Александр Ватаманюк

Беспроводная сеть своими руками

Убедитесь сами: без проводов проще!

Из книги вы узнаете:

- о стандартах беспроводной связи
- о юридических ограничениях
- как выбрать, установить и настроить оборудование
- как настроить сеть
- как сделать работу в сети безопасной

ПИТЕР®

Александр Ватаманюк

БЕСПРОВОДНАЯ СЕТЬ своими руками

ПИТЕР®

Москва · Санкт-Петербург · Нижний Новгород · Воронеж
Ростов-на-Дону · Екатеринбург · Самара · Новосибирск
Киев · Харьков · Минск
2006

А. И. Ватаманюк

Беспроводная сеть своими руками

Заведующий редакцией	*Д. Гурский*
Руководитель проекта	*М. Моисеева*
Литературный редактор	*А. Алехна*
Художник	*С. Расолько*
Корректоры	*О. Бортник, Д. Клевицкий*
Верстка	*Е. Зверев*

ББК 32.973.202
УДК 004.725.5

Ватаманюк А. И.

В21 Беспроводная сеть своими руками. — СПб.: Питер, 2006. — 192 с.: ил.

ISBN 5-469-01384-7

Вы хотите создать домашнюю или офисную сеть? Тогда вы должны быть готовы к тому, что вам придется провести немало времени с дрелью и перфоратором, глотать пыль в подвале или испытывать страх высоты на крыше, «воевать» с ЖЭСом за протянутый между домами провод, ругаться с родителям из-за испорченного ремонта — в общем, всех проблем и не перечислишь. Однако неприятностей можно избежать, построив сеть на основании беспроводных технологий.

Прочитав эту книгу, вы будете знать все необходимое для того, чтобы суметь самостоятельно создать беспроводную сеть: от теоретических основ беспроводной связи до принципов настройки сети в различных версиях Windows. Книга написана так, что будет понятна пользователю, никогда ранее не занимавшемуся сетями. В то же время отдельные ее разделы откроют немало нового даже опытным системным администраторам.

ISBN 5-469-01384-7

ООО «Питер Пресс», Санкт-Петербург, Петергофское шоссе, 73, лит. А29
Налоговая льгота — общероссийский классификатор продукции ОК 005-93,
том 2; 95 3005 — литература учебная.
Подписано к печати 13.03.06. Формат 70×100$^{1}/_{16}$. Усл. п. л. 15,48.
Тираж 3000. Заказ 589

Отпечатано с готовых диапозитивов в ОАО «Техническая книга»
190005, Санкт-Петербург, Измайловский пр., 29

Краткое содержание

Оглавление

Введение

С недавних пор человек и компьютер стали просто неразлучны. Это произошло, когда в один прекрасный день человек осознал, что компьютер чрезвычайно глубоко проник в его жизнь и отказаться от него практически невозможно.

Сначала компьютеры были каждый сам по себе, затем они объединились в локальную сеть, потом — в глобальную. Трудно представить себе, что будет дальше: компьютер, имплантированный в голову человека, телепатическая связь, виртуальные встречи...

Объединение отдельно стоящих компьютеров в группы позволило достичь невиданных высот как в технологическом плане, так и в сознании человека. Сеть предоставляет пользователям огромное количество разнообразнейших ресурсов, возможность общения и отдыха, серфинг в Интернете, бесплатные звонки в другие страны, участие в торгах на биржах, возможность неплохо зарабатывать и т. д. Чтобы все это получить, нужно начать с малого — создать сеть.

Существуют разные типы и способы построения компьютерных сетей. Наиболее «мощные» технические возможности предоставляет, конечно, проводная сеть. Однако все перспективнее становятся сети, построенные с помощью радиотехнологий, позволяющих приобрести максимальную мобильность и независимость. Пока технологии беспроводных сетей не такие «продвинутые», как технологии их проводных собратьев, но они только продолжают развиваться, и в них скрыт огромнейший потенциал.

В данной книге вы познакомитесь как с теоретическими, так и с практическими основами функционирования сетей. Используя полученные знания, вы сможете построить беспроводную сеть, пусть сначала и небольшую, но все равно это будет настоящая сеть, причем легко модифицируемая. Со временем ваша беспроводная сеть сможет превратиться в достаточно объемную ячейку с большими возможностями. Если взяться за это с умом, то вскоре вы сможете заработать на своей сети приличные деньги — можете не сомневаться!

От издательства

Ваши замечания, предложения и вопросы отправляйте по адресу электронной почты gurski@minsk.piter.com (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

На сайте издательства http://www.piter.com вы найдете подробную информацию о наших книгах.

ГЛАВА 1 Сетевая модель и протоколы передачи данных

- Модель ISO/OSI
- Понятие протокола
- NetBIOS и NetBEUI
- TCP, IP и UDP
- IPX и SPX
- SMTP, POP3 и IMAP
- SLIP, PPP, HTTP и FTP

Наш мир живет и функционирует, основываясь на многих законах и правилах. Конечно, все явления нельзя четко классифицировать или подогнать под общие правила, но, тем не менее, в основе всего сущего лежат законы физики, механики, экономики и, в конце концов, законы природы, которым подчиняются все процессы, происходящие на планете. Если бы ни они, Земля погрузилась бы в полный хаос.

Аналогично построен и компьютерный мир. Правда, к нему применимо скорее понятие стандарта, чем закона. Именно благодаря существованию определенных стандартов производители знают, какими параметрами должно обладать конкретное оборудование и какие функции выполнять, чтобы уметь работать в тех или иных условиях.

Подобные правила и стандарты существуют также в мире сетей, вне зависимости от того, какие они, — проводные или беспроводные. Основными стандартами здесь являются модель взаимодействий ISO/OSI и протоколы передачи данных.

1.1. Модель ISO/OSI

Пожалуй, ключевым понятием в стандартизации сетей и всего, что к ним относится, является модель взаимодействия открытых систем (Open System Interconnection, OSI), разработанная международной организацией по стандартам (International Standards Organization, ISO). На практике применяется название *модель ISO/OSI*.

Описываемая модель состоит из семи уровней. Каждый уровень отвечает за определенный круг задач, выполняя их с помощью специальных алгоритмов — стандартов. Основная задача — достичь глобальной цели, поэтому уровни модели связаны между собой. Таким образом, выполнив свою часть задачи, каждый уровень передает готовые данные следующему уровню. В результате прохождения такой цепочки данные полностью обрабатываются, и их можно использовать.

В зависимости от назначения уровни получили следующие названия: физический, канальный, сетевой, транспортный, сеансовый, уровень представления данных и прикладной (рис. 1.1).

Основные отличия между проводными (Ethernet 802.3) и беспроводными (IEEE 802.11) сетями кроются только в двух нижних уровнях — физическом и канальном. Остальные уровни работают абсолютно одинаково, без каких-либо отличий.

Физический уровень

Физический уровень — первый, самый низкий, уровень. Фактически он представляет собой аппаратную часть сети и описывает способ передачи данных, используя для этого любой имеющийся «под руками» канал — проводной или беспроводной. В зависимости от выбранного канала передачи данных используют соответствующее сетевое оборудование. Параметры передачи данных следует настраивать с учетом

Рис. 1.1. Уровни модели ISO/OSI

особенностей канала: полос пропускания, защиты от помех, уровня сигнала, кодирования, скорости передачи данных в физической среде и т. п.

Фактически всю описанную работу выполняет сетевое оборудование: сетевая карта, мост, маршрутизатор и т. д.

Физический уровень — один из уровней, который отличает беспроводные сети от проводных. Как вы уже, несомненно, поняли, основное отличие между ними заключается в канале передачи данных. Для проводных сетей это радиоволны определенной частоты или инфракрасное излучение, для беспроводных — любая физическая линия, например коаксиал, витая пара или оптоволокно.

Канальный уровень

Главная задача *канального* уровня — удостовериться, что канал готов к передаче данных и ничто не станет угрожать надежности этой операции и целостности передаваемых пакетов. В идеале протоколы канального уровня и сетевое оборудование должны проверить, свободен ли канал для передачи данных, не имеется ли коллизий передачи и т. п.

Такую проверку необходимо выполнять каждый раз, так как локальная сеть чаще всего состоит более, чем из двух компьютеров (хотя даже в таком случае канал может быть занят). Обнаружив, что канал свободен, элементы этого уровня делят данные, которые необходимо передать другому компьютеру, на более мелкие части — кадры. Затем каждый кадр снабжается контрольной сумой и отсылается. Приняв этот кадр, получатель проверяет контрольные суммы и, если они совпадают, принимает его и посылает отправителю подтверждение о доставке. В противном случае получатель игнорирует кадр и фиксирует ошибку, после

чего кадр передается заново. Так, кадр за кадром, передается необходимая информация.

На канальном уровне, как и на физическом, также существуют различия между проводными и беспроводными сетями. Это связано со спецификой сетевого оборудования. Так, доступное на данный момент беспроводное оборудование работает только в полудуплексном режиме: в один момент времени данные могут только приниматься или только передаваться. Этот недостаток резко уменьшает эффективность обнаружения коллизий в сети и, соответственно, понижает скорость передачи данных.

Поскольку модель ISO/OSI жестко регламентирует действия каждого уровня, то разработчикам пришлось немного модернизировать протоколы канального уровня для работы в беспроводных сетях. В частности, для беспроводной передачи данных используются протоколы CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance, многостанционный доступ к среде передачи с контролем несущей и избежанием коллизий) или DCF (Distributed Coordination Function, распространяемая координирующая функция).

Протокол CSMA/CA предназначен для обнаружения конфликтов при передаче данных. Он использует явное подтверждение доставки данных, сообщающее о том, что передаваемый пакет доставлен и не поврежден.

Данный метод работает следующим образом. Когда один компьютер собирается передать информацию другому, он посылает всем компьютерам сети короткое сообщение — RTS (Ready To Send, готов к передаче), содержащее информацию о получателе и времени, необходимом для передачи данных. Получив такой пакет, все компьютеры прекращают на указанный промежуток времени передачу собственных данных. Компьютер, для которого предназначен пакет, отсылает отправителю сообщение CTS (Clear To Send, свободен для передачи) о готовности к приему данных. Получив такое сообщение, компьютер-отправитель пересылает первую порцию данных и ждет подтверждения доставки пакета. После такого подтверждения передача данных продолжается. Если сообщение об успешной доставке не пришло, то компьютер-отправитель повторно передает необходимый пакет.

Такой метод передачи гарантирует доставку пакетов данных, однако в то же время заметно снижает скорость передачи. Именно поэтому беспроводные сети намного медленнее проводных и останутся таковыми надолго, если не навсегда. Чтобы хоть как-то повысить скорость передачи данных по таким сетям, специальный протокол канального уровня фрагментирует пересылаемые пакеты (разбивает их на более мелкие части), что увеличивает шанс их удачной передачи.

Сетевой уровень

Как и канальный уровень, *сетевой* отвечает за передачу данных между компьютерами. Для этого он использует сформированные данные и параметры двух предыдущих уровней — физического и канального. Главное отличие сетевого уровня

от канального заключается в том, что он умеет передавать данные между сетями с разной топологией — комбинированными. Так, очень часто беспроводные и проводные сети используются в паре. Чаще всего это происходит, если по определенным причинам создать единую проводную сеть физически невозможно.

На сетевом уровне, как и на канальном, данные делятся на пакеты, что позволяет достичь качества и определенной скорости их передачи. Однако, в отличие от канального, сетевой уровень выбирает для передачи данных конкретный маршрут. Процесс выбора оптимального маршрута передачи данных называется *маршрутизацией*.

Как правило, информацию о выборе маршрута предоставляют специальные устройства, установленные в сети, — маршрутизаторы. Специальные таблицы маршрутизаторов содержат информацию о скорости передачи данных между отдельными отрезками сети, трафике, среднем времени передачи и т. д. Основываясь на этой информации, протоколы сетевого уровня могут выбрать оптимальный путь прохождения данных.

Транспортный уровень

Пожалуй, *транспортный* уровень можно отнести к более высоким. Это означает, что данным уровнем управляет программа, а не аппаратные средства.

Транспортный уровень отвечает за надежность передачи данных. Существует несколько способов передачи, которые отличаются друг от друга степенью защищенности и возможностью исправления ошибок. Естественно, это сказывается на времени и скорости передачи информации между конкретными точками.

Способ передачи данных выбирается автоматически, с помощью анализа информации маршрутизаторов сети. Если анализ показывает, что конфликты в сети минимальны, то используется самый простой (а значит, самый быстрый) способ. В противном случае выбирается способ передачи высокой степени надежности с возможностью исправления поврежденных пакетов (этот способ передачи, конечно, более медленный). Какой бы способ ни был выбран, в любом случае информация будет доставлена в целостном виде.

Сеансовый уровень

Сеансовый уровень предназначен для контроля передачи пакетов между компьютерами. В процессе синхронизации принятых и отправленных пакетов протоколы сеансового уровня отслеживают недостающие данные и передают их заново. За счет работы только с недостающими пакетами достигается повышение скорости передачи данных.

Уровень представления

На уровне *представления* данные приводятся к единому стандарту, что позволяет достичь договоренности при их приеме и передаче. Именно на этом уровне

данные могут шифроваться, что повышает безопасность их передачи по сети. Кроме того, часто на уровне представления происходит компрессия информации, благодаря чему повышается скорость передачи данных.

Уровень представления реализуется программно, что позволяет использовать для шифрования данных новейшие достижения.

Прикладной уровень

Прикладной уровень — самый верхний уровень модели ISO/OSI. Его задача — организация взаимодействия с прикладными программами. За это отвечает множество прикладных протоколов, с помощью которых операционная система и программы получают доступ к разнообразным ресурсам сети.

1.2. Понятие протокола

В предыдущем разделе мы кратко рассмотрели модель ISO/OSI, которая описывает работу любого сетевого оборудования и сети в целом. Однако это всего лишь модель, рисунок на бумаге. Для начала работы необходим механизм, реализующий описываемую модель. Таким механизмом является протокол передачи данных, включающий в себя множество протоколов.

Таким образом, *протокол* — набор правил, благодаря которым возможна передача данных между компьютерами. Эти правила работают в рамках модели ISO/OSI и не могут отступать от нее ни на шаг, поскольку это может повлечь за собой несовместимость оборудования и программного обеспечения.

Каждый уровень модели ISO/OSI обладает своими особенностями, и реализовать все особенности в рамках одного протокола невозможно. Мало того, это даже невыгодно, поскольку значительную часть логики можно разрабатывать на уровне аппаратного обеспечения, что приводит к ускорению работы с данными. Исходя из этих соображений, было разработано множество узконаправленных протоколов, каждый из которых с максимальной отдачей и быстродействием выполняет свою задачу.

Протоколы могут быть двух типов: низкоуровневые и высокоуровневые.

- Низкоуровневые протоколы появились достаточно давно и с тех пор не претерпели никаких кардинальных изменений. За длительное время использования таких протоколов в них были найдены и устранены все возможные «дыры» и ошибки.

ПРИМЕЧАНИЕ

Низкоуровневые протоколы реализуются на аппаратном уровне, что позволяет добиться их максимального быстродействия.

- Что касается высокоуровневых протоколов, то они постоянно разрабатываются и совершенствуются. В этом нет ничего плохого, даже наоборот: всегда существует возможность придумать новый, более эффективный, способ передачи данных.

ПРИМЕЧАНИЕ

Как правило, высокоуровневые протоколы реализуются в виде драйверов к сетевому оборудованию для работы в разных операционных системах.

Существует множество различных протоколов, каждый из которых имеет свои особенности. Одни протоколы узконаправленные, другие имеют более широкое применение. Каждая компания разрабатывает свой собственный *стек* (набор) протоколов. Хотя разные стеки протоколов изначально несовместимы, существуют дополнительные протоколы, представляющие собой «мосты» между стеками. Благодаря этому в одной операционной системе можно работать с несколькими несовместимыми между собой протоколами.

Стоит также упомянуть тот факт, что не все протоколы можно использовать в одинаковых условиях. Иногда применение одного протокола выгодно для небольшой группы компьютеров и крайне невыгодно для большого количества компьютеров с несколькими маршрутизаторами и подключением к Интернету.

В следующих разделах вы познакомитесь с наиболее распространенными протоколами и стеками протоколов.

1.3. NetBIOS и NetBEUI

NetBIOS

NetBIOS (Network Basic Input Output System, базовая система сетевого ввода/вывода) — протокол (скорее, интерфейс) прикладного программирования, разработанный в конце 1983 года для компьютеров IBM.

На самом деле NetBIOS не является полноценным протоколом, поскольку описывает только программную часть передачи данных — набор сетевых API-функций. Это означает, что с помощью этого протокола можно только подготовить данные для передачи. Физически же передача может осуществляться только с помощью любого транспортного протокола, например TCP.

Благодаря такой ситуации подготовка передачи данных не привязана к транспортному протоколу, что позволяет использовать для этих целей любой подходящий протокол. Кроме того, неоспоримым достоинством NetBIOS является быстродействие.

Однако, к сожалению, для полноценной работы протокола NetBIOS требуется, чтобы на всех компьютерах сети использовался один транспортный протокол,

иначе компьютеры не смогут синхронизироваться. Основным недостатком NetBIOS является то, что он не поддерживает маршрутизацию, без которой не обходится любая мало-мальски развернутая сеть.

NetBEUI

NetBEUI (NetBIOS Extended User Interface, протокол расширенного пользовательского интерфейса базовой системы сетевого ввода/вывода) — протокол, дополняющий NetBIOS. Благодаря NetBEUI появилась возможность не только описывать программный уровень передачи данных, но и передавать их физически по сети, используя специальные встроенные механизмы этого протокола. Кроме того, значительно возросла надежность и скорость передачи данных.

Основной недостаток NetBEUI, как и NetBIOS, — отсутствие механизма маршрутизации, что делает этот протокол бесполезным в больших сетях. Если же ваша сеть состоит из нескольких компьютеров и не располагает маршрутизатором, то более быстрого протокола вы не найдете.

Итак, протокол NetBEUI не поддерживает маршрутизацию в сети, что не позволяет эффективно использовать его скорость в глобальных сетях. Тем не менее, этот протокол является одним из основных компонентов NT-систем, и его установка происходит автоматически.

1.4. TCP, IP и UDP

TCP

TCP (Transmission Control Protocol, протокол управления передачей данных) — распространенный протокол, разработанный много лет назад. Он используется не только в локальных сетях, но и в сети Интернет, что однозначно характеризует TCP с хорошей стороны.

Главным достоинством протокола является его надежность, достигаемая путем использования подтверждающих пакетов, которые присылаются каждый раз в ответ на полученное сообщение. При этом в первую очередь устанавливается логическая связь между компьютером-отправителем и компьютером-получателем, что гарантирует успешную доставку пакетов.

Еще одним механизмом надежности передачи данных является механизм, отслеживающий время жизни пакета, — TTL (Time To Live, время жизни). Если по истечении заданного времени компьютер-получатель не пришлет подтверждение о доставке очередного пакета данных, то компьютер-отправитель перешлет эти данные повторно. Кроме того, данные будут повторно посланы, если пакет оказался поврежденным и компьютер-получатель его отклоняет, о чем сообщает отправителю.

IP

IP (Internet Protocol, протокол межсетевого взаимодействия) — протокол, который обычно применяется вместе с протоколом TCP. Для работы он использует готовые данные маршрутизации, поэтому не контролирует доставку сообщений адресату. Располагая информацией о маршрутизации между выбранными компьютерами, этот протокол просто добавляет к пакету адрес отправителя и получателя[1] и пересылает его дальше. Дальнейшая судьба отправленных данных неизвестна, поэтому функцию контроля должен выполнять другой протокол, в частности TCP.

Чтобы хоть как-то повысить надежность, протокол IP вкладывает в пакет контрольную сумму, что позволяет компьютеру-получателю удостовериться в том, что пакет принят без ошибок или, в противном случае, отвергнуть его.

Преимуществом протокола является возможность фрагментации (разделения на компьютере-отправителе большого пакета на более мелкие) с последующей их дефрагментацией на компьютере-получателе.

UDP

UDP (User Datagram Protocol, протокол пользовательских дейтаграмм) — один из самых быстрых, но не очень надежных протоколов, которые используют в сети для передачи данных. Он работает практически так же, как и протокол IP, однако после удачного приема пакета компьютер-получатель присылает соответствующее подтверждение. При этом логическое соединение между компьютерами не требуется, то есть пакет отсылается в надежде (или с уверенностью) на то, что нужный компьютер находится в сети и может его принять. Если подтверждение доставки не получено, значит, через некоторое время компьютер-отправитель повторно вышлет необходимый пакет данных.

Как ни странно, протокол UDP применяется в сети достаточно часто. Благодарить за это нужно скорость, с которой он работает. Эта скорость достигается за счет отсутствия необходимости соединения с другими компьютерами, что позволяет использовать трафик сети в нужном направлении. Так, протокол UDP часто используется, например, в сетевых играх или для передачи звуковых данных с интернет-радио (когда надежность доставки пакетов не играет большой роли).

1.5. IPX и SPX

Протоколы IPX и SPX являются представителями стека протоколов, разработанных компанией Novell. В свое время эта компания являлась прямым конкурентом

[1] При работе протокол использует понятие *дейтаграммы* — пакета данных, снабженных служебной информацией о получателе и отправителе.

Microsoft в области сетевых операционных систем: противостояли операционная система Novell Netware и Windows NT. Соответственно, каждая операционная система использовала собственный набор протоколов.

Как известно, компания Novell сдала свои позиции, и первенство завоевали сетевые версии операционной системы Windows NT. Тем не менее протоколы, разработанные Novell, используются до сих пор и будут использоваться еще очень долго.

IPX

IPX (Internetwork Packet eXchange, протокол межсетевого обмена объектами) — один из самых «ходовых» протоколов, используемых на сетевом уровне. Главной его задачей является определение оптимального маршрута между двумя выбранными компьютерами с использованием для этого данных других протоколов.

В первую очередь данный протокол вычисляет адрес компьютера, которому необходимо отправить пакет — дейтаграмму. Определив адрес нужного компьютера, он снабжает дейтаграмму служебной информацией (адресом отправителя и получателя) и отправляет «в путь» по выбранному маршруту.

Однако самостоятельно этот протокол работать не может, поскольку не способен устанавливать соединение между компьютерами. Соответственно, от IPX нельзя ожидать высокой степени надежности доставки пакетов.

SPX

SPX (Sequenced Packet eXchange, последовательный обмен пакетами) — «родной брат» IPX, без которого его нельзя назвать полноценным протоколом. Эти протоколы используются вместе и имеют общее название — IPX/SPX.

Главная задача протокола SPX — установка логического соединения между выбранными компьютерами с последующей передачей подготовленных дейтаграмм.

1.6. SMTP, POP3 и IMAP

Без протоколов SMTP, POP3 и IMAP невозможна работа электронной почты. Надеюсь, что такое электронная почта и как без нее плохо, объяснять не нужно.

Особенностью этих протоколов является их узкая направленность. Это означает, что их принципиально невозможно использовать для других целей, что, к тому же, не имеет смысла. Задача SMTP, POP3 и IMAP — организация обмена электронными сообщениями, и они отлично с ней справляются.

Еще одной особенностью почтовых протоколов является однозадачность. Например, протокол, отсылающий сообщения, не способен их принимать, и наоборот. Именно поэтому такие протоколы работают парами.

SMTP

SMTP (Simple Mail Transfer Protocol, упрощенный протокол пересылки почты) — протокол, основной задачей которого является отсылка подготовленных специальным образом сообщений. Перед тем, как это сделать, протокол устанавливает соединение между компьютерами, что гарантирует доставку сообщения.

Протокол SMTP очень простой и эффективный, однако эта эффективность не распространяется на все задачи и возможности. Так, он не обладает даже простейшим механизмом аутентификации и возможностью шифрования данных при передаче между почтовыми серверами. Самым большим недостатком SMTP является его неспособность к пересылке графики.

Чтобы не отказываться от этого довольно хорошего протокола, было принято решение расширить его несколькими полезными и необходимыми расширениями. Таким расширением, например, является *MIME* (Multipurpose Internet Mail Extensions, многоцелевое расширение почтовой службы в Интернете), благодаря которому существует возможность отсылать файлы любого формата и содержания. Кроме того, разработан стандарт UUENCODE, позволяющий передавать текстовые сообщения в разных кодировках.

POP3

POP3 (Post Office Protocol 3, почтовый протокол версии 3) — почтовый протокол, который используется для приема электронных сообщений с почтового сервера.

Обычно POP3 работает в паре с протоколом SMTP, что позволяет организовать эффективную систему отсылки и приема электронных сообщений.

Интерфейс протокола еще более простой, чем интерфейс SMTP, и с этим связаны определенные неудобства. Так, отсутствует возможность выборочного скачивания письма или просмотра содержимого письма непосредственно на почтовом сервере

IMAP

IMAP (Interactive Mail Access Protocol, протокол интерактивного доступа к электронной почте) — наиболее «продвинутый» почтовый протокол, предназначенный для приема электронных сообщений с почтового сервера. В большинстве случаев более удобным и эффективным является использование протокола IMAP, чем POP3.

К достоинствам протокола относится возможность частичного скачивания письма, разбития принимаемого письма на части с последующим склеиванием и многое другое.

1.7. SLIP, PPP, HTTP и FTP

Данные протоколы предназначены для организации выхода в Интернет и работы в нем с использованием различных браузеров, менеджеров закачек и др.

SLIP и PPP

С протоколами *SLIP* (Serial Line Internet Protocol, протокол последовательного подключения к Интернету) и *PPP* (Point-to-Point Protocol, протокол двухточечной связи) в основном работают провайдеры, которые используют для организации доступа в Интернет выделенные телефонные линии или другие каналы.

SLIP и PPP используются для организации постоянного подключения к Интернету с помощью модема. Для обычного пользователя наличие постоянного соединения с Интернетом является достаточно дорогим, поскольку при этом нужно платить как за время пребывания в Интернете, так и за используемую телефонную линию. Это могут позволить себе только достаточно крупные компании и интернет-провайдеры. Первые из них, как правило, в этом случае располагают одним или несколькими серверами с данными, а также личными веб-страницами, которые должны быть постоянно доступны через Интернет. Вторые используют постоянное подключение, поскольку это их работа.

Протоколы SLIP и PPP работают на нижних уровнях модели взаимодействия открытых систем, что позволяет специальным образом готовить пакеты данных для передачи их другими протоколами, например TCP/IP или IPX/SPX. Главное отличие протокола SLIP от протокола PPP заключается в том, что первый работает только на компьютерах с установленной операционной системой Unix и протоколом TCP/IP, а второй используется на компьютерах, работающих под управлением системы класса Windows NT, которая умеет обращаться практически с любыми протоколами передачи данных.

HTTP

HTTP (HyperText Transport Protocol, гипертекстовый транспортный протокол) — протокол, предназначенный для организации пересылки данных веб-страниц по Интернету или локальной сети. За время своего существования этот протокол претерпел значительные изменения; известно несколько его версий.

Особенностью протокола HTTP является то, что он может передавать любую информацию — текстовую и графическую. Это позволяет использовать при разработке веб-страниц дополнительные средства, которые делают их анимированными и красиво оформленными.

FTP

FTP (File Transfer Protocol, протокол передачи файлов) — протокол, изначально разработанный и применяемый для передачи файлов с помощью Интернета. Без этого протокола было бы невозможным скачивание из Сети музыки, фильмов и других объемных данных, без которых современный пользователь компьютера не может представить свою жизнь. Существует множество программ, которые, используя протокол FTP, позволяют скачивать значительные объемы информации даже в условиях плохого соединения и низкой скорости передачи данных.

ГЛАВА 2 Топология и стандарты

- Архитектура беспроводных сетей
- Методы и технологии модуляции сигнала
- Стандарты Radio Ethernet
- Преимущества и недостатки беспроводной сети

Итак, вы уже знаете, что сеть и все, что с ней связано, основывается на модели взаимодействия открытых систем ISO/OSI, разработанной международной организацией по стандартам. Однако для создания сети этого недостаточно. Главной задачей при проектировании сети является использование правильной сетевой топологии и стандарта, который описывает скорость передачи данных, радиус действия сети, тип оборудования и многое другое.

2.1. Архитектура беспроводных сетей

Развитие беспроводных сетей, как и многое другое, проходит под неусыпным контролем соответствующих организацией. Самой главной среди них является IEEE (Institute of Electrical and Electronic Engineers, Международный институт инженеров электротехники и электроники). В частности, беспроводные стандарты, сетевое оборудование и все, что относится к беспроводным сетям, контролирует рабочая группа WLAN (Wireless Local Area Network, беспроводная локальная вычислительная сеть), в которую входят более 100 представителей различных университетов и компаний-разработчиков сетевого оборудования. Эта комиссия собирается несколько раз в год с целью совершенствования существующих стандартов и создания новых, базирующихся на последних исследованиях и компьютерных достижениях.

В России также существует ассоциация беспроводных сетей передачи данных — «Беседа», которая занимается ведением единой политики в области беспроводных сетей передачи данных. Эта организация контролирует развитие рынка беспроводных сетей, предоставляет разные услуги при подключении, организует создание и развитие новых центров беспроводного доступа и т. д.

Обратимся к архитектуре беспроводных сетей. На сегодняшний день используется два варианта беспроводной архитектуры или, проще говоря, варианта построения сети: *независимая* конфигурация (Ad-Hoc) и *инфраструктурная* конфигурация. Отличия между ними незначительные, однако они кардинально влияют на такие показатели, как количество подключаемых пользователей, радиус сети, помехоустойчивость и т. д.

Какая бы конфигурация сети ни была избрана, стандарты определяют один тип протокола доступа к носителю и разные спецификации для физических каналов[1].

Пакеты данных, передаваемых протоколом по физическому каналу, разбиваются на несколько блоков:

- контрольные и адресные данные — 30 байт;
- информационные данные — 2 Кбайт;
- контрольная сумма информационных данных — 4 байт.

---

[1] Стандарт IEEE 802.11 предусматривает только три метода передачи данных.

Независимая конфигурация (Ad-Hoc)

Режим независимой конфигурации (рис. 2.1) (IBSS — Independent Basic Service Set, независимый базовый набор служб), котрый часто называют «точка-точка», — самый простой в применении. Соответственно, самым простым является построение и настройка сети с использованием независимой конфигурации.

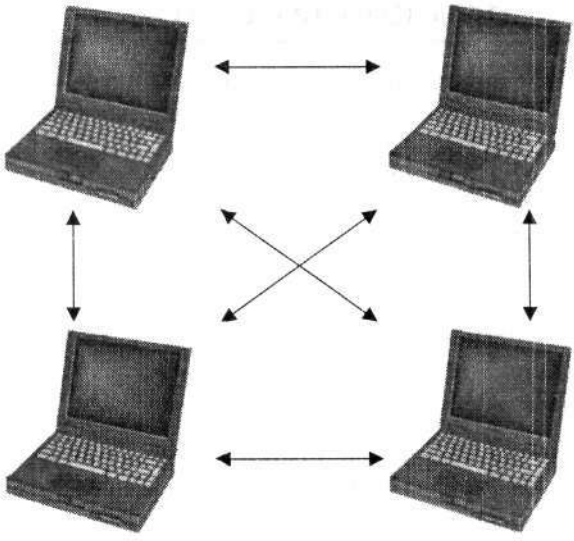

Рис. 2.1. Режим независимой конфигурации

Чтобы объединить компьютеры в беспроводную сеть, достаточно оборудовать каждый компьютер адаптером беспроводной связи. Как правило, такими адаптеры изначально комплектуются переносные компьютеры, что сводит построение сети к настройке соответствующих ресурсов и ограничений.

Обычно такой способ используется для организации хаотичной или временной сети, а также в том случае, если другой способ построения сети по каким-либо причинам не подходит.

Хотя режим независимой конфигурации прост в построении, он обладает некоторыми недостатками, главными из которых являются малый радиус действия сети и низкая устойчивость к помехам, что накладывает определенные ограничения на месторасположение компьютеров сети. Кроме того, подключиться к внешней сети или к Интернету в таком случае очень непросто.

ПРИМЕЧАНИЕ

При соединении двух компьютеров с использованием узконаправленных антенн радиус действия сети увеличивается и может достигать 30 км и более.

Инфраструктурная конфигурация

Инфраструктурная конфигурация, или, как ее еще часто называют, «режим клиент/сервер», — более перспективный и быстроразвивающийся вариант беспроводной сети.

Инфраструктурная конфигурация имеет много преимуществ, среди которых возможность подключения достаточно большого количества пользователей, хорошая помехоустойчивость, высокий уровень контроля подключений и многое другое. Кроме того, имеется возможность использования комбинированной топологии и проводных сегментов сети.

Помимо того, что на компьютерах должны быть установлены адаптеры беспроводной связи, для организации беспроводной сети с использованием инфраструктурной конфигурации необходимо иметь как минимум одну точку доступа (Access Point) (рис. 2.2).

Рис. 2.2. Точка доступа

В этом случае конфигурация называется *базовым набором служб* (BSS — Basic Service Set). Точка доступа может работать автономно или в составе проводной сети и может выполнять функцию моста между проводным и беспроводным сегментами сети. При такой конфигурации сети компьютеры «общаются» только с точкой доступа, которая управляет передачей данных между компьютерами (рис. 2.3).

Конечно, одной точкой доступа сеть может не ограничиваться, что и случается по мере роста сети. В этом случае базовые наборы служб образуют единую сеть, конфигурация которой носит название *расширенного набора служб* (ESS — Extended Service Set). При такой конфигурации сети точки доступа обмениваются между собой информацией, передаваемой с помощью проводного соединения (рис. 2.4) или с помощью радиомостов. Это позволяет эффективно организовывать трафик между сегментами сети (фактически — точками доступа).

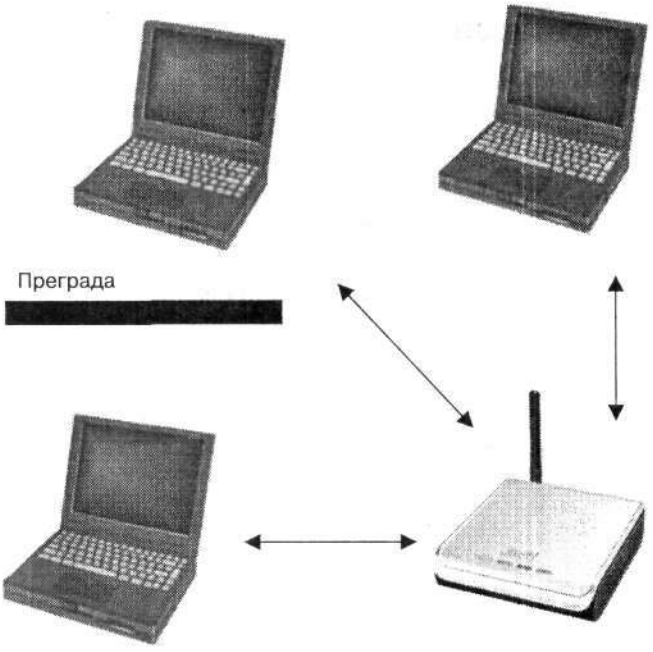

Рис. 2.3. Базовый набор служб инфраструктурной конфигурации

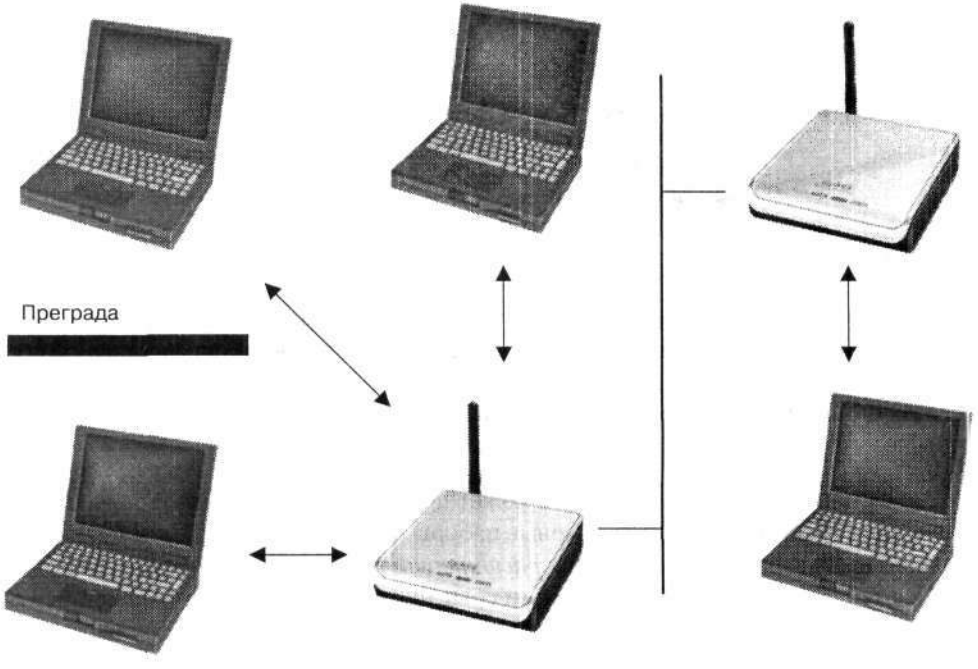

Рис. 2.4. Расширенный набор служб инфраструктурной конфигурации

2.2. Методы и технологии модуляции сигнала

Каждый новый стандарт использует новые, более быстрые и надежные спецификации для физического уровня:

- спецификация для работы в инфракрасном диапазоне;
- DSSS (Direct Sequence Spread Spectrum, расширение спектра прямой последовательностью) — определяет работу устройств в диапазоне радиочастот по радиоканалам с широкополосной модуляцией с прямым расширением спектра методами прямой псевдослучайной последовательности;
- FHSS (Frequency Hopping Spread Spectrum, расширение спектра за счет скачкообразного изменения частоты) — определяет работу устройств в диапазоне радиочастот по радиоканалам с широкополосной модуляцией со скачкообразной перестройкой частоты псевдослучайными методами;
- OFDM (Orthogonal Frequency Division Multiplexing, ортогональное мультиплексирование с разделением частот) — определяет работу устройств в диапазоне радиочастот по радиоканалам с использованием подканалов с разными несущими частотами;
- PBCC (Packet Binary Convolutional Coding, двоичное пакетное свёрточное кодирование) — метод двоичного пакетного свёрточного кодирования;
- технология кодирования Баркера — описывает способ кодирования данных с помощью последовательностей Баркера;
- CCK (Complementary Code Keying, кодирование с помощью комплементарных кодов) — описывает способ дополнительного кодирования битов передаваемой информации;
- CCK-OFDM — описывает способ кодирования данных с помощью гибридного метода, что позволяет увеличить скорость передачи сигнала при невысокой избыточности данных;
- QAM (Quadrature Amplitude Modulation, квадратурная амплитудная модуляция) — описывает способ квадратурной амплитудной модуляции сигнала, который работает на скорости выше 48 Мбит/с.

Первые образцы оборудования работали в диапазоне частот 902–928 МГц. Данные передавались со скоростью 215–860 Кбит/с при использовании метода расширения спектра прямой последовательностью (DSSS). Указанный диапазон частот разбивался на каналы шириной около 5 МГц (при скорости передачи данных 215 Кбит/с таких каналов получалось пять). При максимальной скорости передачи информации спектр сигнала достигал 19 МГц, в результате чего получался только один частотный канал шириной 26 МГц.

Когда появилось подобное оборудование, то используемой скорости передачи данных было достаточно для выполнения многих задач, если сеть состояла из нескольких

компьютеров. Однако чем больше компьютеров подключалось к сети, тем ниже становилась скорость передачи данных. Например, при подключении к сети пяти компьютеров реальная скорость передачи данных в пять раз меньше теоретической. Таким образом, чем больше компьютеров в сети, тем с меньшей скоростью передавались данные, а при теоретической скорости передачи данных 860 Кбит/с возможная скорость передачи вообще составляет «крохи».

Конечно, скорость можно было бы со временем увеличить. Однако начали проявляться последствия других негативных факторов, самым главным из которых стало использование диапазона 900 МГц операторами мобильной связи. Именно этот факт привел к тому, что подобное оборудование для беспроводных сетей не прижилось среди пользователей. В результате анализа сложившейся ситуации было принято решение использовать диапазон частот 2400–2483,5 МГц, а позже – 5,150–5,350 ГГц, 5150–5350 МГц и, наконец, 5725–5875 МГц. Это позволило добиться не только большей пропускной способности таких сетей, но и достаточной защищенности от помех.

Метод DSSS

Смысл метода расширения спектра прямой псевдослучайной последовательностью (DSSS) заключается в приведении узкополосного спектра сигнала к его широкополосному представлению, что позволяет увеличить устойчивость передаваемых данных к помехам.

При использовании метода широкополосной модуляции с прямым расширением спектра диапазон 2400–2483,5 МГц делится на 14 перекрывающихся или три неперекрывающихся канала с промежутком в 25 МГц. Фактически это означает, что разное оборудование может параллельно использовать три канала, при этом не мешая друг другу работать.

Для пересылки данных используется всего один канал. Чтобы повысить качество передачи и снизить потребляемую при этом энергию[1] (за счет снижения мощности передаваемого сигнала), используется последовательность Баркера, которая характеризуется достаточно большой избыточностью. Избыточность кода позволяет избежать повторной передачи данных, даже если пакет частично поврежден.

Метод FHSS

При использовании метода широкополосной модуляции со скачкообразной перестройкой (FHSS) частотный диапазон 2400–2483,5 МГц делится на 79 каналов шириной по 1 МГц. Данные передаются последовательно по разным каналам, создавая некоторую схему переключения между каналами. Всего существует 22 такие схемы, причем схему переключения согласовывают отправитель и получатель дан-

[1] Большое потребление энергии является критичным для переносных компьютеров.

ных. Схемы переключения разработаны таким образом, что шанс использования одного канала разными отправителями минимален.

Переключение между каналами происходит очень часто, что обусловлено малой шириной канала (1 МГц). Поэтому метод FHSS в своей работе использует весь доступный диапазон частот, а значит, и все каналы.

Метод OFDM

Метод ортогонального частотного мультиплексирования (OFDM) является одним из «продвинутых» и скоростных методов передачи данных. В отличие от методов DSSS и FHSS, с его помощью можно параллельно передавать данные по нескольким частотам радиодиапазона. При этом информация разбиваются на части, что позволяет не только увеличить скорость, но и улучшить качество передачи.

Данный метод модуляции сигнала может работать в двух диапазонах — 2,4 и 5 ГГц.

Метод PBCC

Метод двоичного пакетного свёрточного кодирования (BCC) используется при скорости передачи данных 5,5 и 11 Мбит/с. Этот же метод, только слегка модифицированный, используется и при скорости передачи данных 22 Мбит/с.

Принцип PBCC основан на том, что каждому биту информации, который нужно передать, назначаются соответствующие два выходных бита (так называемый *дибит*), созданные в результате преобразований с помощью логической функции XOR и нескольких запоминающих ячеек[1]. Поэтому этот метод называется свёрточным кодированием со скоростью 1/2, а сам механизм кодирования — свёрточным кодером.

ПРИМЕЧАНИЕ

При скорости входных битов *N* бит/с скорость выходной последовательности (после свёрточного кодера) составляет 2*N* бит/с. Отсюда и понятие скорости — один к двум (1/2).

Использование свёрточного кодера позволяет добиться избыточности кода, что, в свою очередь, повышает надежность приема данных.

Чтобы отправить готовый дибит, используется фазовая модуляция сигнала. При этом в зависимости от скорости передачи применяется определенный метод модуляции — двоичная фазовая модуляция (BPSK, скорость передачи — 5,5 Мбит/с) или квадратичная фазовая модуляция (QPSK, скорость передачи — 11 Мбит/с).

[1] В протоколе 802.11b и 802.11g используются свёрточные кодеры, состоящие из шести запоминающих ячеек.

Смысл модуляции заключается в том, чтобы ужать выходной дибит до одного символа, не теряя при этом избыточность кода. В результате скорость поступления данных будет соответствовать скорости их передачи, но при этом они будут обладать сформированной избыточностью кода и более высокой помехозащищенностью.

Метод PBCC также предусматривает работу со скоростью передачи данных 22 и 33 Мбит/с. При этом используется пунктурный кодер и другая фазовая модуляция.

Для примера рассмотрим скорость передачи данных 22 Мбит/с (вдвое выше скорости 11 Мбит/с). В этом случае согласно алгоритму своей работы свёрточный кодер переводит каждые два входящих бита в четыре исходящих. Это приводит к слишком большой избыточности кода, что не всегда приемлемо при определенном уровне помех. Поэтому, чтобы уменьшить лишнюю избыточность, используется пунктурный кодер, задача которого — удаление лишнего бита в группе из четырех битов, выходящих из свёрточного кодера.

Таким образом, каждым двум входящим битам соответствуют три бита, обладающие достаточной избыточностью. Эти три бита проходят через модернизированную фазовую модуляцию (восьмипозиционная фазовая модуляция 8-PSK), которая упаковывает их в один символ, готовый к передаче.

Технология кодирования Баркера

Чтобы повысить помехоустойчивость передаваемого сигнала, то есть увеличить вероятность безошибочного распознавания сигнала на приемной стороне в условиях шума, можно воспользоваться методом перехода к широкополосному сигналу, добавляя в исходный сигнал избыточность. Для этого в каждый передаваемый информационный бит «встраивают» определенный код, состоящий из последовательности так называемых чипов.

Итак, после подбора специальных сочетаний последовательности чипов и превращения исходящего сигнала практически в нераспознаваемый шум при приеме сигнал умножается на специальную корреляционную функцию (код Баркера). В результате этого все шумы становятся в 11 раз слабее, так как остается только полезная часть сигнала — непосредственно данные.

Казалось бы, что можно сделать с сигналом, который состоит из сплошного шума? Оказывается, применив код Баркера, можно достичь гарантированного качества доставки данных.

Технология CCK

Технология шифрования с использованием комплементарных кодов (CCK) применяется для сжатия битов данных, что позволяет достичь повышения скорости передачи информации.

Изначально эта технология использовалась в стандарте IEEE 802.11b, что позволило достичь скорости передачи данных 5,5 и 11 Мбит/с. С помощью CCK можно кодировать несколько битов в один символ. В частности, при скорости передачи данных 5,5 Мбит/с 1 символ равняется четырем битам, а при скорости 11 Мбит/с один символ равен 8 битам данных.

Данный способ кодирования можно описать достаточно сложными системами — математическими уравнениями, в основе которых лежат комплементарные восьмиразрядные комплексные последовательности. Коснемся этой темы лишь поверхностно.

