth включена в пакет Service Pack 2 для ОС Windows XP.

Кроме того, по данным исследовательской компании Allied Business, каждый третий проданный в США в этом году мобильный телефон имеет функциональность Bluetooth.

До недавнего времени одним из основных препятствий на пути распространения технологии Bluetooth являлась сложность ее использования, особенно если вы хотели заставить взаимодействовать несколько устройств Bluetooth друг с другом. Но сейчас благодаря улучшенным мастерам конфигурации и поддержке Bluetooth в составе ОС Windows XP вы можете сконфигурировать эти устройства менее чем за 5 мин.

Связь по технологии Bluetooth устанавливается автоматически и почти мгновенно (на соединение устройств кабелем уходит больше времени). Применение средств Bluetooth, дальность действия которых, как правило, составляет около 10 м, позволяет отказаться от использования кабелей для соединения персональных электронных устройств. Например, с помощью технологии Bluetooth вы можете подключить ноутбук или карманный ПК к сотовому телефону и задействовать последний в качестве беспроводного модема.

Но почему бы в этих же целях не использовать технологию Wi-Fi? Дело в том, что технология Bluetooth специально разработана для замены кабельных соединений (хотя ее можно применить и для имитации работы локальной сети). В отличие от стандарта 802.11 (Wi-Fi) в технологии Bluetooth предусмотрены профиль обнаружения услуг (service discovery) и другие профили, дающие возможность устройствам сразу же после установления беспроводного соединения автоматически предоставлять друг другу требуемые услуги (так, принтер предоставит услугу печати сотовому телефону). Кроме того, в отличие от оборудования стандарта 802.11 средства Bluetooth работают с меньшей выходной мощностью (1 или 10 мВт) и ориентированы на образование одноранговых (ad hoc) сетей. Совершенствованием спецификации Bluetooth (стандарт IEEE 802.15.1) занимается ассоциация Bluetooth Special Interest Group.

Как она работает

Связь по технологии Bluetooth осуществляется в рамках пикосети, состоящей из одного ведущего (master) устройства и до семи ведомых (slave) устройств. Еще 254 устройства могут находиться в состоянии «парковки» и ожидать подключения к пикосети. Пользовательское устройство, инициирующее связь, является ведущим и управляет работой ведомых устройств в пикосети.

Оборудование Bluetooth использует частотный диапазон 2,4 ГГц (в этом же диапазоне функционируют устройства стандартов 802.11b и 802.11g) и реализует технологию расширения спектра радиосигнала по-

средством скачкообразного изменения частоты (Frequency Hopping — FH).

Чтобы не мешать работе друг друга, одна пикосеть (например, ноутбук, связанный с сотовым телефоном) отличается от другой (сотовой телефон, взаимодействующий с гарнитурой) последовательностью осуществления частотных скачков. В асимметричной конфигурации пропускная способность соединения Bluetooth может достигать 721 Кбит/с в одном направлении и 57,6 Кбит/с в другом. В симметричной же конфигурации скорость передачи данных в обоих направлениях одинакова и составляет 432,6 Кбит/с. Кроме того, пикосеть способна поддерживать три дуплексных 64-Кбит/с голосовых канала. Таким образом, пропускной способности средств Bluetooth вполне хватает для установления модемных соединений, осуществления голосовой связи, синхронизации карманных компьютеров и передачи оцифрованных изображений с низким или средним разрешением, но ее недостаточно для работы с такими устройствами, как цифровые видеокамеры.

Следует также учитывать, что два устройства Bluetooth соединяются друг с другом только в том случае, если поддерживают один и тот же профиль Bluetooth, который представляет собой набор функций, основанных на протоколах Bluetooth. В данной технологии определены профили последовательного порта (Serial Port Profile — SPP), коммутируемого доступа (dial-up networking), гарнитуры, устройства hands-free, подключения к ЛВС, факса, передачи файла и синхронизации. Итак, если сотовый телефон поддерживает только профиль устройства hands-free, а гарнитура — только профиль гарнитуры, они не будут взаимодействовать.

Профиль SPP имитирует работу соединения с последовательным портом RS-232, что дает возможность любому приложению, работающему с этим портом, использовать вместо него средства Bluetooth. Версия спецификации Bluetooth с номером 1.2 была принята в ноябре прошлого года. В ней определена поддержка адаптивной технологии FH, повышающей помехоустойчивость оборудования, а также предусмотрены уменьшение времени установления соединения, повышение качества передачи речи и расширенная поддержка распределенной сети (scatternet). О распределенной сети Bluetooth говорят в том случае, если одно и то же устройство работает в двух пикосетях. Спецификация версии 1.2 совместима со спецификацией версии 1.1.

Следуйте инструкциям

Устройствами Bluetooth просто пользоваться, если они правильно сконфигурированы. Обязательно читайте инструкции производителей

оборудования! Многие средства Bluetooth комплектуются управляющими утилитами и мастерами, помогающими конфигурировать их. В зависимости от выполняемой задачи вам, возможно, придется воспользоваться мастерами третьих фирм. Например, с помощью утилиты Communication Manager компании AT&T Wireless конфигурируют ноутбуки, чтобы передавать и принимать пакеты данных посредством Bluetooth-совместимых телефонов по сети AT&T Wireless. Поддержка Bluetooth в составе ОС Windows XP поможет вам сконфигурировать соответствующие устройства с помощью единого (для продуктов разных производителей) пользовательского интерфейса.

Любой технически «подкованный» пользователь справится с конфигурированием устройств Bluetooth, но у людей, не обладающих техническими знаниями, с этим могут возникнуть трудности. Если вы, являясь ИТ-специалистом предприятия, отвечаете за техническую поддержку пользователей, которым предстоит работать с определенными устройствами Bluetooth, то заранее сконфигурируйте эти устройства для них или порекомендуйте им использовать проверенные вами простые инсталляционные мастера.

Если устройство Bluetooth сконфигурировано должным образом, установление соединения в дальнейшем осуществляется автоматически. Впрочем, многие устройства Bluetooth могут запрашивать разрешение на установление соединения при поступлении соответствующего запроса извне. Эту функцию легко отключить, но помните о том, что она полезна с точки зрения обеспечения информационной безопасности.

В последнее время технология Bluetooth подверглась жесткой критике из-за атак типа Bluesnarfing, приводящих к краже данных с устройств Bluetooth. На самом деле в этой технологии предусмотрены неплохие методы аутентификации и шифрования, но эффективность их действия зависит от правильной конфигурации устройств и разумного подхода к их применению. Как это бывает с оборудованием Wi-Fi, установленные по умолчанию параметры работы средств Bluetooth могут и не обеспечивать защиты данных.

Вот несколько советов по повышению уровня информационной безопасности сетей Bluetooth.

1. Реализуйте стратегию защиты этих сетей.

2. Не используйте устройства Bluetooth для передачи строго конфиденциальных данных. Даже при правильной их конфигурации опытный и настойчивый хакер способен перехватить эти данные.

3. Спаривайте ваши устройства в физически защищенном месте. Если хакер перехватит информацию, передаваемую в ходе процесса спаривания, он сможет успешно атаковать их.

4. При спаривании устройств задействуйте только надежный PIN-код. Совместно с другими параметрами он используется для получения ключа шифрования. Надежным считается такой PIN-код, который представляет собой трудно угадываемую комбинацию из восьми или более букв и цифр.

5. После спаривания сконфигурируйте ваши устройства, как неподдающиеся обнаружению (другими устройствами Bluetooth). Эта мера предосторожности существенно затруднит подключение кого бы то ни было к вашим устройствам.

6. Задействуйте функцию запрашивания разрешения на установление соединения, что сделает связь по технологии Bluetooth более безопасной.

7. Отключайте средства Bluetooth, если вы не пользуетесь ими.

8. Отмените спаривание с потерянными или украденными устройствами, ведь с их помощью хакер может связаться с другими вашими устройствами, с которыми они были спарены.

Применение гарнитуры Bluetooth избавляет от надоедливого соединительного провода, имеющегося у обычного наушника сотового телефона, но помните о том, что аккумулятор этой гарнитуры (как и аккумулятор сотового телефона) время от времени нужно подзаряжать.

Что последует за Bluetooth

Bluetooth — это хорошо разработанная технология беспроводной связи, но она не предназначена для передачи изображений с высоким разрешением, музыкальных файлов и видеоинформации, а также для синхронизации больших баз данных. Для этих целей разработана новая сверхширокополосная технология UWB, которая может стать опасным конкурентом для Bluetooth. В отличие от обычных схем модуляции радиосигнала в технологии UWB предусмотрено использование коротких радиоимпульсов, обеспечивающих маломощное излучение в широкой полосе частот. Но до того времени, когда средства UWB получат широкое распространение, у технологии Bluetooth имеются хорошие шансы закрепиться на рынке (в течение ближайших нескольких лет) в качестве дополнения к новым технологиям, подобным UWB.

Антенны для устройств беспроводных ЛВС

До недавнего времени разработчики оборудования для беспроводных ЛВС (БЛВС) не уделяли должного внимания проектированию антенн. Например, антенны некоторых ноутбуков, которые представляют собой проложенные внутри корпуса машин куски провода, даже не были сориентированы для оптимального функционирования. Широко используемые в точках доступа антенны, предназначенные для разнесенного приема радиосигналов, работают ненамного лучше этих проводов.

Однако ситуация меняется. Новые «интеллектуальные» антенны от компаний Airgo Networks, Motia, Vivato и других производителей существенно улучшают характеристики устройств БЛВС, в том числе повышают их дальность действия. Если в будущем вы планируете задействовать «интеллектуальные» антенны или хотите использовать возможности имеющихся антенн по максимуму, то вам следует знать их параметры. Это так же важно, как знание характеристик вносимого затухания, волнового сопротивления и перекрестных наводок кабеля проводной ЛВС.