Технология CCK-OFDM

Технология гибридного кодирования CCK-OFDM используется при работе оборудования как с обязательными, так и с возможными скоростями передачи данных.

Как ранее упоминалось, при передаче информации применяются пакеты данных, имеющих специальную структуру. Эта структура содержит, как минимум, служебный заголовок. При использовании гибридного кодирования CCK-OFDM служебный заголовок пакета строится с помощью CCK-кодирования, а сами данные — с помощью OFDM-кодирования.

Технология QAM

Технология квадратурной амплитудной модуляции (QAM) используется при высоких скоростях передачи данных (начиная со скорости 24 Мбит/с). Ее суть заключается в том, что скорость передачи данных повышается за счет изменения фазы сигнала и изменения его амплитуды. При этом используются модуляции 16-QAM и 64-QAM, которые позволяют кодировать 4 бита в одном символе при 16 разных состояниях сигнала (в первом случае) и 6 битов в одном символе при 64 разных состояниях сигнала (во втором).

Обычно 16-QAM используется при скорости передачи данных 24 и 36 Мбит/с, а модуляция 64-QAM — при скорости передачи данных 48 и 54 Мбит/с.

2.3. Стандарты Radio Ethernet

Рассмотрим все существующие стандарты IEEE 802.11, которые предписывают использование определенных методов и скоростей передачи данных, методов модуляции, мощности передатчиков, полос частот, на которых они работают, методов аутентификации, шифрования и многое другое.

С самого начала сложилось так, что некоторые стандарты работают на физическом уровне, некоторые — на уровне среды передачи данных, а остальные — на более высоких уровнях модели взаимодействия открытых систем ISO/OSI.

Существуют следующее группы стандартов:

- IEEE 802.11a, IEEE 802.11b и IEEE 802.11g описывают работу сетевого оборудования (физический уровень);
- IEEE 802.11d, IEEE 802.11e, IEEE 802.11i, IEEE 802.11j, IEEE 802.11h и IEEE 802.11r — параметры среды, частоты радиоканала, средства безопасности, способы передачи мультимедийных данных и т. д.;
- IEEE 802.11f и IEEE 802.11c — принцип взаимодействия точек доступа между собой, работу радиомостов и т. п.

IEEE 802.11

Стандарт IEEE 802.11 был «первенцем» среди стандартов беспроводной сети. Работу над ним начали еще в 1990 году. Как и полагается, этим занималась рабочая группа из IEEE, целью которой было создание единого стандарта для радиооборудования, которое работало на частоте 2,4 ГГц. При этом ставилась задача достичь скорости 1 и 2 Мбит/с при использовании методов DSSS и FHSS соответственно.

Работа над созданием стандарта закончилась через 7 лет. Цель была достигнута, но скорость, которую обеспечивал новый стандарт, оказалась слишком малой для современных потребностей. Поэтому рабочая группа из IEEE начала разработку новых, более скоростных, стандартов.

Разработчики стандарта 802.11 учитывали особенности сотовой архитектуры системы. Почему сотовой? Очень просто: достаточно вспомнить, что волны распространяются в разные стороны на определенный радиус. Получается, что внешне зона напоминает соту. Каждая такая сота работает под управлением базовой станции, в качестве которой выступает точка доступа. Часто соту называют *базовой зоной обслуживания*.

Чтобы базовые зоны обслуживания могли общаться между собой, существует специальная распределительная система (Distribution System, DS). Недостатком распределительной системы стандарта 802.11 является невозможность роуминга.

Стандарт IEEE 802.11 предусматривает работу компьютеров без точки доступа, в составе одной соты. В этом случае функции точки доступа выполняют сами рабочие станции.

Этот стандарт разработан и ориентирован на оборудование, функционирующее в полосе частот 2400–2483,5 МГц. При этом радиус соты достигает 300 м, не ограничивая топологию сети.

IEEE 802.11a

IEEE 802.11a — наиболее перспективный стандарт беспроводной сети, который рассчитан на работу в двух радиодиапазонах — 2,4 и 5 ГГц. Используемый метод

OFDM позволяет достичь максимальной скорости передачи данных 54 Мбит/с. Кроме этой, спецификациями предусмотрены и другие скорости:

- обязательные — 6, 12 и 24 Мбит/с;
- необязательные — 9, 18, 36, 48 и 54 Мбит/с.

Этот стандарт также имеет свои преимущества и недостатки. Из преимуществ можно отметить следующие:

- использование параллельной передачи данных;
- высокая скорость передачи;
- возможность подключения большого количества компьютеров.

Недостатки стандарта IEEE 802.11a такие:

- меньший радиус сети при использовании диапазона 5 ГГц (примерно 100 м);
- большая потребляемая мощность радиопередатчиков;
- более высокая стоимость оборудования по сравнению с оборудованием других стандартов;
- для использования диапазона 5 ГГц требуется наличие специального разрешения.

Для достижения высоких скоростей передачи данных стандарт IEEE 802.11a использует в своей работе технологию квадратурной амплитудной модуляции QAM.

IEEE 802.11b

Работа над стандартом IEEE 802.11b (другое название — IEEE 802.11 High rate, высокая пропускная способность) была закончена в 1999 году, и именно с ним связано название Wi-Fi (Wireless Fidelity, беспроводная точность).

Работа данного стандарта основана на методе прямого расширения спектра (DSSS) с использованием восьмиразрядных последовательностей Уолша. При этом каждый бит данных кодируется с помощью последовательности дополнительных кодов (CCK). Это позволяет достичь скорости передачи данных 11 Мбит/с.

Как и базовый стандарт, IEEE 802.11b работает с частотой 2,4 ГГц, используя не более трех неперекрывающихся каналов. Радиус действия сети при этом составляет около 300 м.

Отличительной особенностью этого стандарта является то, что при необходимости (например, при ухудшении качества сигнала, большой удаленности от точки доступа, различных помехах) скорость передачи данных может уменьшаться вплоть до 1 Мбит/с[1]. Напротив, обнаружив, что качество сигнала улучшилось, сетевое

[1] Предусмотрено поэтапное снижение скорости: 5,5 Мбит/с, затем 2 Мбит/с и, наконец, 1 Мбит/с.

оборудование автоматически повышает скорость передачи до максимальной. Этот механизм называется *динамическим сдвигом скорости*.

ПРИМЕЧАНИЕ

Кроме оборудования стандарта IEEE 802.11b, часто встречается оборудование IEEE 802.11b+. Отличие между этими стандартами заключается лишь в скорости передачи данных. В последнем случае она составляет 22 Мбит/с благодаря использованию метода двоичного пакетного свёрточного кодирования (PBCC).

IEEE 802.11d

Стандарт IEEE 802.11d определяет параметры физических каналов и сетевого оборудования. Он описывает правила, касающиеся разрешенной мощности излучения передатчиков в диапазонах частот, допустимых законами.

Этот стандарт очень важен, поскольку для работы сетевого оборудования используются радиоволны. Если они не будут соответствовать указанным параметрам, то могут помешать другим устройствам, работающим в этом или близлежащем диапазоне частот.

IEEE 802.11e

Поскольку по сети могут передаваться данные разных форматов и важности, существует потребность в механизме, который бы определял их важность и присваивал необходимый приоритет. За это отвечает стандарт IEEE 802.11e, специально разработанный с целью передачи потоковых видео- или аудиоданных с гарантированными качеством и доставкой.

IEEE 802.11f

Стандарт IEEE 802.11f разработан с целью обеспечения аутентификации сетевого оборудования (рабочей станции) при перемещении компьютера пользователя от одной точки доступа к другой, то есть между сегментами сети. При этом вступает в действие протокол обмена служебной информацией IAPP (Inter-Access Point Protocol), который необходим для передачи данных между точками доступа. При этом достигается эффективная организация работы распределенных беспроводных сетей.

IEEE 802.11g

Наиболее «продвинутым» на сегодняшний день стандартом можно считать стандарт IEEE 802.11g, который унаследовал самые лучшие свойства стандартов IEEE 802.11b и IEEE 802.11b и, кроме того, обладает многими собственными полезными качествами. Целью создания данного стандарта было достижение скорости передачи данных 54 Мбит/с.

Как и IEEE 802.11b, стандарт IEEE 802.11g разработан для работы в частотном диапазоне 2,4 ГГц. IEEE 802.11g предписывает обязательные и возможные скорости передачи данных:

- обязательные — 1; 2; 5,5; 6; 11; 12 и 24 Мбит/с;
- возможные — 33, 36, 48 и 54 Мбит/с.

Для достижения таких показателей используется кодирование с помощью последовательности дополнительных кодов (CCK), метод ортогонального частотного мультиплексирования (OFDM), метод гибридного кодирования (CCK-OFDM) и метод двоичного пакетного свёрточного кодирования (PBCC).

Стоит отметить, что одной и той же скорости можно достичь разными методами, однако обязательные скорости передачи данных достигаются только с помощью методов CCK и OFDM, а возможные скорости — с помощью методов CCK-OFDM и PBCC.

Преимуществом оборудования стандарта IEEE 802.11g является совместимость с оборудованием IEEE 802.11b. Вы сможете легко использовать свой компьютер с сетевой картой стандарта IEEE 802.11 для работы с точкой доступа стандарта IEEE 802.11g, и наоборот. Кроме того, потребляемая мощность оборудования этого стандарта намного ниже, чем аналогичного оборудования стандарта IEEE 802.11a.

IEEE 802.11h

Стандарт IEEE 802.11h разработан с целью эффективного управления мощностью излучения передатчика, выбором несущей частоты передачи и генерации нужных отчетов. Он вносит некоторые новые алгоритмы в протокол доступа к среде MAC (Media Access Control, управление доступом к среде), а также в физический уровень стандарта IEEE 802.11a.

В первую очередь это связано с тем, что в некоторых странах диапазон 5 ГГц используется для трансляции спутникового телевидения, для радарного слежения за объектами и т. п., что может вносить помехи в работу передатчиков беспроводной сети.

Смысл работы алгоритмов стандарта IEEE 802.11h заключается в том, что при обнаружении отраженных сигналов (интерференции) компьютеры беспроводной сети (или передатчики) могут динамически переходить в другой диапазон, а также понижать или повышать мощность передатчиков. Это позволяет эффективнее организовать работу уличных и офисных радиосетей.

IEEE 802.11i

Стандарт IEEE 802.11i разработан специально для повышения безопасности работы беспроводной сети. С этой целью созданы разные алгоритмы шифрования

и аутентификации, функции защиты при обмене информацией, возможность генерирования ключей и т. д.:

- AES (Advanced Encryption Standard, передовой алгоритм шифрования данных) — алгоритм шифрования, который позволяет работать с ключами длиной 128, 192 и 256 бит;
- RADIUS (Remote Authentication Dial-In User Service, служба дистанционной аутентификации пользователя) — система аутентификации с возможностью генерирования ключей для каждой сессии и управления ими, включающая в себя алгоритмы проверки подлинности пакетов и т. д.;
- TKIP (Temporal Key Integrity Protocol, протокол целостности временных ключей) — алгоритм шифрования данных;
- WRAP (Wireless Robust Authenticated Protocol, устойчивый беспроводной протокол аутентификации) — алгоритм шифрования данных;
- CCMP (Counter with Cipher Block Chaining Message Authentication Code Protocol) — алгоритм шифрования данных.

IEEE 802.11j

Стандарт IEEE 802.11j разработан специально для использования беспроводных сетей в Японии, а именно — для работы в дополнительном диапазоне радиочастот 4,9–5 ГГц[1]. Спецификация предназначена для Японии и расширяет стандарт 802.11a добавочным каналом 4,9 ГГц.

ПРИМЕЧАНИЕ

На данный момент частота 4,9 ГГц рассматривается как дополнительный диапазон для использования в США. Из официальных источников известно, что этот диапазон готовится для использования органами общественной и национальной безопасности.

Данным стандартом расширяется диапазон работы устройств стандарта IEEE 802.11a.

IEEE 802.11n

На сегодняшний день стандарт IEEE 802.11n — самый перспективный из всех стандартов, касающихся беспроводных сетей. К сожалению, пока он только разрабатывается, но возможности, которые он открывает, выглядят очень заманчиво.

Данный стандарт должен обеспечить скорость передачи данных, минимальным значением которой будет 100 Мбит/с, что фактически равняется наиболее распространенной скоростью в проводных сетях стандарта Ethernet 802.3.

[1] Буква j в стандарте совсем не означает, что это «японский» стандарт. Это обычное алфавитное обозначение очередности стандартов.

IEEE 802.11n будет использовать метод ортогонального частотного мультиплексирования (OFDM) и квадратурную амплитудную модуляцию (QAM). Это должно обеспечить не только высокую скорость передачи данных, но и полную совместимость со стандартами IEEE 802.11a, IEEE 802.11и IEEE 802.11g.

Для увеличения скорости передачи данных планируется использовать несколько новых технологий, одной из которых является технология с множественным вводом/выводом (MIMO — Multiple Input Multiple Output). Ее смысл заключается в параллельной передаче данных по разным каналам с применением нескольких передающих антенн. Кроме того, подразумевается расширение частотного канала до 40 МГц.

IEEE 802.11r

Ни в одном беспроводном стандарте толком не описаны правила роуминга, то есть перехода клиента от одной зоны к другой. Это намереваются сделать в стандарте IEEE 802.11r.

2.4. Преимущества и недостатки беспроводной сети

В любом начинании есть свои преимущества и недостатки, однозначно определяющие выбор той или иной технологии в конкретных условиях. Не обошла эта участь и беспроводные сети.

Преимущества беспроводных сетей

Легкость создания и реструктуризации

Пожалуй, это преимущество беспроводной сети является основным. Оно означает, что для организации работоспособной и достаточно быстрой беспроводной сети достаточно приложить минимум усилий, а самое главное — это потребует минимум затрат. Дело даже не в том, что создавать «обычную» сеть иногда просто лень (бывает и такое), а в том, что, располагая одной или более точками доступа, можно соединить в единую локальную сеть отдельно стоящие здания или компьютеры, находящиеся на большом расстоянии друг от друга.

Кроме того, беспроводную сеть можно быстро, красиво (без кучи проводов) и эффективно создать, когда организовывать проводную сеть накладно: на различных конференциях, выставках, выездных семинарах и т. п. Не стоит также забывать о зданиях, в которых прокладка кабельной системы несовместима с исторической ценностью: это касается музеев, памятников архитектуры и т. п.

Что касается реструктуризации, то здесь дело обстоит совсем просто: добавьте новый компьютер — и готово. Хотите создать подключение Ad-Hoc — пожалуйста, хотите с точкой доступа — опять же...

Мобильность

Лучшие технологии, которые есть в нашем мире, остаются лучшими, только если они могут предложить определенную, желательно очень солидную, универсальность. На сегодняшний день неоспоримым преимуществом является универсальная мобильность, которая позволяет человеку заниматься своим делом в любых условиях, где бы он ни находился. Мобильные телефоны, персональные ассистенты, переносные компьютеры — представители технологии, которая вносит в жизнь человека эту самую мобильность.

С появлением беспроводных сетей и соответствующих компьютерных технологий мобильность приобрела более широкое значение. Теперь она позволяет соединить между собой любые способные на связь устройства, которых так много в современном мире. Обладая мобильным устройством, вы можете спокойно передвигаться по городу и быть уверенным, что всегда останетесь на связи и сможете получить самую последнюю информацию. Рано или поздно пословицу «Если гора не идет к Магомету, Магомет идет к горе» можно будет несколько переиначить: «Если вы не хотите прийти к сети, сеть сама придет к вам».

Возможность подключения к сети другого типа

Преимуществом беспроводной сети является то, что ее всегда можно подключить к проводной. Для этого достаточно воспользоваться совместимым портом[1] на точке доступа или радиомосте. При этом вы получите доступ к ресурсам сети без всяких ограничений.

Именно эта возможность используется при подключении к общей сети удаленных зданий и точек, проложить к которым проводную сеть или невозможно, или слишком дорого.

Высокая скорость доступа в Интернет

Располагая точкой доступа с подключением к Интернету, вы сможете организовать доступ в Интернет для всех компьютеров локальной сети. При этом скорость соединения будет намного выше, чем могут предоставить обычные и даже xDSL-модемы.

Доступ по беспроводной сети — достаточно серьезная альтернатива такому дорогому решению, как оптоволоконный канал. Прокладку такого канала не могут позволить себе даже крупные компании, чего не скажешь о покупке точки доступа или радиокарты, которую может приобрести обычный пользователь. Дело только за суммой, которую вы готовы выложить за предоставленный канал. Канал со скоростью 2 Мбит/с и более уже давно не считается большой роскошью в странах Европы, США или Канады. Такое же настроение постепенно переходит и в СНГ.

---

[1] Как правило, на любой точке доступа находится порт с разъемом RG45, что позволяет подключиться к распространенным проводным сетям стандарта 100 Base-TX или 1000 Base-TX.

Недостатки беспроводных сетей

Низкая скорость передачи данных

Какой бы быстрой ни была сеть, этой скорости всегда не хватает. Особенно остро эта проблема касается беспроводной сети. Дело в том, что реальная скорость передачи данных в такой сети отличается от теоретической в силу многих причин. К таким причинам можно отнести, например, количество преград на пути сигнала, количество подключенных к сети компьютеров, особенности построения пакетов данных (большой объем служебных данных), удаленность компьютеров и многое другое.

Для примера рассмотрим стандарт IEEE 802.11g.

В табл. 2.1 представлены радиусы действия сети при разных условиях использования.

Таблица 2.1. Радиус работы сети при разных условиях использования

Условия использования	Радиус сети, м
Открытая местность, зона прямой видимости	До 300
Открытая местность с препятствиями	До 100
Большой офис	До 40
Жилой дом	До 20

В табл. 2.2 отображено соотношение скорости передачи данных и расстояния, на котором она действует.

Таблица 2.2. Соотношение скорости передачи данных и дальности

Скорость передачи данных, Мбит/с	Радиус сети, м
1	До 100
11	До 40
54	До 14

Безопасность

Безопасность работы в сети, проводной или беспроводной, всегда ставилась превыше всего. Особенно важен этот вопрос для организаций, которые работают с деньгами или другими материальными ценностями.

Безопасность работы в беспроводной сети, по сравнению с ее «подругой», проводной сетью, немного ниже из-за недостаточно серьезных механизмов аутентификации и шифрования. Это доказал первый протокол шифрования — WEP, который

кодировал данные с помощью ключа длиной 40 бит. Оказывается, чтобы вычислить такой самый ключ, достаточно в течение 2–3 часов проанализировать перехваченные пакеты. Конечно, неопытному пользователю такое сделать сложно, но для специалиста это не представляет особой проблемы.

Правда, не все так плохо, как кажется. Как вам известно, со временем стали использоваться другие алгоритмы шифрования, более умные и более «запутанные», которые могут кодировать данные с помощью ключей длиной до 256 бит. Однако при этом возникла ситуация выбора между методом шифрования и скоростью, поскольку увеличение длины ключа приводит к увеличению служебного заголовка, а значит, к заметному снижению скорости передачи данных.

Высокий уровень расхода энергии

Этот негативный фактор в основном касается только пользователей, которые работают в беспроводной сети с помощью переносных компьютеров и других мобильных устройств. Как известно, энергия аккумуляторов, которые питают такие устройства, не является безграничной, и любое «лишнее» устройство приводит к быстрому истощению запаса. Конечно, существуют механизмы, позволяющие сводить потребление энергии к минимуму, но в любом случае энергия расходуется, причем достаточно быстро.

Несовместимость оборудования

Вопросы совместимости всегда интересовали пользователей, поскольку никому не понравится, если его устройство вдруг перестанет работать в связи с заменой оборудования беспроводной сети.

Обычно практикуется следующий подход: оборудование, разработанное раньше, способно работать с оборудованием, разработанным позже. Это называется обратной совместимостью. Что касается оборудования для беспроводных сетей, то этот принцип работает далеко не всегда.

На данный момент активно используется беспроводное оборудование стандартов IEEE 802.11a, IEEE 802.11b и IEEE 802.11g. Кроме того, в последнее время встречается оборудование с «второстепенными» стандартами типа IEEE 802.11b+ и IEEE 802.11g+, работающими в «непонятных» турборежимах и обеспечивающими удвоенную скорость передачи данных по сравнению с аналогичным оборудованием «родных» стандартов.

Ситуация сложилась таким образом, что совместимых устройств в беспроводных сетях практически не существует. Единственное, что облегчает жизнь, это то, что устройства стандарта IEEE 802.11g (или IEEE 802.11g+) имеют обратную совместимость с устройствами стандарта IEEE 802.11b (или IEEE 802.11b+). Найти же устройство поддерживающее все стандарты, практически нереально, хотя и возможно.

Замечу, что для полной совместимости этих стандартов желательно использовать устройства одного производителя.

ГЛАВА 3 Безопасность сети

- Основные понятия
- Протокол безопасности WEP
- Протокол безопасности WPA
- Идентификатор точки доступа и MAC-фильтрация

3.1. Основные понятия

Как уже упоминалось, безопасность работы в сети играет огромную роль. Это связано с тем, что предприятие, на котором организована сеть, может в своей работе использовать документы и данные, предназначенные только для своих сотрудников. Кроме того, вряд ли кому-то понравится, если с его личными документами сможет ознакомиться любой человек. Следовательно, сеть должна располагать определенными средствами безопасности.

На сегодняшний день используются два типа сетей — проводные и беспроводные.

Что касается проводных сетей, то доступ к ним можно получить лишь подключившись к сети физически, то есть с помощью проводного подключения. Это означает, что контролировать подключение достаточно просто.

Беспроводные сети используют радиоволны, которые распространяются по законам физики и принципу действия передающих антенн в зоне радиуса сети. Контролировать поведение радиоволн практически невозможно. Это означает, что любой человек, у которого есть компьютер или переносное устройство с радиоинтерфейсом, может подключиться к сети, находясь в радиусе ее действия. Вычислить местоположение этого пользователя практически невозможно, поскольку он может быть как рядом, так и на значительном удалении от сети (при использовании антенны с усилителем).

Именно тот факт, что подключиться к беспроводной сети может любой, требует от ее организаторов серьезного отношения к обеспечению достаточного уровня безопасности. Для этого следует использовать существующие стандарты.

Чтобы обеспечить минимальный уровень безопасности в беспроводной сети, необходимо использовать следующие механизмы:

- механизм аутентификации рабочей станции — позволяет определить, кто подключается к беспроводной сети и имеет ли он право на такое подключение;
- механизм защиты информации посредством ее шифрования с помощью специальных алгоритмов.

Если хотя бы один из описанных механизмов не используется, то можно сказать, что сеть является абсолютно незащищенной. Это незамедлительно приведет к негативным последствиям. Как минимум, злоумышленник увеличит трафик вашей сети (Интернет, файловые ресурсы), а при наиболее неблагоприятных условиях сможет навредить другой сети, которая подключена к выбранной беспроводной сети.

На сегодняшний день стандартами предусмотрено использование нескольких механизмов безопасности, позволяющих в той или иной мере защитить беспроводную сеть. Обычно такой механизм содержит в себе как средства аутентификации, так и средства шифрования, хотя бывают и исключения.

Однако проблема защиты сети все еще существует, поскольку каким бы строгим ни был стандарт безопасности, далеко не все оборудование поддерживает его. Часто получается так, что, например, точка доступа поддерживает последние алгоритмы безопасности, а сетевой компьютер этот алгоритм не воспринимает. В результате вся сеть работает с тем стандартом, который поддерживают все компьютеры в сети.

3.2. Протокол безопасности WEP

Протокол безопасности *WEP* (Wired Equivalent Privacy, секретность, эквивалентная секретности проводной сети) — первый протокол безопасности, описанный стандартом IEEE 802.11. Для шифрования данных этот протокол использует ключ с разрядностью от 40 до 104 бит. Кроме того, он дополнительно использует шифрование, основанное на алгоритме кодирования RC4, — алгоритм обеспечения целостности данных.

Что касается шифрования для обеспечения целостности данных, то шифрованием его можно назвать с натяжкой, поскольку для этого процесса используется статическая последовательность длиной 32 бита, которая присоединяется к каждому пакету данных, увеличивая при этом его и без того объемную служебную часть.

Отдельно стоит упомянуть о процессе аутентификации, поскольку без него защиту передаваемой информации нельзя считать минимально достаточной. Изначально стандарт IEEE 802.11 описывает два варианта аутентификации: аутентификация для открытых систем с открытым ключом и аутентификация с общим ключом.

Аутентификация с открытым ключом

Фактически этот метод аутентификации не предусматривает никаких средств безопасности соединения и передачи данных. Выглядит это следующим образом. Когда двум компьютерам нужно установить связь, отправитель посылает получателю специально сформированный пакет данных, называемый кадром аутентификации. В свою очередь адресат, получив такой пакет, понимает, что требуется аутентификация с открытыми ключами и в ответ отправляет аналогичный кадр. На самом деле эти кадры аутентификации, естественно, отличаются друг от друга и по сути содержат только информацию об отправителе и получателе информации.

Аутентификация с общим ключом

Данный уровень аутентификации подразумевает использование общего ключа секретности, которым владеют только отправитель и получатель информации. В этом случае процесс аутентификации выглядит следующим образом.

Чтобы начать передачу данных, отправителю необходимо «договориться» с получателем. Для этого он посылает кадр аутентификации, содержащий информацию

о себе и тип ключа шифрования. Получив кадр аутентификации, адресат в ответ посылает пробный текст, зашифрованный с помощью указанного ключа (используется 128-битный ключ алгоритма шифрования WEP). Получив пробный зашифрованный текст, отправитель пытается его декодировать с помощью договоренного ключа шифрования. Если изначальный текст совпадает с результатом расшифровки (используются контрольные суммы зашифрованного и расшифрованного сообщений), то отправитель посылает получателю сообщение об успехе аутентификации. Только после этого данные передаются с использованием указанного ключа шифрования.

Кажется, все выглядит достаточно просто и эффективно. На самом же деле практическое использование метода шифрования WEP показало, что алгоритм кодирования имеет явные прорехи в механизме безопасности, которые нельзя скрыть даже с помощью длинного ключа шифрования. Благодаря сторонним тестировщикам и хакерам оказалось, что, проанализировав достаточно большой объем трафика сети (3–7 млн пакетов), можно вычислить ключ шифрования. В таком случае не спасет даже 104-битный ключ шифрования. Остается только радоваться тому факту, что развитие компьютерных технологий и стандартов не стоит на месте и на смену старым технологиям приходят новые.

Конечно, это совершенно не означает, что протокол безопасности WEP не годится совсем. Для небольших беспроводных сетей, состоящих из нескольких компьютеров, такой защиты вполне достаточно, поскольку трафик сети в этом случае сравнительно небольшой и для его анализа и взлома ключа шифрования нужно потратить значительно больше времени.

Что же касается больших, развернутых беспроводных сетей, то использование в них протокола WEP небезопасно и крайне не рекомендуется. Стоит также учитывать, что в Интернете представлено множество специализированных утилит, которые позволяют взломать защиту WEP-протокола и обеспечить доступ к беспроводной сети. Именно поэтому для обеспечения нужного уровня безопасности лучше использовать более современные протоколы шифрования, в частности протокол безопасности WPA.

Конечно, можно использовать ключи шифрования максимальной длины, но не стоит забывать о том, что это чревато уменьшением скорости передачи данных за счет увеличения их избыточности.

Другим выходом из описанной ситуации можно считать использование направленных антенн передачи сигнала. В некоторых условиях это хороший выход, но в организации домашних беспроводных сетей этот подход не применим.

3.3. Протокол безопасности WPA

Протокол безопасности WPA пришел не смену протоколу безопасности WPE в силу понятных причин, главной из которых является практическая незащищен-

ность WPE. Именно эта незащищенность сдерживала развитие и распространение беспроводных сетей. Однако с выходом протокола WPA все стало на свои места.

Протокол безопасности *WPA* (Wi-Fi Protected Access, защищенный доступ Wi-Fi) был стандартизирован в 2003 году и сразу стал востребован. Главным отличием протокола WPA от WPE стало наличие динамической генерации ключей шифрования, что позволило кодировать каждый отправляемый пакет собственным ключом шифрования. Кроме того, каждое устройство в сети снабжается дополнительным ключом, который меняется через определенный промежуток времени.

Аутентификация происходит с применением протокола аутентификации EAP (Extensible Authentication Protocol, расширяемый протокол аутентификации) с помощью службы (сервера), дистанционной аутентификации RADIUS или предварительно согласованного общего ключа. При этом аутентификация подразумевает вход пользователя после ввода логина и пароля, которые проверяются на сервере аутентификации RADIUS.

Для шифрования данных используется модернизированный алгоритм шифрования RC4, основанный на протоколе краткосрочной целостности ключей TKIP. Это позволяет не только повысить уровень защищенности данных, но и сохранить обратную совместимость с протоколом безопасности WEP.

Шифрование базируется на использовании случайного вектора инициализации IV (Initialization Vector, вектор инициализации) и WEP-ключа, которые складываются и в дальнейшем используются для кодирования пакетов. Результатом такого складывания может стать огромное количество разных ключей, что позволяет добиться практически стопроцентной защиты данных.

Кроме того, протокол безопасности WPA поддерживает усовершенствованный стандарт шифрования AES. Этот стандарт использует защищенный алгоритм кодирования, который намного эффективнее алгоритма RC4. Однако за это приходится платить повышенным трафиком и, соответственно, уменьшением пропускной способности сети.

ПРИМЕЧАНИЕ

Для работы с протоколом безопасности WPA необходимо, чтобы все устройства, подключенные к сети, располагали его поддержкой. В противном случае будет использоваться стандартный протокол безопасности WPE.

3.4. Идентификатор точки доступа и MAC-фильтрация

Каков бы ни был уровень безопасности, его всегда недостаточно. Однако это совсем не означает, что этот уровень должен быть настолько высоким, насколько возможно. Всегда должен быть достигнут компромисс, особенно если учесть, что

каждый дополнительный алгоритм защиты «съедает» у сети часть пропускной способности, что снижает скорость передачи данных в сети.

Обеспечением минимального уровня безопасности можно считать использование идентификатора точки доступа и MAC-фильтрации адресов устройств.

Идентификатор точки доступа

Любая точка доступа, которая участвует в работе беспроводной сети, характеризуется идентификатором расширенного сервисного набора (ESSID – Extended Service Set ID), который представляет собой восьмибитный код. Если в сети присутствует несколько точек доступа, то в целях безопасности всем им присваивается одинаковый идентификатор.

Фактически ESSID — это название вашей беспроводной сети, которое вы можете изменять, используя как буквы, так и цифры. Вы можете изменить это название в любой момент, не забывая при этом сообщить каждому подключенному компьютеру ESSID. Компьютер, который не будет знать ESSID, не сможет подключиться к вашей сети.

Чтобы еще больше усложнить задачу взломщикам сети, можно настроить точку доступа таким образом, чтобы она не транслировала ESSID в эфир.

MAC-фильтрация

«Природным» способом защиты беспроводной сети можно считать фильтрацию по MAC-адресу. Дело в том, что MAC-адрес (Media Access Control, управление доступом к среде) — уникальный идентификатор, который присвоен любому сетевому оборудованию. Этот идентификатор используется с момента появления первых сетевых устройств, и изменить его невозможно. Итак, применяя фильтр по MAC-адресам в точке доступа, вы можете эффективно отсеивать «непрошеных гостей», тем самым дополнительно защищая свою беспроводную сеть.

ГЛАВА 4 Сетевое оборудование

- Адаптер
- Точка доступа
- Мост
- Маршрутизатор
- Антенна

Основу любой сети, естественно, составляет оборудование — активное и пассивное. Именно оно позволяет подключать компьютер к сети, передавать данные, маршрутизировать пакеты в комбинированных сетях и т. д.

К сетевому оборудованию, которое используется в беспроводных сетях, относятся сетевой адаптер, точка доступа, мост, маршрутизатор, принт-сервер и многое другое. Кроме того, сюда же можно отнести антенны, служащие для усиления или узкой направленности сигнала.

4.1. Адаптер

Как уже упоминалось, сетевой адаптер служит для подключения компьютера (или другого устройства) к имеющейся сети. Существует достаточно много видов сетевых адаптеров. Они отличаются друг от друга производителем, техническими особенностями и типом интерфейса. Наибольшее распространение получили адаптеры с интерфейсом PCI и USB производства компаний D-Link, ASUSTek, 3Com SureCom, Trednet и др. Кроме того, часто можно встретить адаптеры с дополнительными устройствами, например flash- или HDD-накопителем.

D-Link Air Xpert DWL-AG650

Сетевой адаптер D-Link Air Xpert DWL-AG650 (рис. 4.1) предназначен для ноутбуков и переносных компьютеров, снабженных соответствующим разъемом (слот 32-bit CardBus).

Рис. 4.1. Сетевой адаптер D-Link Air Xpert DWL-AG650

Особенность данного адаптера в том, что он является универсальным устройством, способным работать в беспроводных сетях стандарта IEEE 802.11a, IEEE 802.11b IEEE 802.11g. Это означает, что, подключив его к ноутбуку, вы можете не беспокоиться о несовместимости каких-либо стандартов.

Данный беспроводной адаптер обеспечивает скорость передачи данных до 54 Мбит/с при использовании стандартов IEEE 802.11a и IEEE 802.11g и 11 Мбит/с в сетях стандарта IEEE 802.11b.

Что касается вопросов безопасности, то такой адаптер поддерживает протокол безопасности WPA с использованием протокола TKIP и аутентификации с помощью сервера RADIUS. Кроме того, обеспечена поддержка более старого протокола безопасности WAP (Wareless Access Protocol, протокол беспроводного доступа).

D-Link DWL-G122

Сетевой адаптер беспроводной связи D-Link DWL-G122 (рис. 4.2) предназначен для работы в компьютерах, снабженных интерфейсом USB.

Рис. 4.2. Адаптер D-Link DWL-G122

Такой адаптер может работать в сетях стандартов IEEE 802.11g и IEEE 802.11b, обеспечивая при этом скорость передачи данных 54 и 11 Мбит/с соответственно. Для подключения устройства используется скоростной порт USB 2.0, который присутствует практически в любом компьютере. Это означает, что, подсоединив устройство к порту, вы сразу же можете начать работать в сети.

В адаптере реализована поддержка протокола безопасности WPA с использованием протокола TKIP и аутентификации с помощью сервера RADIUS. Кроме того, устройство поддерживает более старый протокол безопасности WAP.

В табл. 4.1 приведены некоторые характеристики рассматриваемого устройства.

Таблица 4.1. Технические и другие характеристики сетевого адаптера D-Link DWL-G122

Параметр/характеристика	Значение
Интерфейс	USB 2.0
Поддерживаемые стандарты	IEEE 802.11b, IEEE 802.11g
Диапазон частот	2,4–2,497 ГГц

Продолжение ⇩

Таблица 4.1 *(продолжение)*

Параметр/характеристика	Значение
Скорость передачи данных	54; 48; 36; 24; 18; 12; 11; 9; 6; 5,5; 2 и 1 Мбит/с
Используемые технологии и схемы модуляции сигнала	DSSS, DQPSK, DBPSK, OFDM, CCK
Безопасность	WEP (64/128 бит), WPA
Тип антенны	Встроенная внутренняя антенна
Радиус действия	До 100 м — в помещении, до 400 м — вне помещения
Индикаторы на корпусе	Link, Act

3Com OfficeConnect Wireless 11g (3CRWE154G72)

Сетевой адаптер 3Com OfficeConnect Wireless 11g (3CRWE154G72) (рис. 4.3) предназначен для установки в ноутбуки и переносные компьютеры, снабженные соответствующим разъемом (слот 32-bit CardBus).

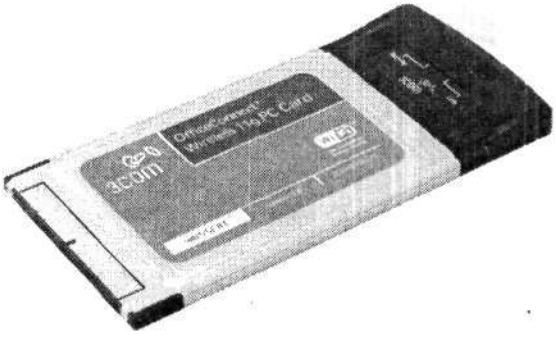

Рис. 4.3. Адаптер 3Com OfficeConnect Wireless 11g (3CRWE154G72)

Данный адаптер рассчитан на работу в небольших офисах или квартирах, обеспечивая при этом устойчивую работу в сетях стандартов IEEE 802.11b и IEEE 802.11g и скорость передачи данных до 11 и 54 Мбит/с соответственно. При этом карта обладает механизмами динамического выбора скорости передачи данных (Dynamic Rate Shifting) в зависимости от трафика и условий окружающей среды.

В адаптере реализована поддержка протокола безопасности WPA с использованием 256-разрядных ключей шифрования и протокола безопасности WAP с использованием 128-разрядных ключей.

3Com 11a/b/g Wireless PCI Adapter (3CRDAG675)

Представленный на рис. 4.4 сетевой адаптер беспроводной связи 3Com 11a/b/g Wireless PCI Adapter (3CRDAG675) предназначен для установки в PCI-слот персонального компьютера.

Рис. 4.4. 3Com 11a/b/g Wireless PCI Adapter (3CRDAG675)

Особенностью этого адаптера является способность работать в сетях стандартов IEEE 802.11a, IEEE 802.11b и IEEE 802.11g, что делает его абсолютно универсальным в применении. При этом при работе в сетях стандарта IEEE 802.11a и IEEE 802.11g достигается скорость передачи данных 54 Мбит/с (108 Мбит/с — в турборежиме).

Данный адаптер снабжен множеством дополнительных средств для безопасности и аутентификации, что делает его одним из самых надежных беспроводных адаптеров на рынке. В частности, он поддерживает протоколы шифрования WPA, AES (128-битный ключ) и WEP(40/64-, 128- и 152-битный ключ), механизмы аутентификации MD5, 802.1x и EAP.

Отдельно можно отметить факт наличия в адаптере механизмов автономной балансировки нагрузки (Autonomous Load Balancing), что позволяет добиться максимальной скорости передачи данных и механизма динамического изменения скорости передачи информации (Dynamic Rate Shifting), позволяющего подобрать скорость соединения в зависимости от текущего трафика в сети и условий окружающей среды.

3Com OfficeConnect Wireless 54Mbps 11g USB Adapter (3CRUSB10075)

Сетевой адаптер беспроводной связи 3Com OfficeConnect Wireless 54Mbps 11g USB Adapter (3CRUSB10075) (рис. 4.5) предназначен для работы в персональных или переносных компьютерах, снабженных интерфейсом USB.

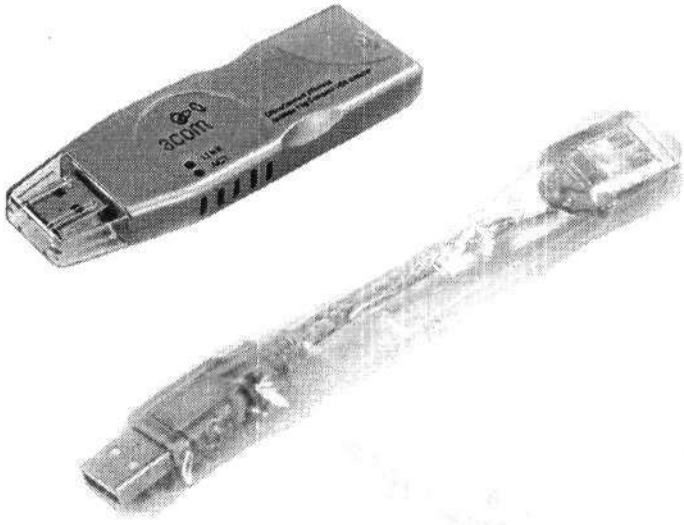

Рис. 4.5. *3Com OfficeConnect Wireless 54Mbps 11g USB Adapter (3CRUSB10075)*

Адаптер рассчитан на работу в беспроводных сетях стандартов IEEE 802.11g и IEEE 802.11b. При этом скорость передачи данных может достигать 54 и 11 Мбит/с соответственно.

В адаптере реализована технология шифрования данных WPA и базовое шифрование WEP с использованием последней версии стандарта аутентификации 802.1x (TKIP, RADIUS).

Благодаря наличию механизма Dynamic Rate Shifting адаптер умеет выбирать скорость передачи данных исходя из загруженности сети и условий окружающей среды.

SureCom EP-9321-g1 54M Wireless LAN PCI Adapter

Сетевой адаптер беспроводной связи SureCom EP-9321-g1 54M Wireless LAN PCI Adapter (рис. 4.6) предназначен для установки в PCI-слот персонального компьютера.

Производитель SureCom зарекомендовал себя как достаточно известный производитель проводного и беспроводного сетевого оборудования. Правда, его популярность заключается в основном в дешевизне оборудования, хотя это и не означает, что качество оборудования страдает.

Данный беспроводной адаптер рассчитан на работу в беспроводных сетях стандартов IEEE 802.11g и IEEE 802.11b, обеспечивая при этом скорость передачи данных 54 и 11 Мбит/с соответственно. Из особенностей адаптера можно отметить *наличие антенны*, которую можно удалять от адаптера на длину ее шнура (1,5–2 м).

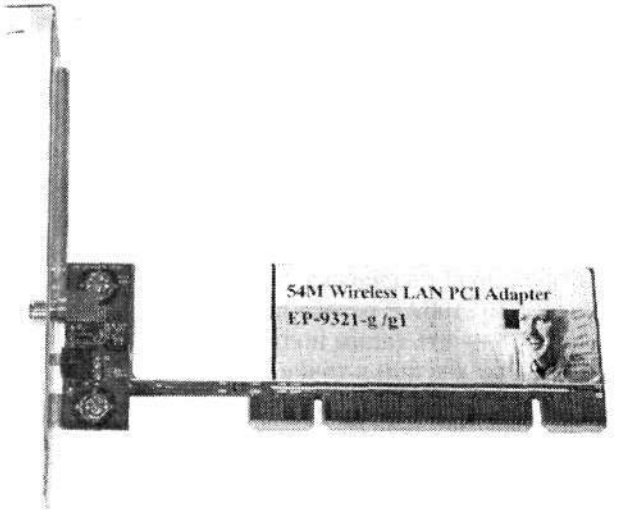

Рис. 4.6. SureCom EP-9321-g1 54M Wireless LAN PCI Adapter

4.2. Точка доступа

D-Link DWL-2100AP

Производитель D-Link достаточно распространен на территории СНГ. Кроме всего прочего, эта компания занимается разработкой оборудования для работы в беспроводных сетях.

Точка доступа D-Link DWL-2100AP (рис. 4.7) — распространенное устройство, сочетающее в себе не только свойства точки доступа, но и беспроводные мост, клиент и повторитель. Данный факт делает это устройство универсальным для организации работы беспроводной сети.

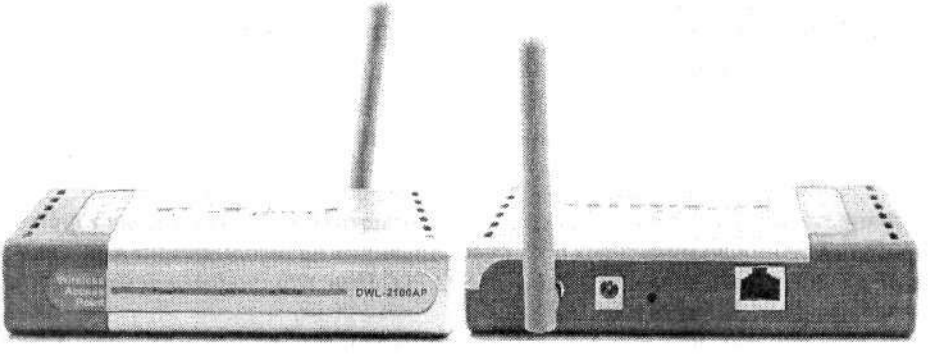

Рис. 4.7. Точка доступа D-Link DWL-2100AP (вид спереди и сзади)

Рассматриваемая точка доступа умеет работать с беспроводными сетями стандартов IEEE 802.11b и IEEE 802.11g, обеспечивая при этом максимальную скорость передачи данных: 54 Мбит/с (108 Мбит/с — в турборежиме). При этом существует возможность подключения сегмента сети стандарта Fast Ethernet 802.3 со скоростью передачи данных 10/100 Мбит/с.

Данное устройство поддерживает протоколы безопасности WPE и WPA. В последнем случае используется протокол целостности временного ключа TKIP. Аутентификация пользователей происходит с помощью сервера RADIUS. Кроме того, если у некоторых клиентов сети отсутствует поддержка аутентификации с помощью сервера RADIUS, то D-Link DWL-2100AP готова предоставить механизм WPA Pre-Shared Key, позволяющий получать таким пользователям временный ключ шифрования каждый раз при подключении к точке доступа.

Следует отметить наличие встроенного механизма DHCP, который позволяет назначать IP-адреса компьютерам, подключенным к беспроводной сети.

В табл. 4.2 приведены некоторые характеристики рассматриваемого устройства.

Таблица 4.2. Технические и другие характеристики точки доступа D-Link DWL-2100AP

Параметр/характеристика	Значение
Поддерживаемые стандарты	IEEE 802.11b, IEEE 802.11g
Диапазон частот	2,4–2,4835 ГГц
Скорость передачи данных	108 Мбит/с (при использовании устройств D-Link DWL-G650: H/W C1, C2 и выше, DWL-G520: H/W A3, B1, B2 и выше); 54; 48; 36; 24; 18; 12; 11; 9; 6; 5,5; 2 и 1 Мбит/с
Используемые технологии и схемы модуляции сигнала	DSSS, DQPSK, DBPSK, BPSK, QPSK, 16QAM, 64QAM, OFDM, CCK
Безопасность	WEP (64/128/152 бит), WPA, TKIP, MIC, IV Expansion, Shared Key, аутентификация 802.1x
Радиус действия	До 100 м — в помещении, до 400 м — вне помещения
Индикаторы на корпусе	Power, LAN (10/100Мбит/с), WLAN

3Com OfficeConnect Wireless 11a/b/g (3CRWE454A72)

Точка доступа 3Com OfficeConnect Wireless 11a/b/g (3CRWE454A72) (рис. 4.8) является продуктом производителя 3Com, который всегда славился своими качественными и функциональными устройствами связи. Такая участь не обошла и эту точку доступа.

Из особенностей данной точки доступа можно отметить то, что она может функционировать в беспроводных сетях всех существующих на сегодняшний день стандартов: IEEE 802.11a, IEEE 802.11b и IEEE 802.11g. При этом достигается скорость передачи данных 54 Мбит/с.
Данное устройство обеспечивает поддержку протоколов безопасности WEP с 40/64- и 128-битными ключами, а также протокола WPA с 256-битным шифрованием.

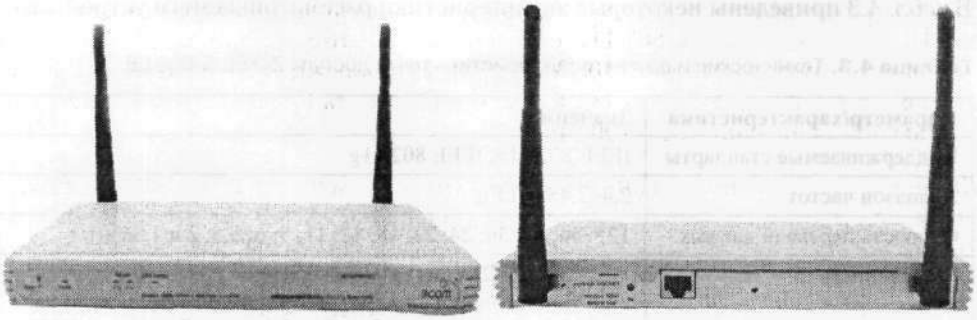

Рис. 4.8. Точка доступа 3Com OfficeConnect Wireless 11a/b/g (3CRWE454A72)

Следует также отметить наличие в данной точке доступа механизма динамического изменения скорости передачи данных и механизма выбора наименее зашумленного канала (Clear Channel Select), с помощью которых можно организовать бесперебойную и надежную беспроводную связь.

ZyXEL G-560 EE

Компания ZyXEL издавна славится качеством своих устройств. В частности, провайдеры и другие компании, готовые выложить деньги за проверенное качество и функциональность, предпочитают устанавливать модемы ZyXEL.

Точка доступа ZyXEL G-560 EE (рис. 4.9) рассчитана на работу в беспроводных сетях стандарта IEEE 802.11b и IEEE 802.11g и обеспечивает высокое качество связи и функциональность. Из особенностей данной точки доступа можно отметить то, что при использовании ее вместе с оборудованием от ZyXEL стандарта IEEE 802.11g+ скорость передачи данных может составить до 125 Мбит/с. Кроме того, наличие механизма динамического изменения скорости передачи данных позволяет устройству всегда оставаться на связи.

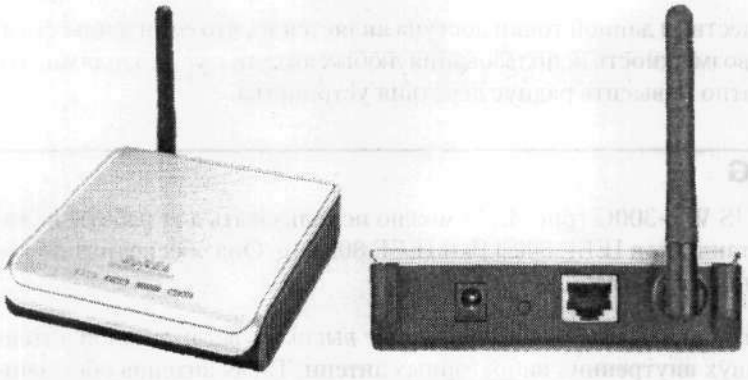

Рис. 4.9. Точка доступа ZyXEL G-560 EE

В табл. 4.3 приведены некоторые характеристики рассматриваемого устройства.

Таблица 4.3. Технические и другие характеристики точки доступа ZyXEL G-560 EE

Параметр/характеристика	Значение
Поддерживаемые стандарты	IEEE 802.11b, IEEE 802.11g
Диапазон частот	2,4–2,4835 ГГц
Скорость передачи данных	125; 54; 48; 36; 24; 22; 18; 12; 11; 9; 6; 5,5; 2 и 1 Мбит/с
Безопасность	WEP (64/128/256 бит), аутентификация 802.1x, WPA; средства упрощенной настройки сетевой безопасности и ключей шифрования (One-Touch Internet Security, OTIST), блокировка трафика между беспроводными клиентами (intra-BSS), фильтрация MAC-адресов, ограничение количества подключенных пользователей, ретрансляция SSL
Тип антенны	Внешняя, не отсоединяемая, дипольная
Радиус действия	До 100 м — в помещении, до 300 м — вне помещения
Встроенная память	SDRAM — 8 Мбайт, Flash-память — 2 Мбайт
Индикаторы на корпусе	PWR, ETHN, WLAN, OTIST

ZyXEL G-560 EE можно рекомендовать как устройство с большим набором функциональных возможностей, максимальным уровнем безопасности и высокой скоростью передачи данных. Наличие встроенной интеллектуальной системы безопасности позволяет очень быстро настроить параметры безопасности устройства, что немаловажно для достаточно крупной беспроводной сети.

TRENDnet TEW-510APB

TRENDnet TEW-510APB — неплохая по функциональным особенностям точка доступа (рис. 4.10), позволяющая работать в беспроводных сетях стандартов IEEE802.11a, IEEE 802.11b и IEEE 802.11g. При этом в режимах IEEE802.11a и IEEE 802.11g может достигаться максимальная скорость передачи данных 108 Мбит/с.

Большим преимуществом данной точки доступа является то, что ее антенны съемные. Это означает возможность использования любых антенн с усилителями, что позволит многократно повысить радиус действия устройства.

ASUS WL-300G

Точку доступа ASUS WL-300G (рис. 4.11) можно использовать для работы в беспроводных сетях стандартов IEEE 802.11b и IEEE 802.11g. Она обеспечивает скорость передачи данных до 54 Мбит/с.

Особенностью этого устройства является наличие высокочувствительной антенны, состоящей из двух внутренних вибраторных антенн. Такая антенна обеспечивает высокое качество связи. Кроме того, существует возможность подключения

Рис. 4.10. Точка доступа TRENDnet TEW-510APB

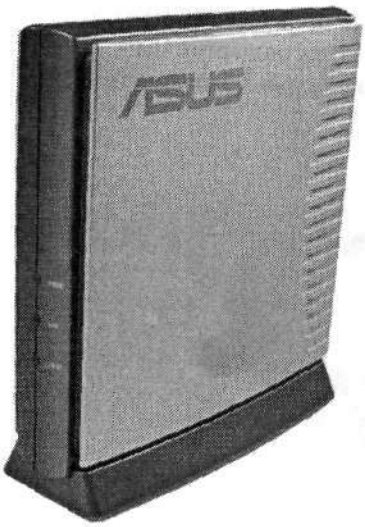

Рис. 4.11. ASUS WL-300G

дополнительной внешней антенны с большим уровнем усиления. Именно поэтому ASUS WL-300G считают самой мощной точкой доступа на рынке беспроводных устройств.

Точку доступа можно также использовать в режиме маршрутизатора. Кроме того, интересной особенностью данного устройства является возможность питания от кабеля Ethernet с помощью функции Power Over LAN.

4.3. Мост

Предназначение *моста* — создание связи между двумя отдельными сетями, чтобы при их соединении получилась комбинированная сеть. Беспроводной мост организует такое соединение с помощью радиоволн.

Из особенностей беспроводного моста можно отметить возможность связи с любой точкой доступа или другим беспроводным мостом, находящимся в радиусе действия сети, а также возможность подключения к беспроводной сети проводных клиентов. Для этих целей на беспроводном мосте устанавливают хотя бы одно гнездо для подключения Ethernet-кабеля. Как правило, это разъем RJ-45, позволяющий подключаться к сетям стандарта Ethernet 802.3 10/100Base-TX и подобным.

Кроме того, беспроводные мосты можно использовать для увеличения радиуса действия сети, поскольку они представляют собой приемопередатчики с достаточно большой мощностью.

3Com 11a/b/g Wireless LAN Workgroup Bridge (3CRWE675075)

Беспроводной мост 3Com 11a/b/g Wireless LAN Workgroup Bridge (3CRWE675075) (рис. 4.12) предназначен для работы в беспроводных сетях стандартов IEEE 802.11a, IEEE 802.11b и IEEE 802.11g. Это позволяет организовать работу подсетей с максимальной скоростью в нужном стандарте.

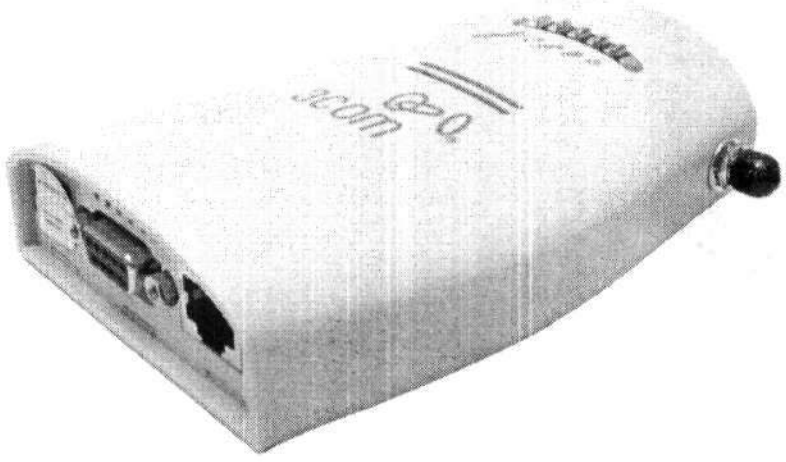

Рис. 4.12. Беспроводной мост 3Com 11a/b/g Wireless LAN Workgroup Bridge (3CRWE675075)

Мост обладает функцией Auto Network Connect (автоматическое подключение к сети), которая позволяет отслеживать перемещение устройства между подсетями и в то же время поддерживать установленную связь.

TRENDnet TEW-413APBO High Power Wireless Outdoor AP Bridge

Беспроводной мост TRENDnet TEW-413APBO High Power Wireless Outdoor AP Bridge (рис. 4.13) предназначен для использования в сетях стандартов IEEE 802.11b и IEEE 802.11g.

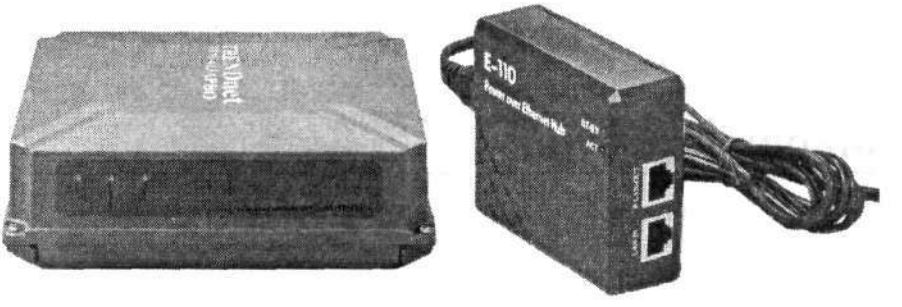

Рис. 4.13. Беспроводной мост TRENDnet TEW-413APBO High Power Wireless Outdoor AP Bridge

Данное устройство может выполнять функции как беспроводного моста, так и точки доступа. При этом очень впечатляет радиус действия этого устройства, достигающий показателя 17 км в режиме беспроводного моста и стандарта IEEE 802.11b.

В табл. 4.4 приведены некоторые характеристики рассматриваемого устройства.

Таблица 4.4. Технические и другие характеристики беспроводного моста TRENDnet TEW-413APBO High Power Wireless Outdoor AP Bridge

Параметр/характеристика	Значение
Поддерживаемые стандарты	IEEE 802.11b, IEEE 802.11g
Диапазон частот	2,4–2,4835 ГГц
Скорость передачи данных	54; 48; 36; 24; 18; 12; 11; 9; 6; 5,5; 2; 1 Мбит/с
Используемые технологии и схемы модуляции сигнала	OFDM, DQPSK, DBPSK,CCK
Безопасность	WEP (64/128 бит), WPA, TKIP, AES, аутентификация 802.11x, возможность запрета рассылок по SSID (Service Set ID, идентификатор сервисного набора), фильтрация по MAC-адресу (40 разрешающих или запрещающих записей)
Мощность передатчика	19 ± 1 дБВт
Чувствительность приемника	54 Мбит/с — 80 дБВт, 11 Мбит/с — 84 дБВт
Радиус действия	Стандарт IEEE 802.11b — до 4 км в режиме точки доступа, до 17 км — в режиме беспроводного моста. Стандарт IEEE 802.11g —до 1 км в режиме точки доступа и до 4 км в режиме беспроводного моста

Продолжение ⇩

Таблица 4.4 *(продолжение)*

Параметр/характеристика	Значение
Порты на корпусе	Порт Ethernet RJ-45 — 10/100 Мбит/с
Антенна	Внешняя, коннектор N-Type
Индикаторы на корпусе	RF Activity (Wireless), LAN, Power

При отсутствии возможности питания от сети переменного тока устройство поддерживает функцию питания от сети Ethernet.

4.4. Маршрутизатор

Данное устройство предназначено для маршрутизации пакетов между сетевыми устройствами, которые могут находиться в разных сегментах сети. Главной особенностью маршрутизации является фильтрация пакетов с отсылкой только тех, которые предназначены данному сегменту сети или конкретному устройству.

Кроме маршрутизации, беспроводной адаптер, как правило, содержит несколько разъемов RJ-45, к которым можно подключать проводные клиенты сети стандарта Ethernet 802.3.

3Com OfficeConnect Wireless 11g Cable/DSL Router (3CRWE554G72)

Представленный на рис. 4.14 маршрутизатор 3Com OfficeConnect Wireless 11g Cable/DSL Router (3CRWE554G72) рассчитан на функционирование в беспроводных сетях стандартов IEEE 802.11b и IEEE 802.11g. Он обеспечивает работу 253 пользователей, из которых 128 подключены к беспроводной сети.

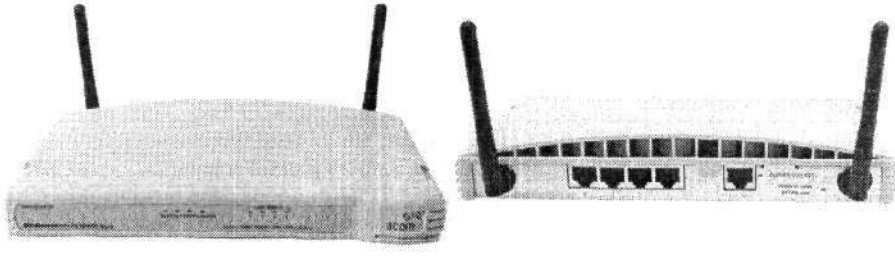

Рис. 4.14. Маршрутизатор 3Com OfficeConnect Wireless 11g Cable/DSL Router (3CRWE554G72)

Данный маршрутизатор позволяет осуществлять статическую маршрутизацию, фильтрацию по URL-адресам[1] или ключевым словам, а также создавать списки

1 При подключении к Интернету маршрутизатор блокирует переходы к нежелательным веб-ресурсам с помощью URL-адресов.

контроля доступа и др. Особенностью этого устройства является наличие механизма управления пакетами Packet bursting (пакетная передача данных), позволяющего повышать скорость передачи путем работы с большим количеством пакетов.

В табл. 4.5 приведены некоторые характеристики рассматриваемого устройства.

Таблица 4.5. Технические и другие характеристики маршрутизатора 3Com OfficeConnect Wireless 11g Cable/DSL Router (3CRWE554G72)

Параметр/характеристика	Значение
Поддерживаемые стандарты	IEEE 802.11b, IEEE 802.11g
Диапазон частот	2,4–2,4835 ГГц
Скорость передачи данных	54; 48; 36; 24; 18; 12; 11; 9; 6; 5,5; 2; 1 Мбит/с
Безопасность	WEP (40/64/128 бит), WPA (256 бит), фильтрация по URL или ключевому слову, списки контроля доступа, запрещение рассылок по SSID, фильтрация по MAC-адресу
Мощность передатчика	17 дБВт
Радиус действия	До 100 м — в помещении, до 457 м — вне помещения
Порты на корпусе	Четыре порта Ethernet RJ-45 — 10/100 Мбит/с, порт WAN — 10/100 Мбит/с
Антенна	Две встроенные внешние антенны
Индикаторы на корпусе	Power, LAN port status link, LAN speed, LAN activity, WLAN port status link, WLAN activity, Alert/diagnostics

Главное предназначение такого маршрутизатора — разделение кабельного или DSL-соединения с Интернетом между подключенными кабельными и беспроводными клиентами. Кроме того, маршрутизатор выполняет функцию измерения интенсивности трафика, позволяющую четко контролировать использование Интернета каждым подключенным пользователем.

ASUS WL-500g Deluxe Wireless 4-in-1 Router

Маршрутизатор ASUS WL-500g Deluxe Wireless 4-in-1 Router (рис. 4.15) разработан для использования в беспроводных сетях стандартов IEEE 802.11b и IEEE 802.11g и обеспечивает скорость передачи данных до 54 Мбит/с.

Этот маршрутизатор обладает двумя USB-портами и рассчитан на подключение Flash-накопителя, веб-камеры, сетевого принтера и звуковых колонок.

В маршрутизаторе реализовано множество функций, позволяющих организовать эффективную работу в сети. В частности, пользователи разделены на четыре группы, каждой из которых присвоен определенный приоритет трафика. Мало того, каждому пользователю можно назначить отдельный приоритет в зависимости от его потребностей. Очень интересной является возможность подключения веб-камеры и колонок, что позволяет передавать как видео, так и звук.

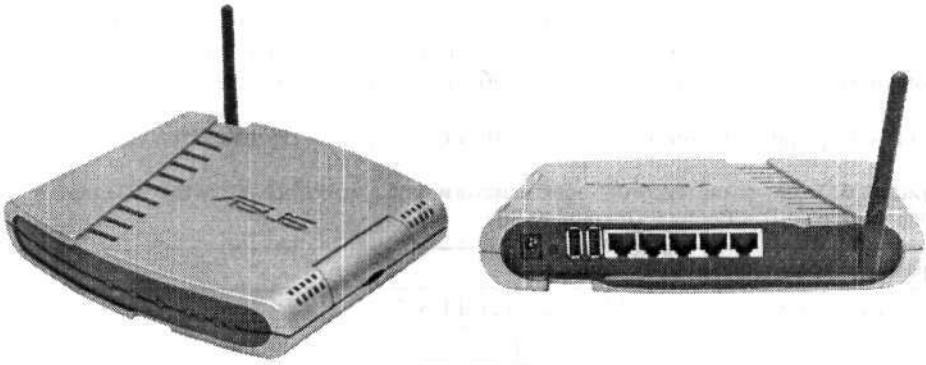

Рис. 4.15. Маршрутизатор ASUS WL-500g Deluxe Wireless 4-in-1 Router

TRENDnet TEW-611BRP MIMO Wireless Router

Маршрутизатор TRENDnet TEW-611BRP MIMO Wireless Router (рис. 4.16) предназначен для работы в беспроводных сетях стандартов IEEE 802.11b и IEEE 802.11g и обеспечивает скорость передачи данных до 108 Мбит/с.

Рис. 4.16. Маршрутизатор TRENDnet TEW-611BRP MIMO Wireless Router

Данный маршрутизатор позволяет более эффективно обрабатывать запросы, особенно при большом трафике в сети. При этом используются приоритеты обработки и автоматический выбор скорости передачи данных.

ZyXEL P-334WT Wireless g+ Broadband Router with Firewall

Маршрутизатор ZyXEL P-334WT Wireless g+ Broadband Router with Firewall (рис. 4.17) рассчитан на работу в беспроводных сетях стандартов IEEE 802.11b и IEEE 802.11g. Он способен обеспечить скорость передачи данных до 125 Мбит/с.

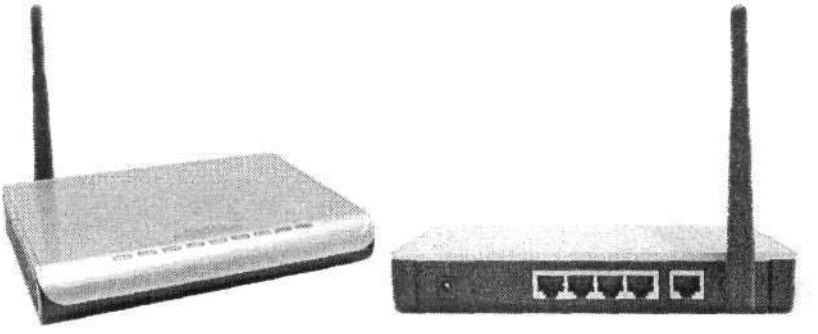

Рис. 4.17. Маршрутизатор ZyXEL P-334WT Wireless g+ Broadband Router with Firewall

Данное устройство обладает неплохими возможностями, которые позволяют сети работать с максимальной скоростью и безопасностью. В частности, в маршрутизатор встроена функция автоматической настройки максимально возможных параметров безопасности (OTIST, One-touch Intelligent Security Technology, интеллектуальная система безопасности «одним нажатием»), запускаемая буквально одним щелчком.

4.5. Антенна

Значение антенны в беспроводной сети трудно переоценить. Известно, что главный бич беспроводной сети — помехи и малый радиус действия. Так вот, используя антенны с усилителями разной мощности, можно добиться уверенного приема сигнала на достаточно больших расстояниях, что играет очень важную роль во многих ситуациях.

D-Link DWL-50AT

Антенна D-Link DWL-50AT (рис. 4.18) является всенаправленной и используется в помещении. Она позволяет расширить площадь покрытия беспроводной сети стандартов IEEE 802.11b и IEEE 802.11g.

Данная антенна используется для подключения к любым беспроводным устройствам, снабженным разъемом Reverse SMA.

ANT24-1201

D-Link ANT24-1201 (рис. 4.19) — достаточно мощная всенаправленная антенна, позволяющая расширить площадь покрытия беспроводной сети стандартов IEEE 802.11b и IEEE 802.11g.

В табл. 4.6 приведены некоторые характеристики рассматриваемого устройства.

Корпус антенны сделан из материала, устойчивого к погодным условиям, что позволяет использовать данное устройство вне помещения. Кроме того, в состав комплекта входят блоки грозозащиты и заземления.

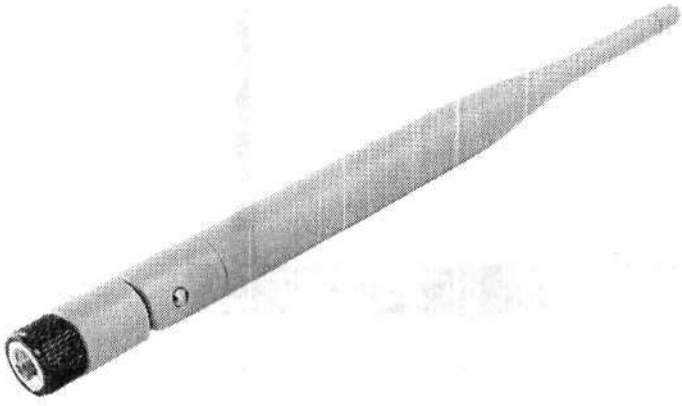

Рис. 4.18. Антенна D-Link DWL-50AT

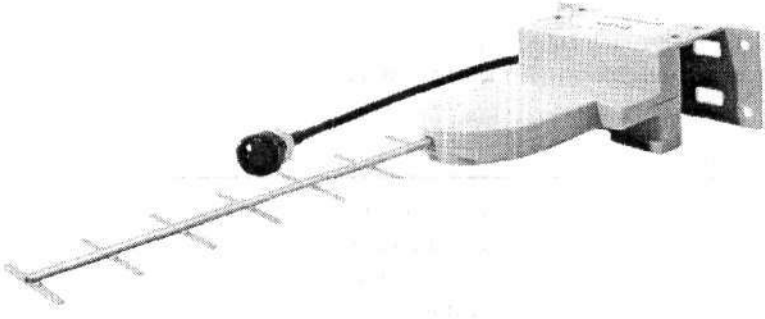

Рис. 4.19. Антенна D-Link ANT24-1201

Таблица 4.6. Технические и другие характеристики антенны D-Link ANT24-1201

Параметр/характеристика	Значение
Поддерживаемые стандарты	IEEE 802.11b, IEEE 802.11g
Диапазон частот	2,4–2,5 ГГц
Разъем	Reverse SMA
Коэффициент усиления	12 дБ
Максимальная мощность	50 Вт
Теоретически возможный радиус сети	При работе с внешними точками доступа: на скорости 1 Мбит/с — 1,5 км, на скорости 11 Мбит/с — 500 м. При работе с внутренними точками доступа: на скорости 1 Мбит/с — 2,5 км, на скорости 11 Мбит/с — 1 км

TRENDnet TEW-IA06D

Антенна TRENDnet TEW-IA06D (рис. 4.20) является направленной и предназначена для установки в помещениях. Она расширяет площадь покрытия беспроводной сети стандартов IEEE 802.11b и IEEE 802.11g.

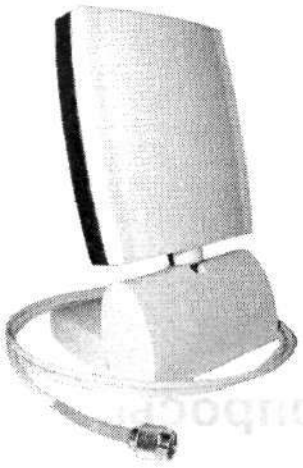

Рис. 4.20. Антенна TRENDnet TEW-IA06D

Эта антенна обладает приятным внешним видом и хорошо вписывается в обстановку офиса.

ZyXEL Ext 106

Микрополосковая антенна ZyXEL Ext 106 (рис. 4.21) является всенаправленной (секторная диаграмма направленности) и предназначена для установки в помещениях. Она позволяет расширить площадь покрытия беспроводной сети стандартов IEEE 802.11b и IEEE 802.11g.

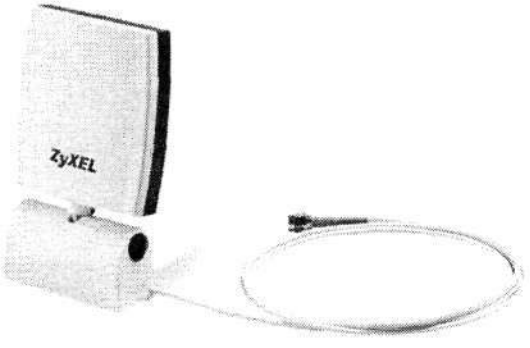

Рис. 4.21. Антенна ZyXEL Ext 106

Антенна имеет достаточно привлекательный вид и похожа на современные плоские акустические системы, недавно появившиеся в продаже.

ГЛАВА 5 Правовые вопросы

При создании в офисе или дома беспроводной сети следует знать, что использование радиодиапазона, в котором работают устройства сети, может создавать помехи в работе других устройств, которые находятся в пределах радиуса сети. Это особенно критично, если ваш офис или дом расположен, например, рядом с больницей, физической лабораторией и т. п.

Ситуацию контролируют специальные органы, которые отвечают за правильное (законное) использование выделенного диапазона частот. Поэтому, если вы хотите быть законопослушными гражданами, обязательно зарегистрируйте установку своего беспроводного оборудования.

За порядком использования радиочастот следит Государственная комиссия по радиочастотам (ГКРЧ). Именно она разрабатывает различные положения о работе с частотами, а также о ввозе, покупке и реализации радиоустройств. До недавнего времени на лицензирование беспроводной сети приходилось тратить много времени, собирая целую кипу различных разрешений. Сейчас, с выходом последнего положения об использовании радиочастот, процесс лицензирования и использования беспроводной сети предельно упростился.

Существует узаконенный порядок оформления беспроводной сети. Соответствующих положений достаточно много, и человеку, неискушенному в правовых вопросах, разобраться в них достаточно трудно. Не так давно вышла упрощенная инструкция, описывающая порядок действий при регистрации и использовании беспроводного оборудования. Приведу это положение.

ПОЛОЖЕНИЕ о порядке использования на территории Российской Федерации внутриофисных систем передачи данных в полосе частот 2400–2483,5 МГц

1. Общие положения

1.1. Настоящее Положение разработано на основании решений ГКРЧ от 25.09.2000 (протокол № 2/7) и от 29.10.2001 (протокол № 13/2) и определяет порядок использования на территории Российской Федерации радиоэлектронных средств (РЭС) внутриофисных систем беспроводной передачи данных, работающих в полосе частот 2400–2483,5 МГц.

1.2. Для организации на территории Российской Федерации внутриофисных систем беспроводной передачи данных, работающих в полосе частот 2400–2483,5 МГц, допускается использование только сертифицированных РЭС с техническими характеристиками, которые соответствуют обобщенным тактико-техническим данным, утвержденных решением ГКРЧ от 29.10.2001 (протокол № 13/2).

1.3. Использование юридическими и физическими лицами полосы частот 2400–2483,5 МГц для организации на территории Российской Федерации внутриофисных

систем беспроводной передачи данных разрешается на вторичной основе при условии непредъявления претензий о возможных помехах от РЭС военного и гражданского назначения, а также от высокочастотных установок промышленного, научного, медицинского и бытового применения, использующих указанную полосу радиочастот.

1.4. Использование (эксплуатация) юридическими и физическими (индивидуальные предприниматели без образования юридического лица) лицами, а также физическими лицами на территории Российской Федерации внутриофисных систем беспроводной передачи данных разрешается только при наличии разрешений на их эксплуатацию, оформленных установленным порядком.

1.5. Действие настоящего Положения не распространяется на радиоэлектронные средства Минобороны России и ФАПСИ, а также на федеральные органы исполнительной власти Российской Федерации (организации), которые находятся на частотном обеспечении Минобороны России и ФАПСИ, при приобретении и использовании (эксплуатации) этими федеральными органами исполнительной власти Российской Федерации (организациями) внутриофисных систем для решения своих целевых задач.

2. Порядок получения разрешений на ввоз радиоэлектронных средств внутриофисных систем беспроводной передачи данных на территорию Российской Федерации

2.1. Ввоз РЭС внутриофисных систем на территорию Российской Федерации юридическими и физическими лицами с целью их дальнейшей реализации (продажи) на внутреннем рынке Российской Федерации и/или использования на территории Российской Федерации, а также для проведения сертификационных испытаний осуществляется по разрешениям ФГУП «Главный радиочастотный центр» без оформления частных решений ГКРЧ для каждого конкретного заявителя.

Ввоз на территорию Российской Федерации типов (моделей) РЭС внутриофисных систем, технические параметры которых не соответствуют обобщенным тактико-техническим данным, утвержденным решением ГКРЧ от 29.10.2001 (протокол № 13/2), осуществляется по разрешениям ФГУП «Главный радиочастотный центр», оформленным на основании отдельных решений ГКРЧ.

2.2. Юридические лица для получения разрешения на ввоз РЭС внутриофисных систем беспроводной передачи данных с целью их сертификации представляют в ФГУП «Главный радиочастотный центр» следующие документы:

- заявку с указанием конкретных типов и количества ввозимых РЭС внутриофисных систем, банковских и почтовых (юридического и фактического адресов) реквизитов;
- копию договора с сертификационным центром (лабораторией) на проведение сертификационных испытаний ввозимого типа РЭС внутриофисных систем.

2.3. Юридические лица для получения разрешения на ввоз РЭС внутриофисных систем беспроводной передачи данных с целью их последующей продажи на внутреннем рынке Российской Федерации представляют в ФГУП «Главный радиочастотный центр» следующие документы:

- заявку с указанием конкретных типов и количества ввозимых РЭС внутриофисных систем, банковских и почтовых (юридического и фактического адресов) реквизитов;
- нотариально заверенные копии свидетельства о государственной регистрации и Устава организации;
- копии сертификатов соответствия на приобретаемые типы РЭС, заверенные установленным порядком (нотариально, органом по сертификации или держателем подлинника сертификата).

2.4. Юридические лица для получения разрешения на ввоз РЭС внутриофисных систем беспроводной передачи данных с целью их последующей эксплуатации на территории Российской Федерации представляют в ФГУП «Главный радиочастотный центр» следующие документы:

- заявку с указанием конкретных типов и количества ввозимых РЭС внутриофисных систем, банковских и почтовых (юридического и фактического адресов) реквизитов;
- нотариально заверенные копии свидетельства о государственной регистрации и Устава организации;
- копии сертификатов соответствия на приобретаемые типы РЭС, заверенные установленным порядком (нотариально, органом по сертификации или держателем подлинника сертификата);
- копии разрешений ФГУП «Главный радиочастотный центр» на использование полосы радиочастот 2400–2483,5 МГц для эксплуатации РЭС внутриофисных систем.

2.5. Физические лица могут осуществлять ввоз на территорию Российской Федерации сертифицированных РЭС внутриофисных систем для использования в личных целях по разрешениям ФГУП «Главный радиочастотный центр».

Физические лица для получения разрешения на ввоз РЭС внутриофисных систем с целью их использования в личных целях представляют в ФГУП «Главный радиочастотный центр» следующие документы:

- заявку с указанием конкретных типов и количества ввозимых РЭС внутриофисных систем;
- копии сертификатов соответствия на приобретаемые типы РЭС, заверенные установленным порядком (нотариально, органом по сертификации или держателем подлинника сертификата);

- копии разрешений ФГУП «Главный радиочастотный центр» на использование полосы радиочастот 2400–2483,5 МГц для эксплуатации РЭС внутриофисных систем;
- нотариально заверенную копию паспортных данных с указанием места постоянной регистрации.

3. Порядок получения разрешений на реализацию (продажу) РЭС внутриофисных систем

3.1. Реализация (продажа) РЭС внутриофисных систем осуществляется юридическими лицами в установленном порядке по разрешениям ФГУП Радиочастотных центров соответствующих федеральных округов, оформляемым по месту юридического адреса лица, осуществляющего их реализацию.

3.2. Юридические лица для получения разрешения на реализацию (продажу) РЭС внутриофисных систем представляют в ФГУП «Радиочастотный центр» соответствующего федерального округа следующие документы:

- заявку с указанием типов реализуемых РЭС внутриофисных систем;
- адреса пунктов продажи (реализации) РЭС;
- нотариально заверенные копии свидетельства о государственной регистрации и Устава организации;
- копии разрешений ФГУП «Главный радиочастотный центр» на ввоз из-за границы РЭС внутриофисных систем;
- копии сертификатов соответствия на реализуемые типы РЭС, заверенные установленным порядком (нотариально, органом по сертификации или держателем подлинника сертификата).

3.3. Юридические лица для продления сроков действия выданных разрешений на реализацию представляют документы, указанные в п. 3.2 настоящего Положения.

3.4. Юридические лица при необходимости внесения изменений в выданные разрешения на реализацию представляют только документы, содержащие сведения о конкретных фактах, вызвавших такие изменения, а также связанные с ними дополнительные документы.

3.5. Реализация (продажа) РЭС внутриофисных систем разрешается только юридическим и физическим лицам, оформившим установленные в разделе 4 настоящего Положения разрешения ФГУП «Главный радиочастотный центр» на использование полосы частот 2400–2483,5 МГц для эксплуатации РЭС внутриофисных систем.

4. Порядок получения разрешений на использование полосы частот 2400–2483,5 МГц для эксплуатации РЭС внутриофисных *систем на территории* Российской Федерации

4.1. Разрешения на использование полосы частот 2400–2483,5 МГц для эксплуатации РЭС внутриофисных систем оформляются ФГУП «Главный радиочастотный центр».

4.2. Юридические и физические лица для получения разрешений на использование полосы частот 2400–2483,5 МГц для эксплуатации РЭС внутриофисных систем предоставляют в ФГУП «Главный радиочастотный центр» заявку по форме 1-БД (приложение № 1 к настоящему Положению).

4.3. ФГУП «Главный радиочастотный центр» в течение 30 дней рассматривает представленные материалы и при отсутствии замечаний по ним направляет в адрес заявителя финансовые документы для оплаты за проведенные работы. После поступления финансовых средств на расчетный счет ФГУП «Главный радиочастотный центр» заявителю выдается разрешение на использование полосы радиочастот 2400–2483,5 МГц для эксплуатации РЭС внутриофисных систем.

4.4. ФГУП «Главный радиочастотный центр» копии указанного разрешения направляет ФГУП «Радиочастотный центр» соответствующего федерального округа, а также в соответствующее государственное учреждение «Управление государственного надзора за связью и информатизацией в Российской Федерации» по месту установки РЭС.

5. Порядок получения разрешений на приобретение РЭС внутриофисных систем на территории Российской Федерации

5.1. Разрешение на приобретение РЭС внутриофисных систем (указанных в приложении к решению ГКРЧ от 29.10.2001 (протокол N 13/2) типов (моделей)) выдается:

- ФГУП «Главный радиочастотный центр» для целей дальнейшей реализации (продажи) на территории Российской Федерации;
- ФГУП «Радиочастотный центр» соответствующего федерального округа для целей их дальнейшей эксплуатации.

5.2. Юридические лица для получения разрешения на приобретение РЭС внутриофисных систем с целью их дальнейшей реализации (продажи) на территории Российской Федерации представляют в ФГУП «Главный радиочастотный центр» следующие документы:

- заявку с указанием конкретных типов и конкретного количества приобретаемых РЭС внутриофисных систем, банковских и почтовых (юридического и фактического адресов) реквизитов;
- копии сертификатов соответствия на приобретаемые типы РЭС, заверенные установленным порядком (нотариально, органом по сертификации или держателем подлинника сертификата);
- нотариально заверенные копии свидетельства о государственной регистрации и Устава организации.

5.3. Юридические и физические лица для получения разрешения на приобретение РЭС внутриофисных систем с целью их дальнейшей эксплуатации представляют

в ФГУП «Радиочастотный центр» соответствующего федерального округа следующие документы:

- заявку с указанием типов РЭС внутриофисных систем;
- копии разрешений ФГУП «Главный радиочастотный центр» на использование полосы частот 2400–2483,5 МГц для эксплуатации.

6. Порядок получения разрешений на эксплуатацию РЭС внутриофисных систем на территории Российской Федерации и их регистрации

6.1. ФГУП «Радиочастотные центры» соответствующих федеральных округов на основании разрешений на использование полосы радиочастот 2400–2483,5 МГц, выданных заявителям по п. 4.3, осуществляют выдачу юридическим и физическим лицам разрешений на эксплуатацию РЭС внутриофисных систем, а также проводят их регистрацию.

6.2. ФГУП «Радиочастотный центр» соответствующего федерального округа в течение десяти дней после выдачи разрешения на эксплуатацию направляет во ФГУП «Главный радиочастотный центр» копию разрешения на эксплуатацию.

7. Контроль над использованием РЭС внутриофисных систем на территории Российской Федерации

7.1. Юридические и физические лица, осуществляющие эксплуатацию РЭС внутриофисных систем, несут ответственность за соблюдение ими установленного настоящим Положением порядка использования РЭС внутриофисных систем.

В случае создания помех действующим «внешним» радиосетям, работающим в полосе радиочастот 2400–2483,5 МГц, юридические или физические лица, эксплуатирующие РЭС внутриофисных систем, должны принять необходимые организационно-технические меры по устранению помех и предоставить в адрес ФГУП «Радиочастотные центры» соответствующих федеральных округов согласованный с оператором действующей «внешней» сети протокол об отсутствии помех. В случае непринятия указанных мер по устранению помех или невозможности устранения помех действующим «внешним» сетям ранее выданные разрешения на использование полосы радиочастот 2400–2483,5 МГц для эксплуатации и разрешение на эксплуатацию РЭС внутриофисных систем аннулируются.

7.2. ФГУП «Главный радиочастотный центр» направляет в в/ч 21882 выданные юридическим и физическим лицам копии разрешений на использование полосы частот 2400–2483,5 МГц для эксплуатации РЭС внутриофисных систем передачи данных.

Приложение № 1

Форма № 1-БД

Заявка на назначение (присвоение) полосы частот 2400–2483,5 МГц для РЭС внутриофисной сети беспроводной передачи данных

Общие сведения

1. Полное наименование юридического, физического лица заявителя _____
_____
2. Почтовый адрес _____
3. Номер телефона, факс _____
4. Регистрационный номер и дата регистрации заявки _____

Тактико-технические данные РЭС

1. Адрес места установки РЭС (почтовый адрес, номер помещений или этажа)
_____
2. Наименование, тип (условный шифр) РЭС _____
3. Фирма-производитель РЭС _____
4. Эквивалентная изотропно излучаемая мощность, мВт _____
5. Тип антенны _____
(интегрированная или специализированная)
6. Номер сертификата соответствия _____
7. Организация, получившая сертификат _____

Тактико-технические данные РЭС внутриофисной сети передачи данных соответствуют обобщенным характеристикам, утвержденных решением ГКРЧ от 29 октября 2001 года (протокол № 13/2).

Подпись: должность, ФИО _____
(Заявка заверяется подписью ответственного лица и печатью)

МП

Примечание

1. Заявка представляется в двух экземплярах.
2. Заявитель несет ответственность за достоверность представляемых данных.

ГЛАВА 6 Что необходимо для построения сети

- Режим Ad-Hoc
- Режим инфраструктуры

В предыдущих главах книги мы рассмотрели практически все теоретические вопросы, касающиеся беспроводных сетей стандарта IEEE 802.11. Пришло время применить полученные знания на практике и научиться строить беспроводные сети разных конфигураций.

В первую очередь необходимо точно представить, что понадобится для создания сети. Как известно, стандартами описаны только два варианта построения сети — инфраструктурный режим и режим Ad-Hoc («точка-точка»). Хотя они и похожи друг на друга, все-таки существуют определенные отличия, которые необходимо учитывать при планировании сети.

6.1. Режим Ad-Hoc

Вариант построения беспроводной сети Ad-Hoc является более простым из двух существующих. Очень часто его используют, когда необходимо быстро соединить небольшое количество компьютеров (от двух до пяти), расположенных недалеко друг от друга, чтобы получить мобильную и быстро модернизируемую сеть. Кроме того, этот вариант незаменим, когда необходимо быстро и с минимальными усилиями передать данные с одного компьютера на другой.

Напомню, что основными недостатками такого варианта построения сети является малый радиус действия и низкая помехозащищенность (см. разд. 2.1).

Рассмотрим условия успешного построения беспроводной сети в режиме Ad-Hoc.

- **Прямая видимость между подключаемыми компьютерами**. При подключении в режиме Ad-Hoc очень важным фактором, влияющим на скорость работы сети, является расположение компьютеров в пределах прямой видимости. Это связано с тем, что мощность передатчиков беспроводных адаптеров несколько ниже, чем, например, мощность точек доступа. Соответственно, радиус действия такой сети примерно вдвое меньше, чем радиус сети, построенной с применением инфраструктурного режима (то есть с использованием точки (точек) доступа).

  Увеличить радиус действия сети Ad-Hoc можно практически единственным способом: применяя более мощные антенны. Однако для этого нужно, чтобы все адаптеры поддерживали сменные антенны.

  Если между компьютерами существуют преграды, например стены офиса, то радиус работы сети резко сократится. Скорость при этом может снизиться до минимальной.

- **Стандарт беспроводных адаптеров**. Как известно, от стандарта, в котором работают сетевые адаптеры, зависит скорость передачи данных в сети. Мало того, если на одном компьютере установлено устройство, стандарт которого поддерживает более низкую скорость передачи данных, то скорость работы всей сети будет равна скорости этого адаптера. Поэтому рекомендуется использовать адаптеры единого стандарта.

  Если выполнить это условие достаточно трудно, то желательно по крайней мере не использовать адаптеры со скоростью передачи данных менее 11 Мбит/с

(стандарт IEEE 802.11b). Наиболее эффективным в таком случае будет применение адаптеров со стандартами IEEE 802.11b+ и IEEE 802.11g, что позволит достичь теоретической скорости передачи данных 22 Мбит/с.

- **Количество подключенных компьютеров**. Количество подключенных компьютеров играет важную роль в успешности работы сети независимо от ее типа (проводная или беспроводная). Это связано в первую очередь с особенностями процесса обмена информацией между компьютерами. Для беспроводных сетей, особенно при использовании режима Ad-Hoc, этот фактор является особенно важным.

  Когда один пользователь хочет передать другому файл, обмен данными с остальными компьютерами очень сильно тормозится, что приводит к определенным задержкам при передаче информации. Представьте, что несколько пользователей одновременно обмениваются файлами или скачивают данные с одного компьютера. В этом случае пропускная способность сети сводится практически к нулю.

  Поэтому при планировании будущей сети не забывайте, что для успешного функционирования сети в режиме Ad-Hoc следует ограничить количество подключений (от двух до пяти). Если это количество превышает рекомендуемое, то более выгодным решением в этой ситуации будет использование точки доступа и режима инфраструктуры.

Для построения беспроводной сети в режиме Ad-Hoc можно использовать любые доступные беспроводные адаптеры. Это могут быть адаптеры USB, PCI, PC Card и др. Выбор устройства зависит от того, какие компьютеры подключены к сети и какой способ подключения беспроводного адаптера им более всего подходит или выгоден.

Если вы хотите, чтобы сеть работала максимально быстро и устойчиво, используйте адаптеры одного производителя, например D-Link, 3Com или других. Это позволит использовать некоторые фирменные возможности, которыми часто обладают адаптеры: например, повышенную скорость передачи данных (108 или 125 Мбит/с). Поэтому, прежде чем покупать оборудование, обязательно ознакомьтесь с отзывами, узнайте его технические характеристики. Проще всего это сделать, посетив веб-сайт производителя. Кроме того, очень полезно почитать отчеты о тестировании выбранных вами устройств разными тестовыми лабораториями.

6.2. Режим инфраструктуры

Создание сети в режиме инфраструктуры подходит в ситуации, когда к сети необходимо подключить достаточно большое количество пользователей. Кроме того, именно этот режим применяют для соединения двух сетей в одну или подключения точки доступа к маршрутизатору.

При использовании точки доступа количество компьютеров в сети может доходить до 253. Конечно, подключать такое количество пользователей не следует, поскольку это может привести к полному упадку сети.

Точка доступа — самое главное устройство в беспроводной сети, и от его расположения зависит очень многое. Не стоит забывать о том, что точка доступа является связующим звеном между компьютерами, которые зачастую располагаются в самых невероятных местах.

Рассмотрим условия успешного создания сети в режиме инфраструктуры.

- **Расположение точки доступа**. Точка доступа снабжена более мощным передатчиком, чем беспроводной адаптер, поэтому она позволяет поддерживать связь на более длинных дистанциях и с большей «силой». Однако это совсем не означает, что ей «по зубам» такие препятствия, как стены, потолки, деревья, дома и т. д. Любое такое препятствие создает помехи для распространения радиоволн и снижает радиус действия сети в несколько раз.