Параметры антенн

Любая антенна выполняет две основные функции. Работая на прием, она преобразует электромагнитную волну в электрический сигнал. Последний затем обрабатывается беспроводным устройством, в результате чего получаются цифровые данные. При передаче информации антенна преобразует электрический сигнал в электромагнитную волну, которая излучается в окружающее пространство. Для передачи потоков данных по радиоволнам используются сложные схемы модуляции.

От того, как хорошо антенна осуществляет эти функции, зависят возможность подключения пользователей к БЛВС и скорость передачи данных. Если антенна не будет излучать радиоволны должным образом, интерфейсы БЛВС (адаптируясь к низкому уровню сигнала) снизят свои максимальные скоро-сти передачи, что приведет к уменьшению производительности сети. Подходящая антенна должна обеспечивать требуемое радиопокрытие и минимизировать уровень сигналов БЛВС, выходящих за пределы обслуживаемого здания.

Итак, рассмотрим параметры антенн. В качестве базы для сравнения способности разрабатываемых антенн усиливать радиосигнал радиоинженеры используют гипотетический изотропный излучатель. Он излучает радиосигнал равномерно по всем направлениям, поэтому его диаграмма направленности (ДН) имеет вид сферы.

Коэффициент усиления (КУ) такой антенны равен 0 дБ, а КУ любой другой антенны выражают в децибелах относительно изотропного излучателя.

ДН антенны может быть представлена в виде трехмерного изображения или как два двухмерных графика. Самым распространенным типом антенн в БЛВС является всенаправленный диполь. Такими антеннами оснащены многие точки доступа. Будучи ориентированным перпендикулярно поверхности земли, в азимутальной плоскости диполь излучает сигнал равномерно по всем направлениям, а его ДН в этой плоскости (при использовании полярных координат) имеет форму окружности, в центре которой находится сам диполь. При этом предполагается, что она установлена перпендикулярно поверхности земли. В отличие от сферической ДН изотропного излучателя ДН этой антенны как бы растянута в азимутальной плоскости, т. е. большую часть энергии радиоволн она излучает по горизонтали, что, собственно, и обеспечивает ее более высокий КУ (2,2 дБ) по сравнению с КУ изотропного излучателя. Увеличение КУ антенны способствует росту дальности действия радиосистемы. Оснащенная антенной с такой ДН точка доступа обеспечит радиопокрытие большого помещения, при этом уровень ее излучения на соседних этажах здания будет низким. Если же антенну ориентировать горизонтально, то излучаемый ею сигнал будет распространяться и между этажами. При каждом увеличении КУ антенны на 3 дБ уровень принимаемого ею сигнала удваивается.

Специалисты конструируют и остронаправленные антенны, которые фокусируют электромагнитную энергию в узкий луч. К таким антеннам относятся большие параболические антенны, с помощью которых организуют наземные радиолинии длиной до 40 км и более. Названные антенны имеют КУ до 25 дБ и выше.

Варианты реализации антенн

Для оптимизации радиопокрытия к точкам доступа нередко подключают внешние антенны. Возможность их подключения имеется во многих точках доступа, предназначенных для корпоративных сетей. Однако Федеральная комиссия по связи США запрещает применение внешних антенн с устройствами, работающими в некоторых частотных полосах диапазона частот 5 ГГц. Поэтому работающие в этих полосах точки доступа вам придется использовать с имеющимися у них антеннами.

Ведущие производители точек доступа, такие, как компании Cisco Systems, Proxim и Symbol Technologies, предлагают несколько видов антенн для своих продуктов. Другие же производители, включая большинство компаний, недавно вышедших на рынок БЛВС со своими беспроводными коммутаторами, оснащают свои точки доступа фиксированными всенаправленными антеннами. Точка доступа компании Airespace поддерживает внешние антенны и работает с интегрированной направленной пластинчатой антенной, что обеспечивает большую дальность действия, чем конкурирующие продукты.

Ноутбуки оснащают беспроводными сетевыми адаптерами PC Card или Mini-PCI. Первые имеют простую всенаправленную антенну. В корпусе ноутбука такой адаптер расположен горизонтально, и, как правило, так же ориентирована его антенна, которая в основном излучает вверх и вниз, а не по сторонам, что уменьшает дальность связи. Стоит отметить адаптер FriendlyNET AL1511 фирмы Asante, оснащенный выдвижными антеннами Xwing. Это устройство обладает самой большой дальностью связи. Оно не самое прочное, но его вертикально ориентированные антенны работают хорошо, помогая обеспечить надежную связь в тех случаях, когда компьютер находится на границе зоны действия сети. Некоторые 2,4-ГГц беспроводные сетевые адаптеры имеют гнездо для подключения внешней антенны.

Беспроводной сетевой адаптер Mini-PCI обычно работает с расположенной в ноутбуке антенной. Как правило, эти антенны — двухдиапазонные, т.е. имеют элементы, функционирующие в диапазонах частот 2,4 и 5 ГГц. Антенну лучше всего размещать по периметру дисплея ноутбука, но тогда для связи ее с беспроводным сетевым адаптером потребуется использовать кабель, в котором радиосигнал будет затухать (потери в антенном кабеле ноутбука составляют 3 дБ и более). Поэтому многие производители размещают антенну рядом с адаптером Mini-PCI, который расположен под клавиатурой ноутбука. К сожалению, при такой компоновке антенна этого адаптера работает хуже, чем антенна платы PC Card.

Антенны становятся «интеллектуальнее»

Хорошей новостью для пользователей БЛВС является то, что антенны устройств этих сетей становятся «интеллектуальнее» и эффективнее в работе.

Простейшие «интеллектуальные» антенны, предназначенные для разнесенного приема радиосигналов, широко используются в точках доступа и адаптерах БЛВС. Такая антенна состоит из двух элементов (излучателей) и внутреннего коммутатора, подсоединяющего к приемнику тот элемент, который принимает более мощный сигнал. Она помогает уменьшить негативный эффект многолучевого распространения радиоволн, вызванного их отражением от разных предметов, в результате чего

один и тот же переданный радиосигнал многократно (с разной временной задержкой) поступает на вход приемника точки доступа, что приводит к сильному ослаблению принимаемого сигнала.

Для увеличения зоны действия БЛВС требуются еще более «интеллектуальные» антенны, к которым относятся фазированные антенные решетки. Такой решеткой, состоящей из большого числа излучателей, оборудован коммутатор Wi-Fi компании Vivato. Он функционирует как точка доступа, а его решетка наводит радиолуч на клиентское устройство стандарта 802.11. Данная антенная система увеличивает дальность связи (особенно на улице). Однако фазированные антенные решетки, как правило, имеют значительные габаритные размеры и стоят дорого.

Еще один вариант реализации «интеллектуальной» антенны — адаптивная решетка. Такие решетки разрабатывают фирма Motia и другие производители. В них принятые элементами решетки сигналы умножаются на определенные весовые коэффициенты, а затем суммируются. Адаптивная решетка может быть реализована в виде дополнительной подсистемы, подсоединяемой к имеющемуся устройству Wi-Fi.

Этот подход является довольно перспективным, но, чтобы потенциальные заказчики смогли воспользоваться всеми преимуществами того или иного варианта построения «интеллектуальной» антенны, необходимо внести существенные изменения в стандарты на БЛВС. Рабочая группа IEEE 802.11n разрабатывает стандарт на БЛВС следующего поколения, обеспечивающую скорость передачи данных до 100 Мбит/с. В действующих сегодня стандартах 802.11a и 802.11g определена максимальная скорость передачи 54 Мбит/с, а ее реальные значения составляют 25–30 Мбит/с.

Аналитики предполагают, что в стандарте 802.11n будет предусмотрена возможность использования устройств типа MIMO (Multiple Input, Multiple Output), работающих с несколькими антеннами. Такой продукт уже разработан компанией Airgo.

В упомянутом стандарте должны появиться и другие новшества. Так, для поддержки 100-Мбит/с скорости передачи данных на значительные расстояния потребуется существенно изменить MAC-уровень 802.11, что чревато возникновением проблем с обратной совместимостью беспроводных устройств. Следите за развитием стандарта 802.11n и за появлением на рынке поддерживающих его устройств. Они будут высокопроизводительными и (благодаря некоторым перспективным антеннам) «интеллектуальными».

Функционирование устройств Wi-Fi на физическом уровне

Осенью 1999 г. была создана организация Wireless Ethernet Compatibility Alliance (сейчас ее название Wi-Fi Alliance), которой принадлежит бренд Wi-Fi. На проведенной ею в то время пресс-конференции представитель этой организации назвал технологию Wi-Fi беспроводным аналогом Ethernet (wireless Ethernet). Когда же один из журналистов усомнился в правильности такого сравнения, ему было сказано, что технологии Wi-Fi и Ethernet очень похожи, поскольку в них предусмотрен конкурентный доступ узлов сети к среде передачи данных и имеется много общего в реализации канального уровня.

Однако сходство названных технологий на этом и заканчивается. Они существенно отличаются друг от друга на физическом уровне. Если трафик сетей Ethernet локализован в более или менее защищенных от воздействия внешней среды электрических и оптических кабелях, то трафик систем Wi-Fi передается по радиоволнам и при этом подвержен влиянию помех и атмосферных осадков, которые могут парализовать работу системы.

Производители средств Wi-Fi стараются не афишировать возможные проблемы в их работе, связанные с их физическим уровнем. Вместо этого они подчеркивают простоту инсталляции и сетевой интеграции оборудования Wi-Fi. Вам следует знать об этих проблемах и, чтобы успешно управлять большими беспроводными ЛВС (БЛВС), нужно еще разбираться в основах радиотехники. Здесь вполне уместно провести аналогию с сетями Ethernet, для эффективного администрирования которых необходимы знания в области структурированных кабельных систем.

Основы радиосвязи

Подобно модемам для коммутируемых линий и кабельным модемам, устройства Wi-Fi модулируют передаваемые сигналы. С помощью разных методов модуляции они преобразуют получаемые от компьютера цифровые сигналы в аналоговые радиочастотные. Скорость передачи данных с помощью модулированной несущей зависит от ряда факторов, в том числе от ширины полосы пропускания канала связи и типа используемого метода модуляции. По сравнению с простыми методами (или схемами) модуляции (например, BPSK, реализуемый 1-Мбит/с устройствами БЛВС), сложные методы модуляции (например, 64-QAM, поддерживаемый 54-Мбит/с оборудованием) обеспечивают более высокую скорость передачи данных. Но при использовании сложных методов мо-

дуляции устойчивость работы радиосистемы к воздействию шума снижается.

Поскольку по мере распространения в атмосфере радиосигнал затухает, разработчикам и пользователям радиосистем приходится искать компромисс между скоростью передачи данных и дальностью связи. Радиоволны в атмосфере затухают быстрее, чем радиочастотные сигналы, передаваемые кабельными модемами по гибридным (оптоволоконным и коаксиальным) кабельным системам.

Сети Wi-Fi работают в нелицензируемых (в США) частотных диапазонах 2,4–2,4835 (ISM-диапазон); 5,15–5,35 и 5,725–5,825 ГГц (UNII-диапазоны). Ширина полосы пропускания радиоканала систем Wi-Fi равна 22 МГц.

Устройства, предназначенные для работы в нелицензируемых диапазонах, должны быть спроектированы таким образом, чтобы сводить к минимуму вероятность негативного влияния (на их функционирование) взаимных помех. По этой причине устройства Wi-Fi имеют небольшую выходную мощность и устойчивы к воздействию не очень сильных помех, которые создаются другими устройствами, функционирующими в том же диапазоне.

Помехоустойчивость устройств Wi-Fi обеспечивается расширением спектра передаваемых сигналов. Хотя системы, реализующие технологии расширения спектра, работают довольно надежно, почти невозможно создать многосотовую БЛВС, не столкнувшись с проблемами в работе ее устройств, вызванными помехами.

Любое устройство Wi-Fi, будь то плата PC Card, беспроводной сетевой адаптер для настольного ПК или точка доступа, функционирует как приемопередатчик, т. е. передает и принимает радиосигналы. Стоит отметить, что 5-ГГц радиосигналы устройств стандарта 802.11a затухают сильнее, чем 2,4-ГГц сигналы, особенно когда на пути их распространения встречаются стены или другие объекты.

Мало того что приемникам приходится работать с очень слабыми сигналами, они еще испытывают воздействие радиочастотных шумов. К числу их источников относятся высокоскоростной центральный процессор ноутбука и микроволновая печь. Однако современные радиосистемы функционируют даже при очень низком отношении сигнал/шум.

Ватты и децибелы

Выходная мощность радиотехнических устройств обычно измеряется в ваттах. В отличие от стереосистем, которые могут иметь выходную мощность 500 Вт, оборудование Wi-Fi излучает значительно менее мощ-

ные сигналы — до 200 мВт. Поскольку радиосредства работают с маломощными сигналами, инженеры предпочитают выражать их уровень в логарифмических единицах, называемых децибелами (дБ). При определении уровня сигнала по отношению к одному милливатту используется сокращение «дБм» (dBm). Уровню сигнала в 0 дБм соответствует мощность 1 мВт.

Если мощность сигнала менее 1 мВт, его уровень отрицателен. Например, чувствительность беспроводного сетевого адаптера стандарта 802.11b при пропускной способности 2 Мбит/с может равняться -90 дБм.

Запомните два полезных в инженерной практике правила. Увеличение или уменьшение уровня сигнала на 3 дБ означает увеличение или уменьшение его мощности в два раза. Увеличение же уровня сигнала на 10 дБ соответствует десятикратному увеличению его мощности. Таким образом, если 0 дБм равняется 1 мВт, то 10 дБм — 10, 20 дБм — 100 и 30 дБм — 1000 мВт, или 1 Вт. С помощью этих правил несложно определить, что уровню сигнала в 23 дБм соответствует мощность 200 мВт.

Усиление и потери

В состав радиопередатчиков входят усилители мощности, повышающие уровень передаваемого сигнала. Для увеличения дальности связи разработчики беспроводного оборудования могут повышать его выходную мощность, но при этом они не должны выходить за пределы налагаемых (регулирующими органами) ограничений на характеристики этого оборудования. И еще, чем выше выходная мощность, тем больше потребляется электроэнергии (что сокращает срок службы батареи ноутбука) и рассеивается тепла (ноутбук нагревается сильнее).

Дальность связи можно повысить и за счет применения направленных антенн. Такая антенна фокусирует передаваемый сигнал в определенном направлении и обеспечивает повышение уровня принимаемого сигнала.

Чтобы беспроводная сеть функционировала нормально, суммарное усиление взаимодействующих устройств должно быть выше затухания передаваемого радиосигнала. Затухание радиосигнала в атмосфере (по причине его рассеивания в ней) называется потерями в свободном пространстве.

В зданиях, где работают БЛВС, имеют место и другие виды потерь, в том числе потери, обусловленные поглощением (стенами, межэтажными перекрытиями и дверями), рассеиванием (из-за хаотических отражений от различных поверхностей) и рефракцией (изменением направления распространения волны при прохождении ее через объект,

например, стеклянную стену) радиоволн. Уровень потерь зависит от частоты радиосигнала. Например, 5-ГГц радиосигнал поглощается межэтажными перекрытиями и стенами сильнее, чем 2,4-ГГц.

Хотя возможность установления радиосвязи зависит в первую очередь от параметров оборудования и потерь передаваемого сигнала, на работу БЛВС влияет и такой фактор, как многолучевое распространение радиоволн, вызванное их отражением от разных предметов. В результате этого один и тот же переданный радиосигнал многократно (с разной временной задержкой) поступает на вход приемника, что может значительно ослабить принимаемый сигнал.

Инженеры продолжают искать методы борьбы с негативным эффектом многолучевого распространения радиоволн. Сегодня с этой целью многие устройства Wi-Fi оснащены двумя антеннами, что иногда помогает. В большинстве случаев надежность работы радиосистемы при многолучевом распространении зависит от конструкции ее радиоприемника. По этой причине беспроводная сетевая плата с высокой выходной мощностью может уступать по дальности действия плате с меньшей мощностью, но с улучшенными возможностями работы в условиях многолучевого распространения радиоволн.

Результаты тестирования

Параметр, который вычисляется как разность выраженных в децибелах значений мощности передатчика и чувствительности приемника, называют системным усилением оборудования или бюджетом радиолинии. Так, соответствующий стандарту 802.11b сетевой адаптер Cisco Aironet имеет максимальную выходную мощность 20 дБм, а чувствительность радиоприемника точки доступа Cisco 1200 составляет -85 дБм (при максимальной пропускной способности 11 Мбит/с). Следовательно, при использовании этого оборудования бюджет радиолинии равен 105 дБ.

При недостаточно высоком отношении сигнал/шум пропускная способность систем Wi-Fi уменьшается из-за возникновения ошибок в пакетах данных и их повторной передачи. Чтобы устранить эти негативные явления, по мере уменьшения уровня принимаемого сигнала системы Wi-Fi автоматически переходят на менее эффективный метод модуляции, снижая тем самым свою максимальную скорость передачи данных (при этом помехоустойчивость повышается). В системах стандарта 802.11b максимальная скорость снижается постепенно — с 11 до 5,5 Мбит/с, затем до 2 и, наконец, до 1 Мбит/с. Когда же уровня сигнала перестает хватать и для работы системы на скорости 1 Мбит/с, связь прерывается.

Понимание основ функционирования радиосистем поможет вам эффективнее использовать средства обследования места развертывания БЛВС и средства поиска неисправностей в ее работе и тем самым улучшить планирование и обслуживание этой сети.

Словарь терминов Wi-Fi

WLAN (Wireless Local Area Network) — беспроводная локальная сеть. Помимо этого сокращения для обозначения беспроводных сетей разного масштаба употребляют термины WPAN (Wireless Personal Area Network) и WWAN (Wireless Wide Area Network). WPAN, иначе беспроводная персональная сеть, служит для связи компьютера с периферийными устройствами (клавиатура, мышь и т.д.). Сюда можно отнести стандарты Bluetooth и IrDa, которые обеспечивают связь на расстоянии до 10 метров. WWAN — глобальная беспроводная сеть, служит для обозначения сетей городских масштабов. По большей части, этот термин употребляется для сетей будущего.

Wi-Fi. Сети, построенные на базе оборудования, поддерживающего стандарт 802.11b, получили название — Wi-Fi-сети. Стоит упомянуть об одной интересной особенности стандарта 802.11b. Если хотя бы один клиент подключается к сети на малой скорости (причиной может стать большая удаленность или сильное ослабление радиосигнала окружающей средой), скорость передачи данных ограничивается для всех остальных пользователей до уровня скорости медленного клиента. Это ограничение устанавливается для обеспечения стабильного режима доступа всех клиентов сети базисным механизмом выбора скорости для каждого пользователя, который используется в стандарте CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance). Как следствие, скорость передачи данных даже при высокоскоростном подключении может упасть с 11 Мбит/с до 1 Мбит/с. Такое падение скорости вполне приемлемо при доступе в Интернет, когда скорость подключения к провайдеру сравнима с нижним порогом в Wi-Fi-сети, но легко замечается при интенсивной работе в локальной сети.