  При размещении точки доступа следует учитывать все препятствия, которые могут располагаться между точкой доступа и подключенными к ней компьютерами.

  Если точка доступа находится внутри офиса или дома, постарайтесь разместить ее между компьютерами приблизительно по центру, чтобы по возможности достичь расположения в зоне прямой видимости максимального количества компьютеров. Это позволит им работать в сети с максимальной скоростью и минимальными помехами.

  Если точка доступа расположена вне помещения, то следует обеспечить прямую видимость между точкой и наиболее удаленными объектами сети.

- **Защита от погодных явлений**. Погодные явления являются критичным фактором, если антенна точки доступа или сама точка доступа находится на открытом воздухе. В таком случае она особенно уязвима. Точку доступа обязательно следует оборудовать механизмом грозозащиты, чтобы предотвратить выход ее «внутренностей» из строя во время грозы, когда в воздухе накапливается много статической энергии, способной попасть через антенну внутрь устройства и повредить электронные схемы.

  Именно поэтому при планировании сети позаботьтесь о том, чтобы все наружные точки доступа или только точки, антенны которых находятся вне здания, были оборудованы таким защитным механизмом.

- **Защита от статического электричества**. Любое электронное устройство, питающееся от сети переменного напряжения, должно быть обязательно заземлено. Если этого не сделать, то оборудование может повредиться или даже полностью выйти из строя. Не доводите свое оборудование до такого состояния!

В следующих подразделах подробнее рассмотрим оборудование, необходимое для создания беспроводной сети в режиме инфраструктуры.

Точка доступа

Точка доступа — обязательное устройство для создания сети в инфраструктурном режиме, поэтому к ее выбору необходимо отнеситесь внимательно.

Существует достаточно много моделей точек доступа. В принципе, вы можете использовать любую, так как каждая точка доступа способна организовать работу беспроводной сети. Однако далеко не все делают это на высоком уровне.

Выбирая это устройство, не поскупитесь и приобретите точку доступа, обладающую некоторыми оригинальными функциями или дополнительными средствами безопасности. Обязательно остановитесь на точке доступа, скорость передачи данных которой будет максимально возможной. Помните: время идет и технологии не стоят на месте. Может случиться так, что вскоре появится новый стандарт, позволяющий передавать данные со скоростью, намного более высокой, чем та, которую поддерживает ваша старая точка доступа. Выбрав точку доступа с максимальным быстродействием, вы обеспечите наибольшую возможную пропускную способность вашей беспроводной сети.

При выборе точки доступа обязательно узнайте, какими дополнительными сетевыми функциями она обладает. Лучшим решением будет выбор точки доступа, способной работать в качестве маршрутизатора или моста. Рано или поздно это вам обязательно пригодится.

Кроме того, желательно, чтобы точка доступа обладала несколькими Ethernet-портами. Это позволит вам подключить к беспроводной сети большее количество проводных пользователей.

Мост

Мост — устройство, которое может пригодиться далеко не всем. Так, для функционирования беспроводной сети, состоящей из десятка компьютеров, мост не нужен. Однако для крупной сети, состоящей из разных топологий и технологий, мост — незаменимая вещь.

Как упоминалось в разд. 4.3, основной задачей беспроводного моста является соединение сегментов проводной и беспроводной сети в единую комбинированную сеть. Поэтому при выборе модели моста ориентируйтесь на радиус действия, поскольку расстояние между этими сегментами может быть достаточно большим. Обязательно проследите, чтобы мост соответствовал максимально возможным протоколам безопасности и шифрования данных.

Маршрутизатор

Маршрутизатор — достаточно бесполезное устройство для небольшой беспроводной сети, но для крупной офисной сети он крайне необходим.

Помимо маршрутизации пакетов между разными сегментами беспроводной сети, это устройство может выполнять различные функции. С его помощью можно продлевать сеть, предоставлять общий доступ в Интернет и многое другое.

Если вы используете маршрутизатор, то на него ложится важная работа и он должен обладать неординарными функциями. Поэтому при выборе маршрутизатора

следует руководствоваться наличием встроенного брандмауэра, списков ограничений и других полезных функций, которые могут пригодиться при работе в Интернете.

Мощность передатчика

Мощность передатчиков сетевых устройств играет большую роль в функционировании сети. Особенно важен этот показатель для сети большого радиуса действия.

Существуют жесткие правила, регламентирующие мощность передатчиков. Использование большей мощности может вызвать сильные помехи радиоустройств находящихся рядом, особенно тех, которые работают в том же диапазоне радиочастот, что и беспроводная сеть.

Если вы все-таки хотите увеличить мощность передатчиков, об этом обязательно должны знать органы контроля за использованием частот. Кроме того, в таком случае следует оформить соответствующие документы.

Беспроводные адаптеры

Беспроводные адаптеры, используемые при подключении компьютеров, могут быть разных производителей и стандартов. Однако только при установке оборудования одного стандарта вы сможете использовать все возможные функции и доступные скорости. Это значит, что, работая, например, хотя бы с одним сетевым адаптером стандарта IEEE 802.11b, вы тем самым ограничиваете скорость сети показателем 11 или 22 Мбит/с, даже если сеть способна функционировать на скорости 108 или 125 Мбит/с.

При выборе адаптеров также старайтесь останавливаться на устройствах одного производителя, что гарантирует их полную совместимость с оборудованием в сети.

Кабель

Когда сеть становится достаточно большой, рано или поздно приходится использовать маршрутизатор или мост. Кроме того, часто необходимо объединить беспроводной сегмент сети с проводным, для чего нужно соединить точку доступа или беспроводной маршрутизатор с имеющимся Ethernet маршрутизатором. В таком случае следует подготовить шнур с разъемом RG-45, поскольку именно этот разъем обычно находится на панели маршрутизатора.

Обычно необходимый кабель поставляется вместе с точкой доступа, однако его длина, как правило, оставляет желать лучшего. Для изготовления кабеля большей длины выполните следующие действия.

1. Приготовьте обжимной инструмент, два коннектора RG-45 и два резиновых колпачка (для закрытия коннекторов после монтажа).
2. Определившись с длиной, аккуратно обрежьте оба конца кабеля резаком специального обжимного инструмента или обычными ножницами. Предварительно

на каждый конец необходимо надеть резиновый колпачок таким образом, чтобы его широкая часть была обращена к концу кабеля.

3. Снимите с концов кабеля кусочек внешней изоляции длиной примерно 12–15 мм. Для этого воспользуйтесь резаком обжимного инструмента или ножом (во втором случае будьте внимательны, чтобы не повредить изоляцию проводников).
4. Сняв внешнюю изоляцию кабеля, вы увидите четыре пары проводников, скрученных попарно. Их необходимо расплести и выровнять, отделив друг от друга.
5. Следующий шаг — взаимное расположение проводников согласно существующему сетевому стандарту. Этого стандарта необходимо придерживаться каждый раз, когда создается кабель RG-45.

   На рис. 6.1 приведен пример расположения проводников согласно стандарту EIA/TIA–568B.

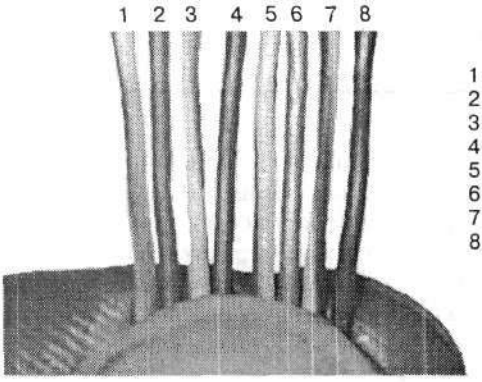

Рис. 6.1. Взаимное расположение проводников по стандарту EIA/TIA–568B

6. Расположив проводники так, как в приведенном примере, убедитесь, что их длина составляет не более 15 мм. При необходимости проводники следует укоротить до нужной длины.
7. Возьмите коннектор двумя пальцами левой руки (если вы правша) и расположите его таким образом, чтобы окошко разъема находилось сверху, а пластмассовая защелка — снизу.
8. Двумя пальцами правой руки сожмите проводники, расположенные, как на рис. 6.1. Далее вставьте проводники в коннектор, для чего медленно введите их концы в окошко разъема. При этом обязательно следите за равномерностью расположения проводников.
9. Плотно вставив проводники в коннектор, еще раз убедитесь в правильности их расположения согласно выбранному стандарту. Затем вставьте коннектор в соответствующее гнездо обжимного инструмента и, сильно сжав инструмент до упора, зафиксируйте проводники в коннекторе.
10. Наденьте на обжатый коннектор резиновый колпачок, чтобы защитить место соединения проводников и коннектора. Кабель готов к использованию.

ГЛАВА 7 Подключение беспроводного оборудования

- Подключение USB-адаптера
- Подключение PCI-адаптера
- Подключение точки доступа

В качестве примера рассмотрим подключение беспроводного USB-адаптера D-Link DWL-G122, беспроводного PCI-адаптера OvisLink WL-8000PCI и точки доступа D-Link DWL-2100AP при создании сети в режиме Ad-Hoc и в режиме инфраструктуры.

Подключение беспроводного устройства ничем не отличается от подключения любого другого устройства, например звуковой или видеокарты, если не считать того что на подсоединение PCI-адаптера приходится тратить больше сил.

7.1. Подключение USB-адаптера

Для подключения беспроводного USB-адаптера можно воспользоваться USB-портом, расположенным на задней или передней панели системного блока (рис. 7.1) Совсем неплохо, если порт поддерживает спецификацию USB 2.0.

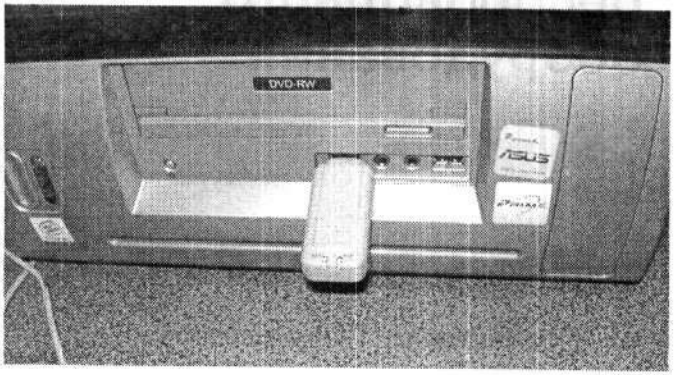

Рис. 7.1. Подключаем USB-адаптер к USB-порту на передней панели корпуса

В случае адаптера D-Link DWL-G122 данное действие облегчается тем, что вместе с устройством в комплект входит удлинительный шнур (рис. 7.2), позволяющий не только легко подключить адаптер, но еще и расположить его в месте, удобном для вас или обеспечивающем наилучшее качество связи.

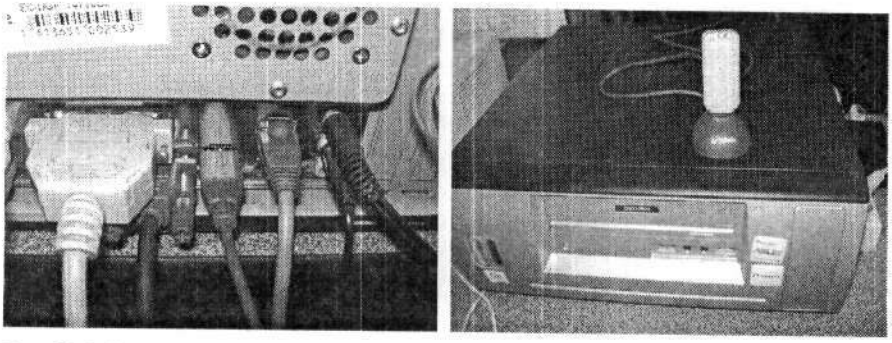

Рис. 7.2. Слева — подключение удлинителя к USB-порту на задней панели системного блока, справа — размещение самого USB-адаптера

Если компьютеры в сети располагаются близко и между ними нет больших преград, то адаптер со спокойным сердцем можно включить в USB-порт, расположенный на задней панели системного блока.

7.2. Подключение PCI-адаптера

Для подключения PCI-устройства выполните следующие действия.

1. Снимите с корпуса крышку.
2. Отыщите свободный PCI-слот и выломайте соответствующую ему заглушку (или выкрутите, если заглушки держатся на шурупах) (рис. 7.3). Предварительно желательно приложить адаптер к выбранному PCI-слоту, чтобы точно выяснить, какую заглушку необходимо убрать.

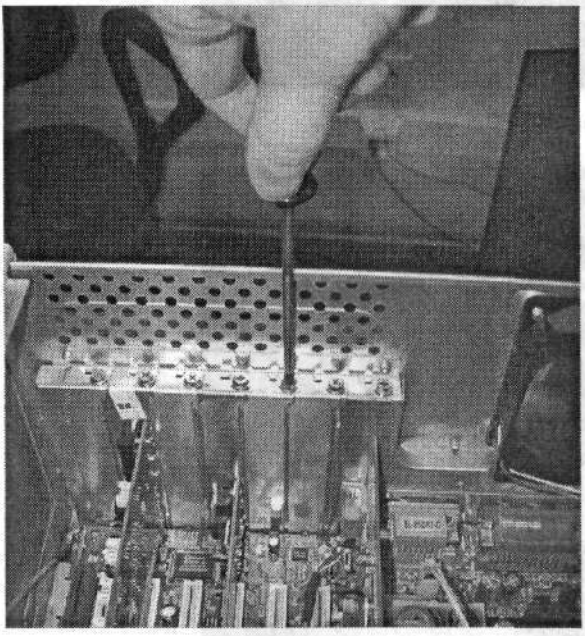

Рис. 7.3. Выкручиваем (выламываем) заглушку

3. Аккуратно вставьте адаптер, следя за тем, чтобы не произошел перекос устройства, который может привести к повреждению слота (рис. 7.4). Предварительно рекомендуется снять антенну, поскольку неосторожное движение может привести к ее поломке.

   Обязательно убедитесь в том, что обе части контактной площадки устройства вставлены до конца, иначе в процессе использования устройства могут происходить непредвиденные сбои или перезагрузка компьютера.
4. Установив адаптер, прикрутите антенну на прежнее место (рис. 7.5).

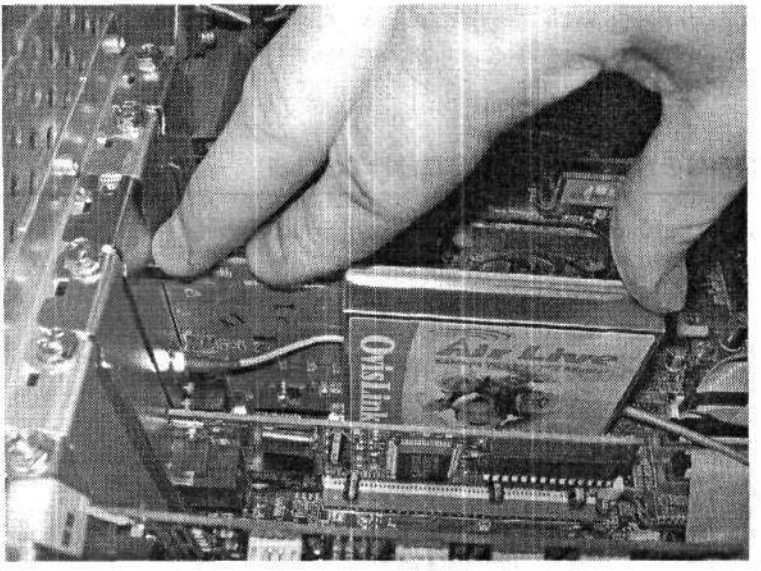

Рис. 7.4. Аккуратно вставляем адаптер в PCI-слот

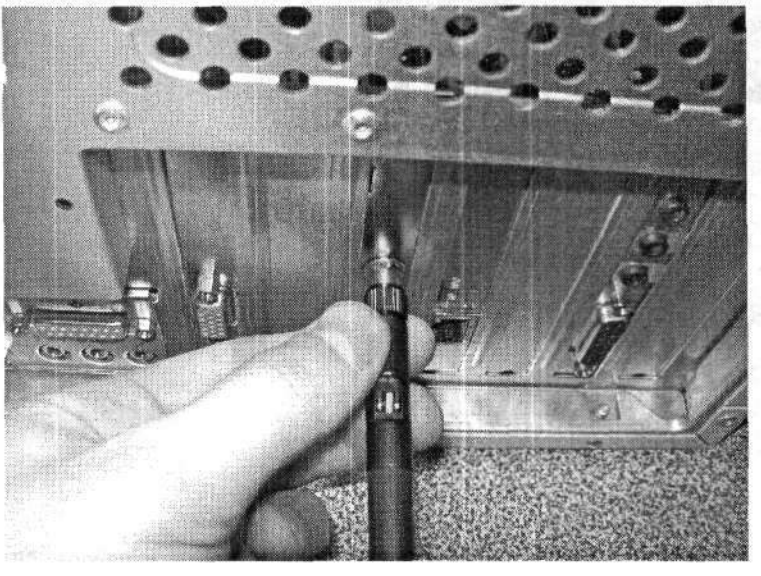

Рис. 7.5. Прикручиваем антенну

7.3. Подключение точки доступа

Подключение точки доступа D-Link DWL-2100AP не вызывает никаких трудностей. Достаточно подключить блок питания и вкрутить антенну, чтобы устройство начало работать (рис. 7.6). При этом точку доступа можно расположить в любом

месте, наилучшим образом подходящем для организации надежной и быстрой связи с компьютерами сети.

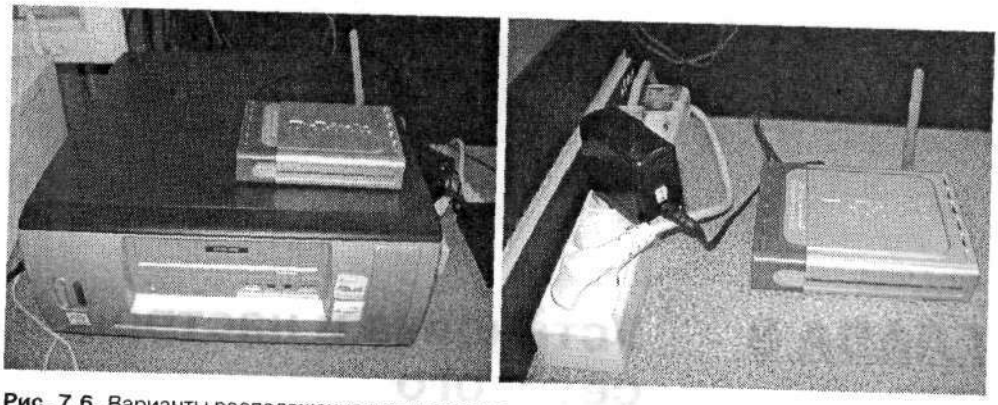

Рис. 7.6. Варианты расположения точки доступа

По умолчанию параметры точки доступа настроены таким образом, что она готова для работы в беспроводной сети. Вы можете в любой момент ознакомиться с этими настройками или изменить их с помощью браузера. Для этого достаточно включить точку доступу и на любом компьютере, подключенном к сети, ввести в адресную строку браузера адрес `http://192.168.0.50`. Однако при изменении параметров точки доступа лучше подключить ее к маршрутизатору или даже к Ethernet-карте компьютера. Это позволит в любой момент получить к ней доступ, даже если установлены такие параметры, при которых точка доступа не работает, а значит, не функционирует и беспроводная сеть.

ГЛАВА 8 Установка и настройка сетевого оборудования

- Установка драйвера для D-Link DWL-G122
- Установка драйвера для OvisLink WL-8000PCI
- Установка программного обеспечения для D-Link DWL-2100 AP

Вместе с адаптерами поставляются драйверы для работы в операционных системах Microsoft Windows 98/Me/2000/XP. Как правило, драйверы находятся на компакт-диске, поэтому для их установки компьютер должен быть оборудован приводом чтения компакт-дисков.

8.1. Установка драйвера для D-Link DWL-G122

USB-адаптер D-Link DWL-G122 — достаточно распространенное устройство, часто приобретаемое пользователями для работы в сети. Легкость подключения и множество настраиваемых функций делают его незаменимым при организации беспроводных сетей разных масштабов.

В комплект поставки также входит компакт-диск, содержащий программное обеспечение, в том числе драйверы для работы устройства в разных системах. На компакт-диске находится программа установки, которая сама определяет тип операционной системы и устанавливает нужные драйверы.

После загрузки компакт-диска в привод на экране появится окно программы установки (рис. 8.1). К сожалению, она имеет только английский интерфейс, но это не должно вызвать затруднений.

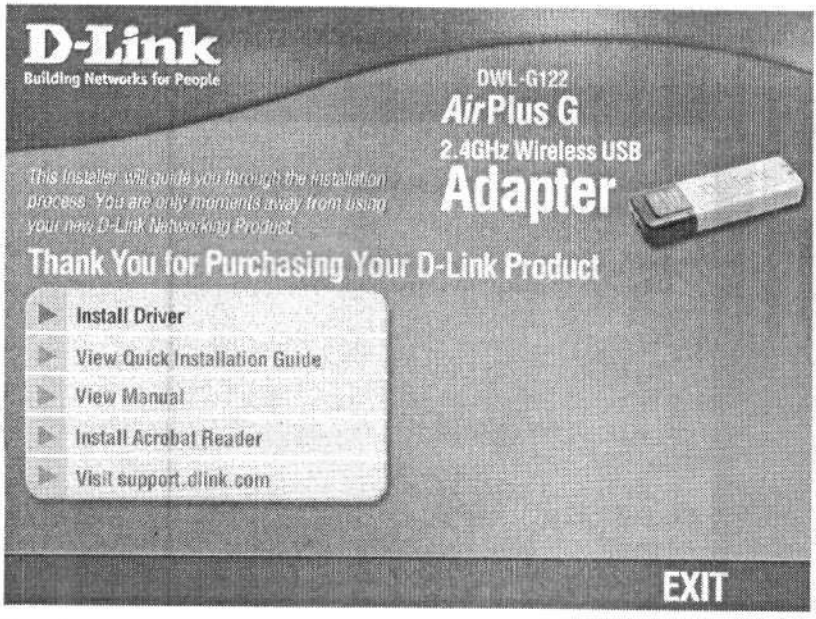

Рис. 8.1. Программа установки

С целью помочь пользователю производители записывают на компакт-диск документацию (на английском языке) с пошаговым описанием процесса установки

драйвера. Чтобы прочесть эту информацию, достаточно выбрать в меню автозапуска пункт View Quick Installation Guide (Просмотреть руководство по быстрой установке) или View Manual (Просмотреть руководство).

ПРИМЕЧАНИЕ

Документация представлена в виде PDF-файлов, поэтому для ее просмотра вам понадобится программа Adobe Acrobat Reader. Если данное приложение у вас не установлено, то его можно инсталлировать, выбрав в меню автозагрузки пункт Install Acrobat Reader (Установить Acrobat Reader).

Существует два пути инсталляции драйвера. Первый — установка вручную с последующим подключением беспроводного адаптера. Второй вариант заключается в подключении адаптера к USB-порту, после чего система сама обнаружит новое устройство, для которого нужно установить драйвер.

Первый путь более простой, поскольку требует минимального участия в процессе установки. Рассмотрим этот вариант.

Чтобы начать процесс установки, выберите в окне, показанном на рис. 8.1, пункт Install Driver (Установить драйвер). Процессом будет управлять мастер установки, который будет подсказывать возможные варианты действий. Сразу после запуска мастера вы увидите окно приветствия с сообщением о начале установки AirPlus G Wireless (рис. 8.2). Для продолжения нажмите кнопку Next (Далее).

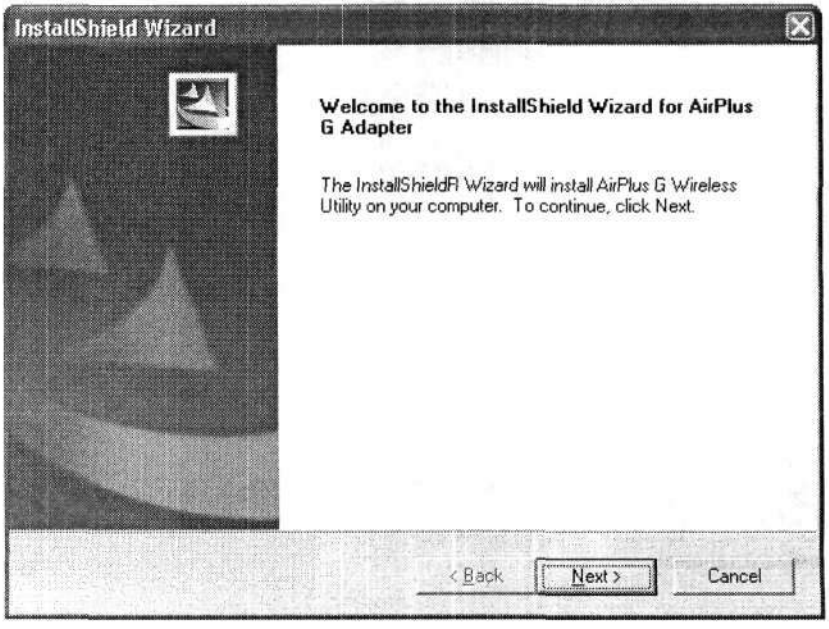

Рис. 8.2. Для начала установки нажимаем кнопку Next (Далее)

После этого на экране появится следующее окно мастера, в котором вам предложат выбрать папку для файлов установки (рис. 8.3). По умолчанию все файлы устанавливаются в каталог Program Files, находящийся на системном диске. Однако если вас не устраивает такой ход событий, то всегда можно указать другое месторасположение, нажав кнопку Browse (Обзор). При ее нажатии появится стандартное системное окно выбора каталога, в котором вы сможете выбрать не только нужный диск, но и папку.

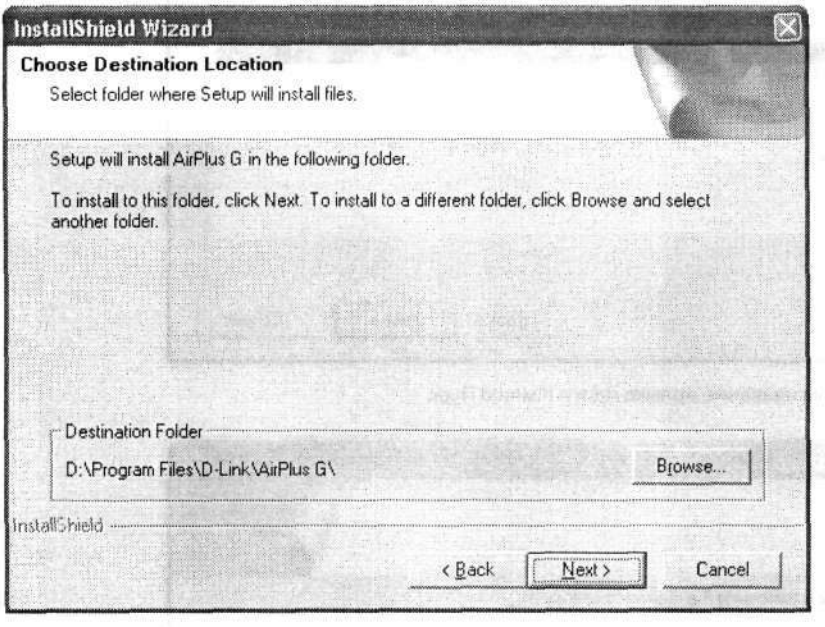

Рис. 8.3. Указываем месторасположение файлов

После выбора папки полный путь к ней автоматически появится в области Destination Folder (Папка назначения).

Для продолжения процесса установки нажмите кнопку Next (Далее).

В следующем окне (рис. 8.4) вам предложат указать название ярлыка папки, создаваемого в меню Пуск. Особого смысла менять название, присвоенное по умолчанию, нет (это, конечно, не относится к любителям следовать пословице «Нормальные герои всегда идут в обход»).

В любом случае для продолжения процесса установки нажмите кнопку Next (Далее). После этого начнется копирование файлов на жесткий диск компьютера (рис. 8.5).

Процесс копирования занимает совсем немного времени, и после его окончания появится последнее окно мастера, в котором вас попросят перезагрузить компьютер, чтобы все изменения вступили в силу (рис. 8.6). Раз просят — лучше перезагрузить,

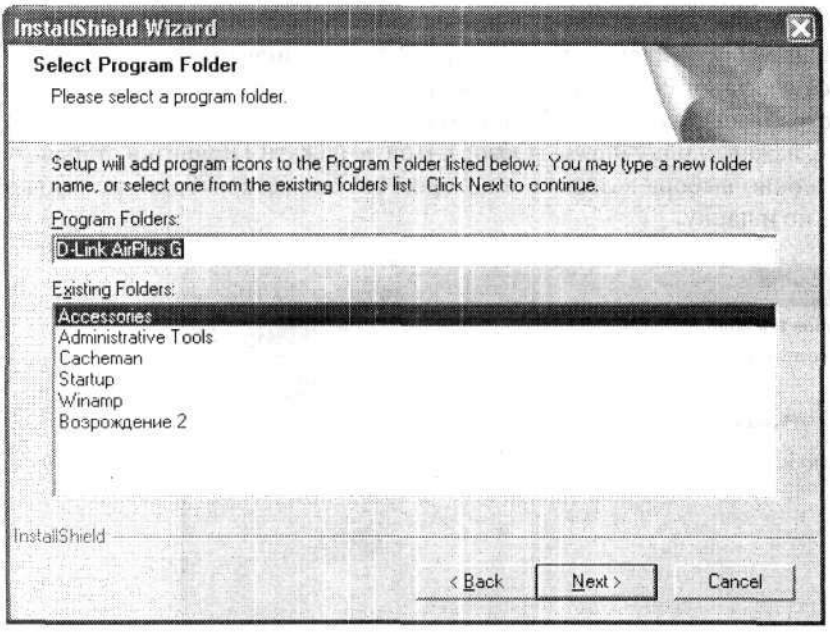

Рис. 8.4. Вводим название ярлыка папки в меню Пуск

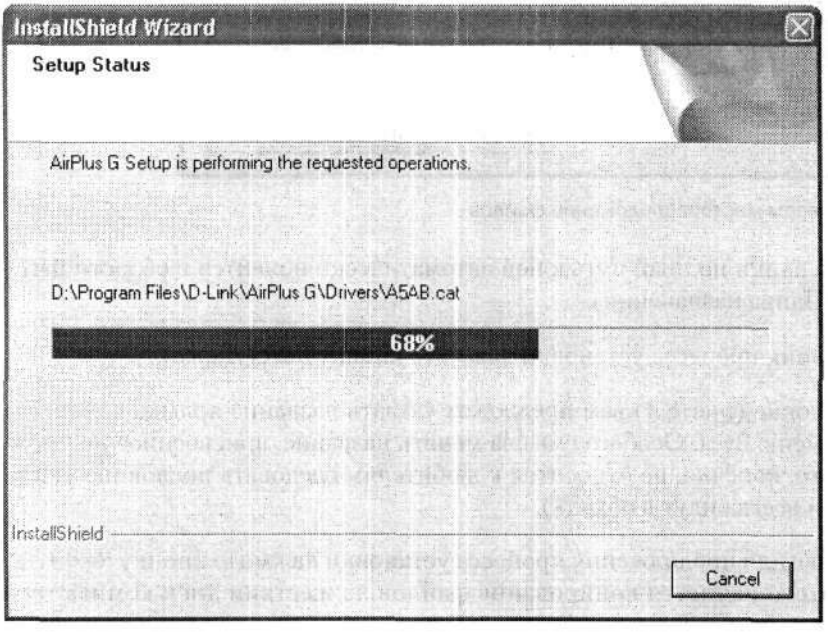

Рис. 8.5. Идет процесс копирования файлов

хотя делать это совсем не обязательно, поскольку после подключения адаптер в любом случае сразу же начнет работать.

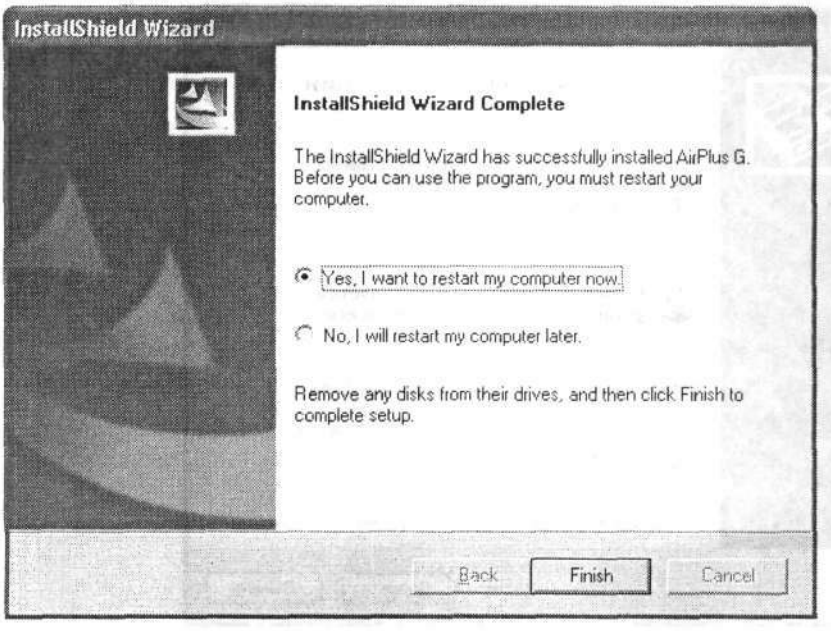

Рис. 8.6. Установка закончена, требуется перезагрузка компьютера

8.2. Установка драйвера для OvisLink WL-8000PCI

После установки сетевого контроллера OvisLink WL-8000PCI в PCI-слот и загрузки операционной системы в области уведомлений появится сообщение о том, что обнаружен новый сетевой контроллер (рис. 8.7).

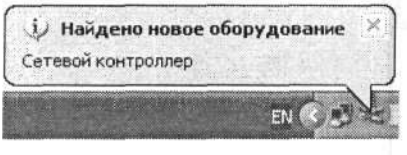

Рис. 8.7. Обнаружен новый сетевой контроллер

Поскольку вы не устанавливали драйверы ранее, то операционная система их не найдет.

Через некоторое время появится окно, в котором вам предложат выбрать вариант установки программного обеспечения. Наиболее подходящей будет автоматическая установка.

Загрузите компакт-диск с программным обеспечением в привод, выберите в окне, изображенном на рис. 8.8, пункт Автоматическая установка (рекомендуется) и нажмите кнопку Далее.

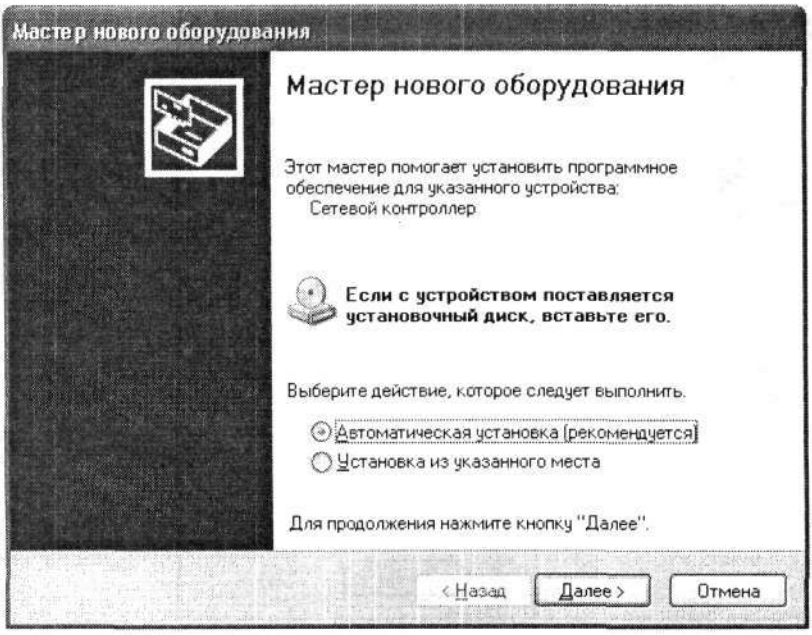

Рис. 8.8. Используем автоматическую установку

После этого мастер установки произведет поиск драйверов на компакт-диске и в случае обнаружения попытается их инсталлировать. Возможно, при этом на экране появится окно с сообщением о том, что устанавливаемое программное обеспечение не тестировалось на совместимость с операционной системой (рис. 8.9). В появлении такого предупреждения нет ничего странного: оно вызвано механизмом защиты операционной системы.

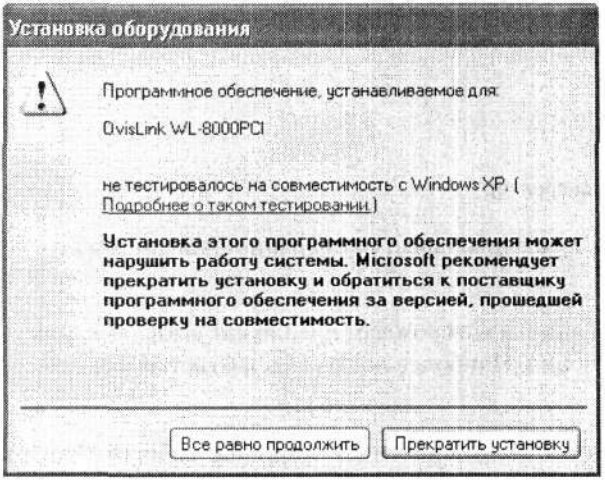

Рис. 8.9. Предупреждение системы

Для продолжения процесса установки нажмите кнопку Все равно продолжить.

После этого мастер установки начнет копировать необходимые файлы, сохраняя их в папку с операционной системой (рис. 8.10).

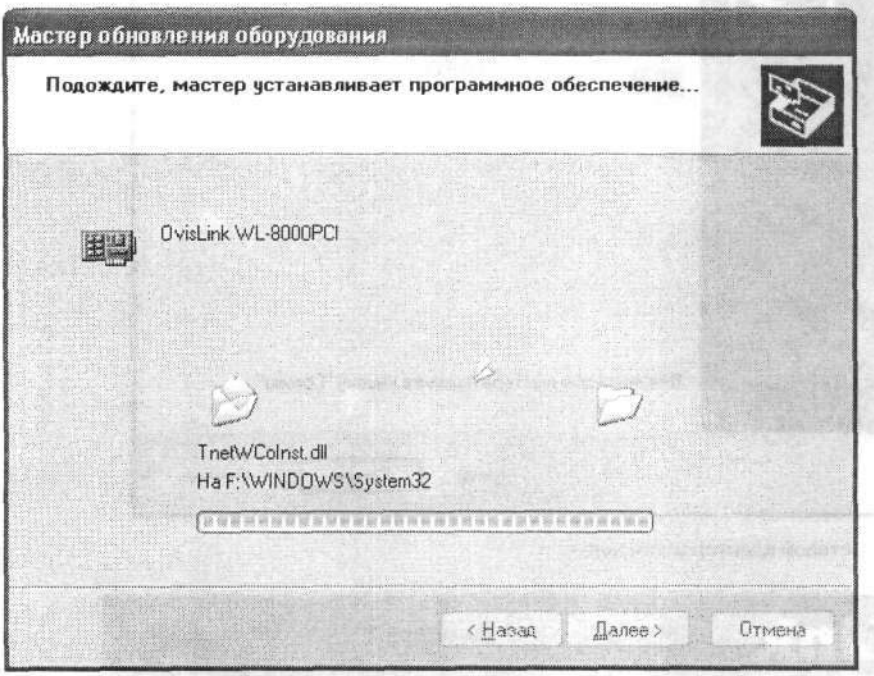

Рис. 8.10. Идет копирование необходимых файлов

Об окончании процесса установки свидетельствует появление финального окна, сообщающего о том, что мастер завершил инсталляцию необходимых программ для сетевого адаптера OvisLink WL-8000PCI (рис. 8.11).

8.3. Установка программного обеспечения для D-Link DWL-2100 AP

Точка доступа является готовым продуктом, который может работать с прописанными по умолчанию заводскими установками. Однако, несмотря на это, следует установить специальное программное обеспечение, с помощью которого можно будет контролировать и изменять параметры ее работы.

На компакт-диске, поставляемом в комплекте с точкой доступа, имеется специальное программное обеспечение для этих целей.

После загрузки компакт-диска в привод на экране появится окно программы установки (рис. 8.12).

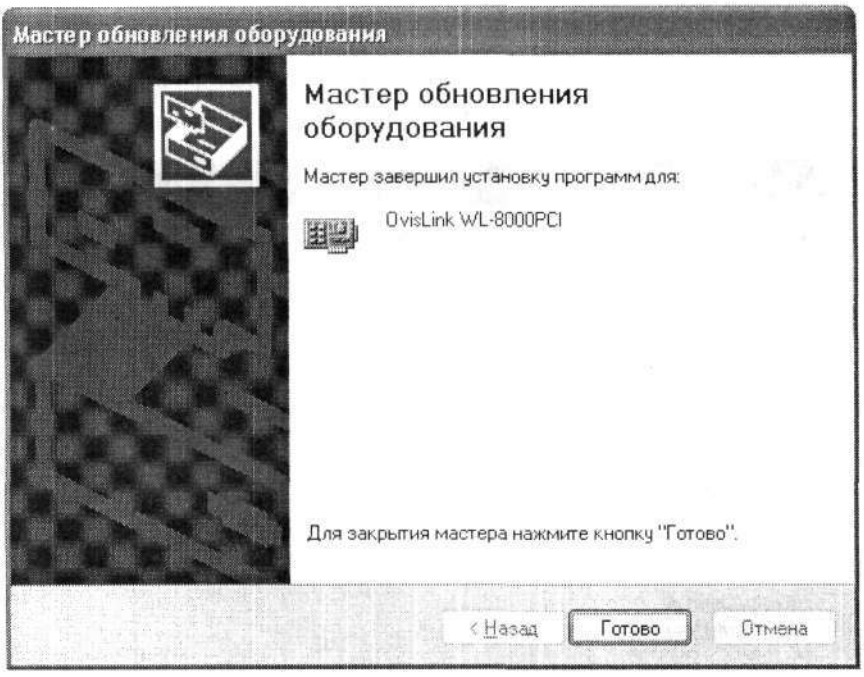

Рис. 8.11. Сетевой адаптер установлен

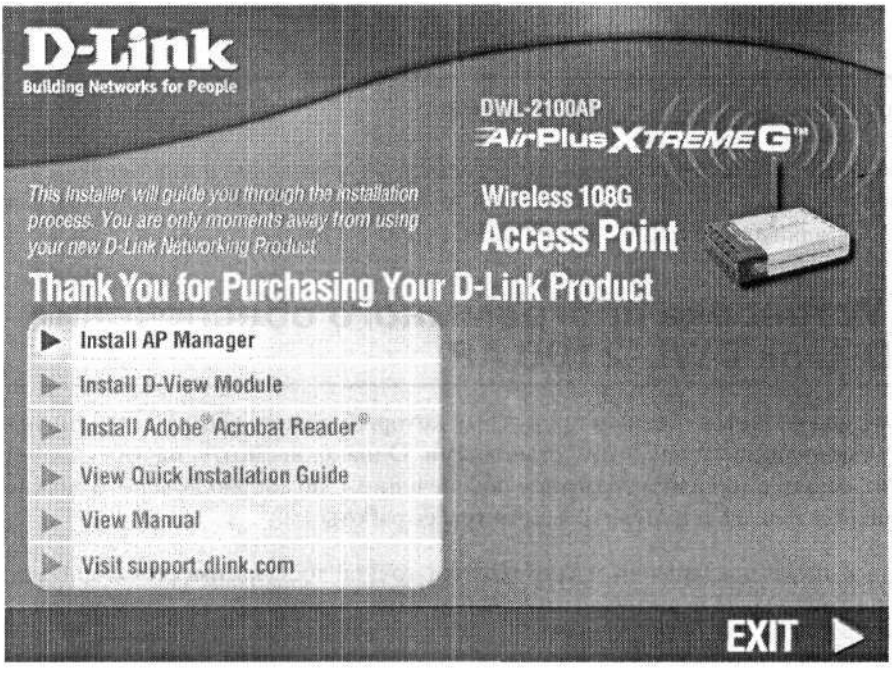

Рис. 8.12. Окно программы установки

Прежде чем начать инсталляцию программного обеспечения, можно ознакомиться с документацией, которая описывает не только процесс установки, но и некоторые характеристики устройства и его требования к системе. Для этого воспользуйтесь пунктами View Quick Installation Guide (Просмотреть руководство по быстрой установке) или View Manual (Просмотреть руководство) меню автозапуска.

Для просмотра документации вам потребуется программа Adobe Acrobat Reader. Дистрибутив шестой версии данной программы вы найдете на компакт-диске с программным обеспечением к точке доступа.

Чтобы начать процесс установки программного обеспечения, выберите в меню автозагрузки пункт Install AP Manager (Установить менеджер ТД). Начнет работу мастер установки программного обеспечения для точки доступа.

В первом окне мастер предупредит вас, что перед установкой необходимо удалить старую версию программного обеспечения (при ее наличии на компьютере) (рис. 8.13).

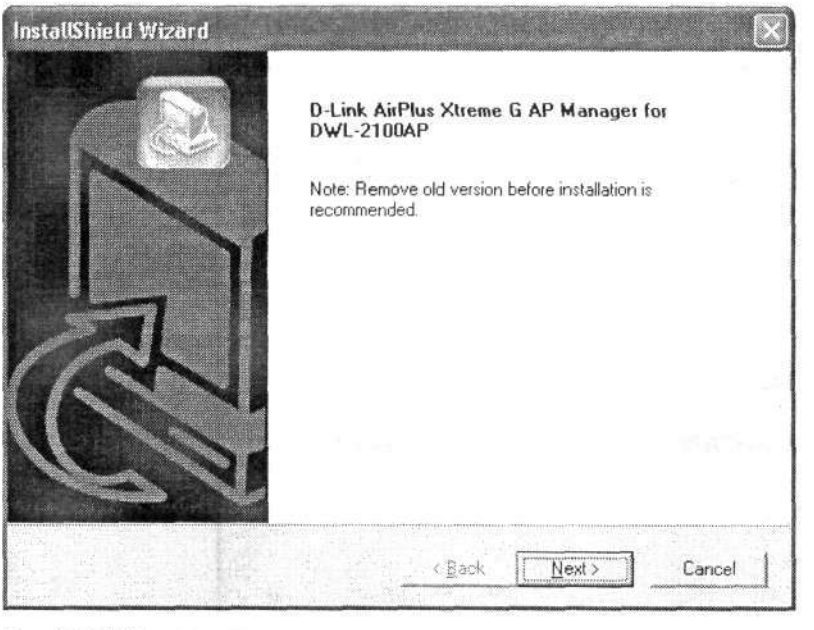

Рис. 8.13. Окно приветствия мастера

Для продолжения нажмите кнопку Next (Далее). В следующем окне вам предложат изменить папку, в которую следует устанавливать необходимые файлы (рис. 8.14). Если вас устраивает папка, заданная по умолчанию (Program Files), то просто нажмите кнопку Next (Далее).