WNIC (Wireless Network Interface Card) — беспроводная сетевая карта, также иногда употребляется термин «беспроводной сетевой интерфейс».

WAP или AP (Wireless Access Point) — узел беспроводного доступа или «точка доступа». Это оборудование позволяет взаимодействовать беспроводным рабочим станциям с ресурсами уже существующей кабельной сети (Ethernet). Являясь точкой перехода (мостом) из беспроводной сети в кабельную сеть и участвуя как посредник в сетевых взаи-

модействиях беспроводных клиентов при работе сети в режиме инфраструктуры, узел доступа может выполнять некоторые ограничительные функции для активности беспроводных клиентов.

SSID (Service Set Identifier) — идентификатор беспроводной сети. Несмотря на работы по стандартизации беспроводных сетей молодость данной технологии еще заметна в различных мелочах, в том числе и в названиях. Часто производители оборудования и программного обеспечения для обозначения одних и тех же понятий используют различную терминологию, что может вызвать некоторое смущение у пользователя. Например, наряду с термином «идентификатор SSID» используются следующие наименования: имя сети (Network Name или сокр. NN), предпочтительная сеть (Preferred Network), идентификатор ESSID, и область обслуживания беспроводной сети.

WEP (Wired Equivalent Privacy) — метод поточного кодирования передаваемых данных. Основан на алгоритме RC4. Система отправителя инициализирует программу кодирования двумя значениями: вектором инициализации (IV) и секретным ключом. Каждый бит получившегося в результате кодирующего ключа складывается с соответствующим битом тела (нагрузки) пакета с применением логической операции XOR. В заголовок каждого зашифрованного сетевого пакета добавляется значение IV, примененное для его кодирования. Для следующего пакета выбирается другое значение IV. При расшифровке для каждого бита зашифрованного сообщения и кодирующего ключа также применяется операция XOR. В результате получаем расшифрованные данные.

Вектор инициализации — IV (Initialization Vector). Значение длиной в 24 бита, генерируемое случайным образом.

ICV (Integrity Check Value) — контрольная сумма данных.

MAC (Media Access Control) — аппаратный адрес.

VPN — защищенное сетевое соединение, использующее протоколы шифрования и туннелирования для создания безопасного подключения клиента к частной сети. Используется для работы в потенциально опасных коммуникационных средах, где существует возможность перехвата данных (например, в Интернет).

Взлом криптозащиты. Операция XOR к двум сообщением, зашифрованным одинаковыми парами значений секретного ключа и есть не что иное, как XOR к соответствующим незашифрованным данным. После чего сами исходные данные легко восстанавливаются.

Система обнаружения вторжения — NIDS (Network Intrusion Detection System).

Системы ловушки — Honeypot, Honeynets.

WPA (Wi-Fi Protected Access). Базируется на «временном протоколе целостности ключей» — TKIP (Temporary Key Integrity Protocol). Задача, решаемая TKIP: не допустить повторного использования кодирующих ключей. Это достигается динамической заменой используемого в WEP статического ключа новым ключом, вычисленным на основании старого секретного ключа, вектора инициализации и порядкового номера сетевого пакета. Также предусмотрена дополнительная проверка целостности сообщений — MIC (Message Integrity Check), при которой наряду с полезными данными учитываются MAC адреса источника и получателя.

Тип брандмауэра (firewall). Один из первых вопросов, который может встать перед новичком, — это вопрос выбора между брандмауэром типа «Stateful Inspection» или «Stateful Packet Inspection» (SPI). Для ответа на него нужно представлять, как работает маршрутизатор.

Все устройства потребительского уровня основаны на трансляции сетевых адресов (Network Address Translation, NAT). Эта технология позволяет осуществлять множественный доступ компьютеров локальной сети (каждый из которых имеет собственный внутренний IP-адрес) в Интернет, используя один внешний IP-адрес, полученный у провайдера. NAT обеспечивает основные функции брандмауэра, пропуская в сеть только те данные из Интернета, которые поступили в результате запроса от компьютера из локальной сети. Поскольку NAT подразумевает просмотр маршрутизатором содержимого каждого проходящего пакета, то почему бы такой режим не отнести к SPI?

На самом деле этот вопрос до сих пор не имеет однозначного ответа, частично это связано с неправильным использованием терминов при описании ранних продуктов на основе NAT. Кроме того, среднестатистическому покупателю весьма проблематично убедиться в работе SPI. С практической точки зрения различие NAT и SPI не столь велико, здесь вопрос заключается в том, что нужно пользователю. Маршрутизаторы потребительского уровня на базе SPI обычно отличаются от своих родственников NAT наличием такой возможности, как уведомление об атаке по электронной почте, хотя и из этого правила могут быть исключения. Кроме того, благодаря буквам SPI, некоторые производители пытаются повысить стоимость своего оборудования.

Рекомендация: если единственным различием функциональности устройств является наличие SPI у одного из них, то выбирайте его в том случае, если вы планируете использовать перенаправление множества портов или осуществлять доступ к внутреннему серверу из Интернета. В противном случае «чистый» NAT сможет полностью со всем справиться.

Особенности порта WAN. Немного прояснив вопрос о NAT и SPI, перейдем к более практическим вещам — например, как подключиться к Интернету?

Примечание: под широкополосным модемом (broadband modem) мы понимаем устройство для подключения к Интернету, использующее любой из способов широкополосной связи. Это может быть любой модем для выделенной линии.

Тип соединения. Большинство маршрутизаторов оборудованы портом 10BaseT Ethernet для подключения к широкополосному модему. Почему не 10/100? Просто потому, что большинство соединений работают на скорости 1-2 Мбит/с, в лучшем случае, поэтому производители могут немного сэкономить, используя чип на 10BaseT. Некоторые модели оборудованы последовательным портом для WAN-соединения, что позволяет использовать их совместно с обычными модемами (для коммутируемых линий) или соответствующими модемами для выделенных линий (или ISDN-адаптерами). Некоторые модели поддерживают функцию автоматического установления резервного модемного соединения «auto-failover» при разрыве основного подключения и автоматическое переключение обратно при восстановлении последнего.

Получение параметров IP. Когда маршрутизатор уже приобретен и подключен к линии, нужно еще раз убедиться, что он поддерживает метод получения IP-адреса и тип аутентификации, используемые провайдером. Сначала обратимся к способам задания IP-адреса, которые есть у всех устройств, затем рассмотрим методы аутентификации.

Динамический IP-адрес (Dynamic IP). В этом способе, который также называют «DHCP-клиент», маршрутизатор автоматически получает свой IP-адрес, адреса шлюза по умолчанию и сервера DNS. Подобный способ достаточно широко распространен — он предоставляет провайдеру достаточную гибкость при конфигурировании своей сети. Негативная сторона заключается в том, что полученный IP-адрес может смениться в любой момент, и удаленные приложения, работающие на основе IP-адресов, не смогут работать. К счастью, решить эту проблему помогают провайдеры динамического DNS, например TZO, которые позволяют найти вас по имени независимо от текущего IP-адреса.

Статический IP-адрес (Static IP). Этот метод идеально подходит для тех, кто собирается использовать серверы и не желает связываться с динамическим DNS. Здесь требуется самостоятельно указать IP-адрес, адрес шлюза по умолчанию и адрес сервера DNS, предоставленные провайдером. Такой вариант предоставляют не все провайдеры, а те, которые предоставляют, могут взимать за это дополнительную плату.

Методы аутентификации. Вообще, у провайдеров существует множество способов для проверки подлинности пользователей. Рассмотрим наиболее распространенные из них.

- Коммутируемый доступ и ISDN. Пользователи этих двух способов, вероятно, заметили, что в маршрутизаторах с последовательным портом в разделе настройки удаленного доступа есть также место для указания номера телефона провайдера, имени пользователя и пароля.
- По MAC-адресу. Все устройства, обладающие IP-адресом, имеют и MAC-адрес. MAC-адреса уникальны для любого сетевого оборудования (по крайней мере, предполагается, что они уникальны) и используются в процессе присвоения IP-адресов. MAC-адреса (также известные как адреса физические) состоят из двенадцати шестнадцатиразрядных цифр (то есть, шести байт). Чтобы обеспечить уникальность MAC-адресов, каждому производителю сетевого оборудования выделяется свой диапазон, а конкретный адрес в рамках диапазона присваивается случайным образом.

Примечание: MAC-адрес может быть записан в одном из трех видов. Ниже приведены три варианта записи одного и того же MAC-адреса:

```
00fe3c812eab
00-fe-3c-81-2e-ab
00:fe:3c:81:2e:ab
```

MAC-адреса не чувствительны к регистру, поэтому для их написания можно использовать как строчные, так и заглавные буквы (A-F).

Провайдеры, использующие кабельные модемы, часто применяют именно этот метод аутентификации — вы даже можете не знать, что они используют именно его. Однако все сомнения рассеются, как только вы попытаетесь подключить модем к другому компьютеру или маршрутизатору. Поэтому если соединение перестало работать сразу после установки нового оборудования или через некоторое время после этого, вполне вероятно, что провайдер проводит аутентификацию именно по MAC-адресу.

Такой метод является источником проблем: при установке нового маршрутизатора необходимо звонить провайдеру и сообщать новый MAC-адрес в службу поддержки, что приводит к дополнительным временным издержкам. Некоторые провайдеры добавляют в свою базу данных MAC-адресов диапазоны, используемые наиболее известными маршрутизаторами, и запрещают их использование. (Кроме того, некоторые

провайдеры отслеживают MAC-адреса устройств, находящихся в сети, и отключают маршрутизаторы без предупреждения или объяснения).

К счастью, разработчики маршрутизаторов придумали обходное решение — сегодня практически все модели позволяют автоматически «клонировать» MAC-адрес компьютера, к которому он подключен, или даже указывать адрес ранее использовавшегося адаптера в качестве внешнего MAC-адреса. Оба способа избавляют от необходимости звонка в службу поддержки.

- PPPoE. Протокол Point-to-Point Protocol over Ethernet (или PPPoE) является относительно новым методом аутентификации. Его продвижению способствовали DSL-провайдеры Интернета. Этот метод требует лишь указания имени и пароля, но использует протокол, позволяющий выполнять аутентификацию, мониторинг и контроль множества виртуальных подключений. То есть провайдер получает возможность отслеживать и производить расчеты раздельно для пользователей. Однако такая возможность есть только в том случае, если вы арендовали сразу несколько IP-адресов. Но она мало распространена. Большинство пользователей предпочитают устанавливать маршрутизатор с NAT для выхода в Интернет с нескольких компьютеров.

PPPoE сегодня поддерживают почти все маршрутизаторы, однако качество реализации, то есть стабильность работы, сильно отличается. Некоторые проблемы PPPoE связаны с прошивкой маршрутизаторов, некоторые — с различиями в реализациях PPPoE провайдерами. Если провайдер использует PPPoE, то стоит выбирать маршрутизатор с его поддержкой, а также со следующими возможностями:

Контроль подключения (Connection Controls). Здесь можно встретить несколько различных параметров, отвечающих за продолжительность поддержания соединения в случае отсутствия сетевой активности и действия при разрыве соединения. Большинство маршрутизаторов настроены по умолчанию так, чтобы автоматически восстанавливать соединение при обнаружении сетевой активности, однако у маршрутизаторов Linksys данная опция вынесена в настройки «**Connect on Demand**» (Подключение по требованию). Параметр «**Maximum Idle Time**» (Максимальное время ожидания) определяет время, через которое маршрутизатор разорвет соединение при отсутствии сетевой активности. Опция «**Auto-Reconnect**» (Автоматическое восстановление соединения) позволяет маршрутизатору автоматически восстановить соединение при его разрыве.

Сохранение соединения (Keep Alive). Одна из наиболее серьезных проблем соединений PPPoE заключается в достаточно частых самопроизвольных разрывах. Некоторые провайдеры разрывают широкополосное соединение намеренно, также как и провайдеры коммутируемого доступа, после некоторого периода неактивности, у других просто неправильно настроены серверы PPPoE. Функция «**Keep Alive**» позволяет поддерживать соединение, посылая пакеты данных через заданные промежутки времени.

Другие параметры аутентификации (Other Authentication needs). Некоторые провайдеры PPPoE требуют статического задания IP-адреса и/или «**Service Name**» (Имени службы). При выборе маршрутизатора убедитесь, что он поддерживает все необходимые функции.

Имя узла (Host Name). Метод аутентификации по имени узла использовался провайдером @Home до тех пор, пока он не распался. В этом случае требуется установить «**Host Name**» (Имя узла) (в Windows это называется «**Имя компьютера**» (Computer Name)) на выданное провайдером длинное имя. @Home был одним из наиболее крупных провайдеров, поэтому большинство маршрутизаторов поддерживают возможность задания имени маршрутизатора и последующую передачу его провайдеру в ответ на запрос.

TAS. TAS расшифровывается как «Toshiba Authentication Service» и также известен как «RR login». Протокол применяет аутентификацию по имени пользователя/паролю, используя для этого небольшую клиентскую программу, которая должна работать на компьютере, подключенном к кабельному модему. Большинство маршрутизаторов этот протокол не поддерживают (продукты ZyXEL и некоторые OEM-модели Netgear являются исключениями). Если ваш провайдер использует именно этот способ аутентификации, то вам остается либо подыскать маршрутизатор с его поддержкой, либо искать какие-то обходные пути.

Сервер DHCP. Все модели маршрутизаторов поддерживают сервер DHCP, благодаря чему возможно автоматическое предоставление клиентам локальной сети настроек TCP/IP, необходимых для получения доступа в Интернет. Не все маршрутизаторы имеют одинаковый набор настроек DHCP-сервера, поэтому обратите внимание на следующее:

Диапазон адресов (Address Range control). Этот параметр определяет тот диапазон адресов, которые распределяет сервер. Некоторые модели позволяют указать только начальный адрес диапазона. Другие позволяют указать начальный и конечный адреса. Последнее решение является более гибким и позволяет не беспокоиться о том, что выданные сервером адреса будут конфликтовать со статически заданными адресами в сети.

Резервирование IP-адресов (IP reservation). В этом пункте можно задать поддиапазон адресов DHCP-сервера, который будет зарезервирован, — адреса из него выдаваться не будут.

Имя домена (Domain Name). DHCP-сервер также раздает адреса DNS-серверов провайдера, но вы можете настроить его и на раздачу клиентам имени домена. Если провайдер не указывает полные имена (FQDN) на своих серверах (например, как @Home), то вам придется самому настроить эту функцию, чтобы клиенты локальной сети могли работать с почтой, новостями и другими сервисами.

Примечание: FQDN включает в себя имя узла, домена и информацию о домене верхнего уровня, например, www.home.com, или mail.home.com. Не-FQDN имя обычно содержит только имя хоста, например mail, news, POP3.

Включение/Выключение (Enable/Disable). Данный параметр отвечает за включение/выключение DHCP-сервера. Он будет полезен при использовании в беспроводных маршрутизаторах и при наличии DHCP-сервера в сети.

Список клиентов (Client Listing). Иногда необходимо узнать, кто подключен к сети. Эта функция, как минимум, показывает соответствие IP-адресов MAC-адресам для клиентов DHCP-сервера, получивших у него адрес. Некоторые модели также позволяют просмотреть имя компьютера-клиента, выполнить принудительное обновление адресов или отключить клиента.

Перенаправление портов, виртуальные серверы (Port Mapping, Forwarding, Virtual Server). Вообще, здесь может быть множество других названий, однако суть от этого не меняется: данная функция позволяет оставлять открытые порты в брандмауэре. Она требуется для большинства интернет-приложений, которым необходима возможность передавать запросы из внешнего сегмента сети (WAN) во внутренний (LAN).

Существует несколько способов реализации перенаправления портов, при выборе стоит исходить из требований используемых приложений. Рассмотрим типы перенаправления портов.

Статическое перенаправление портов (Static Single Ports). Это простейшая форма перенаправления портов. При ее использовании необходимо задавать соответствия между портами, используемыми приложениями и IP-адресами машин, на которых эти приложения работают. В результате запрос снаружи на IP-адрес вашего маршрутизатора будет автоматически перенаправлен на указанный внутренний сервер. Некоторые маршрутизаторы позволяют определять также используемый для

этого протокол (TCP или UDP). Другие автоматически производят перенаправление порта для обоих протоколов.

Примечание: статически можно перенаправлять порт только на один IP-адрес. Другими словами, если нескольким пользователям необходимо использовать одно и то же приложение, или если в сети присутствует несколько серверов одного типа, то для каждого из них придется задействовать свой порт. Некоторые приложения это позволяют, некоторые — нет.

Таким образом, если у вас немного приложений, и они используют по одному-два порта (например, web- или ftp-сервер), то этот способ вполне приемлем. Хотя максимальное число перенаправляемых портов может различаться у разных моделей, обычно устройства позволяют задать до десяти таких портов.

Статическое перенаправление группы портов схоже с одиночными портами, только в данном случае, можно указывать не отдельные порты, а их группы. Как и прежде, перенаправление диапазона портов возможно только для одного IP-адреса. Такая возможность полезна в том случае, если необходимо обеспечить работу приложений, использующих большое количество портов, например, игр или аудио/видеоконференций. Здесь количество групп портов также варьируется от одной модели к другой, хотя обычно также предлагается около десяти.

Демилитаризованная зона, внешний сервер (DMZ, Exposed Server). Данная функция позволяет виртуально поместить компьютер, находящийся в локальной сети, в глобальную сеть до брандмауэра. Подчеркну слово «виртуально», поскольку на самом деле машина физически остается подключенной к сегменту LAN. Другими словами, в этом случае осуществляется перенаправление всех портов на один внутренний IP-адрес. Эта функция осуществляется внутренней прошивкой маршрутизатора, и в некоторых моделях до сих пор не работает должным образом.

Динамическое перенаправление портов (Dynamic, Triggered Mapping). Иногда у этой функции встречается и другое название — «**Special Applications**» (Специальные приложения). Цель данной функции направлена на преодоление ограничения статического перенаправления, когда один номер порта можно перенаправить только на один внутренний IP-адрес. Настройка выполняется точно так же, как в случае статических привязок, за исключением указания свойства «trigger» (и иногда протокола). После активации данной функции маршрутизатор следит за исходящим трафиком, то есть за тем трафиком локального сегмента, который направлен в Интернет и соответствует заданному критерию. Если такой трафик обнаружен, то маршрутизатор запоминает IP-адрес компьютера, от которого исходит этот трафик. При поступлении данных обратно, в

локальный сегмент, включается перенаправление портов, и данные пропускаются внутрь. После завершения передачи перенаправление отключается, и любой другой компьютер может создать новое перенаправление уже на свой IP-адрес. Таким образом, создается иллюзия того, что сразу несколько компьютеров одновременно используют перенаправление одного и того же порта, хотя на самом деле в один момент времени только один компьютер может использовать перенаправление.

Примечание: событие, по которому осуществляется динамическое перенаправление должно происходить во внутреннем сегменте сети, поэтому его нельзя использовать для организации работы нескольких серверов, находящихся в сегменте LAN и использующих один порт. Другими словами, если необходимо, чтобы работали два web-сервера, нужно настроить статические перенаправления на два различных порта и соответствующим образом настроить серверы.