В следующем окне мастер предложит ввести название ярлыка программной группы в меню Пуск (рис. 8.15). Если вас не устраивает название, заданное по умолчанию, можете ввести любое другое.

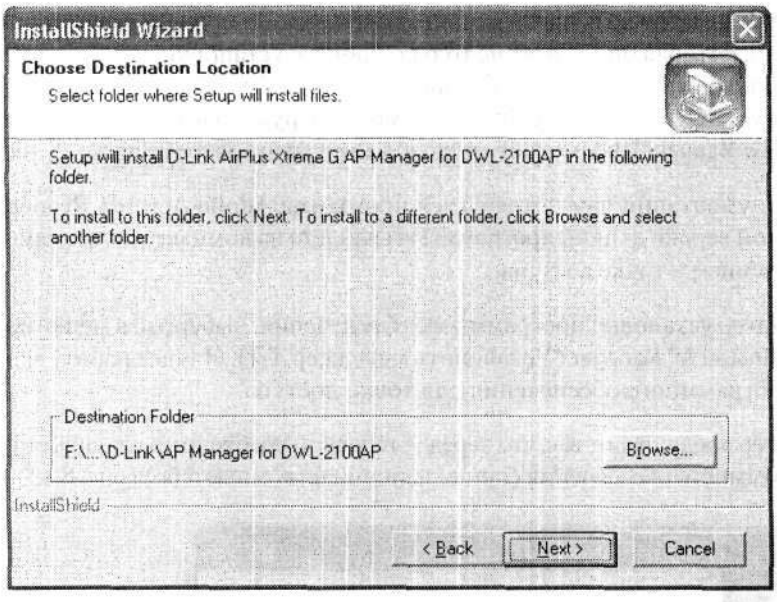

Рис. 8.14. Указываем папку, в которую будут устанавливаться нужные файлы

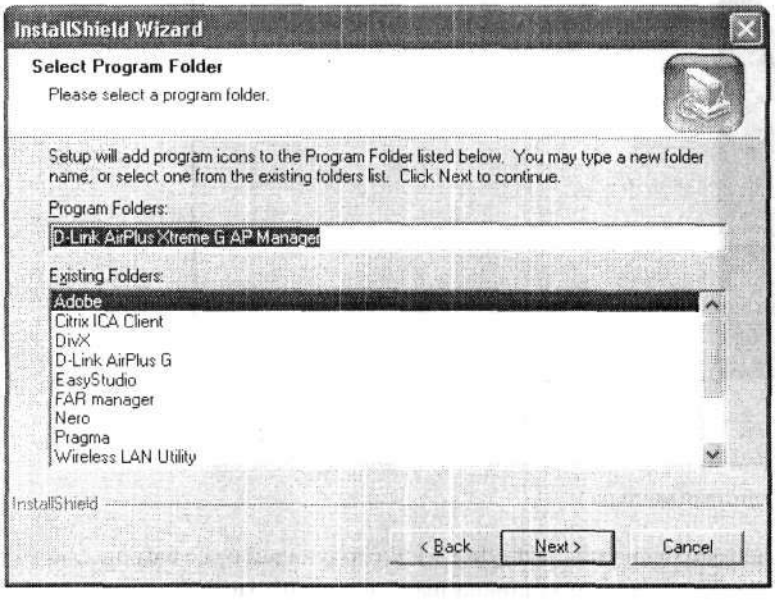

Рис. 8.15. Указываем название ярлыка в меню Пуск

Для продолжения процесса установки нажмите кнопку Next (Далее).

Только после этого начнется непосредственно процесс установки, который, по сути, заключается в копировании нужных файлов в указанный каталог (рис. 8.16).

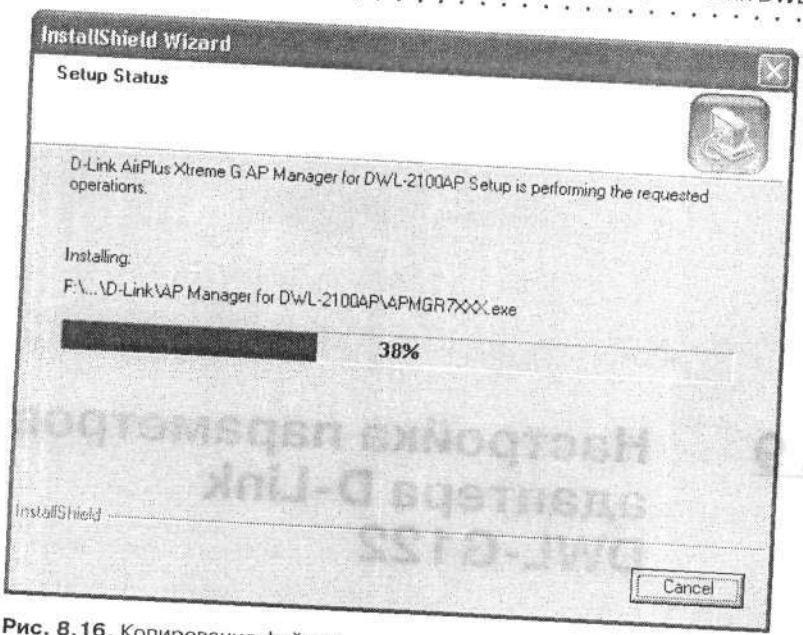

Рис. 8.16. Копирование файлов

Процесс установки заканчивается появлением окна, в котором сообщается, что программное обеспечение для точки доступа установлено (рис. 8.17).

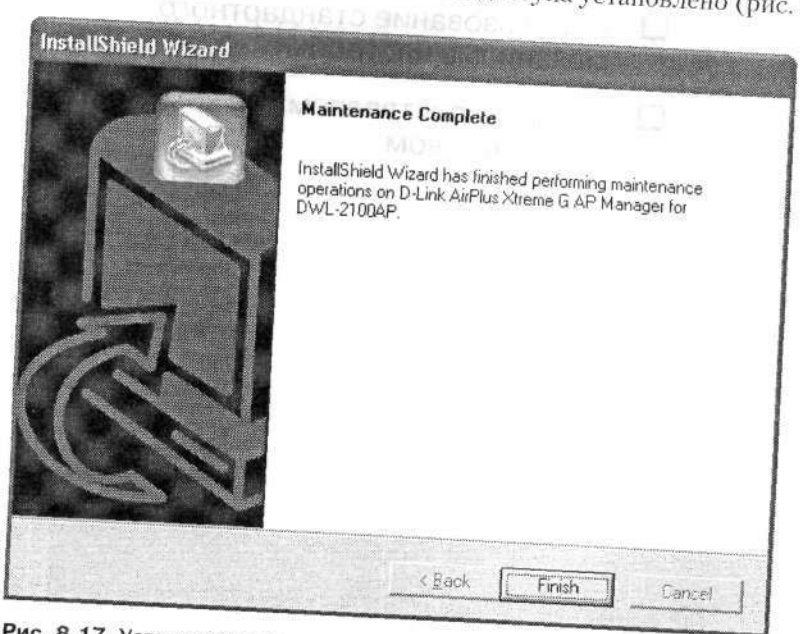

Рис. 8.17. Установка программного обеспечения завершена

После нажатия кнопки Finish (Готово) точка доступа готова к работе.

ГЛАВА 9 Настройка параметров адаптера D-Link DWL-G122

- ❑ Использование стандартного механизма настройки
- ❑ Утилита, поставляемая в комплекте с устройством

В комплект поставки беспроводных устройств, как правило, входят утилиты для управления их работой. Установив драйверы для адаптеров, можно воспользоваться соответствующими утилитами, чтобы настроить режимы их работы. В частности, вы можете настроить режим сети, уровень безопасности, прописать SSID, указать протокол безопасности и многое другое.

Данные параметры необходимо задать независимо от того, в каком режиме будет работать сеть. В любом случае нужно назначить одинаковый SSID всем устройствам и обязательно настроить нормальный уровень безопасности сети.

Рассмотрим параметры беспроводного USB-адаптера D-Link DWL-G122, которые вы можете при необходимости настроить на свое усмотрение.

После установки драйвера для беспроводного адаптера D-Link DWL-G122 в области уведомлений появится значок в виде буквы D.

В дальнейшем параметры адаптера можно будет настраивать, щелкнув правой кнопкой мыши на данном значке и выбрав в появившемся меню пункт Wireless Network (Беспроводная сеть), как показано на рис. 9.1, или просто дважды щелкнув на значке.

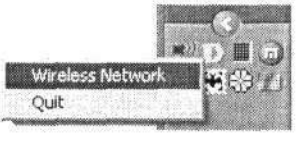

Рис. 9.1. Выбор пункта Wireless Network (Беспроводная сеть) для настройки адаптера

По умолчанию, даже если запустить родную утилиту конфигурирования адаптера, запустится стандартный мастер конфигурирования Windows. Вы можете воспользоваться им, однако «родная» утилита позволяет настраивать намного больше параметров, чем стандартный мастер настройки оборудования Windows.

Рассмотрим примеры использования обоих вариантов настройки и способы переключения между ними.

9.1. Использование стандартного механизма настройки

По умолчанию Windows предлагает настроить адаптер с помощью стандартных механизмов. Чтобы изменить это, необходимо самостоятельно указать вариант настройки беспроводного соединения. Как это сделать, рассказано в следующем разделе.

Чтобы запустить стандартный механизм настройки, дважды щелкните на значке в виде буквы D в области уведомлений. Замечу, что если вы зададите по умолчанию настройку с помощью «родной» утилиты, то для запуска стандартного мастера нужно будет открыть окно Сетевые подключения. Для этого выполните команду

Пуск ▸ Сетевое окружение и в появившемся окне в области Сетевые задачи щелкните на ссылке Отобразить сетевые подключения. Щелкните правой кнопкой мыши на значке нужного беспроводного соединения и выберите в контекстном меню пункт Свойства

На экране появится окно свойств беспроводного соединения (рис. 9.2), в котором настраивают его параметры. Здесь же можно настроить параметры самого адаптера.

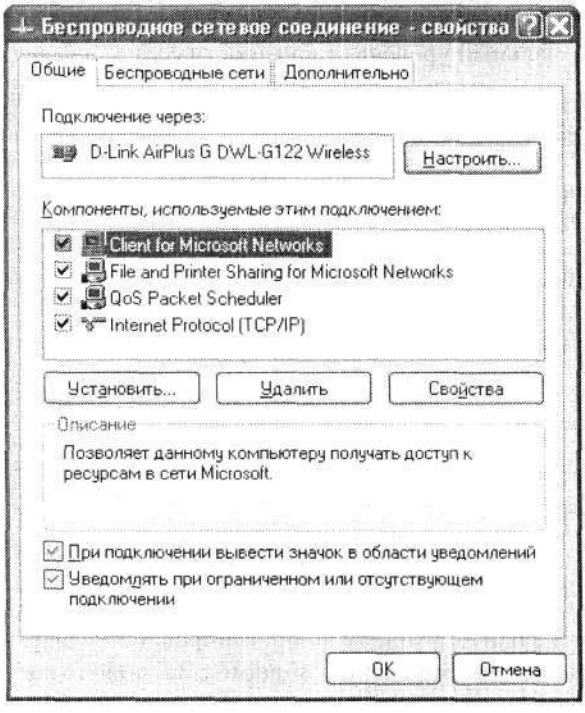

Рис. 9.2. Окно свойств беспроводного соединения

Чтобы изменить настройки адаптера, нажмите кнопку Настроить. При этом откроется окно свойств беспроводного адаптера, содержащее несколько вкладок с параметрами и другой полезной информацией.

Перейдите на вкладку Дополнительно этого окна. Именно здесь можно настроить параметры, влияющие на работу устройства в сети (рис. 9.3).

Чаще всего на данной вкладке настраивают следующие параметры.

- Network Type — режим, в котором функционирует сеть. Доступны два значения этого параметра: 802.11 Ad Hoc (режим Ad-Hoc) и Infrastructure (режим инфраструктуры).
- SSID — уникальный идентификатор сети, используемый для создания определенной группы компьютеров, способных работать вместе. В качестве SSID может выступать любое словосочетание или набор цифр и букв. Главное, чтобы

вы смогли впоследствии повторить это сочетание при настройке другого беспроводного адаптера, точки доступа, маршрутизатора и остального оборудования, рассчитанного на работу в данной группе.

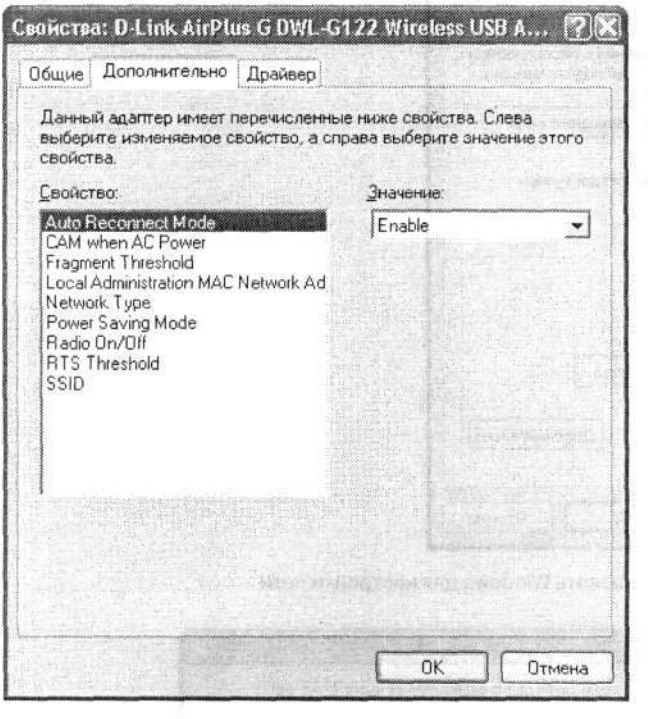

Рис. 9.3. Содержимое вкладки Дополнительно

9.2. Утилита, поставляемая в комплекте с устройством

Чтобы использовать для настройки беспроводного адаптера его «родную» утилиту, необходимо произвести некоторые дополнительные изменения.

В окне свойств беспроводного соединения (см. рис. 9.2) перейдите на вкладку Беспроводные сети и снимите флажок Использовать Windows для настройки сети (рис. 9.4).

После этого для конфигурирования беспроводного адаптера будет использоваться утилита, поставляемая вместе с ним. Чтобы убедиться в этом, дважды щелкните на значке D в области уведомлений на Панели задач.

В результате появится окно программы настройки, содержащее пять вкладок. По умолчанию открыта вкладка Link Info (Сведения о соединении), содержащая информацию о соединении: режим сети, используемый беспроводной стандарт, скорость соединения, SSID и др. (рис. 9.5).

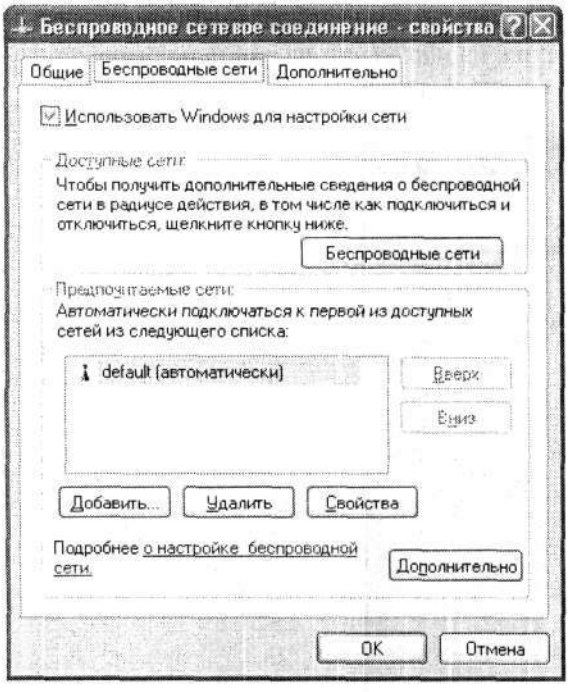

Рис. 9.4. Снимаем флажок Использовать Windows для настройки сети

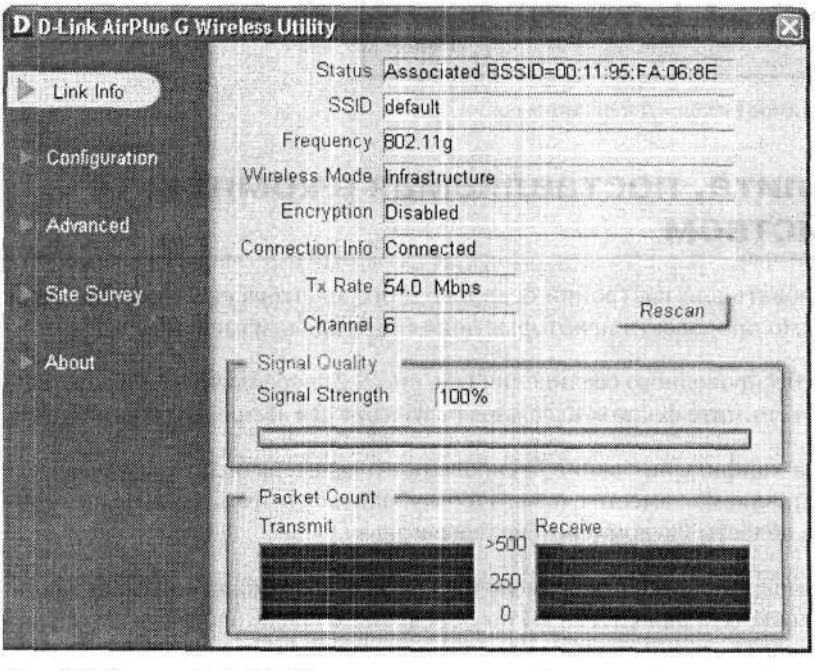

Рис. 9.5. Вкладка Link Info (Сведения о соединении) окна программы конфигурирования

Параметрами работы устройства управляют на вкладках Configuration (Конфигурация) и Advanced (Расширенные настройки). Кроме того, настраивать параметры подключения ко всем найденным точкам доступа можно на вкладке Site Survey (Обзор узлов). Рассмотрим эти вкладки более подробно.

Вкладка Configuration (Конфигурация) содержит следующие параметры (рис. 9.6).

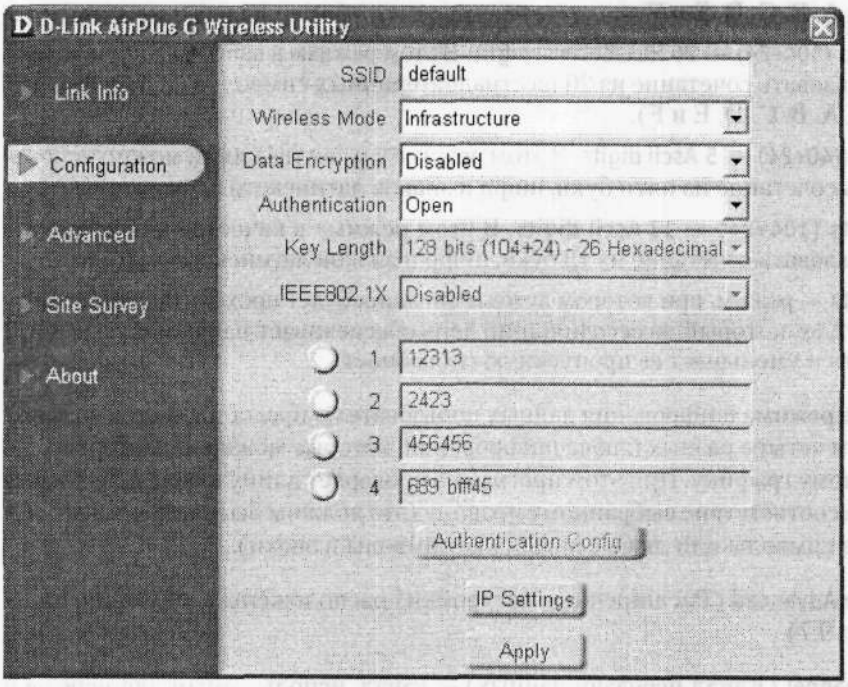

Рис. 9.6. Окно программы конфигурирования, вкладка Configuration (Конфигурация)

- SSID — уникальный идентификатор сети. По умолчанию для любого беспроводного устройства значение этого параметра задано как default. В дальнейшем это значение обязательно следует сменить на что-то более оригинальное и к тому же неизвестное для пользователей, не подключенных к сети.
- Wireless Mode (Беспроводной режим) — режим, в котором планируется использовать данное беспроводное устройство. Доступны два значения этого параметра: Infrastructure (режим инфраструктуры) и Ad-Hoc (режим «точка-точка»).
- Data Encryption (Шифрование данных) — способ шифрования данных, ориентированный на существующие технологии и протоколы безопасности. Шифрование данных можно включить и выключить установкой соответствующих значений: Enabled (Разрешено) и Disabled (Запрещено). Чтобы обеспечить приемлемую защиту сети, естественно, шифрование следует разрешить.
- Authentication (Аутентификация) — способ прохождения аутентификации при подключении к выбранному устройству. От выбранного способа будет зависеть

используемый в дальнейшем протокол безопасности. Существует несколько вариантов: Open (Открытая), Shared (Разделенная), WPA и WPA-PSK.

- Key Length (Длина ключа) — длина ключа, который будет использоваться при шифровании данных. Доступны следующие варианты:
  - 64 bits (40+24) — 10 Hexadecimal digits. В этом режиме в качестве ключа можно использовать сочетание из 10 шестнадцатиричных символов (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E и F).
  - 128 bits (104+24) — 26 Hexadecimal digits. В этом режиме в качестве ключа можно использовать сочетание из 26 шестнадцатеричных символов (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E и F).
  - 64 bits (40+24) — 5 Ascii digits. В этом режиме в качестве ключа можно использовать сочетание из пяти букв, цифр и знаков латинского алфавита.
  - 128 bits (104+24) — 13 Ascii digits. В этом режиме в качестве ключа можно использовать сочетание из 13 букв, цифр и знаков латинского алфавита.
- IEEE802.1X — режим, при котором аутентификация будет проходить по стандарту IEEE 802.1x, который на сегодняшний день обеспечивает наибольшую защиту сети, хоть и уменьшает ее пропускную способность.

При выборе режима шифрования данных пользователю предоставляется возможность ввести четыре разных ключа шифрования, которые можно использовать по произвольному графику. При этом программа проверяет длину ключа и вводимые символы на соответствие выбранному правилу (это должны быть только шестнадцатеричные символы или любые латинские символы и знаки).

На вкладке Advanced (Расширенные настройки) расположены следующие параметры (рис. 9.7).

- Adhoc Channel (Канал передачи данных) — канал, используемый для передачи данных. Согласно сетевому стандарту 802.11g, весь диапазон частот разбит на 13 каналов, которые могут использоваться для нужд передатчика. Значением данного параметра может быть любой из этих 13 каналов. Задайте конкретный канал, если вы уверены, что его не использует ни один из возможных близкорасположенных маршрутизаторов или точек доступа. Это позволяет обеспечить минимальную зашумленность эфира и, как следствие, повысить стабильность работы и пропускную способность сети.
- Profile IP Settings (Использование IP-шаблонов) — утилита конфигурирования адаптера D-Link DWL-G122, с помощью которой можно настраивать несколько шаблонов с параметрами подключения к разным точкам доступа. Чтобы эти шаблоны можно было автоматически использовать, следует задать для параметра Profile IP Settings (Использование IP-шаблонов) значение Enable (Разрешить). Если использование шаблонов не планируется, то лучше выбрать значение Disable (Запретить).
- Power Mode (Режим энергопотребления). Так как при работе передатчика беспроводного адаптера используется достаточно много энергии, что очень критично

для пользователей переносных и наладонных компьютеров, стандартами предусмотрен режим энергосбережения. Данному параметру можно задать одно из трех значений: Disable (Запретить), Min Saving (Минимальное сбережение энергии) или Max Saving (Максимальное сбережение энергии). Необходимое значение следует выбирать в зависимости от потребностей и конкретной ситуации.

- Launch Utility on Startup (Запускать утилиту при старте) — параметр, название которого говорит само за себя. Если задать значение Enable (Разрешить), то утилита конфигурирования адаптера будет запускаться вместе с загрузкой системы. Когда все параметры адаптера будут настроены и опробованы, лучше установить для данного параметра значение Disable (Запретить).
- Data Packet Parameter (Параметры пакетов данных) — область, в которой настраивают параметры формирования пакетов с данными. Поскольку для шифрования данных могут использоваться разные методы и ключи шифрования, то размер служебной части пакета с данными может значительно изменяться. Чем большим он будет, тем меньше места останется для полезных данных. Правильно подобрав значения в полях области Data Packet Parameter (Параметры пакетов данных), можно искусственно улучшить производительность сети.

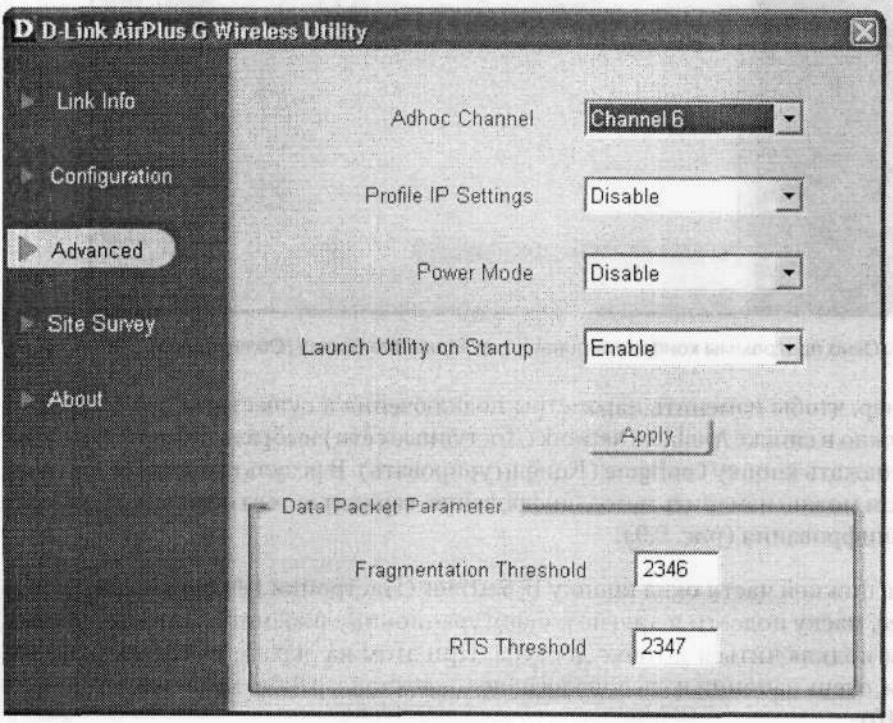

Рис. 9.7. Окно программы конфигурирования, вкладка Advanced (Расширенные настройки)

Вкладка Site Survey (Обзор узлов) (рис. 9.8) содержит очень важную информацию, касающуюся найденных точек доступа, а также шаблоны с настройками, которые

можно использовать при подключении к этим точкам доступа. В любой момент вы можете посмотреть SSID точки доступа, ее MAC-адрес, мощность сигнала, а также узнать, к какой точке в данный момент подключен ваш адаптер. Кроме всего прочего, можно конфигурировать параметры подключения к точкам доступа, добавлять новые, производить фильтрацию по выбранным параметрам и т. д.

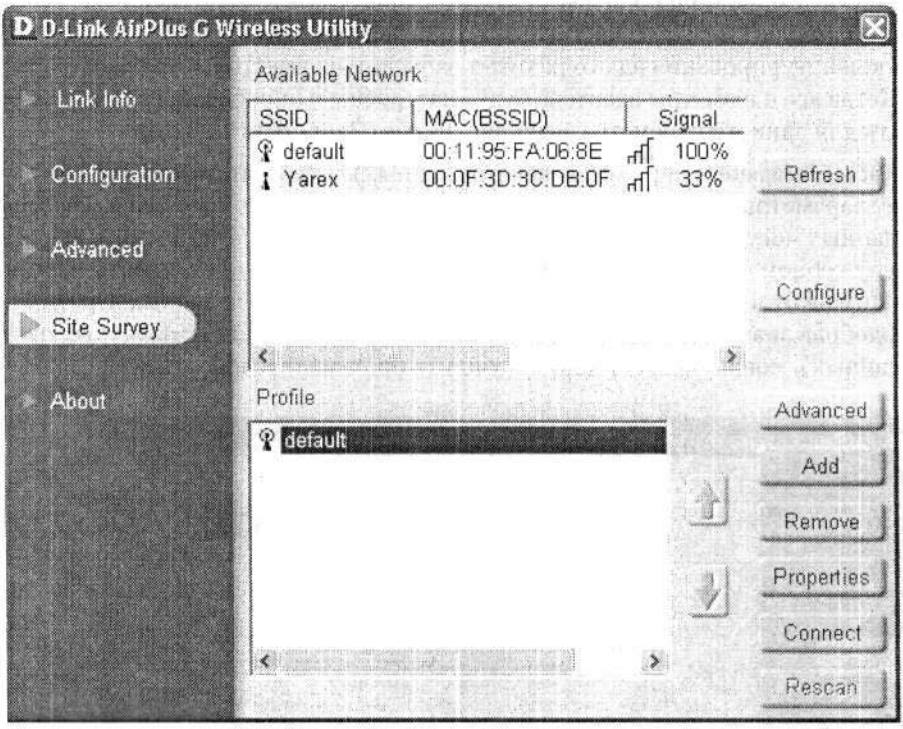

Рис. 9.8. Окно программы конфигурирования, вкладка Site Survey (Обзор узлов)

Например, чтобы изменить параметры подключения к существующей точке доступа, нужно в списке Available Network (Доступные сети) выбрать нужную точку доступа и нажать кнопку Configure (Конфигурировать). В результате откроется окно, в котором можно изменить метод шифрования, вариант аутентификации и указать ключи шифрования (рис. 9.9).

Нажав в нижней части окна кнопку IP Settings (Настройки IP), можно настроить IP-адрес, маску подсети и другие конфигурационные параметры, чтобы нужным образом подключиться к точке доступа. При этом на экране появится окно настройки, очень напоминающее аналогичное окно стандартного механизма Windows (рис. 9.10).

В этом окне можно указать IP-адрес, маску подсети, адрес шлюза, адреса предпочитаемого и дополнительного DNS-серверов, настроить адрес прокси-сервера и многое другое, что обязательно пригодится вам при настройке общего доступа в Интернет.

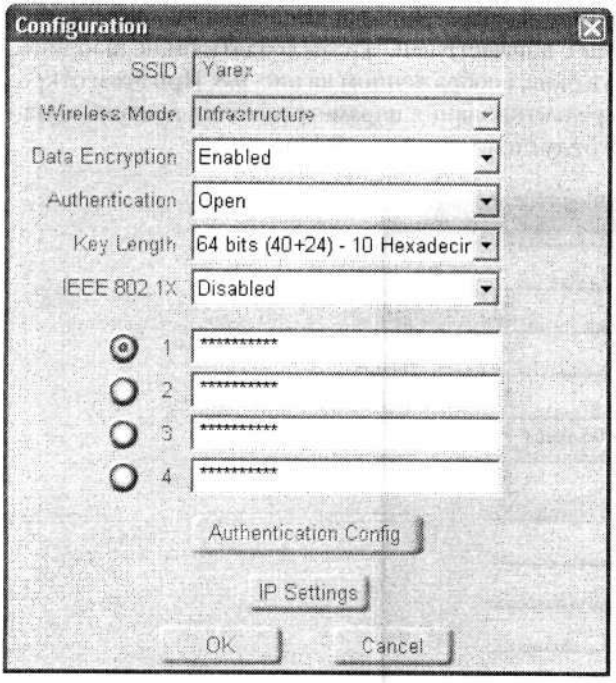

Рис. 9.9. Изменение параметров подключения к сети

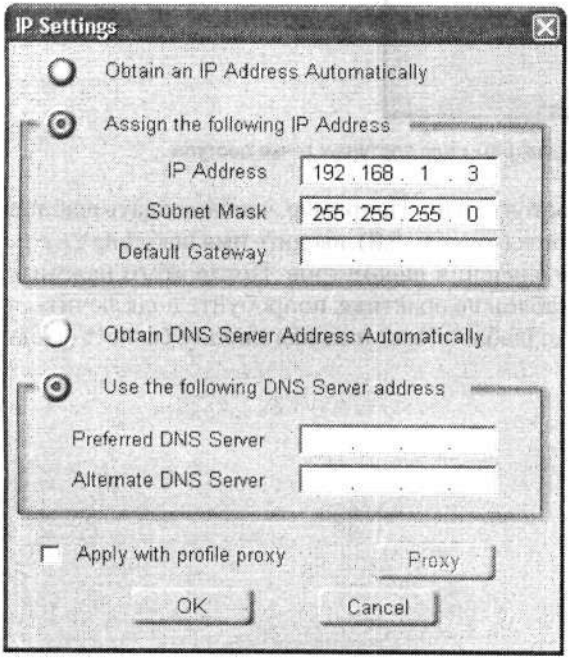

Рис. 9.10. Настраиваем IP-адрес, маску подсети и другие параметры

Если вы не хотите постоянно изменять параметры подключения к точке доступа, можно использовать шаблоны с параметрами. Чтобы создать такие шаблоны, нажмите кнопку Add (Добавить) в окне, изображенном на рис. 9.8. При этом откроется окно, напоминающее окно редактирования параметров точки доступа, однако в данном случае многие поля будут пустыми (рис. 9.11).

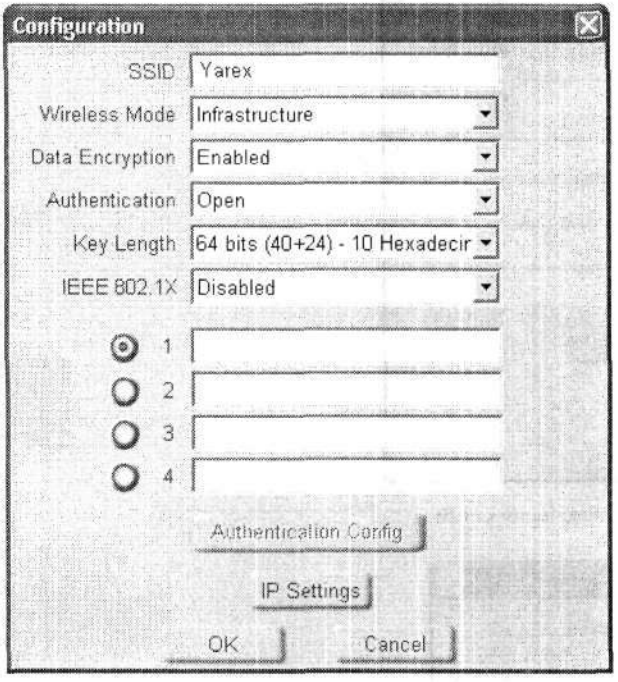

Рис. 9.11. Окно создания шаблона с параметрами для доступа к точке доступа

Пустые поля нужно заполнить самостоятельно. Например, чтобы создать шаблон для подключения к точке доступа Yarex (см. рис. 9.8), введите имя шаблона `Yarex` и задайте все остальные известные значения параметров. После этого нажмите кнопку OK и проверьте созданный шаблон на практике: попробуйте подключиться к настроенной сети, выбрав в списке шаблон Yarex и нажав кнопку Connect (Подключиться).

ГЛАВА 10 Настройка параметров адаптера OvisLink WL-8000PCI

Вместе с установкой драйвера для беспроводного устройства OvisLink WL-8000PCI инсталлируется и конфигурационная утилита, позволяющая настраивать параметры этого устройства.

После установки драйвера значок утилиты конфигурирования устройства появится в области уведомлений Панели задач (рис. 10.1). Этот значок напоминает зеленый шар, хотя с формой шара программисты, создававшие эту фигуру, явно промахнулись, и он получился слегка обрубленным.

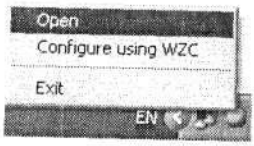

Рис. 10.1. Значок «родной» утилиты конфигурирования устройства

Чтобы запустить утилиту конфигурирования, достаточно щелкнуть на значке утилиты правой кнопкой мыши и в появившемся контекстном меню выбрать пункт Open (Открыть). Можно также просто дважды щелкнуть на этом значке. В результате на экране появится окно программы конфигурирования, содержащее несколько вкладок (рис. 10.2). Рассмотрим содержимое вкладок более подробно.

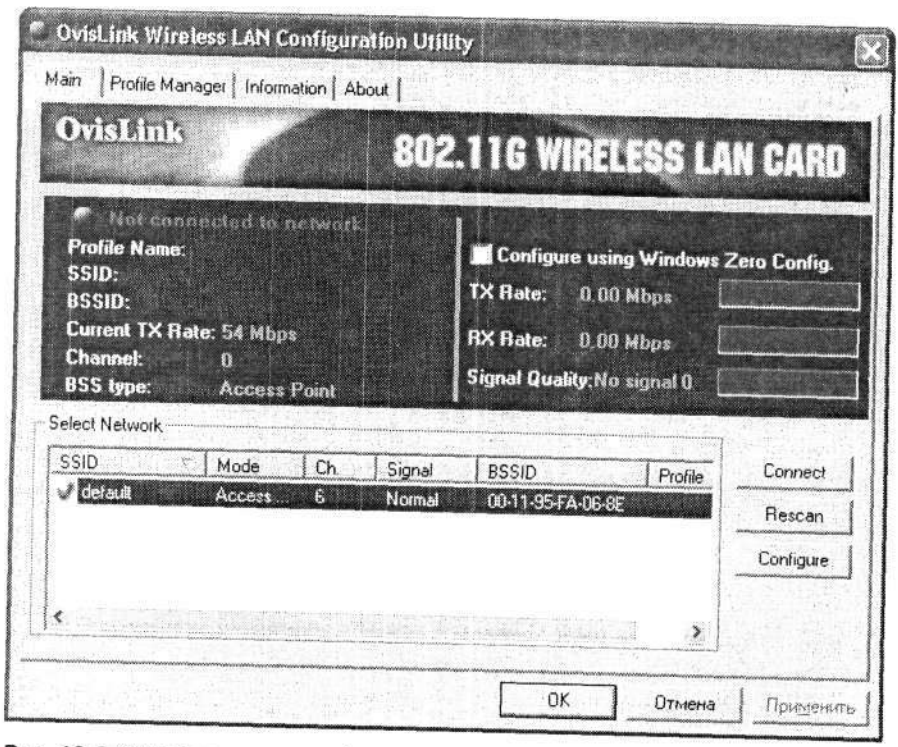

Рис. 10.2. Окно программы конфигурирования

На рис. 10.2 открыта вкладка Main (Главная). Здесь отображается список найденных точек доступа и их некоторые характеристики. В верхней части окна вы увидите подробное описание параметров точки доступа, к которой в данный момент подключен ваш беспроводной адаптер. В частности, здесь отображаются SSID, текущая скорость подключения, номер используемого канала, а также исходящая и входящая скорости передачи/приема данных.

Чтобы подключиться к точке доступа, достаточно отметить ее указателем мыши и нажать кнопку Connect (Подключить). При этом будет автоматически создан шаблон с параметрами подключения к точке, которые вы сможете в дальнейшем редактировать. Так, в рассматриваемом примере при подключении к имеющейся точке доступа с идентификатором сессии default (по умолчанию) автоматически создается шаблон с аналогичным именем — default (рис. 10.3).

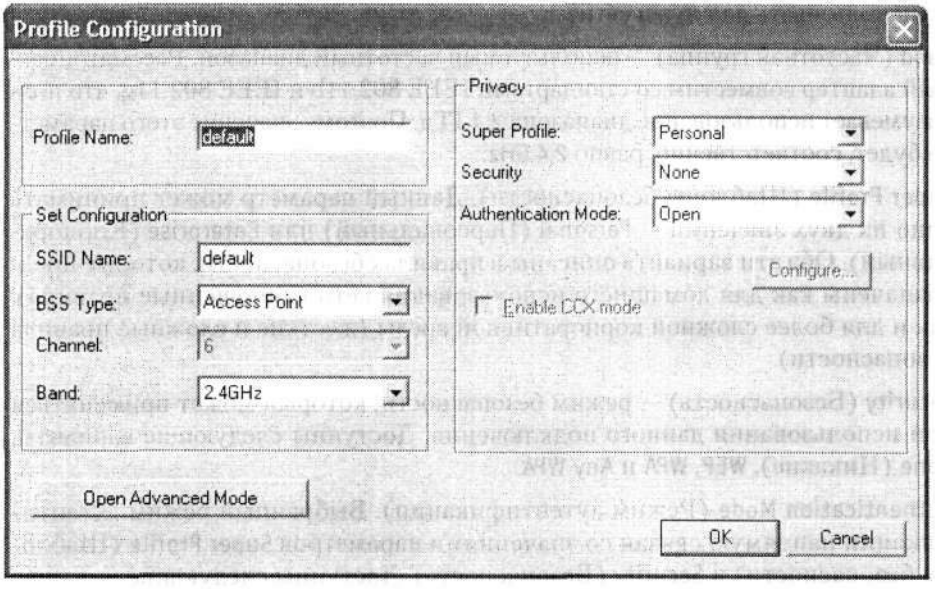

Рис. 10.3. Шаблон подключения к выбранной точке доступа

В этом шаблоне можно настроить следующие параметры.

- Profile Name (Имя шаблона) — название шаблона. В качестве названия можно задать любое словосочетание, поскольку особой смысловой нагрузки оно не несет. Лучше, конечно же, присвоить шаблону имя, совпадающее с SSID точки доступа. В таком случае вам будет легче впоследствии обнаружить и настроить этот шаблон, если их накопится достаточно много.
- SSID Name (Идентификатор сети) — уникальный идентификатор, однозначно определяющий сеть. Данный идентификатор обязательно должен совпадать с идентификатором точки доступа (или другого беспроводного адаптера), если, конечно, вы все еще планируете работать в сети. Благодаря этому идентификатору

несколько компьютеров могут организовать уникальную сетевую группу. Изначально у многих беспроводных устройств значение параметра SSID Name (Идентификатор сети) задано равным default (по умолчанию). По понятным причинам этот идентификатор в дальнейшем следует заменить уникальным, известным лишь «посвященным».

- BSS Type (Режим работы) — режим, в котором работает данное беспроводное устройство. Доступно два варианта: Access Point (Точка доступа) и peer-to-peer («точка-точка»). Выберите необходимое значение, исходя из типа построения сети.
- Channel (Канал) — канал, используемый согласно беспроводным стандартам. Такой канал представляет собой небольшой диапазон частот, взятый из общего диапазона, в котором работает беспроводное устройство. Например, согласно стандарту IEEE 802.11g, таких каналов может быть 13 и любой из них можно использовать для нужд сети.
- Band (Частотная группа) — используемый частотный диапазон. Рассматриваемый адаптер совместим со стандартами IEEE 802.11b и IEEE 802.11g, что подразумевает использование диапазона 2,4 ГГц. Поэтому значение этого параметра будет, соответственно, равно 2,4 GHz.
- Super Profile (Шаблоны безопасности). Данный параметр может принимать одно их двух значений — Personal (Персональный) или Enterprise (Корпоративный). Оба эти варианта описаны в правилах безопасности, которые предназначены как для домашнего использования сети (упрощенные правила), так и для более сложной корпоративной среды (жесткие и сложные правила безопасности).
- Security (Безопасность) — режим безопасности, который может применяться при использовании данного подключения. Доступны следующие варианты: None (Никакие), WEP, WPA и Any WPA.
- Authentication Mode (Режим аутентификации). Выбранный режим аутентификации напрямую связан со значениями параметров Super Profile (Шаблоны безопасности) и Security (Безопасность). Доступны следующие режимы: Open (Открытая), Auto switch (Автоматическое переключение), Shared Keys (Разделенные ключи), TLS и PSK (Pre-shared Key). При изменении режима аутентификации, а также значений параметров Super Profile (Шаблоны безопасности) и Security (Безопасность) изменяется и количество доступных вариантов настройки параметров безопасности.

Например, если установить для параметра Security (Безопасность) значение WEP, а после этого нажать кнопку Configure (Конфигурировать), то на экране появится окно с настройками ключей шифрования (рис. 10.4). Здесь предлагается ввести до четырех ключей разной длины. При этом из раскрывающегося списка Key Format (Формат ключа) можно выбрать формат ввода: HEX или ASCII. Максимальная длина ключа может составлять 256 бит, что составляет 58 шестнадцатеричных символов или 29 символов ASCII.

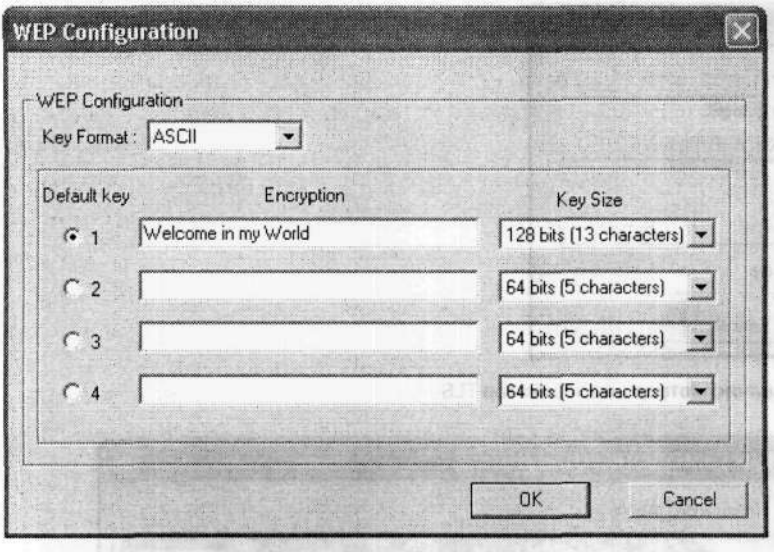

Рис. 10.4. Ввод ключей шифрования

Если у вас нет желания работать с устаревшим WEP-протоколом, то можно воспользоваться всеми преимуществами протокола WPA.