Примечание: динамические перенаправления прекрасно подходят для служб, использующих кратковременные запрос и передачу данных, поскольку если один компьютер использует перенаправление данного порта, то в этот момент времени другой компьютер перенаправление этого порта использовать не может. Если нужно настроить работу приложений, которым необходим постоянный поток данных, (например потоковое аудио и видео, интернет-телефония и многое другое), которые занимают порт на длительное время, то динамическое перенаправление в этом случае помогает мало.

Привязка сервера Loopback (Mapped Server, Loopback). Если на маршрутизаторе настроено перенаправление портов на серверы, находящиеся в сегменте LAN, то добраться до них из этого же сегмента можно достаточно просто — указав внутренний IP-адрес сервера. Пользователи, находящиеся с другой стороны маршрутизатора — WAN, могут обратиться к серверу через внешний адрес маршрутизатора.

Функция «Loopback» позволяет пользователям, находящимся во внутреннем сегменте, обращаться к такому серверу по внешнему IP-адресу маршрутизатора (или по имени, если оно задано). Такая возможность избавит пользователей, находящихся в одной локальной сети с сервером, от необходимости запоминать внутренние адреса, позволив обращаться к серверу точно так же, как всем остальным пользователям, находящимся снаружи маршрутизатора.

Контроль доступа, фильтрация портов (Access Control, Port filtering). В некоторых ситуациях необходимо ограничивать круг пользователей, имеющих доступ к сервисам Интернета: например, разрешить доступ только к электронной почте или только к web-страницам. Для этой цели почти у всех маршрутизаторов есть возможность ограничения доступа.

Работает это следующим образом: задаются группы пользователей (на самом деле это группы IP-адресов). Затем для каждой группы указываются сервисы (используемые ими порты), которые разрешается использовать группе.

Различные модели маршрутизаторов позволяют реализовать различные уровни контроля, хотя обычно можно либо разрешить доступ только к указанной группе сервисов (номерам портов), или разрешить доступ ко всем, кроме указанной группы. Когда пользователь пытается использовать неразрешенную службу, например AOL Instant Messenger, она просто не будет работать. Это может показаться странным для пользователей, которые не были предупреждены о фильтрации. Поэтому многие модели маршрутизаторов в данном случае покажут сообщение о том, что доступ к этой службе закрыт.

Обычно маршрутизаторы позволяют задать четыре группы, возможное количество портов в группе различается. Некоторые модели позволяют одновременно указывать не только одиночные порты, но и их диапазоны, другие — только одиночные порты.

Большинство моделей позволяют только включить блокирование или отключить, однако некоторые поддерживают также блокирование портов по расписанию. Конечно, гибкость расписания не слишком велика, обычно она ограничивается одним периодом времени с указанием дней недели, в которые этот фильтр используется.

Ограничение/фильтрация содержания (Content Control, Content filtering). Данная функция предназначена для ограничения доступа пользователей локальной сети к ресурсам Интернета. Она схожа с такими программами, как Cybersitter, NetNanny, CyberPatrol и другими, но более ограничена в возможностях. Некоторые модели позволяют лишь указать URL или IP-адреса и запретить или разрешить доступ только к ним. Другие поддерживают использование списков фильтрации и позволяют использовать такие списки от третьих фирм. Некоторые модели также позволяют настроить и этот фильтр на работу по расписанию.

VPN (Virtual Private Networking). С постоянным ростом внимания к безопасности компьютерных сетей, возможность поддержки VPN становится все более актуальной, особенно это касается тех, кому необходимо подключаться к сети офиса из дома или из гостиницы в случае командировки. Многие организации позволяют подключаться к своей сети лишь с использованием технологий VPN. Производители маршрутизаторов ответили на спрос решений для VPN поддержкой их в своих устройствах. Возможности туннелирования в маршрутизаторах сильно различаются от модели к модели, поэтому необходимо заранее знать, поддержка какого типа туннелей вам необходима.

Протоколы (Protocols). Два наиболее часто используемых протокола для создания VPN — это PPTP и IPsec. PPTP (поддерживается компанией Microsoft) поддерживается в маршрутизаторах наиболее часто, хотя сегодня большинство моделей также поддерживают и IPsec. Третий протокол, L2TP, распространен не так широко, поэтому если ваше подключение VPN использует именно этот протокол, то убедитесь в его должной поддержке маршрутизатором.

Прохождение (Pass-Thru). Простейшая форма поддержки VPN — это обеспечение сквозного прохождения туннелей через маршрутизатор. Маршрутизатор, поддерживающий этот режим, пропускает через себя инкапсулированные пакеты данных, не просматривая их содержимое. Остается только настроить соответствующее клиентское ПО на компьютерах во внутреннем сегменте, чтобы клиенты из локальной сети могли свободно подключаться к серверу VPN снаружи. Большинство производителей заявляют, что их модели поддерживают прохождение туннелей VPN, однако на самом деле ситуация может оказаться обратной. Иногда проблемы заключаются в ошибках прошивки маршрутизатора, иногда они связаны с невозможностью работы протокола VPN через маршрутизаторы NAT.

Совет: через маршрутизаторы NAT не могут работать подключения VPN, использующие аутентификацию заголовков IPsec (IPsec Header Authentication) или пакеты IPsec с неинкапсулированным шифрованием FMZ.

Также маршрутизаторы различаются по количеству пропускаемых туннелей. Это не так критично для одиночных пользователей, но может играть важную роль для небольших организаций, использующих соединения между несколькими офисами. Одни модели могут поддерживать прохождение только одного туннеля в один момент времени, другие могут пропускать сразу несколько. Третьи могут пропускать несколько туннелей только в том случае, если они направлены на один сервер VPN. То есть два сотрудника из одного офиса не смогут установить подключение к двум различным удаленным VPN-серверам.

Еще одна необходимая функция, касающаяся VPN, — это возможность использования серверов VPN внутри сети. Естественно, для этого необходимо будет установить перенаправление портов, или поместить сервер в DMZ, но если маршрутизатор не знает, как обращаться со специально построенными пакетами данных VPN, клиенты не смогут подключиться к серверу. Поэтому, если необходимо установить сервер VPN за маршрутизатором внутри сети, то сначала стоит убедиться, что маршрутизатор поддерживает прохождение туннелей PPTP или IPsec внутрь.

Конечная точка (End Point). Второе название этой функции — «VPN Edge». Так называется способность маршрутизатора создавать и разрывать туннельное соединение. Благодаря ей маршрутизатор может устанавливать туннели сам, что позволяет не использовать программное обеспечение для VPN на клиентских компьютерах. Кроме того, используя два одинаковых (или почти одинаковых) маршрутизатора, можно создать туннельное соединение между двумя сетями без использования какого-либо дополнительного программного или аппаратного обеспечения.

Ранее такая возможность была доступна в устройствах стоимостью от $500, однако сегодня появляются все новые модели устройств, которые стоят дешевле $100 и поддерживают конечные точки VPN. К примеру, SMC 7004.

При выборе маршрутизатора с такой возможностью следует убедиться в наличии конечной точки PPTP, если она вам нужна (некоторые модели поддерживают конечную точку только для IPsec, а для PPTP есть лишь возможность прохождения туннелей). Кроме того, если необходима возможность доступа к сети, например, во время поездок, убедитесь в наличии в комплекте поставки клиентского приложения VPN, если оно необходимо.

Журналирование (Logging). Журналирование — это способ маршрутизатора «сказать», что он выполнял и, что более важно, чем занимались пользователи. Большинство моделей потребительского уровня обладают достаточно скромными возможностями журналирования и предоставляют лишь поверхностные возможности (в лучшем случае) для просмотра активности определенного пользователя.

Обычно в журнал заносятся три типа записей: административные, «**hack attempts**» (попытки взлома) и трафик пользователей. Административные записи включают в себя такие события как включение/выключение и перезагрузку маршрутизатора. Кроме того, здесь же можно встретить и список попыток административных входов. Записи «Попытки взлома» обычно включают попытки любого доступа к маршрутизатору с внешнего сегмента сети (WAN). Эти попытки обычно не направлены именно на ваш маршрутизатор, а являются результатом сканирования портов всей подсети. Модели с брандмауэрами на базе просмотра содержимого (SPI) могут также определять и записывать потенциально опасные атаки, например Denial of Service (DoS) — отказ в обслуживании, fragmented packet — фрагментированные пакеты и другие, не менее опасные атаки. И, наконец, записи трафик пользователей включают запросы HTTP, FTP и других сервисов Интернет.

Как и упоминалось ранее, интерфейс журналов у большинства моделей чрезвычайно прост, обычно представляет собой просто список событий. Некоторые модели позволяют стирать или сохранять журнал в файл, в то время как другие сохраняют лишь определенное количество событий, а когда журнал переполнится, наиболее старые события будут удаляться, уступая место новым. Еще один тип журналирования — это журналирование URL или web-трафика: в данном случае запоминается количество посещений какого-то web-адреса сервера, без указания точных адресов страниц, поэтому если вам необходимо отслеживать и адреса страниц, то следует озаботиться выбором модели с поддержкой журналирования на внешний сервер.

Для журналирования на сервер используются два метода. Поддержка Syslog позволяет задать адрес машины в локальной сети, на которой запущен сервер или домен syslog. Этот сервис изначально появился в системах unix, а сейчас есть также версии для Windows и MacOS. После установки сервер Syslog позволит маршрутизатору передавать копии журналов, которые затем могут обрабатываться различными программами.

Второй метод — это SNMP trap. Он поддерживается в популярной серии маршрутизаторов Linksys, и для него также существует множество программ. Для работы используется передача данных по протоколу SNMP.

И, наконец, некоторые маршрутизаторы (обычно с брандмауэрами SPI) поддерживают отправку предупреждений и сообщений об атаках по электронной почте. Это позволяет маршрутизатору отправлять сообщение при обнаружении попыток взлома из Интернета, или отсылку некоторых сообщений журнала по расписанию. Весьма удобно, особенно для тех, кто вечно забывает регулярно просматривать журналы событий.

Маршрутизация (Routing). Существуют модели, позволяющие выполнять обычную маршрутизацию (не-NAT). То есть вместо того, чтобы позволять нескольким компьютерам использовать один IP-адрес для доступа в Интернет, маршрутизатор может передавать трафик на компьютеры в локальной сети, имеющие реальные IP-адреса (выданные провайдером). Одна из ключевых функций здесь состоит в том, что компьютеры с реальными IP-адресами могут напрямую связываться со всеми другими компьютерами в Интернете. Естественно, при этом необходимо защищать каждую машину индивидуально.

Есть еще два типа особенностей, относящихся к маршрутизации. Статическая маршрутизация требует указания информации о подключенных подсетях.

Динамическая маршрутизация использует протокол RIP (Routing Information Protocol) для автоматического получения маршрутов от других устройств, использующих этот протокол.

Блокирование запросов ping снаружи (Discard WAN ping, Stealth mode). Одна из основных возможностей всех программ-сканеров портов — это отсылка на исследуемые адреса запроса ping и последующее ожидание ответа. Изначально запросы ping используются для диагностики связи с удаленным компьютером, но теперь ping используют и для обнаружения активных компьютеров. Вы можете блокировать запросы ping — в результате ваш маршрутизатор не будет на них отвечать.

Удаленное администрирование (Remote Administration). При наличии этой возможности можно разрешить административный вход из внешнего сегмента (WAN или Интернет). Ее очень удобно использовать в том случае, если вы часто находитесь в разъездах, и вам необходимо часто изменять настройки маршрутизатора, или если вы отвечаете за работу сразу нескольких маршрутизаторов, расположенных в разных местах. Если такой доступ недостаточно защищен, то он представляет потенциальную опасность — ведь любой злоумышленник тоже может получить доступ к вашей локальной сети, поэтому следует выбирать маршрутизаторы, обеспечивающие максимальную защиту административного доступа. Как минимум, стоит ограничить административный доступ, разрешив его только с одного IP-адреса или с группы адресов. Еще лучше будет возможность задания номера порта, используемого для подключения к консоли администрирования — но данная функция встречается относительно редко. То есть для получения доступа злоумышленнику необходимо будет узнать не только IP-адрес маршрутизатора, но и порт, используемый консолью администрирования.

Сервер печати (Print Server). Эта функция приобрела популярность благодаря старой линейке маршрутизаторов Barricade компании SMC. Она позволяет подключать принтер с параллельным портом к маршрутизатору, а не к компьютеру сети. Таким образом, печать не зависит от работы или доступности какого-то одного компьютера, и, кроме того, вы можете установить принтер в более удобное место. Большинство моделей с серверами печати имеют небольшое количество памяти (ограничивая размер печатаемых файлов), могут не работать с MacOS, и не поддерживают функции двунаправленной передачи данных по LPT-порту. В целом, сервер печати — вещь полезная, особенно с учетом того, что он совсем незначительно увеличивает стоимость устройства.

MTU. Этот параметр позволяет изменять параметр **Maximum Transmission Unit** для маршрутизатора. Наиболее интересно это может показаться для тех, кто использует соединение PPPoE, или для тех, кто

пытается настроить соединение VPN, или то и другое одновременно. Необходимость изменять этот параметр вызвана настройками сетей некоторых провайдеров. Подробнее узнать о том, к чему приводят такие изменения можно на сайте speedguide.net, тем не менее, мы считаем, что вам не стоит изменять этот параметр до тех пор, пока провайдер или производитель не посоветуют это сделать.

Адреса ресторанов и клубов, где есть Wi-Fi

- 938 22 18, просп. Вернадского, 6, влад. 1, м. Университет, пн-вс 12.00 и до последнего клиента
- 209 59 51, Петровка, 30/7, вход с Петровского бульвара, м. Чеховская круглосуточно
- «5 Оборотов», 299 26 00, Садовая-Триумфальная, 22/31, м. Маяковская, вс-чт 12.00-0.00, пт-сб 12.00-5.00
- «Б2», 209 99 09, 209 99 18, Б.Садовая, 8, м. Маяковская, пн-вс 12.00 и до последнего клиента
- «Вермель», 959 33 03, Раушская наб., 4/5, м. Третьяковская, пн-пт 12.00-5.00, сб-вс 18.00-6.00
- «Вертинский», 202 05 70, 202 05 67, Остоженка, 3/14, м. Кропоткинская пн-вс 12.00-0.00
- «Гео парк», 432 99 81,432 57 78, просп. Вернадского, 53, м. Проспект Вернадского, пн-чт, вс 12.00-0.00, пт-сб 12.00-6.00
- «Гранд Империал», 291 60 63, Гагаринский пер., 9/5, м. Кропоткинская, пн-пт 12.00-23.00
- «Гриль Хаус», 246 12 72, Льва Толстого, 18 (в РК «Космик»), м. Парк культуры, вс-ср 12.00-0.00, чт-сб 12.00-5.00, боулинг-клуб, пн-вс 12.00-5.00
- «Дом», 953 72 36, Б.Овчинниковский пер., 24, стр. 4, м. Новокузнецкая, чт-вс 19.00-23.30
- «Древо желаний», 230 23 01, Кожевническая, 11, м. Павелецкая, пн-вс 12.00-0.00
- «Зен Кофе», 152 25 52, Ленинградский просп., 62, м. Аэропорт, пн-вс 8.00-23.00

- «Итальянец», 688 64 01, 688 56 51, Самотечная, 13, м. Цветной бульвар, пн-вс 12.00 и до последнего клиента
- «Консерватория», 783 12 34, Неглинная, 4, гост. «Арарат Парк Хаятт», 10 этаж, м. Кузнецкий Мост, Охотный Ряд, Театральная, пн-вс 12.00-2.00
- «Кофемания», 924 00 75, Рождественка, 6/9, стр. 1, м. Кузнецкий Мост, пн-вс 8.00-23.00
- «Кофемания», 229 39 01, Б.Никитская, 13, м. Александровский сад, Арбатская, пн-вс 8.00-1.00
- «Кофемания», 290 01 41, Кудринская пл., 46/54, м. Баррикадная, Краснопресненская, пн-вс 8.00-1.00
- «Кофетун», 209 14 94, Тверская, 18а, м. Пушкинская, Тверская, Чеховская, круглосуточно
- «Кухмейстер», 953 41 98, Пятницкая, 47, стр. 3, м. Новокузнецкая, Третьяковская, пн-сб 11.00-23.00
- «Лаун-Теннис», кафе, 209 58 92, Тверская, 20/1, стр. 1, м. Пушкинская, Тверская, Чеховская, пн-вс 11.00-5.00
- «Манер», 775 19 59, Петровка, 5, бизнес-центр «Берлинский дом», 1 этаж, м. Кузнецкий Мост, Охотный Ряд, пн-ср, вс 10.00-0.00, чт-сб 9.00-6.00
- «Матрица», (бар в фойе кинотеатра), 933 59 02, Осенний б-р, 7 корп. 1, м. Крылатское, пн-вс 10.00-0.00
- «Место встречи», 229 23 73, Тверская, 17, м. Тверская, пн-вс 11.00-5.00
- «Метрополис», 299 79 74, Садовая-Триумфальная, 4/10, м. Маяковская, круглосуточно
- «Механа Банско», 241 31 32, 244 73 87, Смоленская пл., 9/1, м. Смоленская, пн-чт, вс 12.00-23.00, пт-сб 12.00-2.00
- «Монтана Кофе», 269 16 47, Русаковская, 29, м. Сокольники, пн-пт 7.00-23.00, сб-вс 8.00-22.00
- «Пиноккио», 243 56 88, 243 70 15, Кутузовский просп., 4/2, м. Киевская, пн-вс 12.00-0.00
- «Пицца Экспресс», 937 81 00, 937 82 61, Смоленская пл., 3, Смоленский пассаж, 1 и 2 этажи, м. Смоленская, пн-вс 10.00-22.00

- «Санрайз», 291 87 52, Н.Арбат, 22, м. Арбатская, Смоленская, круглосуточно
- «Санта Фе», 256 14 87, 256 14 28, 256 14 26, Мантулинская, 5/1, стр. 6, м. Улица 1905 года, пн-ср, вс 12.00-0.00, чт-сб 12.00-3.00
- «Скандинавия», 937 56 30, 200 49 86, Палашевская, 7, м. Пушкинская, Тверская, Чеховская, пн-вс 12.00-0.00
- «Старина Мюллер», 259 13 73, 259 02 15, 259 07 00, Шмитовский пр., 2, стр. 1, м. Улица 1905 года, пн-ср 11.00-1.00, чт-вс 13.00-1.00
- «Тинькофф», 777 33 00, Проточный пер., 11, м. Смоленская, пн-вс 12.00-2.00
- «Третий Рим», 924 16 20, Б.Черкасский пер., 13, м. Площадь Революции, пн-пт 9.00-23.00, сб-вс 12.00-23.00
- «Тривия», 209 65 23,М.Бронная, 20а, м. Маяковская, Пушкинская, Тверская, Чеховская, пн-вс 12.00-23.00
- «Улей», 797 43 33, Гашека, 7, м. Маяковская, пн-вс 12.00-2.00
- «Час Пик», 205 20 56, Новинский б-р, 7, стр. 1, м. Смоленская, вс-чт 11.00-0.00, пт-сб 11.00-1.00
- «Шанти», 783 68 68, Мясницкий пр., 2/1, м. Красные Ворота, пн-чт, вс 12.00-0.00, пт-сб 12.00-5.00
- «Шоколадница», 241 06 20, Арбат, 29, м. Арбатская, пн-вс 9.00-23.00
- «Шоколадница», 200 13 37, Б.Дмитровка, 30/1, м. Пушкинская, пн-вс 9.00-0.00
- «Шоколадница», 254 76 36, Б.Грузинская, 2/12, м. Баррикадная, Краснопресненская, круглосуточно
- «Шоколадница», 951 37 03, Климентовский пер., 10, стр. 1, м. Третьяковская, круглосуточно
- «Шоколадница», 249 03 18, Кутузовский просп., 24, м. Кутузовская, круглосуточно
- «Шоколадница», 680 85 15, просп. Мира, 29, м. Проспект Мира, круглосуточно