Например, задав для параметра Security (Безопасность) значение WPA2, вы сможете использовать механизм аутентификации PSK (рис. 10.5) или механизм TLS (рис. 10.6), основывающийся на выдаваемых компьютерам сертификатах доступа.

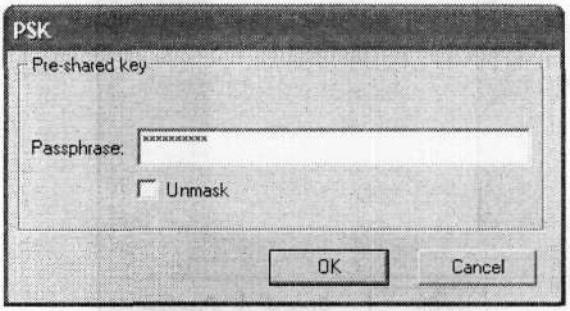

Рис. 10.5. Использование механизма аутентификации PSK

Полностью настроив шаблон, нажмите кнопку OK в окне, изображенном на рис. 10.3. После этого произойдет попытка соединения с точкой доступа. Если все параметры настроены верно, то в главном окне программы конфигурирования (см. рис. 10.2) вы увидите надпись Connected to network (Подключен к сети) и свойства данного подключения.

На вкладке Profile Manager (Менеджер шаблонов) главного окна программы отображаются все используемые шаблоны подключения к разным сетям (рис. 10.7).

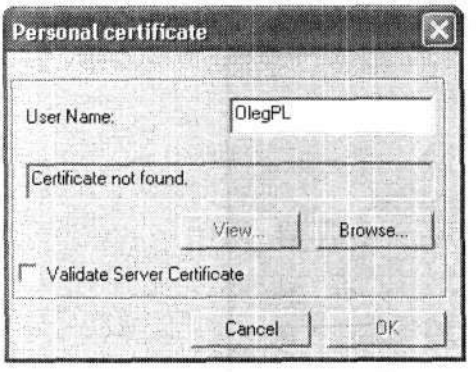

Рис. 10.6. Использование метода сертификатов TLS

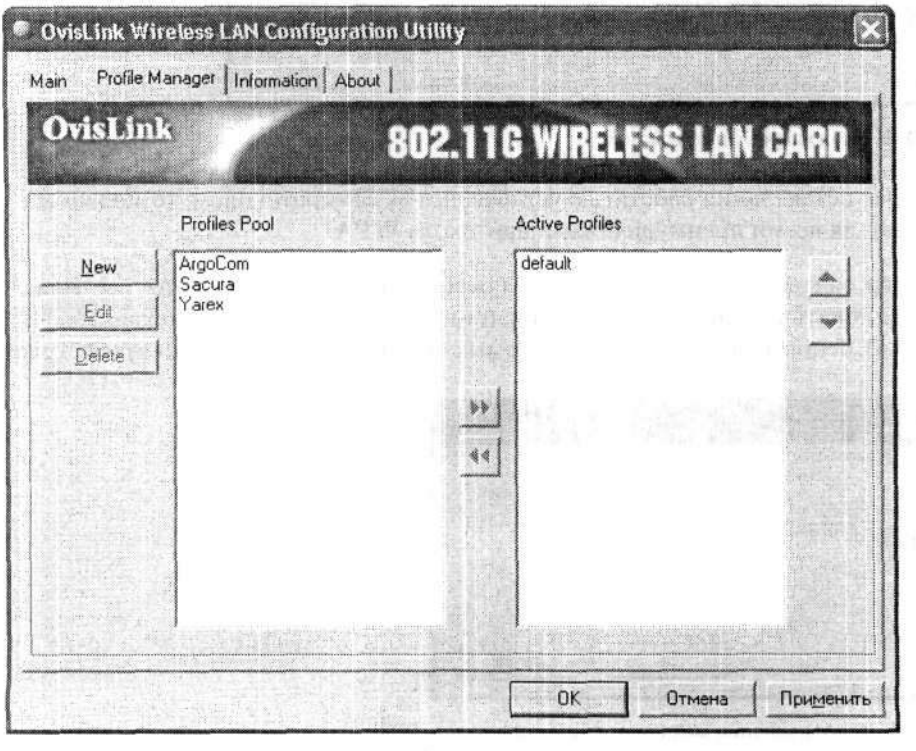

Рис. 10.7. Содержимое вкладки Profile Manager (Менеджер шаблонов)

Здесь их можно изменять, удалять или добавлять новые, как при подключении к точке доступа (см. рис. 10.3–10.6). При этом в правой части окна отображается активный шаблон подключения, а в левой — шаблоны, предназначенные для подключения к другим беспроводным сетям.

На вкладке Information (Сведения) отображаются более подробные сведения об используемом подключении (рис. 10.8). В частности, здесь вы увидите длительность

подключения, информацию, касающуюся отдельных пакетов (принятые, дубликаты, ошибочные и т. д.), сведения о соединении (аутентификация, режим энергосбережения, турборежим и т. д.), а также данные о точке подключения (IP-адрес, маска подсети, MAC-адрес и шлюз).

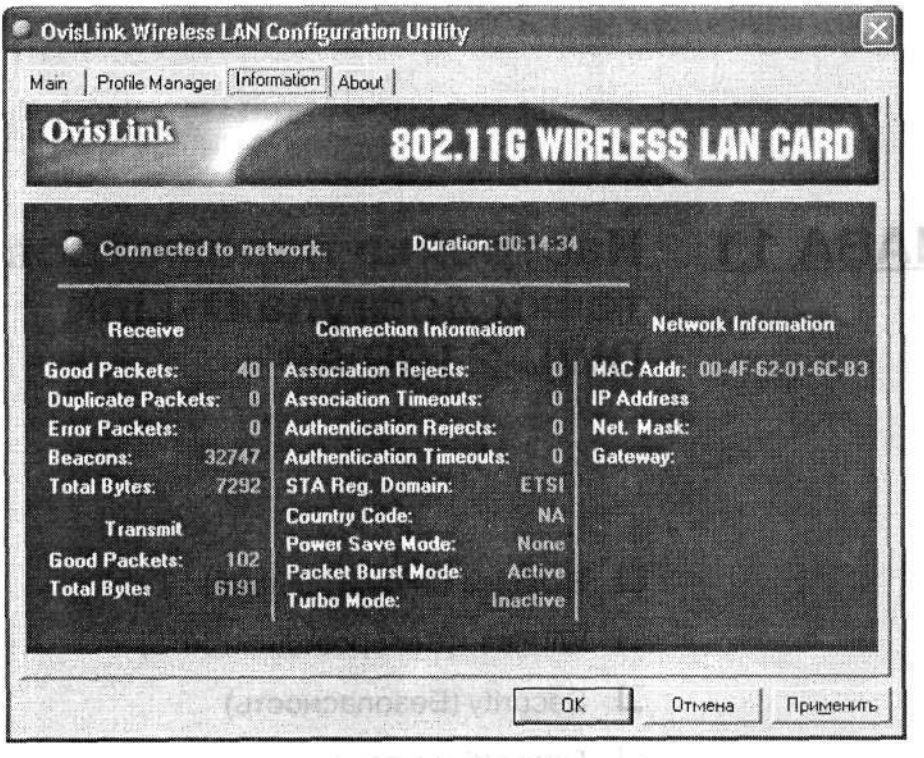

Рис. 10.8. Подробные сведения о текущем подключении

Больше ничего интересно в программе конфигурирования адаптера OvisLink WL-8000PCI вы не найдете. Однако имеющихся возможностей вполне достаточно для организации соединения с разными точками доступа, если вы передвигаетесь между ними или постоянно используете одну точку.

ГЛАВА 11 Настройка параметров точки доступа D-Link DWL-2100 AP

- Вкладка General (Общие)
- Wireless (Беспроводная сеть)
- Security (Безопасность)
- Filters (Фильтры)
- AP Mode (Режим точки доступа)
- DHCP Server (Сервер DHCP)
- Client Info (Сведения о клиентах)
- Multi-SSID (Мульти SSID)

Точка доступа D-Link DWL-2100 AP достаточно популярна среди организаторов беспроводных сетей. Она характеризуется относительно низкой стоимостью и большим количеством технических возможностей. Это устройство может служить не только точкой доступа, но и мостом, повторителем, клиентом с проводным подключением и др.

Настроить параметры работы данной точки доступа можно несколькими способами. В частности, можно использовать веб-интерфейс, доступный по адресу 192.168.0.50, утилиту конфигурирования или системную утилиту Telnet. В любом случае количество параметров, значения которых можно изменить, впечатляет и даже шокирует.

Использование утилиты конфигурирования, поставляемой вместе с устройством, возможно только при наличии Ethernet-подключения к точке доступа или беспроводного подключения с помощью соответствующего адаптера. Это означает, что без установленного беспроводного адаптера вы сможете подключиться к точке доступа только с помощью проводного соединения.

Наилучшим и наиболее безопасным способом управления точкой доступа, конечно же, является непосредственное подключение ее к управляющему компьютеру посредством кабеля, хотя это и не всегда возможно. При этом IP-адрес и маска подсети соединения, с помощью которого вы подключаетесь к точке доступа, должны быть настроены соответствующим образом. В частности, IP-адрес должен быть, например, 192.168.0.51, а маска подсети — 255.255.255.0.

Для этого выполните команду Пуск ▸ Сетевое окружение, затем щелкните на ссылке Отобразите сетевые подключения в области Сетевые задачи. В открывшемся окне Сетевые подключения щелкните правой кнопкой мыши на значке нужного беспроводного соединения и в появившемся контекстном меню выберите пункт Свойства. В результате откроется окно свойств выбранного соединения, в котором отображается название используемого адаптера, а также протоколы и службы, применяемые для организации соединения (см. рис. 9.2).

Обратите внимание на пункт Протокол Интернета (TCP/IP). Щелкните на нем и нажмите кнопку Свойства. В появившемся окне (рис. 11.1) установите переключатель в положение Использовать следующий IP-адрес и введите нужные значения в поля IP-адрес и Маска подсети. После этого можно нажать кнопку OK и попытаться запустить утилиту конфигурирования точки доступа.

Предположим, что для конфигурирования точки доступа вы решили использовать утилиту конфигурирования AP Manager, которая находится на прилагаемом к устройству компакт-диске с программным обеспечением.

После запуска программы на экране появится окно, показанное на рис. 11.2.

В верхней части данного окна находится восемь кнопок, с помощью которых можно вызвать различные окна настроек или ознакомиться с определенной информацией.

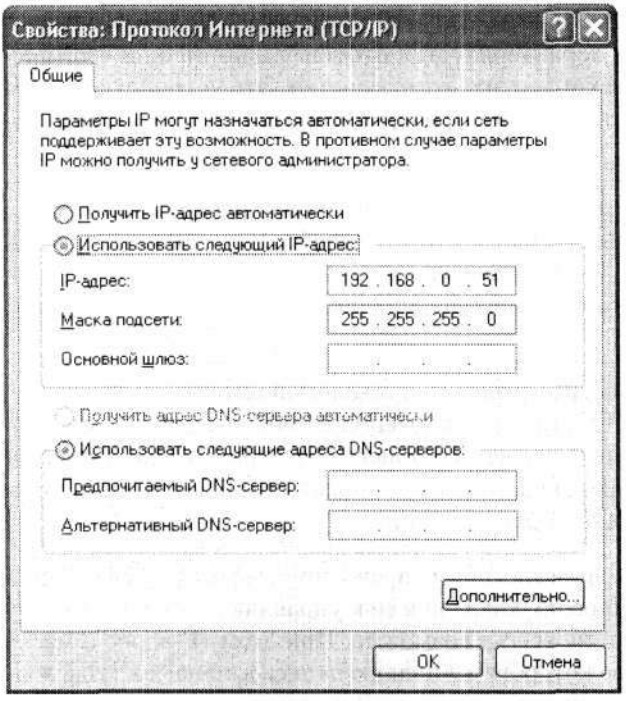

Рис. 11.1. Окно свойств протокола Интернета

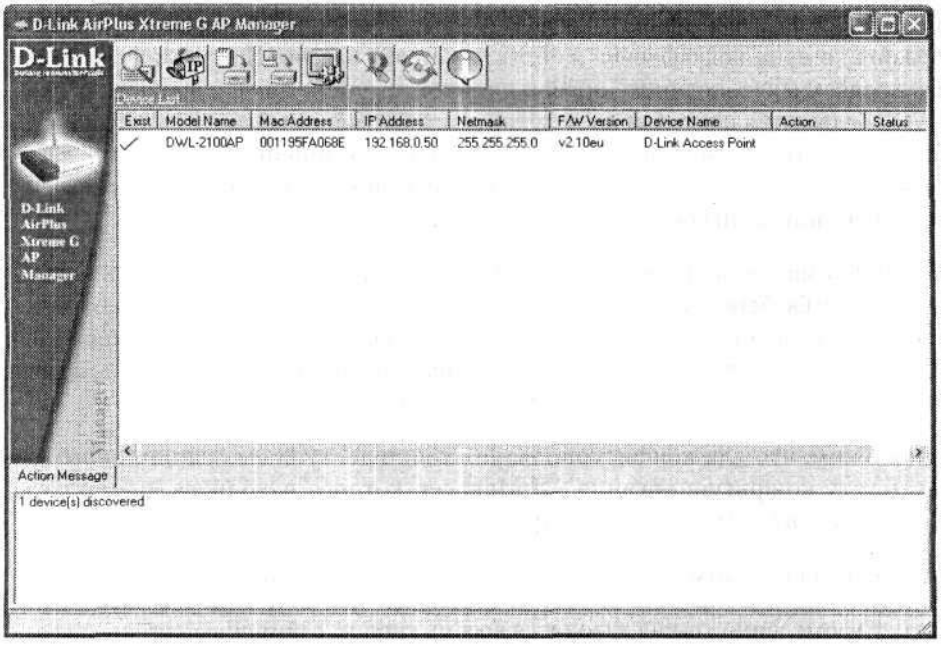

Рис. 11.2. Главное окно программы конфигурирования AP Manager

Поле Device List (Список устройств) предназначено для списка всех найденных точек доступа D-Link DWL-2100 AP с кратким описанием их параметров. В нижней части отображаются события, происходящие с точкой доступа (например, сообщения о настройках или ошибках).

Итак, начнем с самого простого. Нажмите первую кнопку — Discover devices (Поиск устройств) (названия кнопок отображаются во всплывающих подсказках). В результате программа произведет поиск доступных точек доступа и выведет результаты в поле Device List (Список устройств). В рассматриваемом случае программа обнаружила только одну точку доступа (см. рис. 11.2).

По умолчанию данная точка доступа имеет IP-адрес 192.168.0.50 и маску подсети 255.255.255.0. Естественно, с целью безопасности эти значения следует изменить, поскольку любой человек, знающий адрес точки доступа, может попробовать подключиться к ней или взломать точку. Для изменения адреса точки доступа нажмите вторую слева кнопку — Set IP (Установить IP). В результате на экране появится окно (рис. 11.3), содержащее всего два параметра: IP Address (IP-адрес) и IP Netmask (IP-маска сети). Изменив данные значения, нажмите кнопку OK.

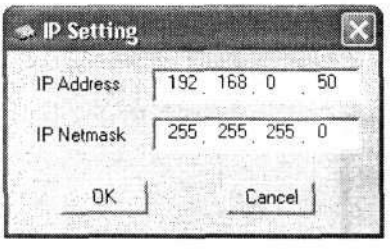

Рис. 11.3. Указываем IP-адрес и маску подсети

Следующий шаг — установка начальных параметров работы точки доступа. Для этого нажмите в окне программы шестую кнопку — Wizard (Мастер). Появится окно мастера настройки точки доступа, в котором вам сообщат, что вы сможете настроить следующие параметры: пароль для подключения к точке доступа, SSID и канал передачи данных, а также режим безопасности (рис. 11.4).

Чтобы начать процесс настройки устройства, нажмите кнопку Next (Далее).

В следующем окне вам предложат ввести пароль, который будет запрашиваться при настройке каких-либо параметров точки доступа (рис. 11.5).

Естественно, данный пароль должен знать только человек, отвечающий за администрирование сети. После ввода нового пароля и подтверждения нажмите кнопку Next (Далее).

В следующем окне вам предложат выбрать канал, по которому будут передаваться данные (рис. 11.6).

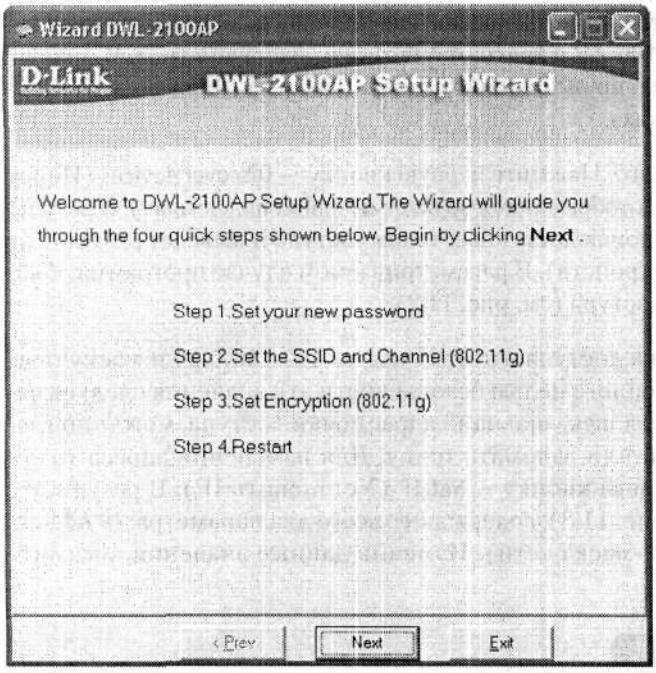

Рис. 11.4. Окно мастера настройки точки доступа

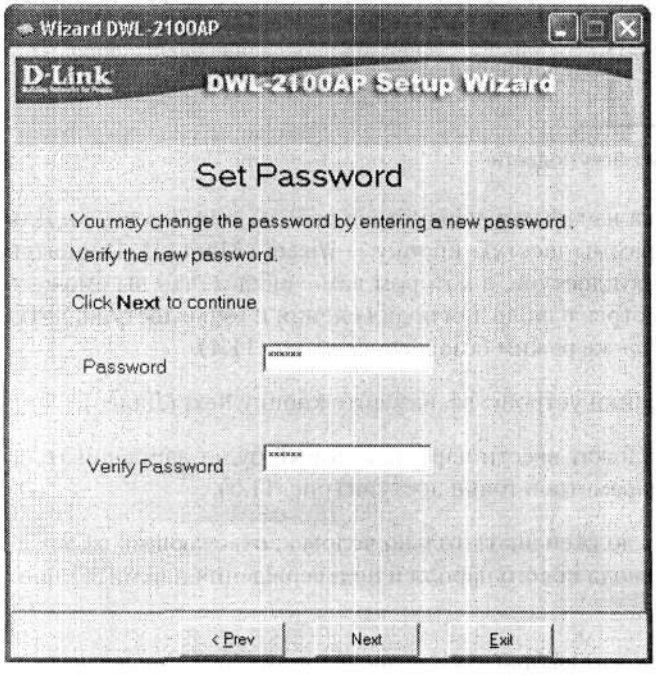

Рис. 11.5. Указываем пароль к точке доступа

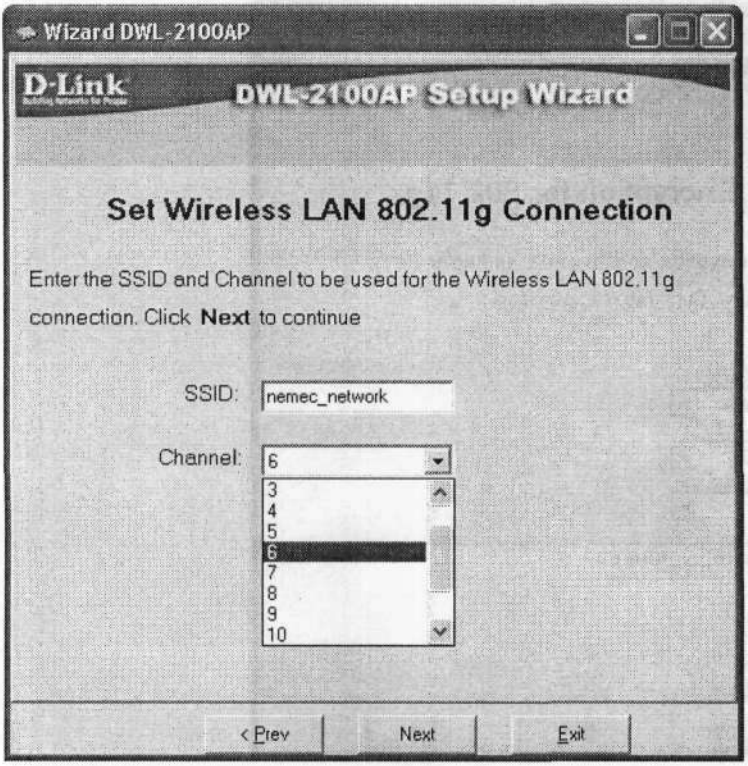

Рис. 11.6. Выбираем канал для передачи данных

Лучше всего выбрать канал таким образом, чтобы он не мешал работе другой точки доступа, хотя теоретически каналы не пересекаются.

В принципе, многие «умные» точки доступа могут при необходимости изменять номер канала автоматически. Однако, как бы там ни было, указать первоначальный канал придется. По умолчанию используется шестой канал, и это значение можно не изменять. Для продолжения установки нажмите кнопку Next (Далее).

В следующем окне (рис. 11.7) вам предложат выбрать начальный режим безопасности, включающий в себя использование протокола WEP с определенной длиной ключа шифрования. Если вы не хотите использовать шифрование (а зря!), оставьте значение параметра WEP равным Disable (Запретить) и нажмите кнопку Next (Далее) для перехода к следующему окну. Если вы все-таки хотите использовать шифрование, то выберите для параметра WEP значение Enable (Разрешить) и в соответствующих полях укажите тип ключа (HEX или ASCII), длину ключа (64, 128 или 152) и сам ключ.

При выборе ключа не рекомендуется использовать какие-либо личные данные, например фамилию, дату рождения или номер телефона, поскольку это может помочь злоумышленникам взломать сеть. Лучше всего применять бессмысленное сочетание символов.

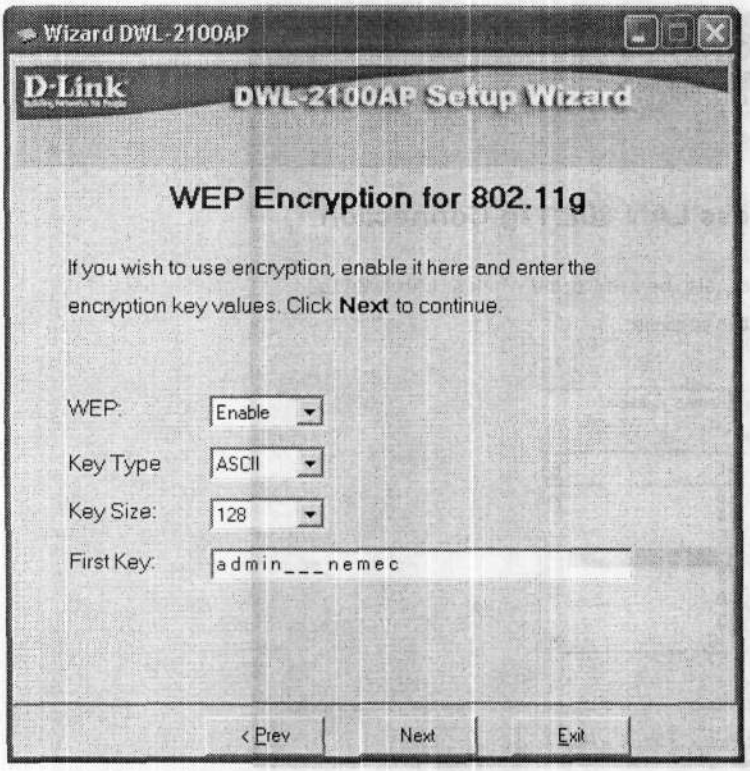

Рис. 11.7. Указываем параметры шифрования и ключ шифрования

ВНИМАНИЕ

При выборе длины ключа обязательно убедитесь в том, что все беспроводные устройства сети смогут работать с таким ключом. Часто бывает такое, что точка доступа поддерживает, например, длину ключа 104 бит, в то время как беспроводной адаптер не поддерживает такой ключ. В итоге беспроводное устройство не сможет подключиться к точке доступа.

После нажатия кнопки Next (Далее) появится последнее окно мастера, в котором сообщается о завершении настройки начальных параметров точки доступа (рис. 11.8).

Если вы хотите что-либо изменить, воспользуйтесь кнопкой Prev (Предыдущая). Если все данные указаны верно, подтвердите их нажатием кнопки Finish (Готово).

Подключение к точке доступа с помощью утилиты конфигурирования также использует пароль доступа к точке доступа. Поэтому перед сохранением выполненных установок программа обязательно предупредит вас, что после применения параметров необходимо задать новый пароль также в системной части утилиты (рис. 11.9).

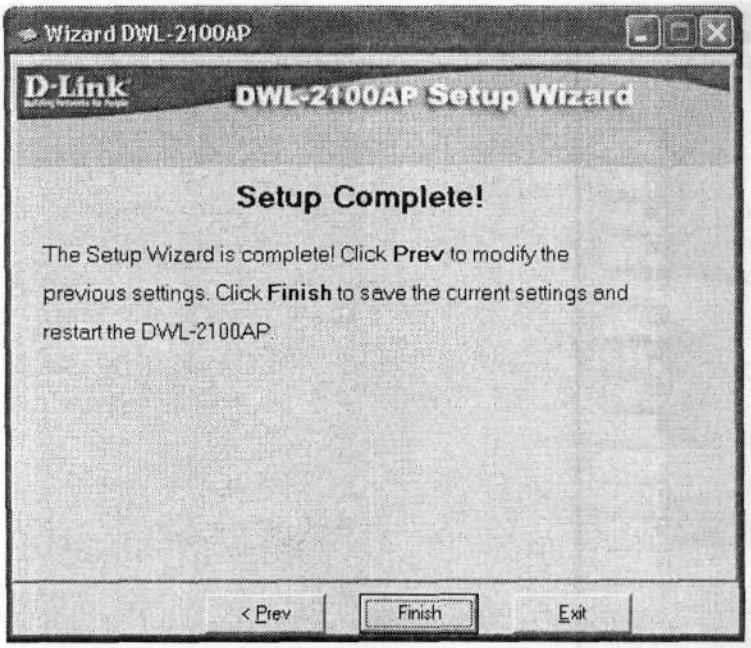

Рис. 11.8. Настройка начальных параметров завершена

Рис. 11.9. Предупреждение программы

После этого программа конфигурирования начнет запись новых параметров в постоянную память точки доступа, что может занять некоторое время.

Следующий шаг — настройка нового пароля для доступа к точке доступа с помощью программы. Для этого нажмите в окне программы кнопку System Settings (Системные установки). Появится окно, показанное на рис. 11.10.

Сверху в данном окне находится поле Access Password (Пароль доступа), в которое и нужно ввести пароль, заданный при настройке точки доступа. После этого нажмите кнопку OK и приступите к более детальной настройке параметров точки доступа.

Чтобы настроить расширенные параметры точки доступа, достаточно дважды щелкнуть в окне утилиты на пункте с информацией о точке доступа или нажать кнопку Devices Settings (Установки устройства). Откроется окно настройки параметров устройства (рис. 11.11).

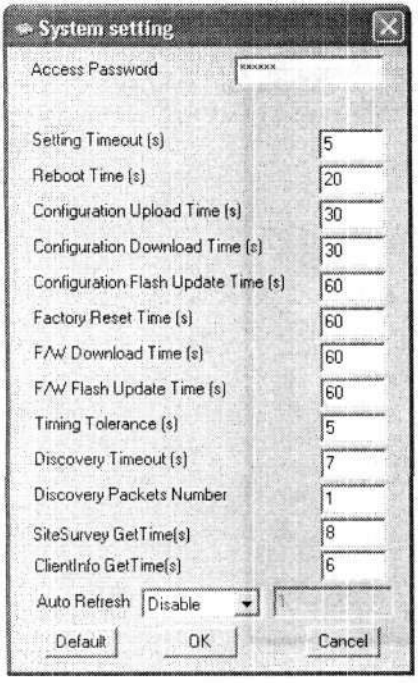

Рис. 11.10. Системные установки утилиты конфигурирования

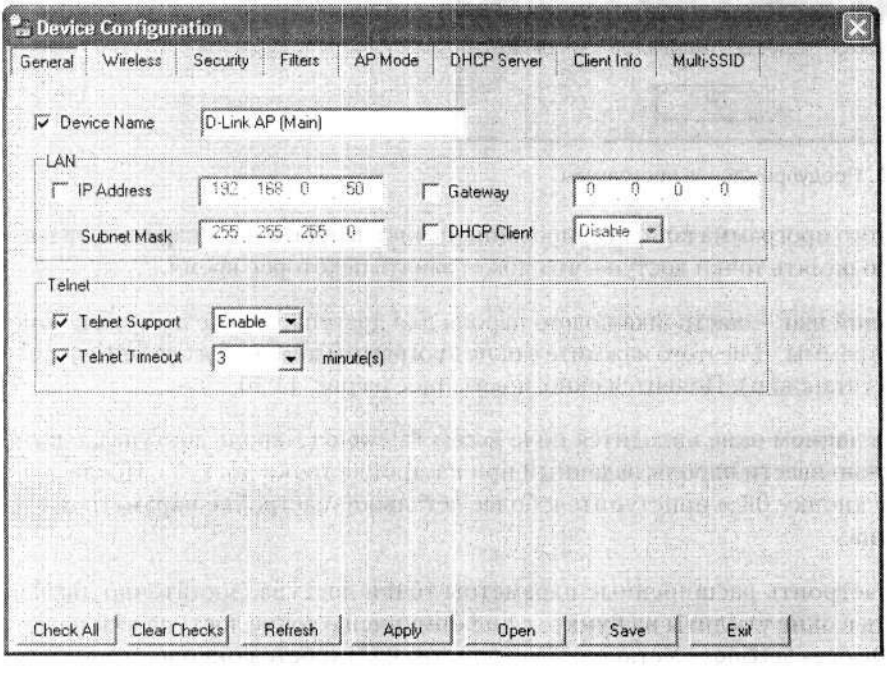

Рис. 11.11. Окно настройки параметров точки доступа

ПРИМЕЧАНИЕ

Любые изменения, внесенные в конфигурацию точки доступа, начинают действовать только после нажатия кнопки Apply (Применить). Вступление в силу новых параметров сопровождается появлением окна, показанного на рис. 11.12.

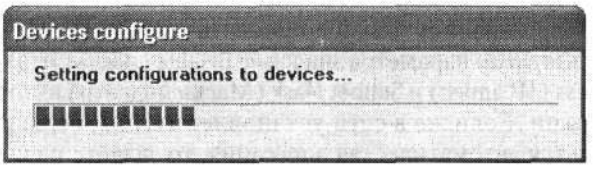

Рис. 11.12. Применение параметров

Внизу каждой вкладки данного окна расположено семь кнопок, каждая из которых выполняет свою функцию. Обратите внимание на кнопки Check All (Отметить все) и Clear Checks (Очистить отмеченное). С помощью данных кнопок можно отметить все параметры или, наоборот, снять метки со всех параметров на всех вкладках. Лучше не использовать данные кнопки, поскольку это может привести к трудно поправимым последствиям. Внимательно просмотрите все вкладки и аккуратно выполните необходимые изменения, чтобы впоследствии не пришлось выяснять причину отказа работы точки доступа или беспроводных адаптеров вашей сети.

Рассмотрим содержимое каждой вкладки.

11.1. Вкладка General (Общие)

По умолчанию в окне свойств точки доступа открыта вкладка General (Общие) (см. рис. 11.11). Она содержит следующие параметры.

- Device Name — имя точки доступа. Изменив значение данного параметра, вы сможете различать точки доступа по названиям. Кроме того, с помощью имени вы сможете, например, описать местоположение данной точки или ее роль в сети. Чтобы ввести название, нужно активизировать данное поле путем установки соответствующего флажка.
- Область LAN отвечает за настройку IP-адреса, маски подсети, шлюза и DHCP-клиента.
  - IP Address (IP адрес) — действующий IP-адрес точки доступа. По умолчанию точка доступа использует IP-адрес 192.168.0.50 и его изменение заблокировано. Если по какой-либо причине вы не хотите использовать этот адрес (например, с целью безопасности), то можно установить флажок IP Address и ввести в соответствующее поле новый IP-адрес.
  - Subnet Mask (Маска подсети). Данный параметр работает в паре с параметром IP Address и отвечает за маску подсети. При изменении IP-адреса (при уста-

новленном флажке IP Address) параметр Subnet Mask также активизируется и вычисляется автоматически в зависимости от введенного IP-адреса.

- Gateway (Шлюз) — IP-адрес шлюза, который может использоваться, например, для подключения к Интернету, а также любому другому маршрутизатору или точке доступа. Чтобы активизировать данный параметр, установите соответствующий флажок. После этого можно ввести в поле нужный адрес.
- DHCP Client (клиент DHCP). Если планируется использовать статический IP-адрес, то необходимо задать для этого параметра значение Disable (Запретить). При этом параметры IP Address (IP адрес) и Subnet Mask (Маска подсети) автоматически станут неактивными. Если же в сети установлен DHCP-сервер и для точки доступа назначается автоматическая адресация, то задайте параметру DHCP Client (клиент DHCP) значение Enable (Разрешить).

- Область Telnet содержит параметры, отвечающие за настройку свойств точки доступа с использованием системной утилиты Telnet.
  - Telnet Support (Поддержка Telnet). Данный параметр может принимать всего два значения: Enable (Разрешить) и Disable (Запретить). С его помощью вы можете управлять использованием утилиты Telnet для конфигурирования устройства[1]. По умолчанию выбрано значение Enable (Разрешить).
  - Telnet Timeout (Задержка отключения Telnet). При возникновении значительных перерывов в работе программы вы можете отключить точку доступа (с целью безопасности). Чтобы задействовать этот механизм, достаточно установить соответствующий флажок и ввести в поле промежуток времени, по прошествии которого точка доступа будет отключена. По умолчанию данный промежуток составляет три минуты. Рекомендуется установить интервал около 10 минут.

11.2. Wireless (Беспроводная сеть)

Вкладка Wireless (Беспроводная сеть) (рис. 11.3) предназначена для настройки таких основных параметров беспроводной сети, как SSID, канал и скорость передачи данных и т. д.

Чтобы настроить параметры, расположенные на этой вкладке, установите флажок Wireless setting (Настройка беспроводной сети).

- SSID. Данный параметр описывает уникальный идентификатор сети, который выступает в качестве связующего звена для всех беспроводных устройств, участвующих в работе сети. По умолчанию для точки доступа D-Link DWL 2100-AP задано значение этого параметра default (по умолчанию). Естественно, в целях безопасности его следует заменить чем-то более уникальным. В рассматриваемом случае параметру SSID присвоено значение nemec_network.

---

[1] С помощью утилиты Telnet вы сможете настроить намного больше параметров, чем при использовании стандартной утилиты конфигурирования.

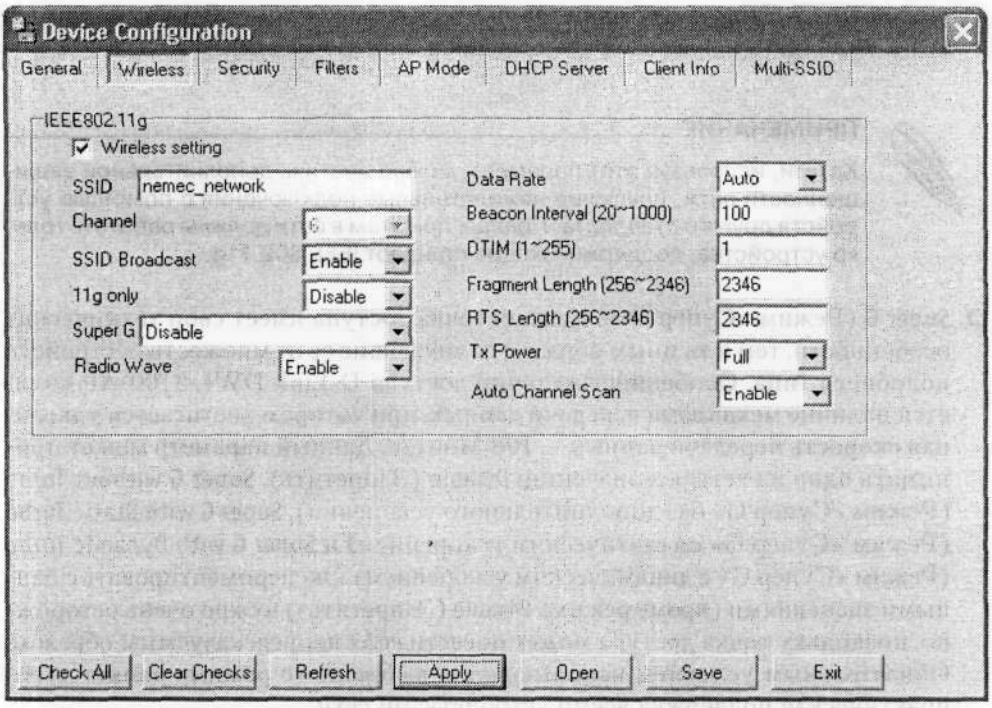

Рис. 11.13. Содержимое вкладки Wireless (Беспроводная сеть)

- Channel (Канал) — номер канала, который будет использоваться для передачи данных в сети. По умолчанию выбран шестой канал, хотя это не имеет никакого практического значения. При использовании параметра Auto Channel Scan (Автоматическое сканирование каналов) точка доступа автоматически выбирает канал. Сведения об этом сообщаются каждому беспроводному устройству сети, и они также автоматически изменяют канал передачи данных. С целью уменьшения взаимных помех можно выбрать канал, который не используется другими точками доступа.
- SSID Broadcast (Транслирование SSID). Данный параметр играет достаточно важную роль в организации безопасной передачи данных в сети. По умолчанию точка доступа *передает* свой SSID всем радиоустройствам в радиусе ее действия, что, естественно, ослабляет защищенность сети. С целью максимально обезопасить себя от посягательств извне рекомендуется отключить подобное радиовещание SSID. Ведь пользователям, которые законно подключают свои компьютеры к сети, данный идентификатор сообщается в любом случае. Зачем же упрощать жизнь злоумышленникам?
- 11g only (Только 11g устройства). Поскольку в работе сети не обязательно участвуют устройства единого стандарта, обязательно следует учитывать значение этого параметра. Если вы планируете использовать устройства любого совместимого типа, то, естественно, данному параметру следует задать значение Disable

(Запретить). Если все устройства поддерживают один стандарт, например IEEE 802.11g, то можно выбрать значение Enable (Разрешить).

ПРИМЕЧАНИЕ

Кстати, используя этот параметр, можно достичь дополнительной защищенности сети, исключив нежелательные подключения с помощью устройств другого стандарта. Правда, при этом в сети должны работать только устройства, поддерживающие стандарт IEEE 802.11g.

- Super G (Режим «Супер G»). Каждая точка доступа имеет свои технические особенности, тем или иным образом отличающие ее от множества устройств подобного типа. Особенностью точки доступа D-Link DWL 2100-AP является наличие механизма передачи данных, при котором достигается удвоенная скорость передачи данных — 108 Мбит/с. Данный параметр может принимать одно из четырех значений: Disable (Запретить), Super G without Turbo (Режим «Супер G» без дополнительного ускорения), Super G with Static Turbo (Режим «Супер G» со статическим ускорением) и Super G with Dynamic Turbo (Режим «Супер G» с динамическим ускорением). Экспериментировать с данными значениями (кроме режима Disable (Запретить)) нужно очень осторожно, поскольку точка доступа может повести себя непредсказуемым образом. Обязательным условием использования выбранного режима является его практическая поддержка всеми устройствами сети.
- Radio Wave (Радиоволны). Данный режим используется для включения и отключения радиоустройства.
- Data Rate (Скорость данных). Данный параметр указывает, с какой скоростью будут передаваться данные в сети, если для параметра Super G (Режим «Супер G») задано значение Disable (Запретить). Доступны такие значения: Auto (Автоматический выбор), 1, 2, 5,5, 6, 9, 11, 12, 18, 24, 36, 48 и 54 Мбит/с. Рекомендуется оставить заданное по умолчанию значение Auto (Автоматический выбор), позволяющее скорости передачи данных автоматически изменяться в зависимости от условий среды.
- Beacon Interval (20~1000) (Интервал сигналов) — частота отсылки пакетов, предназначенных для синхронизации устройств сети. По умолчанию установлено значение 100, чего вполне достаточно для поставленной задачи. Если наблюдаются сбои в работе устройств или качество сигнала оставляет желать лучшего, то данный показатель можно уменьшать до 20, и наоборот, если сеть работает устойчиво, то частоту отсылки таких пакетов можно уменьшить путем повышения интервала вплоть до 1000. При этом не стоит забывать, что чрезмерное уменьшение интервала отсылки пакетов синхронизации приведет к увеличению трафика сети и, как следствие, уменьшению скорости передачи полезной информации.
- DTIM — количество отсылаемых пакетов подтверждения о том, когда будет доступно следующее окно для передачи данных. Такие пакеты отсылаются всем

клиентам сети, чтобы они знали, когда можно начинать вещание. Доступные значения — от 1 до 255, по умолчанию установлено значение 1.

- Fragment Length (Объем пакетов данных) — максимальный размер пакета данных, при достижении которого информация разбивается на более мелкие пакеты. По умолчанию для максимального увеличения пропускной способности сети установлено значение 2346, которое при необходимости можно уменьшить до 256.
- RTS Length (Объем пакета RTS). RTS-пакеты служат для отправки в сеть коротких сообщений о том, что один компьютер хочет передать данные другому. При этом пакет содержит информацию об отправителе и получателе, а также любые другие данные, востребованные на данный момент. По умолчанию размер RTS-пакета составляет 2346 бит, но может быть уменьшен вплоть до 256 бит.
- Tx Power (Мощность сигнала) — показатель мощности, с которой передатчик данного устройства передает данные. Этот параметр может принимать значение Full (Полная мощность), Half (Половина мощности), Quarter (Четверть мощности), Eighth (Восьмая часть мощности) или Min (Минимальная мощность). Для переносных устройств потребляемая мощность играет достаточно важную роль, поэтому, если сеть имеет небольшой диаметр, рекомендуется уменьшить мощность передатчика до уровня, который необходим для досягаемости всех устройств сети. Кроме того, регулируя мощность сигнала, можно обеспечить дополнительный уровень безопасности сети, отсекая возможных удаленных «клиентов».
- Auto Channel Scan (Автоматическое сканирование каналов). Очень полезный параметр, отвечающий за использование механизма автоматического сканирования частотного диапазона с целью выявления наименее зашумленного канала. Доступны два значения — Enable (Разрешить) и Disable (Запретить). По понятным причинам рекомендуется установить для этого параметра значение Enable (Разрешить).

11.3. Security (Безопасность)

На вкладке Security (Безопасность) настраивают параметры безопасности беспроводной сети. Без данных настроек сеть представляет собой легкую цель для любителей «покопаться» в чужих данных и украсть что-то ценное.

Содержимое данной вкладки изменяется в зависимости от значений других параметров. Например, она может выглядеть, как на рис. 11.14.

- В области IEEE802.11g расположены параметры, связанные с настройкой протокола безопасности WEP.
  - Authentication (Аутентификация). Данный параметр отвечает за включение или отключение режима аутентификации. Чтобы включить данный режим, достаточно установить соответствующий флажок и выбрать из списка необходимое

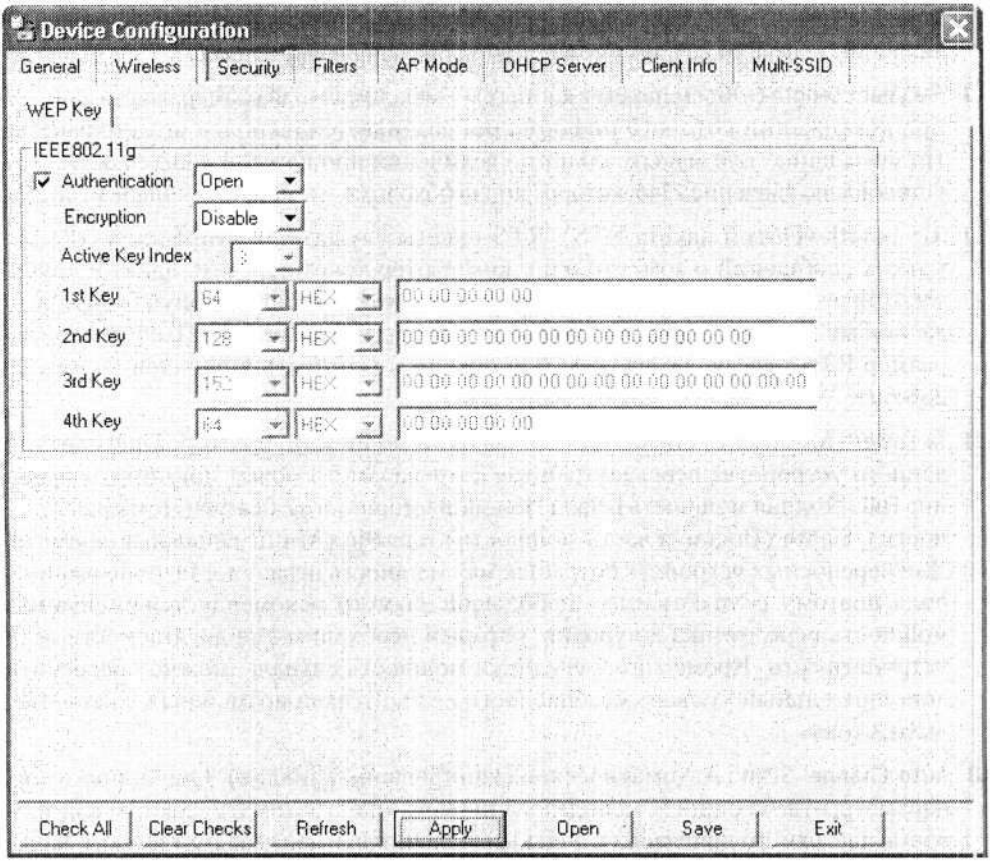

Рис. 11.14. Содержимое вкладки Security (Безопасность)

значение: Open (Открытый), Shared (Разделенный), Both (Оба режима), WPA-EAP или WPA-PSK. При выборе одного из двух последних вариантов в окне появится дополнительная вкладка IEEE.11g WPA с параметрами данного метода аутентификации.

- Encryption (Шифрование). Чтобы включить или отключить использование шифрования, установите для данного параметра значение Enable (Разрешить) или Disable (Запретить) соответственно. Данный параметр доступен, только если параметру Authentication (Аутентификация) присвоено значение Open (Открытый) или Both (Оба). Шифрование рекомендуется использовать в любом случае, иначе в один прекрасный день вы можете обнаружить пропажу важных документов или кражу интернет-трафика.
- Active Key Index (Индекс активного ключа). Данный параметр указывает, какой ключ в данный момент является активным. В принципе, протокол WEP предусматривает использование до четырех ключей шифрования разной длины, однако одновременно несколько ключей применяться не могут. С помощью параметра Active Key Index (Индекс активного ключа) можно указать,

какой из этих ключей следует использовать. В зависимости от указанного номера активизируется конкретный параметр, отвечающий за настройку длины и выбор ключа.

- 1st Key (Первый ключ) — первый ключ шифрования. Можно выбрать длину (64/128/152 бит), символьный тип ключа (HEX или ASCII) и указать сам ключ (сочетание символов выбранного типа).
- 2nd Key (Второй ключ) — второй ключ шифрования. Настройки этого параметра аналогичны предыдущим.
- 3rd Key (Третий ключ) — третий ключ шифрования. Настройки аналогичны.
- 4th Key (Четвертый ключ) — четвертый ключ шифрования. Настройки также аналогичны.

- Область WPA Setting (Настройки WPA) содержит параметры, влияющие на работу протокола безопасности WPA.
  - Cipher Type (Тип шифра) — используемый тип шифрования: Auto (Автоматический выбор), AES или TKIP.
  - Group Key Update Interval (Интервал обновления группового ключа) — интервал времени, по истечении которого произойдет автоматическая замена ключа шифрования. По умолчанию установлено значение 1800, но можно установить его от 300 до 9999999. Задавать слишком малый интервал нежелательно, поскольку это увеличит частоту следования служебных пакетов, в результате чего уменьшится полезная пропускная способность сети. Установка слишком большого интервала не так критична, но в таком случае у злоумышленника будет больше времени для попытки проникновения в сеть.
  - PassPhrase (Пароль) — пароль, применяемый при типе шифрования TKIP. Длина пароля может колебаться от восьми до 63 символов. Учтите, что чем длиннее пароль, тем тяжелее его взломать.
- В области Security Server (Сервер безопасности) можно настраивать параметры RADIUS-сервера аутентификации. Данная область появляется, если параметру Authentication (Аутентификация) присвоено значение WPA-EAP.
  - RADIUS Server (Адрес RADIUS-сервера). Если в сети установлен RADIUS-сервер, то в данном поле следует указать его IP-адрес.
  - RADIUS Port (Порт RADIUS-сервера). Здесь нужно задать порт сервера, через который происходит аутентификация.
  - RADIUS Secret (Пароль RADIUS-сервера). В этом поле указывают пароль доступа к RADIUS-серверу.

11.4. Filters (Фильтры)

На вкладке Filters (Фильтры) (рис. 11.15) настраивают возможность подключения к точке доступа из Ethernet-сети или доступ к параметрам точки доступа для клиентов беспроводной сети.

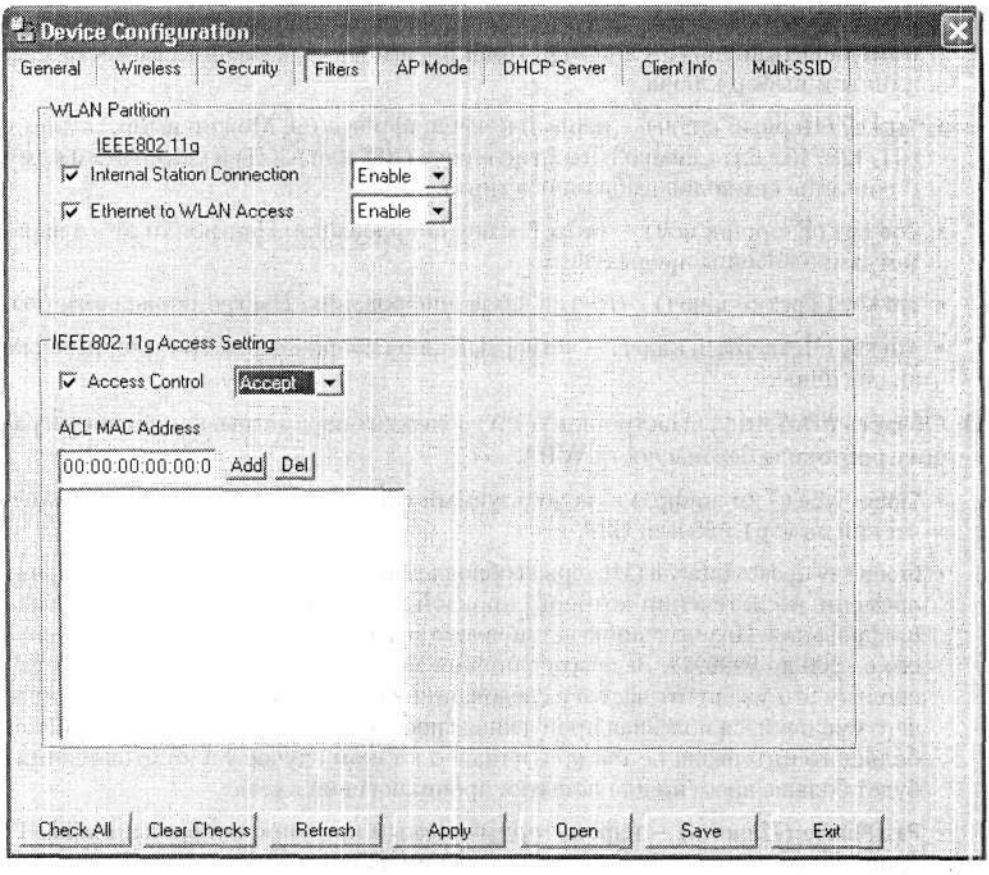

Рис. 11.15. Содержимое вкладки Filters (Фильтры)

Вкладка содержит следующие параметры.

- В области WLAN Partition (WLAN-разделение) расположены параметры настройки доступа из Ethernet-сети к беспроводной.
  - Internal Station Connection (Подключение внутренних станций). Данный параметр отвечает за возможность подключения к точке доступа беспроводных устройств с целью обмена информацией между ними. Если установлено значение Disable (Запретить), то беспроводные станции не смогут подключиться к точке доступа и, соответственно, общаться между собой. По умолчанию этому параметру присвоено значение Enable (Разрешить), и изменять его не рекомендуется. Вы можете задать значение Disable (Запретить), например, при важном администрировании точки доступа, которому не должны мешать беспроводные устройства.
  - Ethernet to WLAN Access (Доступ из сети Ethernet в сеть WLAN). С помощью данного параметра регулируют отношения между клиентами беспроводной сети и проводного сегмента Ethernet. Доступны два значения: Enable (Разрешить)

и Disable (Запретить). При установке значения Disable (Запретить) Ethernet-клиенты не смогут обмениваться информацией с клиентами беспроводной сети, однако клиенты беспроводной сети смогут общаться с клиентами проводной сети. По умолчанию установлено значение Enable (Разрешить), поскольку очень часто точка доступа подключается к маршрутизатору и, соответственно, должен происходить двусторонний обмен данными.

- Область IEEE802.11g Access Setting (Настройка доступа для устройств IEEE802.11g) содержит параметры настройки подключения к точке доступа с использованием списка доступа.

  Access Control (Контроль доступа). С помощью данного параметра организовывают списки подключения к точке доступа, ориентированные на MAC-адреса устройств. Например, введя список MAC-адресов и выбрав для параметра Access Control (Контроль доступа) значение Accept (Принимать), вы позволите этим устройствам подключаться к точке доступа. Если выбрать значение Reject (Отклонять), то устройства с указанным MAC-адресом не смогут подключиться к сети. По умолчанию параметру Access Control (Контроль доступа) присвоено значение Disable (Запретить), отключающее использование этой функции. В таком случае все без исключения устройства смогут подключиться к точке доступа (если не действуют другие правила).

11.5. AP Mode (Режим точки доступа)

Вкладку AP Mode (Режим точки доступа) (рис. 11.16) используют для настройки режима, в котором будет работать точка доступа.

На вкладке расположен только один параметр — AP Mode (Режим точки доступа). При изменении его значения здесь могут появляться дополнительные элементы управления. Данный параметр отвечает за режим, в котором работает устройство, и может принимать следующие значения.

- Access Point (Точка доступа). В этом режиме устройство выполняет свои прямые обязанности — функцию точки доступа. По умолчанию используется именно этот режим.
- WDS with AP. Режим используется для объединения нескольких существующих сетей в одну. При этом выбранная точка доступа является главной. При выборе этого режима на вкладке появляется дополнительный параметр — Remote AP MAC Address (MAC-адреса подключаемых точек доступа), с помощью которого нужно составить список MAC-адресов всех соединяемых точек доступа. Учтите, что при использовании этого режима в качестве всех соединяемых точек доступа должны быть устройства D-Link DWL-2100AP.
- WDS. Данный режим применяют для объединения нескольких существующих сетей в одну. При его выборе на вкладке появляется дополнительный параметр — Remote AP MAC Address (MAC-адреса подключаемых точек доступа), с помощью которого нужно составить список MAC-адресов всех соединяемых точек доступа.

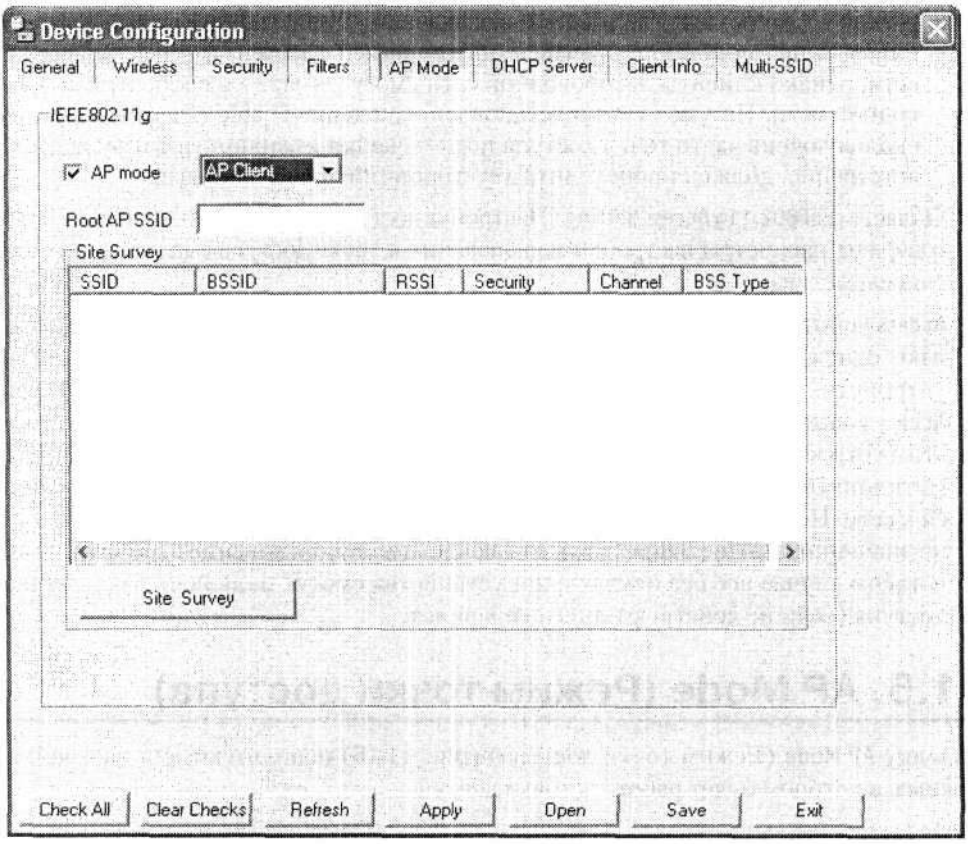

Рис. 11.16. Содержимое вкладки AP Mode (Режим точки доступа)

При использовании этого режима в качестве всех соединяемых точек доступа должны выступать D-Link DWL-2100AP.

- AP Repeater (Повторитель). Режим применяют для увеличения радиуса существующей сети путем ретрансляции сигнала от главной точки доступа. При активизации этого режима на вкладке появляется дополнительный параметр — Remote AP MAC Address (MAC-адреса подключаемых точек доступа), с помощью которого нужно указать MAC-адрес главной точки доступа. Для облегчения настройки этого параметра можно воспользоваться механизмом обзора существующих точек доступа, который запускают нажатием кнопки Site Survey (Обзор узлов).
- AP Client (Клиент). Данный режим используется, когда к беспроводной сети необходимо подключить Ethernet-устройство, например компьютер или принтер. При активизации этого режима на вкладке появляется дополнительное поле — Root AP SSID (SSID точки доступа), в котором нужно указать SSID устройства, выполняющего функции точки доступа. При использовании этого режима указываемой точкой доступа должна быть D-Link DWL-2100AP. Для

облегчения поиска нужного SSID можно воспользоваться механизмом обзора существующих точек доступа, который запускают нажатием кнопки Site Survey (Обзор узлов).

11.6. DHCP Server (Сервер DHCP)

Вкладка DHCP Server (Сервер DHCP) (рис. 11.17) содержит параметры DHCP-сервера, механизм которого встроен в точку доступа D-Link DWL-2100AP.

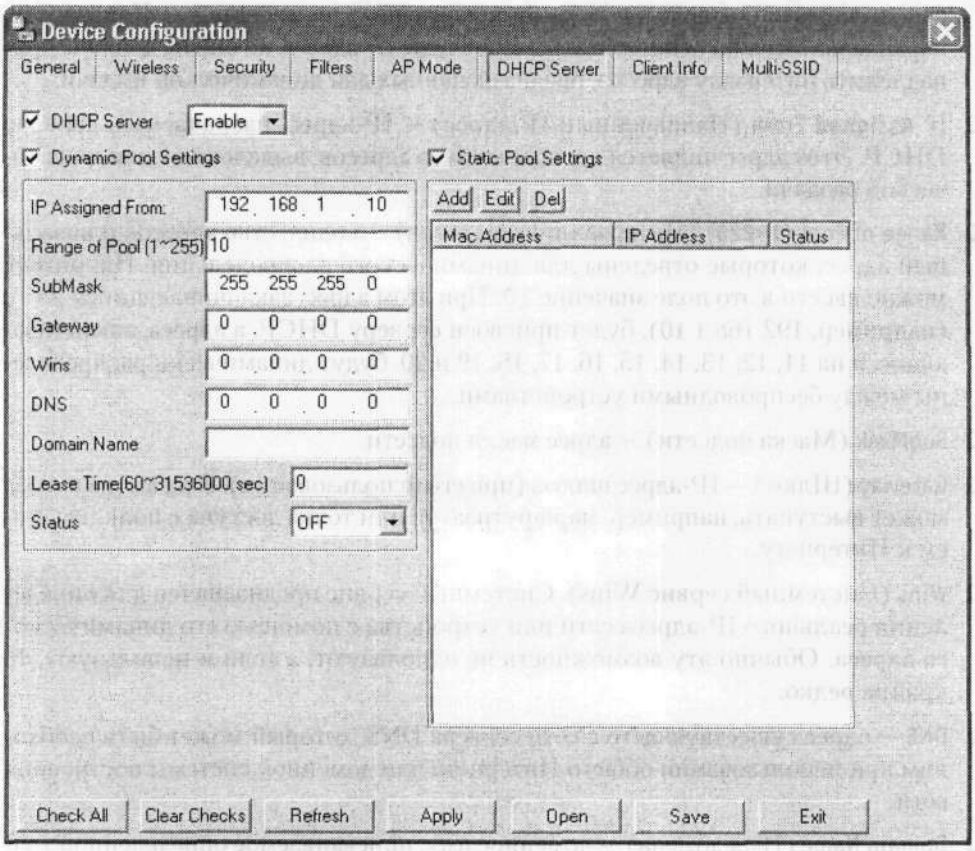

Рис. 11.17. Содержимое вкладки DHCP Server (Сервер DHCP)

На данной вкладке расположены такие параметры.

- DHCP Server (Сервер DHCP). Этот параметр может принимать одно из двух возможных значений — Enable (Разрешить) или Disable (Запретить). Первое активизирует встроенный сервер DHCP, а второе его отключает.

  По умолчанию параметру DHCP Server (Сервер DHCP) задано значение Disable (Запретить). В сети должен быть только один сервер DHCP, который чаще всего

установлен на главной точке доступа. Поэтому, прежде чем задать этому параметру значение Enable (Разрешить), убедитесь, что в сети нет активного сервера DHCP. После включения сервера DHCP активизируются параметры Dynamic Pool Settings (Динамические установки пула адресов) и Static Pool Settings (Статичные установки пула адресов), с помощью которых необходимо настроить пул адресов, выдаваемых устройствам беспроводной сети.

- Dynamic Pool Settings (Динамические установки пула адресов). Задав этому параметру значение Enable (Разрешить), вы активизируете автоматическую раздачу адресов устройствам сети. При этом адреса будут генерироваться динамически, основываясь на интервальных данных, введенных пользователем. Конечно же, параллельно можно использовать и статичные IP-адреса, но они не должны принадлежать интервалу адресов, предназначенных для динамической выдачи.
- IP Assigned From (Назначенный IP-адрес) — IP-адрес, назначаемый серверу DHCP. Этот адрес является первым из пула адресов, выделенных для динамической раздачи.
- Range of Pool (1~225) (Интервал пула адресов) — количество адресов и начальный адрес, которые отведены для динамического распределения. Например, можно ввести в это поле значение 10. При этом адрес, заканчивающийся на 10 (например, 192.168.1.10), будет присвоен серверу DHCP, а адреса, заканчивающиеся на 11, 12, 13, 14, 15, 16, 17, 18, 19 и 20, будут динамически распределены между беспроводными устройствами.
- SubMask (Маска подсети) — адрес маски подсети.
- Gateway (Шлюз) — IP-адрес шлюза (при его использовании). В качестве шлюза может выступать, например, маршрутизатор или точка доступа с подключением к Интернету.
- Wins (Системный сервис Wins). Системный сервис предназначен для определения реального IP-адреса сети или устройства с помощью его динамического адреса. Обычно эту возможность не используют, а если и используют, то крайне редко.
- DNS — адрес существующего в сети сервера DNS, который может быть необходим при использовании общего Интернета или доменной системы построения сети.
- Domain Name (Имя домена) — доменное имя, присваиваемое определенной точке доступа с целью организации доменной системы сети.
- Lease Time (60~31536000 sec) (Продолжительность использования) — временной интервал, в течение которого беспроводные клиенты могут использовать назначенные им динамические адреса. По умолчанию параметру присвоено значение 0, что говорит о том, что адрес может использоваться бесконечно долго.
- Status (Состояние). Значение OFF (Отключить) данного параметра приводит к отключению созданного пула адресов, что аналогично отключению сервера DHCP. По умолчанию параметру задано значение ON (Включить).

- Static Pool Settings (Статичные установки пула адресов). Этот параметр предназначен для назначения статичного адреса важным устройствам сети, например серверам или сетевым принтерам. Для этого следует установить флажок Static Pool Settings (Статичные установки пула адресов), после чего с помощью кнопок Add (Добавить), Edit (Редактировать) и Del (Удалить) настроить список статичных адресов. При этом нужно иметь в виду, что эти адреса не должны принадлежать интервалу адресов, указанных в поле Range of Pool (1~225) (Интервал пула адресов).

11.7. Client Info (Сведения о клиентах)

Вкладка Client Info (Сведения о клиентах) (рис. 11.18) не содержит никаких настраиваемых параметров и является информационной.

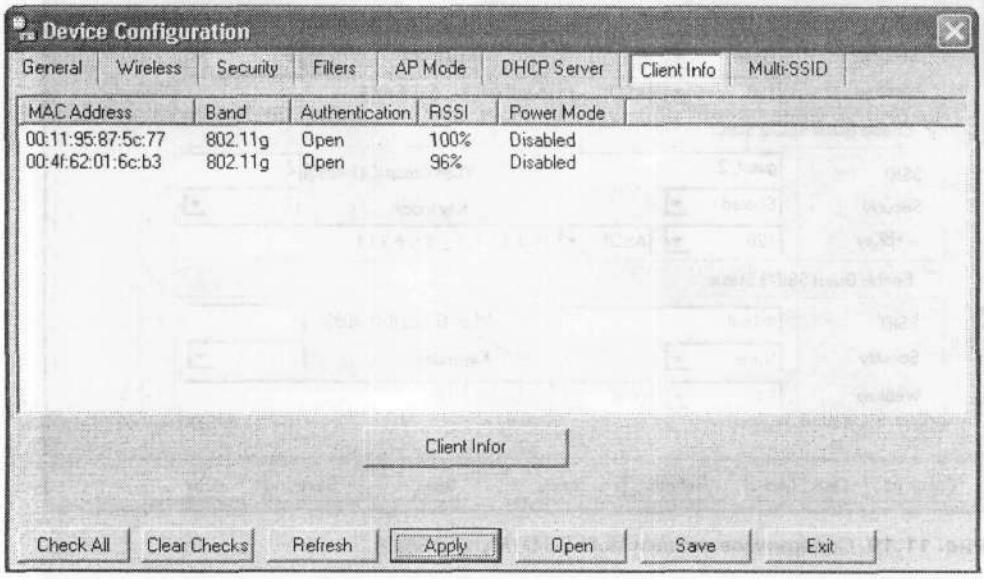

Рис. 11.18. Содержимое вкладки Client Info (Сведения о клиентах)

Здесь можно ознакомиться с информацией о беспроводных клиентах, подключенных к этой точке доступа. Чтобы произвести опрос клиентов, необходимо нажать кнопку Client Infor (Информатор клиентов). В результате вы увидите данные о MAC-адресе, беспроводном стандарте устройства, режиме аутентификации, мощности сигнала и установленном режиме энергосбережения. Например, на рис. 11.18 видно, что к точке доступа в данный момент подключено два беспроводных клиента.

11.8. Multi-SSID (Мульти SSID)

На вкладке Multi-SSID (Мульти SSID) (рис. 11.19) можно настроить дополнительные SSID, чтобы организовывать виртуальные сети и разграничивать подключения

к точке доступа на уровне гостевых SSID. Это возможно благодаря наличию в D-Link DWL-2100AP соответствующего механизма, чем может похвастаться не каждая точка доступа.

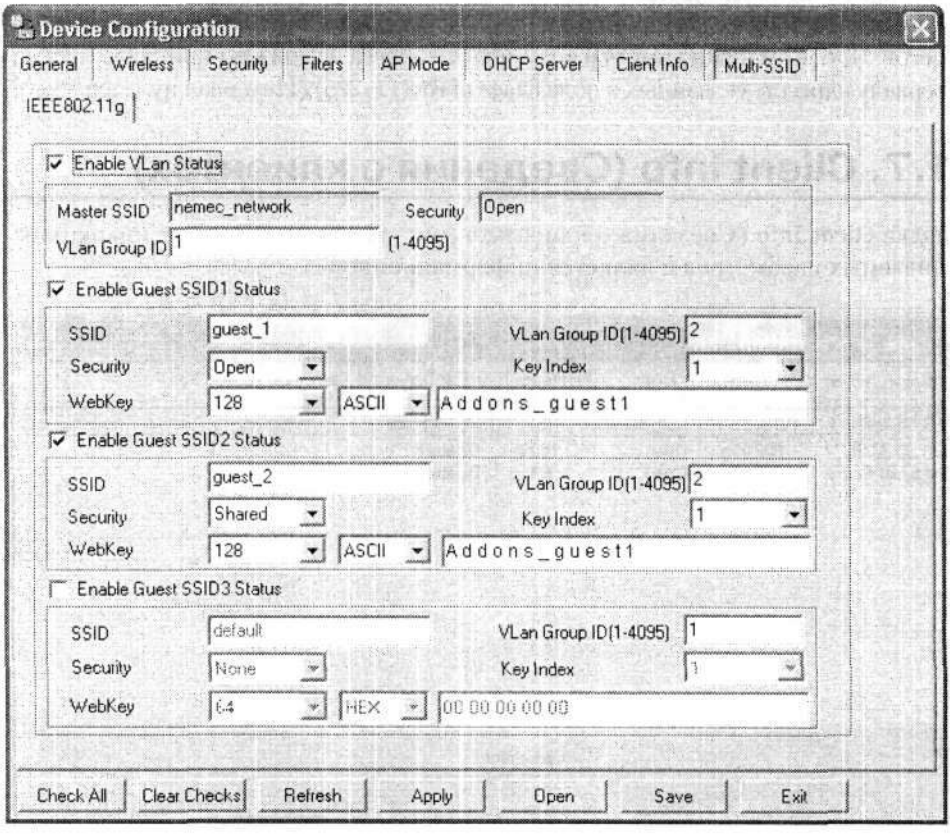

Рис. 11.19. Содержимое вкладки Multi-SSID (Мульти SSID)

На вкладке находятся четыре области с параметрами. При этом параметры, расположенные в трех нижних областях, идентичны, однако относятся к разным SSID. Таким образом, на данной вкладке вы можете настроить до трех разных гостевых SSID.

- Enable VLan Status (Разрешить виртуальные сети). По умолчанию возможность использования нескольких SSID отключена. Чтобы ее включить, необходимо установить данный флажок. После этого следует настроить параметры, расположенные в этой области.
  - Master SSID (Главный SSID). Значение этого поля не изменяется, поскольку оно соответствует значению SSID точки доступа, заданному ранее.
  - Security (Безопасность). Значение этого поля также не подлежит редактированию. Здесь отображается выбранный механизм безопасности, например Open (Открытый) или Shared (Разделенный).

- VLan Group ID (Идентификатор виртуальной группы). Создаваемые виртуальные группы отличаются номерами, для которых выделено более 4000 номеров начиная с единицы. Как правило, основной группе (то есть содержащей главный SSID) присваивают единицу, как и показано на рис. 11.19.

❑ Область Enable Guest SSID1 Status (Разрешить гостевой SSID1) содержит параметры, описывающие дополнительный SSID, в частности SSID1. Чтобы активизировать такую возможность, необходимо установить данный флажок.

- SSID. В этом поле отображается уникальный идентификатор. При выборе этого идентификатора необходимо придерживаться тех же правил, что и при выборе главного SSID. Это особенно важно, если точка доступа не вещает SSID, так как для подключения к сети нужно точно знать его. Использование данного параметра помогает избежать нежелательных подключений к сети.
- Security (Безопасность) — метод аутентификации. Дополнительная настройка метода аутентификации возможна лишь в том случае, если параметру Security (Безопасность) в области Enable VLan Status (Разрешить виртуальные сети) присвоено значение Open (Открытый) или Shared (Разделенный). В таком случае вы можете выбрать из раскрывающегося списка необходимое значение: None (Никакой), Open (Открытый) или Shared (Разделенный).
- WebKey (Ключ). Из этого раскрывающегося списка можно выбрать длину ключа шифрования, который будет применяться для шифрования данных, передаваемых в сети между устройствами, использующими гостевой SSID1. Длина ключа может составлять 64, 128 или 152 бит. После выбора длины необходимо сразу же выбрать тип символьной строки (HEX или ASCII), представляющей ключ, и сам ключ.
- VLan Group ID (Идентификатор виртуальной группы). Создаваемая виртуальная группа должна обладать своим уникальным номером. В его качестве можно использовать любой номер от 1 до 4095, отличный от номера главной виртуальной группы. В рассматриваемом примере главной виртуальной группе присвоен номер 1, а группе с гостевым SSID1 — 2.
- Key Index (Номер ключа). Для шифрования данных может использоваться до четырех ключей разной или одинаковой длины. Переключаться между ними можно с помощью этого раскрывающегося списка.

Таким же образом можно при необходимости настроить еще два гостевых SSID.

ГЛАВА 12 Настройка сети в Windows 2000

- Подключение к сетевой группе
- Настройка протокола TCP/IP
- Предоставление доступа к файловым ресурсам
- Предоставление доступа к принтеру
- Использование сетевых ресурсов

Операционная система Microsoft Windows 2000 является достаточно популярной среди пользователей. Напомню, она является прямой последовательницей системы Windows NT и обладает по сравнению с ней неоспоримыми преимуществами, не говоря уже об уровне защищенности и интеллектуальности.

Существуют разные модификации Windows 2000, однако чаще всего на домашних или офисных клиентских компьютерах установлена версия Microsoft Windows 2000 Professional.

12.1. Подключение к сетевой группе

Для работы компьютера с установленной операционной системой Windows 2000 в беспроводной сети необходимо, чтобы он принадлежал к соответствующей сетевой группе. Поэтому в первую очередь необходимо изменить определенные настройки в свойствах сетевой идентификации компьютера.

Чтобы изменить сетевую идентификацию компьютера, необходимо открыть окно его свойств. Это можно сделать по-разному, например с помощью Панели управления. Для этого выполните команду Пуск ▸ Настройка ▸ Панель управления и в появившемся окне (рис. 12.1) щелкните на значке Система.

Рис. 12.1. Панель управления Windows 2000 Professional

В результате на экране появится окно свойств системы, содержащее несколько вкладок (рис. 12.2). Перейдите на вкладку Сетевая идентификация. Здесь можно не только настроить сетевую идентификацию компьютера, но и увидеть установленные параметры идентификации. Например, в рассматриваемом случае компьютеру присвоено имя my и он принадлежит к группе NONE.

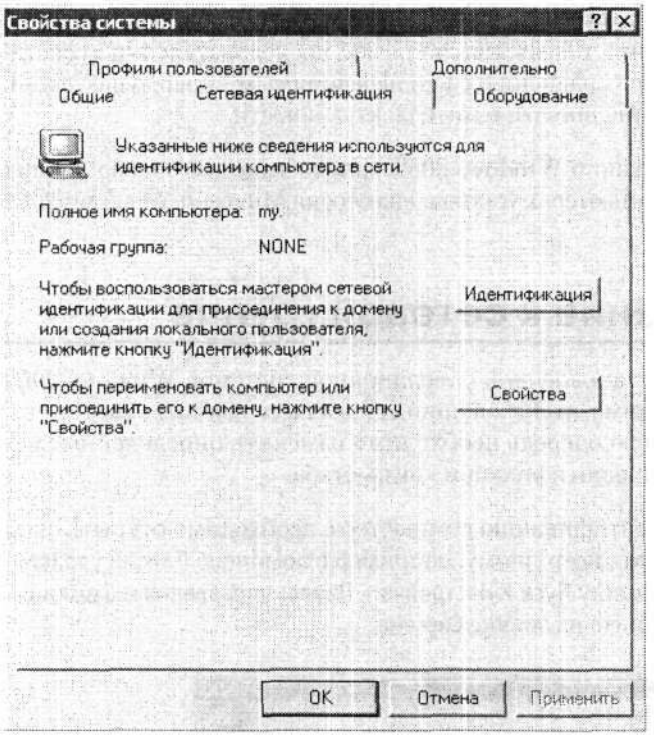

Рис. 12.2. Окно свойств системы

Существует два способа изменения сетевой идентификации. Первый способ занимает больше времени, зато он более информативный и понятный, а также позволяет настраивать подключение к домену, однако не дает возможности изменить сетевое имя компьютера. Второй способ более быстрый; кроме того, с его помощью вы сможете изменить сетевое имя компьютера. Рассмотрим оба способа.

Подключение к сетевой группе без доменной системы

Рассмотрим настройку компьютера для подключения к сетевой группе сети, которая не использует доменную систему.

В окне свойств системы нажмите кнопку Идентификация. Появится окно Мастера сетевой идентификации (рис. 12.3), который будет помогать вам при настройке.

Для запуска процесса настройки нажмите кнопку Далее.

В следующем окне мастер настройки спросит вас, входит ли компьютер в состав корпоративной сети (рис. 12.4). Поскольку вы собираетесь подключить компьютер к существующей сетевой группе, необходимо установить переключатель в положение Компьютер входит в корпоративную сеть, и во время работы я использую его для соединения с другими компьютерами.

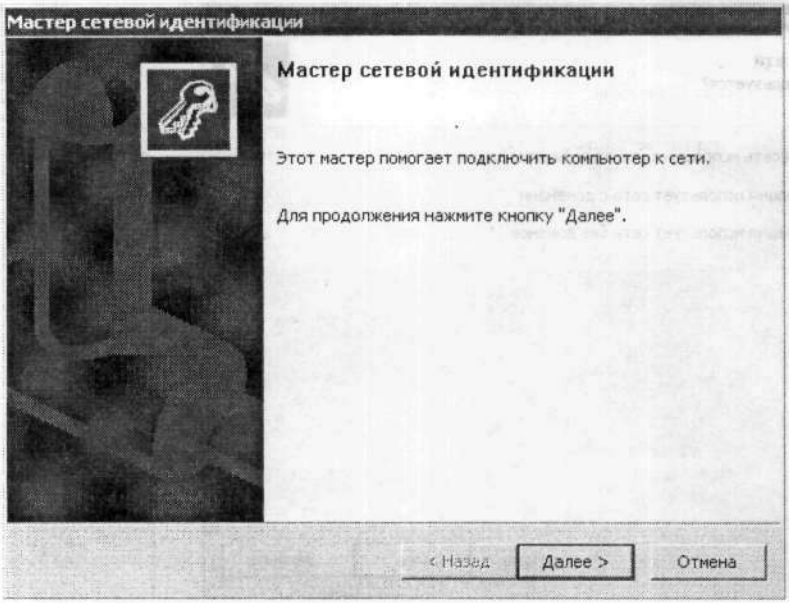

Рис. 12.3. Окно мастера настройки сетевой идентификации

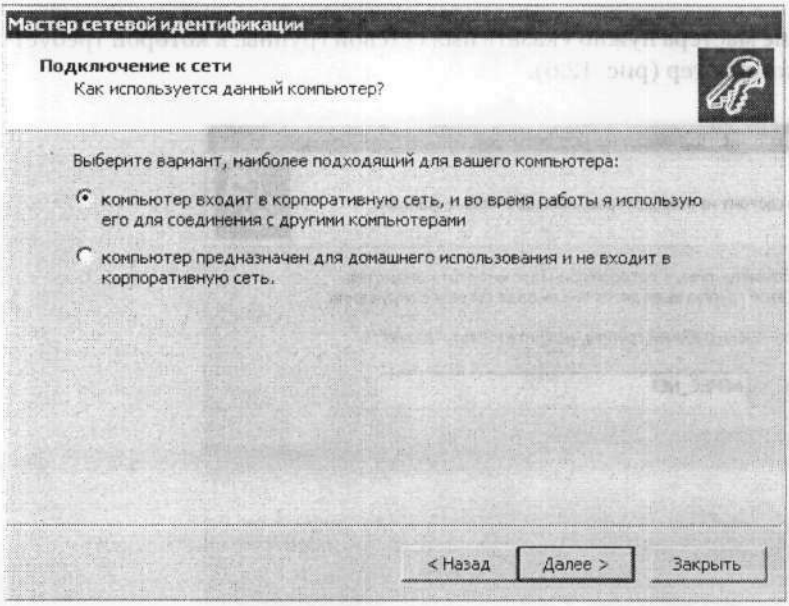

Рис. 12.4. Выбираем первый вариант

После нажатия кнопки Далее откроется окно, в котором мастер спросит вас о типе используемой сети (рис. 12.5). Установите переключатель в положение Моя организация использует сеть без доменов.

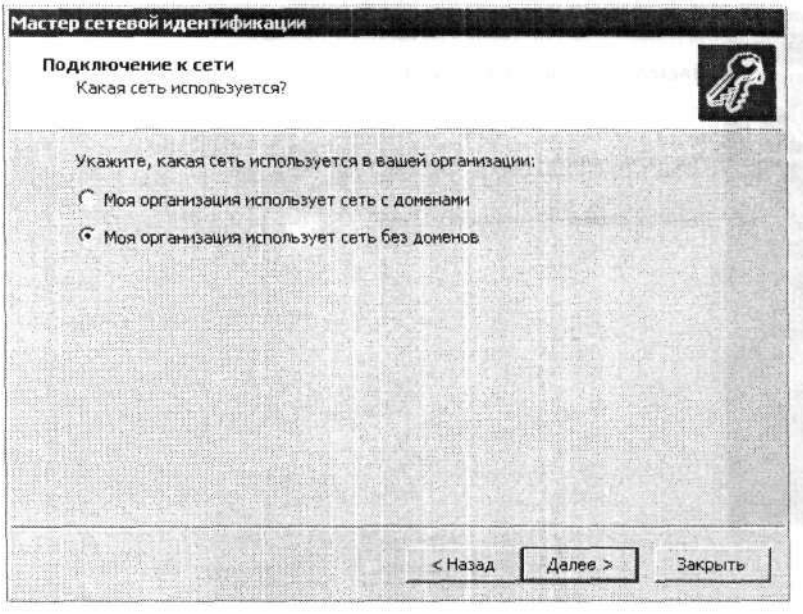

Рис. 12.5. Устанавливаем переключатель в положение Моя организация использует сеть без доменов

В следующем окне мастера нужно указать имя сетевой группы, к которой требуется подключить компьютер (рис. 12.6).

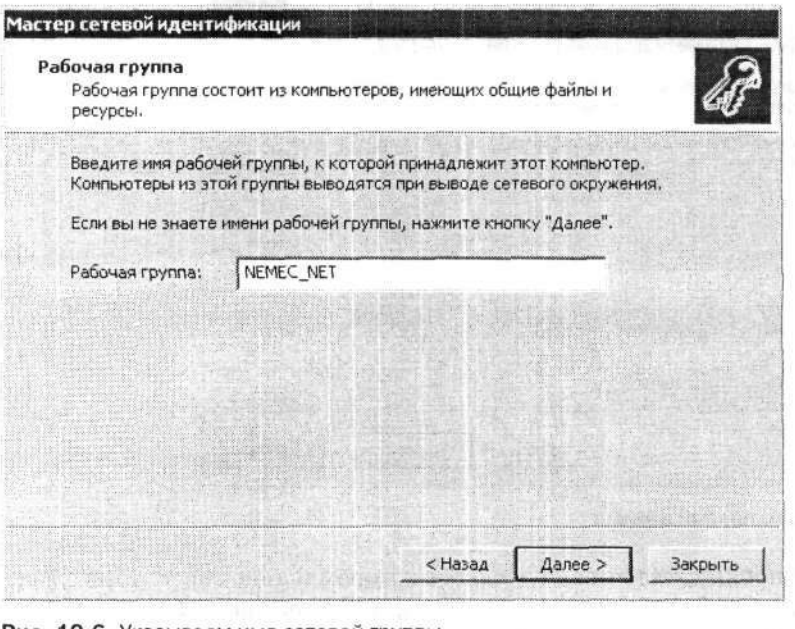

Рис. 12.6. Указываем имя сетевой группы

После нажатия кнопки Далее появится окно, сообщающее о завершении процесса настройки (рис. 12.7).

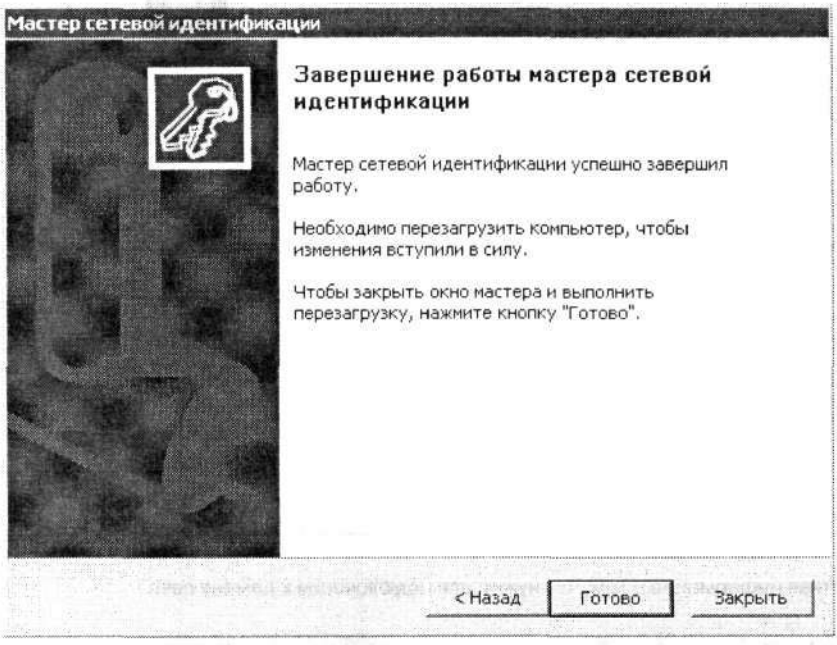

Рис. 12.7. Мастер завершил настройку сетевого идентификатора

Из этого же окна вы узнаете, что для вступления изменений в силу необходимо перезагрузить компьютер. Если вы не планируете продолжать настройку, последуйте этому предложению.

Подключение к сетевой группе с доменной системой

Подключение к сети, использующей доменную систему, в принципе, ничем не отличается от подключения к сети без доменов. Единственная разница в том, что в этом случае необходимо ввести имя пользователя и пароль для доступа к домену. Однако рассмотрим все по порядку.

Начнем с окна, показанного на рис. 12.5. Установите переключатель в положение Моя организация использует сеть с доменами и нажмите кнопку Далее.

Появится информационное окно (рис. 12.8), сообщающее, что для подключения к домену понадобятся, как минимум, имя и пароль пользователя, имеющего право подключения к домену.

Ознакомившись с этой информацией и узнав у администратора сети необходимые данные, нажмите кнопку Далее. Появится окно, в котором следует ввести имя пользователя, пароль и домен (рис. 12.9).

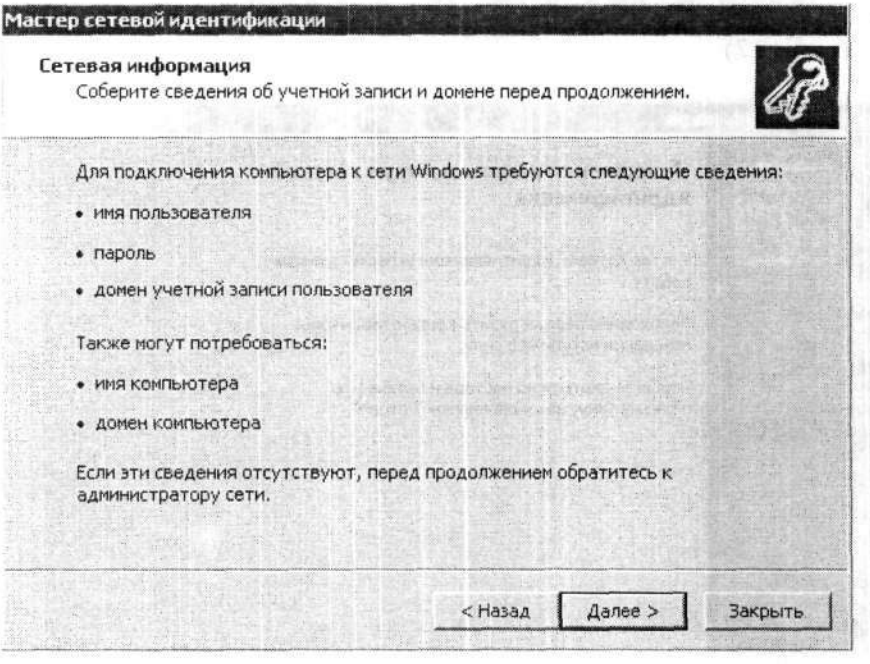

Рис. 12.8. Краткая информация о том, что нужно для подключения к домену сети

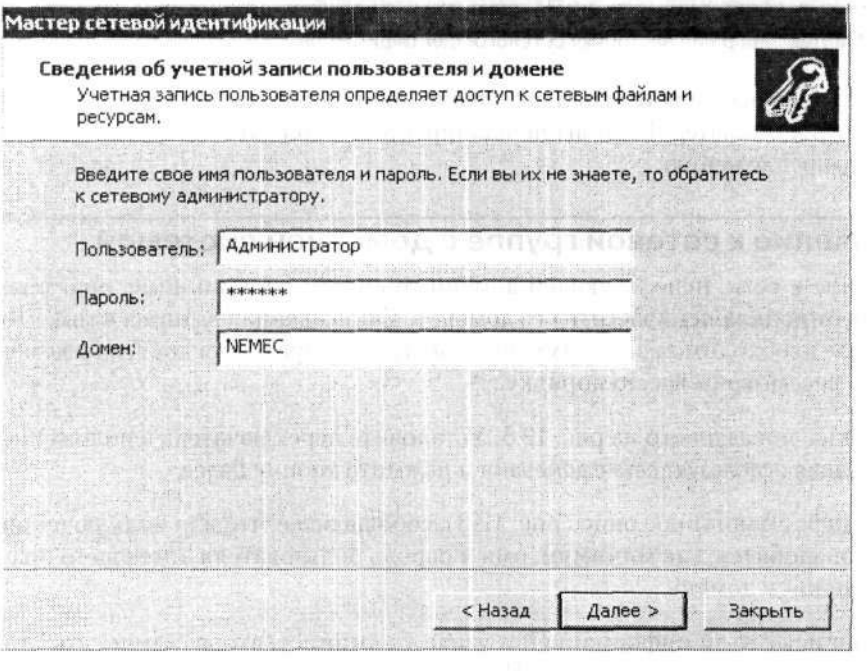

Рис. 12.9. Вводим имя пользователя, пароль и имя домена, к которому необходимо подключиться

ПРИМЕЧАНИЕ

При попытке подключения к домену система проверяет наличие указанного имени пользователя в системе регистрации пользователей, в качестве которой, как правило, выступает системный механизм Active Directory. Естественно, если информация об указанном пользователе отсутствует, получить доступ к домену вы не сможете. В этом случае необходимо обратиться к администратору сети (домена), чтобы ввести новые данные или проверить существование указанного пользователя.

В зависимости от скорости передачи данных в сети и загруженности домена процесс подключения может занять некоторое время, поэтому запаситесь терпением. После успешного подключения необходимо перезагрузить компьютер, чтобы изменения вступили в силу (рис. 12.10).