- «Шоколадница», 924 28 43, Мясницкая, 24/7, м. Чистые пруды, круглосуточно
- «Шоколадница», 203 12 61, Б.Никитская, 14, м. Охотный ряд, вс-чт 8.00-0.00, пт-сб 8.00-1.00
- «Шоколадница», 973 26 96, Новослободская, 36, м. Новослободская, круглосуточно
- «Шоколадница», 238 27 34, Б.Якиманка, 58/2, м. Октябрьская, круглосуточно
- «Штольц», 246 02 53, Саввинская наб., 25-27, м. Киевская, пн-вс 12.00 до последнего клиента
- «Amazonia», 209 96 06, Страстной б-р, 14, м. Пушкинская, пн-вс 12.00-6.00
- «American Bar & Grill», 912 36 15, 912 36 21, Земляной Вал, 59, м. Курская, Чкаловская, пн-вс 10.00-2.00
- «American Bar & Grill», 250 95 25, 251 79 99, 1-я Тверская-Ямская, 2, стр. 1, м. Маяковская, круглосуточно
- «American Bar & Grill», 276 40 96, Воронцовская, 50, м. Пролетарская, пн-ср, вс 10.00-2.00, чт-сб 10.00-5.00
- «American Bar & Grill», 956 48 43, Кировоградская, влад. 14, ТЦ «Глобал Сити», 2 этаж, м. Южная, пн-вс 10.00-0.00
- «Big Pig Pub», 206 82 63, Маросейка, 3/13, м. Китай-город, круглосуточно
- «Bookафе», 200 03 56, Садовая-Самотечная, 13, м. Цветной бульвар, пн-вс 11.00-2.00
- «Cafenet» (интернет-кафе), 145 15 06, Сеславинская, 24, корп. 1, м. Багратионовская, круглосуточно, технический перерыв 8.00-9.30
- «Delifrance», 299 42 84, Тверская, 31, м. Маяковская, пн-чт, вс 9.00-23.00, пт-сб 9.00-23.30
- «F1» (интернет-клуб), 772 38 51, Бирюлевская, 17 (в кинотеатре «5 Звезд-Бирюлево»), м. Царицыно, пн-вс 11.00 до последнего клиента
- «Fame Cafe», 250 00 46, 1-я Тверская-Ямская, 9, стр. 2, м. Маяковская, круглосуточно

- «FAQ-Cafe», 229 08 27, Газетный пер., 9, стр.2, м. Охотный ряд, пн-вс 12.00-6.00
- «Hard Rock Cafe», 244 89 70, 241 98 53, 205 83 26, Арбат, 44/1, м. Смоленская, пн-вс 8.00-23.00
- «II Patio», 290 50 70, Смоленская, 3, м. Смоленская, пн-вс 11.00-23.00
- «II Patio», 298 25 30, Волхонка, 13а, м. Кропоткинская, пн-вс 12.00-0.00
- «Infinity», 255 90 56, 255 90 80, Дружинниковская, 15, м. Краснопресненская, пт-сб 11.00-6.00
- «Le Club», 915 10 42, В.Радищевская, 21, м. Таганская, пн-вс 12.00-0.00
- «Le Gateau», 937 56 78, Тверская, 23, м. Тверская, пн-вс 9.00-1.00
- «Loft», 933 77 13, Никольская, 25, ТК «Наутилус», 6 этаж, м. Кузнецкий Мост, пн-вс 9.00-0.00
- «Monterosso», 912 58 62, Таганская пл., 10/2, м. Таганская, круглосуточно
- «Nixcafe», 221 18 10, 1-я Квесисская, 18, ТЦ «Бутырский», м. Савеловская, круглосуточно
- «No name», 299 97 02, Тверская, 27, стр. 2, м. Маяковская, круглосуточно
- «R&B Cafe», 203 60 08, Староваганьковский пер., 19, стр. 2, м. Александровский сад, Арбатская
- «Starlite Diner», 290 96 38, Б.Садовая, 16, м. Маяковская, круглосуточно
- «Starlite Diner», 959 89 19, Коровий Вал, 9а, м. Добрынинская, Октябрьская, круглосуточно
- «TimeOnline» (интернет-кафе), 254 95 78, Б.Кондратьевский пер., 7, м. Белорусская, круглосуточно
- «TimeOnline» (интернет-кафе), 254 95 78, Манежная пл., 1, стр. 2, ТК «Охотный Ряд», м. Охотный Ряд, круглосуточно
- «Snob's», 775 23 10, 1-й Обыденский пер., 3, м. Кропоткинская, пн-вс 12.00-0.00

- «T.G.I. Friday's», 238 32 00, 238 08 80, Ленинский просп., 1/2, корп. 1, м. Октябрьская, пн-пт 10.00-0.00, сб-вс 12.00-0.00
- «T.G.I. Friday's», 200 39 21, Тверская, 18/2, м. Пушкинская, Тверская, Чеховская, пн-вс 12.00-1.00
- «T.G.I. Friday's», 970 11 86, Земляной Вал, 33, ТЦ «Атриум», 1 и 2 этаж, м. Курская, пн-вс 12.00-0.00
- «T.G.I. Friday's», 780 79 22, Новослободская, 3, м. Новослободская, Менделеевская, пн-вс 12.00-0.00
- «T.G.I. Friday's», 779 42 10, 779 42 11, Гарибальди, 23, ТЦ «Панорама», м. Новые Черемушки, пн-вс 12.00-0.00

Аэропорты

- Аэропорт Домодедово, 504 02 74, 504 02 64, зал международного вылета, VIP-зал, зал ожидания на 2 этаже
- Аэропорт Шереметьево, 730 68 10 (ресторан), ресторан T.G.I. Friday's

Гостиницы

- Балчуг Кемпински, 230 65 00, Балчуг,1, м. Третьяковская
- Ирис Конгресс-Отель, 933 05 33, Коровинское ш., 10, м. Петровско-Разумовская
- Катерина-Сити, 933 04 00, Шлюзовая наб., 6/1, м. Павелецкая
- Марриотт Гранд-отель, 937 00 00, Тверская, 26/1, 1 этаж, м. Маяковская
- Марриотт Роял Аврора, 937 10 00, Петровка, 11/20, м. Театральная
- Марриотт Тверская, 258 30 00, 290 99 00, 1-я Тверская-Ямская, 34, м. Белорусская
- Националь, 258 70 00, 258 70 68, 258 71 70, Моховая, 15/1, стр. 1, м. Охотный Ряд, Театральная
- Пекин, 209 22 15, 209 22 25, Б.Садовая, 5/1, м. Маяковская
- Ренессанс Москва, 931 90 00, 931 98 33, Олимпийский просп., 18/1, м. Проспект Мира

- Рэдиссон САС Славянская, 941 80 20, пл. Европы, 2, м. Киевская
- Татьяна, 721 25 00, Стремянный пер., 11, м. Павелецкая, Серпуховская
- Шератон Палас, 931 97 00, 1-я Тверская-Ямская, 19, м. Белорусская, Маяковская

Список использованных материалов

Сетевые мечтатели и их разоблачение
Олег Нечай

Почувствовать боль!
Олег Парамонов

Воздушные Замки
Георгий Башилов

Беспроводные сети. Взлом и защита
Александр Красоткин

Локальная сеть в мобильном офисе
Баир Гармаев

Без стука
Евгений Золотов

Wi-Fi на практике
Константин Иванов

Беспроводные технологии
Дэйв Молта

Детектор беспроводных сетей PCTEL: ищем точки доступа
Андрей Пировских, Дмитрий Чеканов

Руководство по решению проблем: настройка моста/повторителя WDS
Тим Хиггинс

Руководство по решению проблем: когда беспроводные сети мешают друг другу
Тим Хиггинс

Выбираем КПК для Wi-Fi
Баир Гармаев

Как выбрать беспроводной сетевой адаптер
Дэйв Молта

Wi-Fi в самолете: небо без проводов!
Андрей Пировских

Руководство «сетевика»: Wi-Fi Protected Access (WPA)
Тим Хиггинс

Маршрутизаторы: краткий справочник по терминологии и функциям
Тим Хиггинс

Введение в беспроводные маршрутизаторы
Ули Раес, Аксель Майно, Дэвид Стеллма

Wi-Fi на службе оператора
Вячеслав Ерохин

Возможности технологии Bluetooth
Питер Рисеви

Антенны для устройств беспроводных ЛВС
Дэйв Молта

Беспроводные устройства: как сделать правильный выбор
Питер Рисеви

Функционирование устройств Wi-Fi на физическом уровне
Дэйв Молта

Содержание

Часть 1. Введение

Часть 2. Высокая точность беспроводной передачи данных

Часть 3. Магистральные каналы связи

Часть 4. Путеводитель по стандартам на беспроводные ЛВС

Часть 5. Windows XP SP2: настройка беспроводной сети и брандмауэра

Часть 6. Руководство по решению проблем: настройка моста/повторителя WDS

Часть 7. Когда беспроводные сети мешают друг другу

Часть 8. Руководство «сетевика»: Wi-Fi Protected Access (WPA)

Приложения