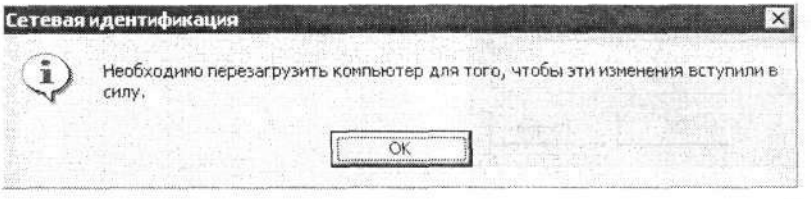

Рис. 12.10. Сообщение системы

Изменение имени компьютера

Имя компьютера — это идентификатор, по которому компьютер определяется в сетевом окружении. Зная этот идентификатор, другие пользователи могут подключиться к ресурсам компьютера.

В принципе, особой смысловой нагрузки изменение имени компьютера не несет. Однако иногда полезно давать компьютеру имя, однозначно указывающее на его владельца или месторасположение.

Чтобы переименовать компьютер, нажмите в окне, изображенном на рис. 12.2, кнопку Свойства. В результате откроется окно, содержащее несколько полей для ввода (рис. 12.11). В поле Имя компьютера нужно ввести требуемый идентификатор.

После нажатия кнопки OK система попросит вас перезагрузить компьютер, чтобы изменения вступили в силу.

12.2. Настройка протокола TCP/IP

Как и в любой другой операционной системе, в Windows 2000 необходимо настроить параметры протокола, используемого при беспроводном подключении. Рассмотрим пример настройки протокола TCP/IP, если в беспроводной сети применяется статичная адресация.

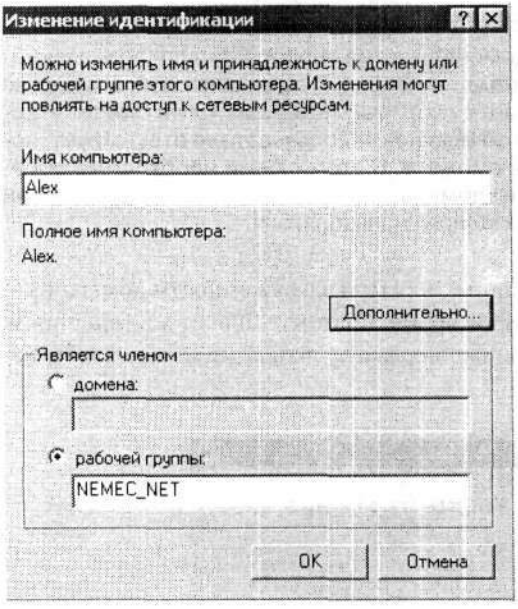

Рис. 12.11. Указываем имя компьютера

Найдите на Рабочем столе значок Мое сетевое окружение, щелкните на нем правой кнопкой мыши и в появившемся контекстном меню (рис. 12.12) выберите пункт Свойства.

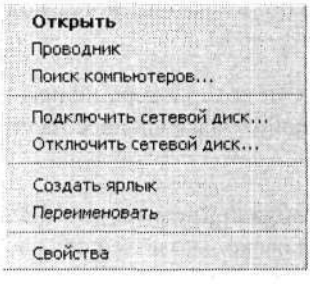

Рис. 12.12. Контекстное меню значка Мое сетевое окружение

В результате на экране появится окно Сеть и удаленный доступ к сети, в котором отобразятся существующие сетевые подключения. Количество сетевых подключений может быть разным в зависимости от количества установленных сетевых адаптеров и сетей, к которым вы подключены.

Щелкните правой кнопкой мыши на значке подключения к беспроводной сети и в появившемся меню выберите пункт Свойства (рис. 12.13).

Откроется окно свойств сетевого подключения, в котором отображены его действующие настройки, а также используемые службы и протоколы (см. рис. 9.2).

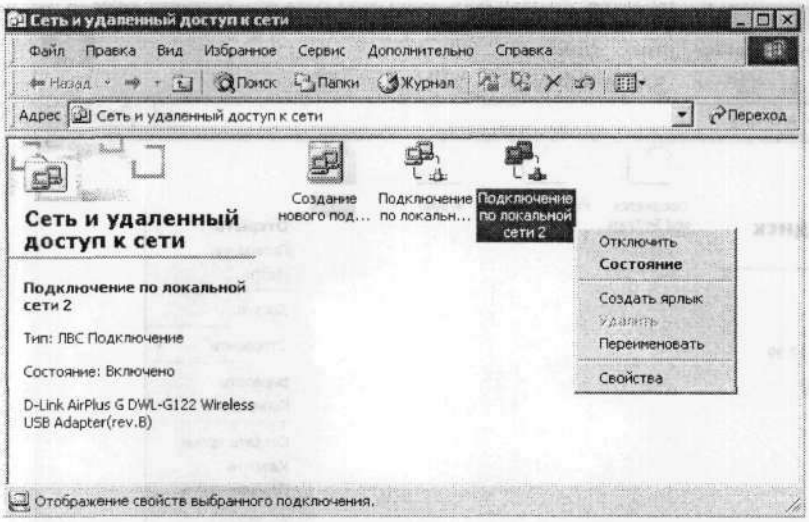

Рис. 12.13. Контекстное меню подключения в окне Сеть и удаленный доступ к сети

Как уже упоминалось, для настройки параметров протокола TCP/IP следует выделить соответствующий пункт и нажать кнопку Свойства (или просто дважды щелкнуть на нем левой кнопкой мыши). В результате откроется окно, в котором можно задать или изменить параметры TCP/IP-протокола. Узнав у администратора сети, какой IP-адрес вы можете использовать для подключения, введите его в соответствующее поле. Затем можно при желании изменить маску подсети.

Если в вашей сети используется интернет-шлюз или DNS-сервер, введите необходимые данные в соответствующие поля данного окна.

После изменения необходимых параметров перезагрузите компьютер.

12.3. Предоставление доступа к файловым ресурсам

Сеть без ресурсов — как автомобиль без колес: вроде все есть, но чего-то не хватает. Основное назначение сети заключается именно в использовании общих ресурсов.

Чтобы открыть доступ к дискам или папкам, можно воспользоваться любым окном, отображающим файлы и папки, например Проводником. Решив, какую папку необходимо предоставить для общего пользования, щелкните на ней правой кнопкой мыши и в появившемся контекстном меню выберите пункт Доступ (рис. 12.14).

Откроется окно свойств выбранного объекта, содержащее несколько вкладок. Чтобы настроить общий доступ к этому объекту, перейдите на вкладку Доступ. Здесь расположено всего несколько параметров, которые можно изменить (рис. 12.15).

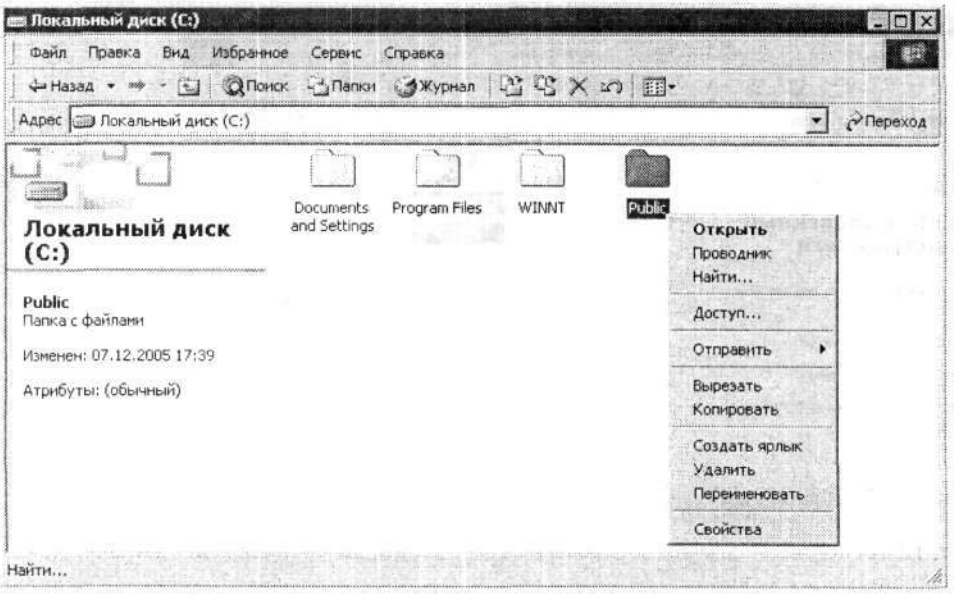

Рис. 12.14. Контекстное меню папки, предназначенной для общего доступа

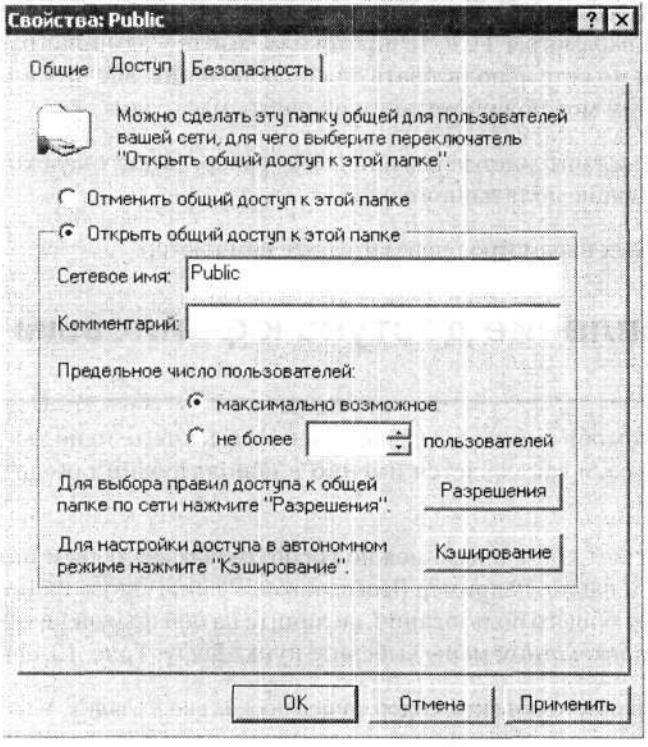

Рис. 12.15. Содержимое вкладки Доступ

Установите переключатель в положение Открыть общий доступ к этой папке. Затем в соответствующих полях укажите имя ресурса и, при необходимости, короткий комментарий. После этого задайте количество одновременных подключений к ресурсу. Если ваш компьютер достаточно маломощный и вы предполагаете частое использование вашего ресурса, то можно настроить одновременный доступ к нему небольшого количества пользователей, например трех или пяти. Если компьютер обладает достаточным быстродействием, то одновременный доступ пользователей можно не ограничивать, установив переключатель в положение максимально возможное.

Самым главным механизмом настройки общего ресурса является назначение прав доступа. Если компьютер не входит в состав домена, то этот процесс очень простой, чего не скажешь о настройке прав в сети, использующей доменную систему.

Для назначения прав доступа нажмите кнопку Разрешения. В результате откроется окно со списком групп и пользователей, которые имеют право на доступ к предоставляемому ресурсу (рис. 12.16). По умолчанию для всех пользователей задан полный доступ к ресурсу. Конечно, по многим причинам, которые даже нет смысла объяснять, это не совсем приемлемо. Поэтому существует возможность назначения отдельных прав для каждой группы или пользователя.

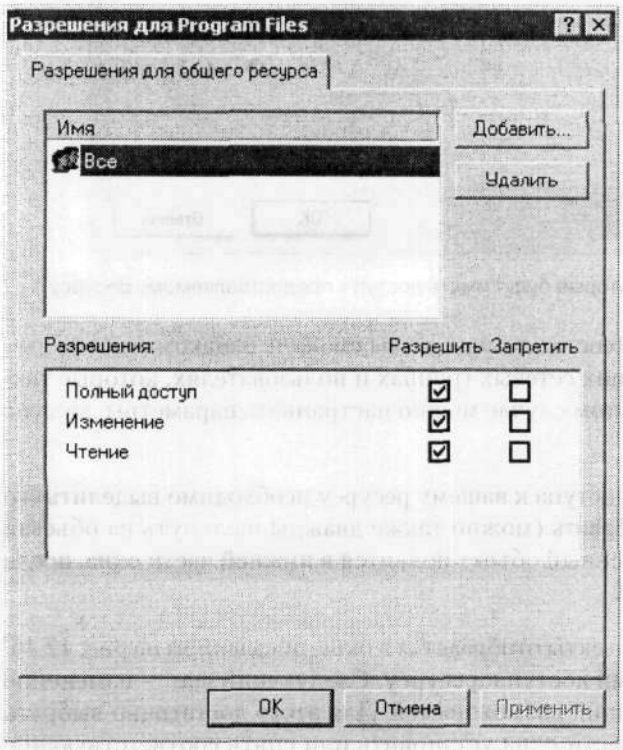

Рис. 12.16. Окно настройки прав доступа

После нажатия кнопки Добавить откроется окно со списком всех найденных сетевых и локальных объектов, которые могут получить доступ к ресурсу (рис. 12.17). Если ваш компьютер не входит в состав домена, то вы не сможете увидеть существующие сетевые группы и пользователей. В этом случае единственное, что можно сделать, — выбрать из списка группу Сеть, которая отвечает за сетевые подключения.

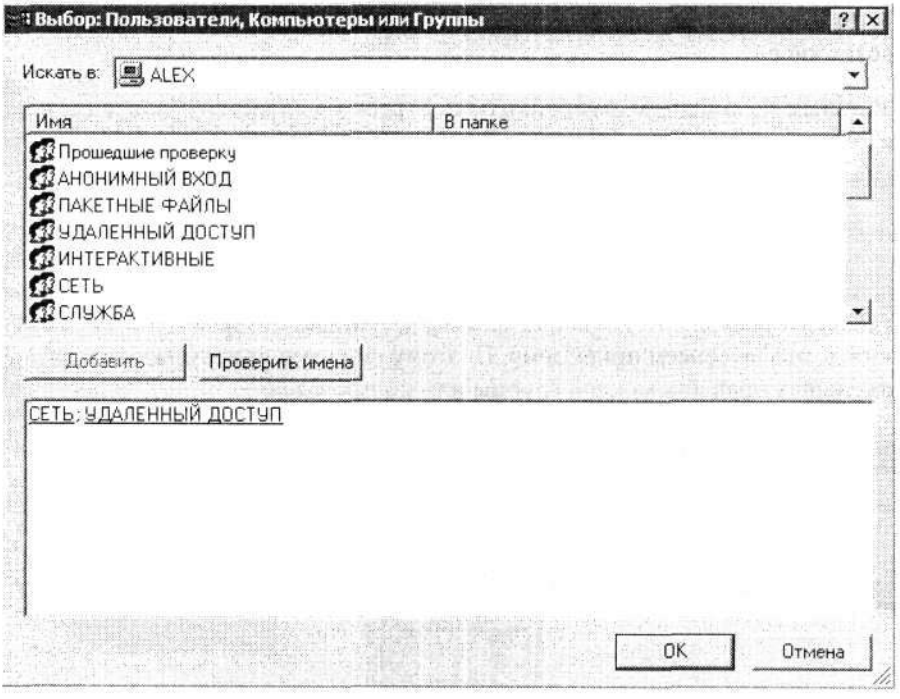

Рис. 12.17. Выбираем объекты, которые будут иметь доступ к предоставляемому ресурсу

Если ваш компьютер входит в состав домена, то вы сможете ознакомиться со сведениями обо всех существующих сетевых группах и пользователях, которые также входят в состав домена. В этом случае можно настраивать параметры доступа с большей скрупулезностью.

Для предоставления объекту доступа к вашему ресурсу необходимо выделить его в списке и нажать кнопку Добавить (можно также дважды щелкнуть на объекте левой кнопкой мыши). Выделенный объект появится в нижней части окна, после чего следует нажать кнопку OK.

В итоге все выбранные вами объекты отобразятся в окне, показанном на рис. 12.16. Им будет предоставлен полный доступ к ресурсу. Следующий шаг — изменение прав, то есть отключение лишних возможностей. Для этого достаточно выбрать объект в списке и в нижней части окна установить или снять соответствующие флажки.

Настроив права доступа, нажмите кнопку OK. Внешний вид значка объекта, предназначенного для общего доступа, изменится (рис. 12.18).

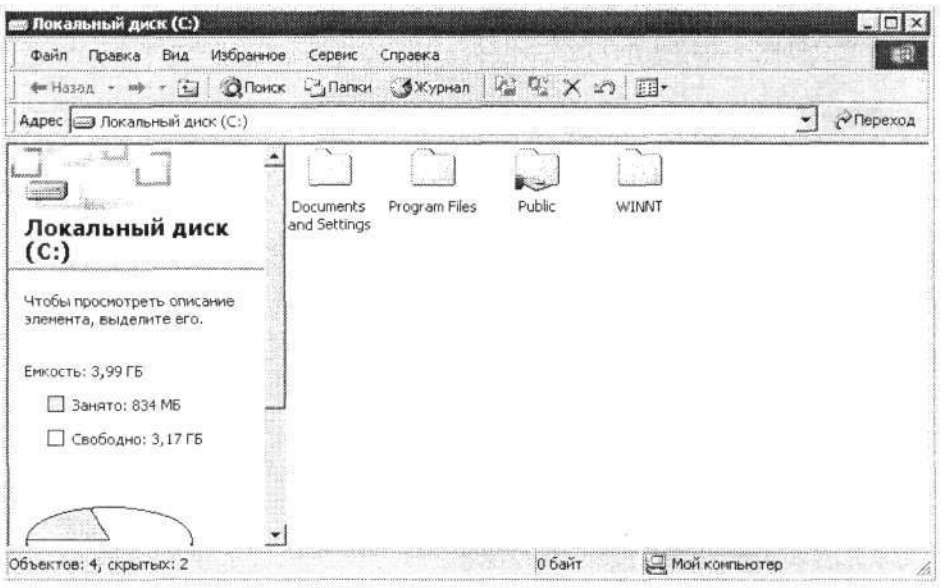

Рис. 12.18. Отображение папки с общим ресурсом

Подобным образом можно предоставить для общего использования любое количество ресурсов. Главное — уследить за их правильным использованием, чтобы потом не пришлось переустанавливать систему в результате сбоя.

12.4. Предоставление доступа к принтеру

Предоставление пользователям сети прав для использования вашего принтера, в принципе, не отличается от предоставления доступа к файловым ресурсам вашего компьютера.

Выполните команду Пуск ▸ Настройка ▸ Принтеры. Откроется окно со списком принтеров, используемых в системе. Выберете из списка принтер, доступ к которому вы хотите открыть. Щелкнув правой кнопкой мыши на значке принтера, выберите в появившемся контекстном меню пункт Общий доступ.

Появится окно свойств выбранного принтера, содержащее множество вкладок. Перейдите на вкладку Доступ и установите переключатель в положение Общий ресурс (рис. 12.19).

Теперь необходимо указать, кто может использовать этот принтер. Для этого перейдите на вкладку Безопасность (рис. 12.20). По умолчанию некоторые пользователи и группы уже имеют доступ к устройству, однако все они являются пользователями

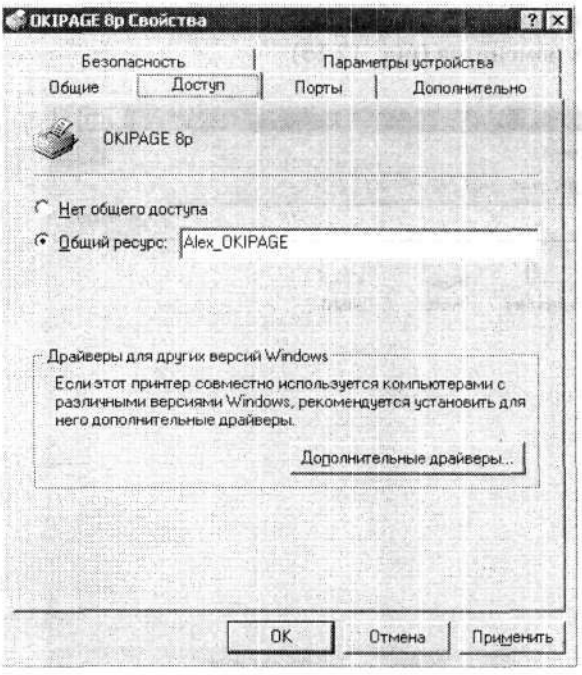

Рис. 12.19. Устанавливаем переключатель в положение Общий ресурс

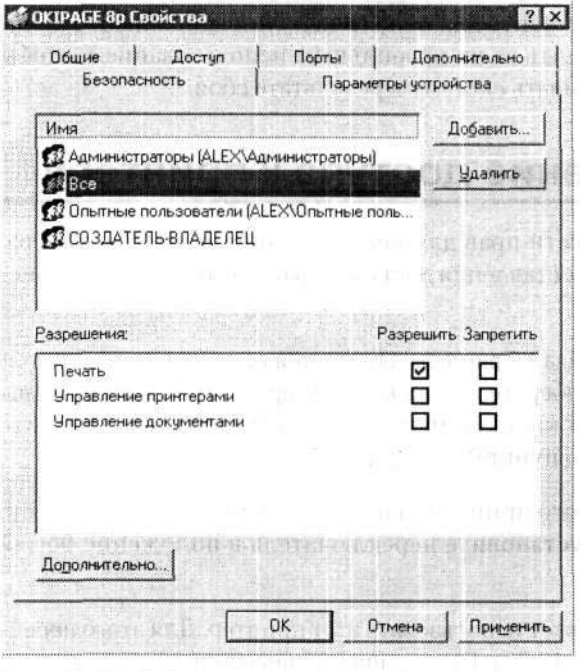

Рис. 12.20. Добавляем пользователей и настраиваем права доступа

данного компьютера. Чтобы разрешить использование принтера компьютерам, подключенным к сети, необходимо нажать кнопку Добавить и выбрать из списка нужные позиции, как при настройке общего доступа к файловым ресурсам.

Выполнив необходимые изменения, нажмите кнопку OK, чтобы подтвердить свои действия. Значок принтера, предоставленного в общее использование, изменит свой внешний вид (рис. 12.21).

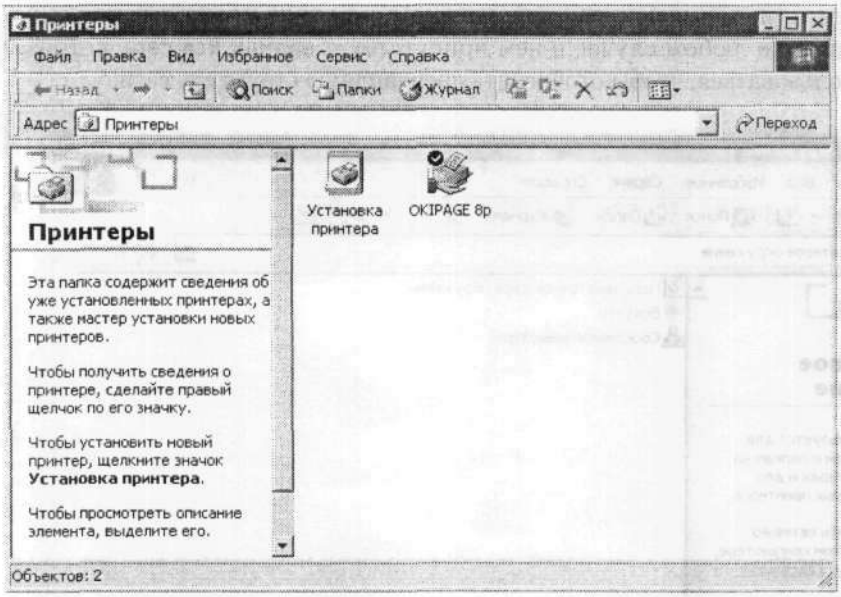

Рис. 12.21. Отображение принтера, предоставленного в общее использование

12.5. Использование сетевых ресурсов

Использовать ресурсы, предоставляемые другими участниками сети, гораздо веселее и спокойнее, чем отдавать в общее распоряжение свои. Кроме того, как правило, большинство общих ресурсов находится на мощных компьютерах с жесткими дисками по 200 Гбайт или серверах, рассчитанных на такое использование.

В любом случае, если вы хотите работать с этими ресурсами, вы должны знать, как получить к ним доступ в самый короткий срок.

Подключение сетевого диска

Использование сетевых файловых ресурсов возможно все время, пока вы находитесь в сети. Естественно, обладатель этого ресурса также должен в этот момент находиться в сети. В таком случае достаточно зайти на нужный компьютер и запустить или переписать необходимый файл, после чего спокойно наслаждаться

результатом. Так можно поступать все время: заходить в сеть, в домен, в сетевую группу, находить нужный компьютер, ждать, пока отобразиться ресурс, и т. д. (со всеми вытекающими отсюда последствиями). Подобная перспектива абсолютно не привлекает. Однако если ресурс действительно нужный, то процедуру его обнаружения можно максимально облегчить, подключив к нему сетевой диск.

Дважды щелкните на значке Мое сетевое окружение, расположенном на Рабочем столе. В результате откроется одноименное окно (рис. 12.22). В зависимости от конфигурации сети (наличия домена, сетевых групп) это окно может выглядеть по-разному, однако в любом случае в нем присутствует значок Вся сеть, которым можно воспользоваться, чтобы отобразить древовидную структуру сети.

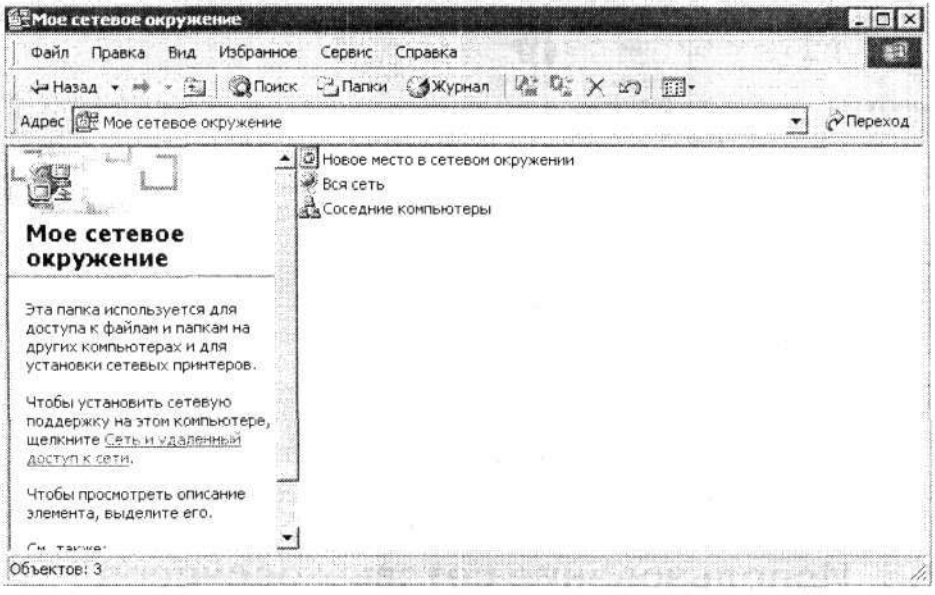

Рис. 12.22. Окно Мое сетевое окружение

Щелкнув на значке Вся сеть, следует войти в домен (если таковой существует), выбрать нужную сетевую группу и найти в ней требуемый компьютер. Войдя на этот компьютер, вы увидите все ресурсы, предоставленные для общего пользования (рис. 12.23). Выбрав общую папку или логический диск, который необходимо подключить к сетевому, щелкните на нем правой кнопкой мыши и в появившемся контекстном меню выберите пункт Подключить сетевой диск.

После этого на экране появится окно с предложением выбрать букву сетевого диска, к которому будет подключена определенная сетевая папка или диск (рис. 12.24). По умолчанию система предлагает использовать первую свободную букву, и, если вас устраивает такой вариант, можно оставить данное значение без изменения. Если вы хотите, чтобы эта папка подключалась каждый раз, когда вы входите в сеть, то попутно можно установить флажок Восстанавливать при входе в систему.

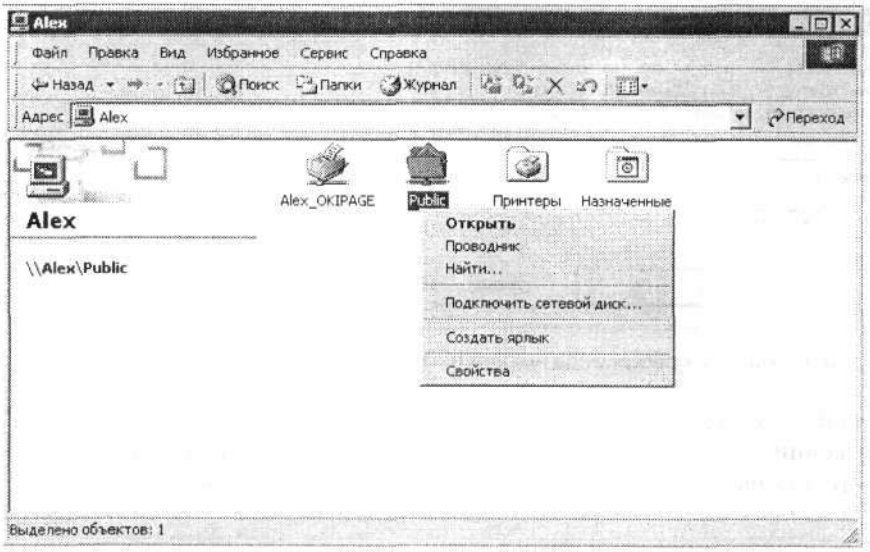

Рис. 12.23. Ресурсы, предоставленные для общего доступа

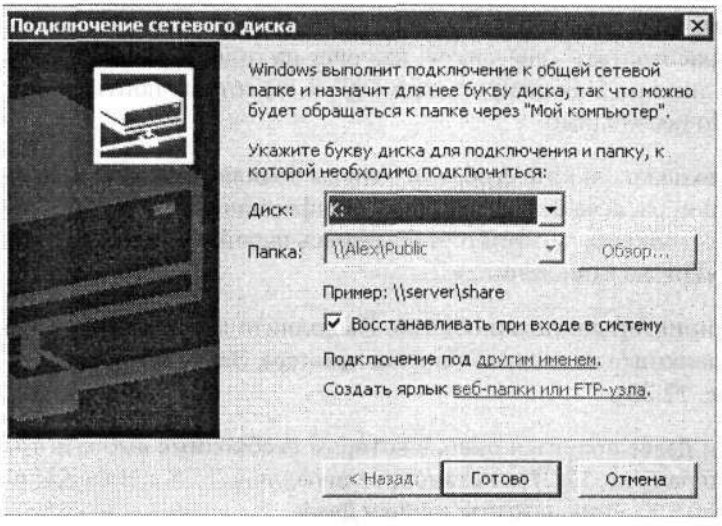

Рис. 12.24. Выбираем букву сетевого диска, с которым будет ассоциироваться выбранная сетевая папка

Вы можете подключить сетевой объект от любого имени, то есть указать имя и пароль другого пользователя (рис. 12.25).

Благодаря этой возможности вы можете работать с данным ресурсом, обходя ограничения, которые могут быть связаны с вашим именем пользователя. Правда, для этого необходимо каким-то образом узнать имя и пароль другого пользователя, однако это уже совсем другая история.

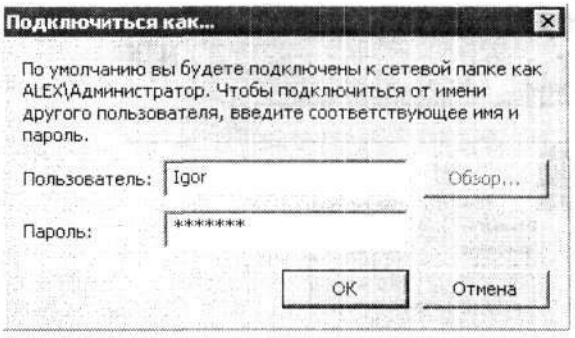

Рис. 12.25. Подключаемся к ресурсу под именем и паролем другого пользователя

Итак, сетевой диск подключен. Теперь данный ресурс не нужно будет искать в сетевом окружении, затрачивая достаточно много времени. Вы сможете сразу перейти к соответствующему сетевому диску. Просто, эффектно и удобно!

Подключение сетевого принтера

Очень часто принтер бывает настолько необходим, что за сиюминутную распечатку нужной информации вы готовы отдать любые деньги. Бывает и так, что нужно максимально быстро распечатать «внезапно», как снег на голову, свалившуюся курсовую работу или диплом. В общем, в таком случае вы готовы пойти на все, лишь бы сделать то, что необходимо.

Чтобы не доводить дело до крайности, особенно если вы подключены к сети, можно со спокойным сердцем распечатать необходимую информацию у сетевого друга, предварительно договорившись с ним и отделавшись парой-тройкой бутылок пива. Мораль проста: «Готовь сани летом...».

Подключить сетевой принтер достаточно легко. Выполните команду Пуск ▸ Настройка ▸ Принтеры и щелкните на значке Установка принтера. Запустится соответствующий мастер (рис. 12.26).

После нажатия кнопки Далее появится окно, в котором необходимо выбрать тип подключаемого принтера (рис. 12.27). Установите переключатель в положение Сетевой принтер. Для продолжения нажмите кнопку Далее.

В следующем окне (рис. 12.28) вам предстоит указать путь к нужному сетевому принтеру. Поскольку вы вряд ли помните этот путь наизусть (если помните, то введите его, включая название принтера, в соответствующее поле), разработчики системы предусмотрели более простой вариант. Установите переключатель в положение Введите имя принтера или нажмите кнопку "Далее" для обзора принтеров и нажмите кнопку Далее.

Мастер установки принтера произведет поиск общих принтеров и отобразит список компьютеров сети, готовых предоставить их для общего использования (рис. 12.29).

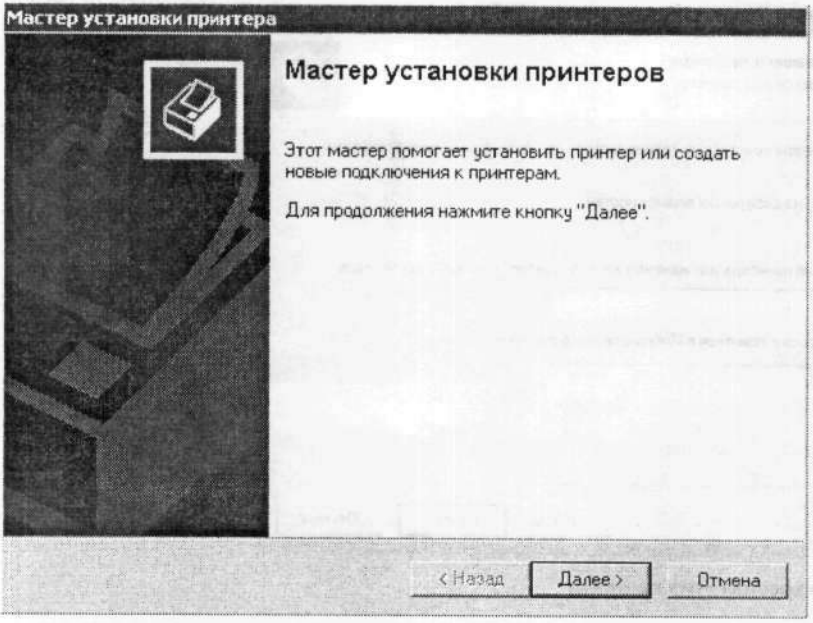

Рис. 12.26. Мастер установки принтеров

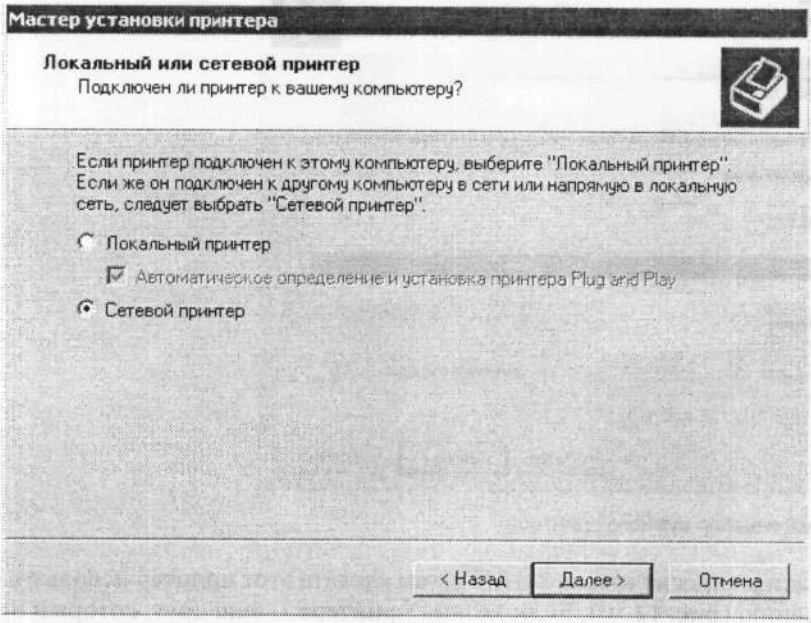

Рис. 12.27. Выбираем тип подключаемого принтера

Единственное, что вам остается, — это указать нужный компьютер и выбрать подключенный к нему принтер.

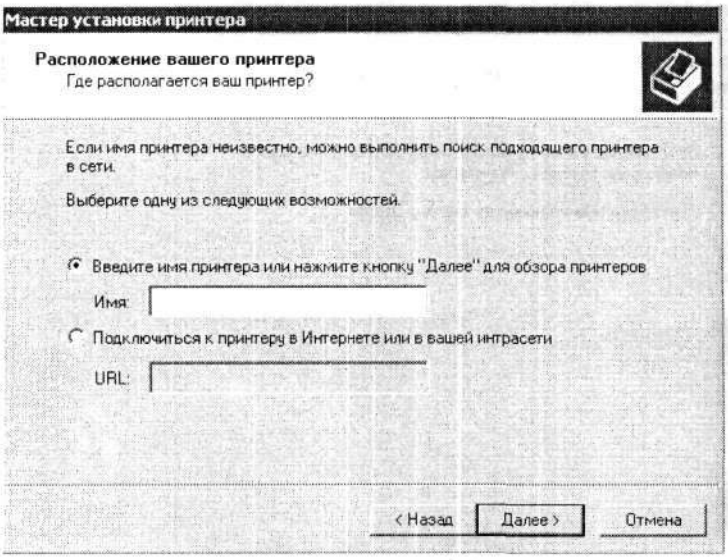

Рис. 12.28. Окно ввода пути к принтеру

Рис. 12.29. Поиск и выбор нужного принтера

После этого мастер спросит вас, не хотите ли вы сделать этот принтер используемым по умолчанию (рис. 12.30). Если хозяин принтера — ваш друг, который не будет против, если вы дни напролет будете эксплуатировать его принтер, тогда смело можете устанавливать переключатель в положение Да. В противном случае лучше ответить на вопрос отрицательно. Впоследствии вы сможете без труда изменить принтер, заданный для использования по умолчанию.

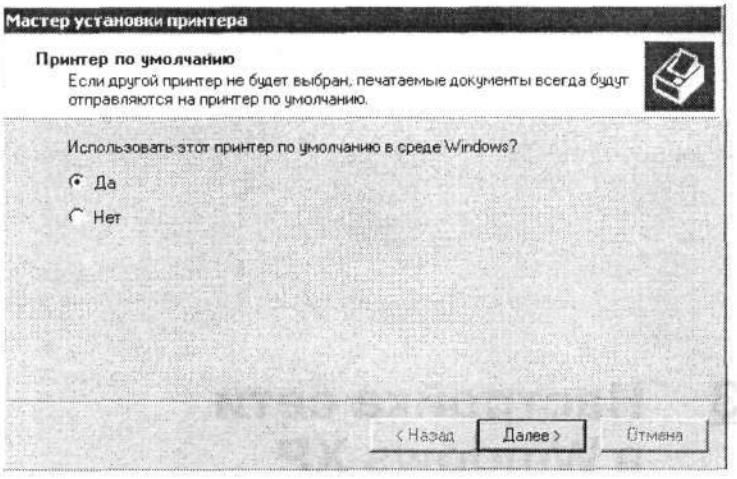

Рис. 12.30. Указываем, будет ли принтер использоваться по умолчанию

После нажатия кнопки Далее мастер сообщит вам, что работа по подключению сетевого принтера завершена (рис. 12.31).

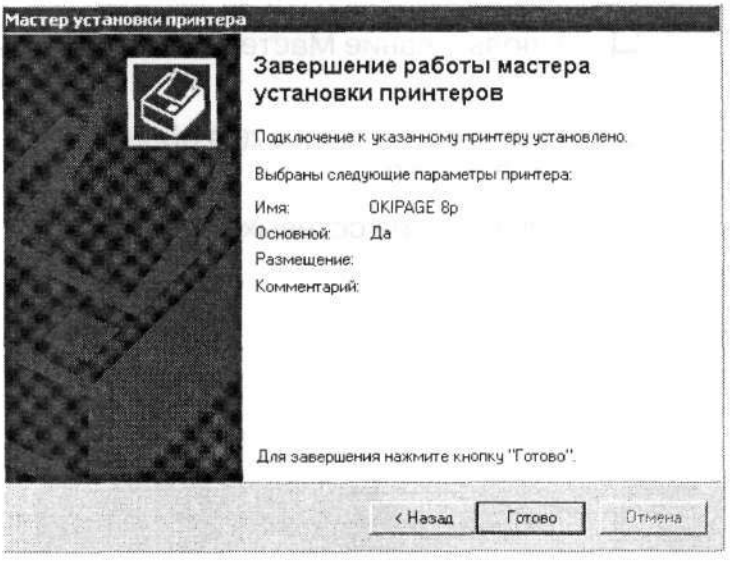

Рис. 12.31. Мастер завершил свою работу

После этого вам остается только нажать кнопку Готово и попробовать послать на принтер любое задание печати. Удачи!

ГЛАВА 13 Настройка сети в Windows XP

- Использование Мастера настройки сети
- Настройка ресурсов для общего пользования
- Подключение сетевых ресурсов

Windows XP — пожалуй, наиболее распространенная на сегодняшний день операционная система, устанавливаемая как на домашние, так и на офисные компьютеры. Благодаря своим возможностям, устойчивости и быстрой работе она более предпочтительна, чем Windows 2000 или Windows NT, не говоря уже об операционных системах Windows 95/98/Me.

13.1. Использование Мастера настройки сети

Самый простой способ подключения к сети компьютера с установленной операционной системой Windows XP — использование встроенного мастера создания сети.

Выполните команду Пуск ▸ Сетевое окружение и в появившемся окне щелкните на ссылке Отобразить сетевые подключения. Откроется окно Сетевые подключения (рис. 13.1).

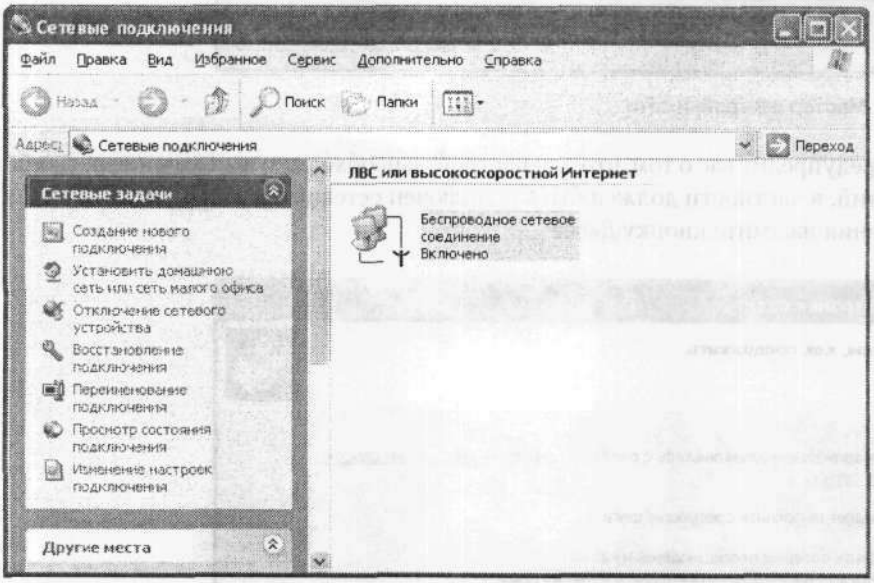

Рис. 13.1. Окно Сетевые подключения

В данном окне отображаются все существующие сетевые подключения, используемые данным компьютером. Это могут быть любые соединения, как проводные, так и беспроводные.

Щелкните в левой части окна на ссылке Установить домашнюю сеть или сеть малого офиса.

В результате на экране появится окно мастера настройки сети (рис. 13.2). Чтобы начать процесс настройки, нажмите кнопку Далее.

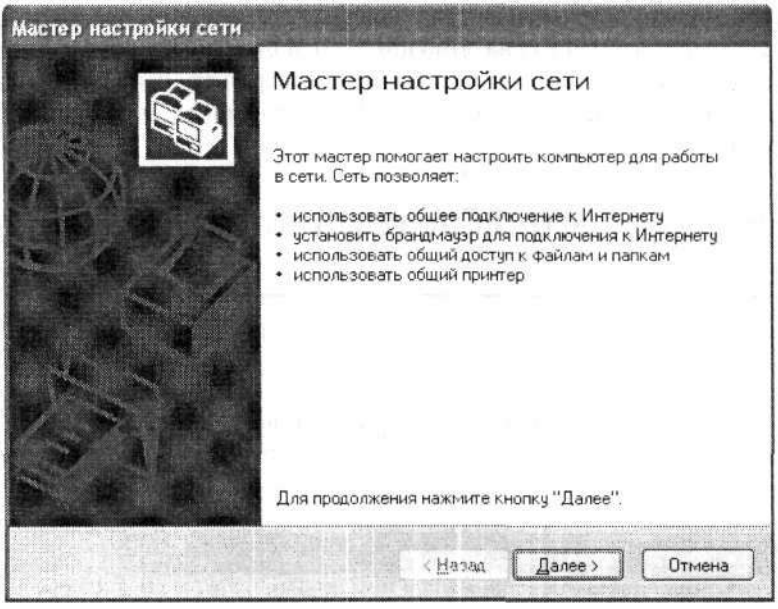

Рис. 13.2. Мастер настройки сети

Мастер предупредит вас о том, что для настройки необходимо выполнение нескольких условий, в частности должен быть подключен сетевой адаптер (рис. 13.3). Для продолжения нажмите кнопку **Далее**.

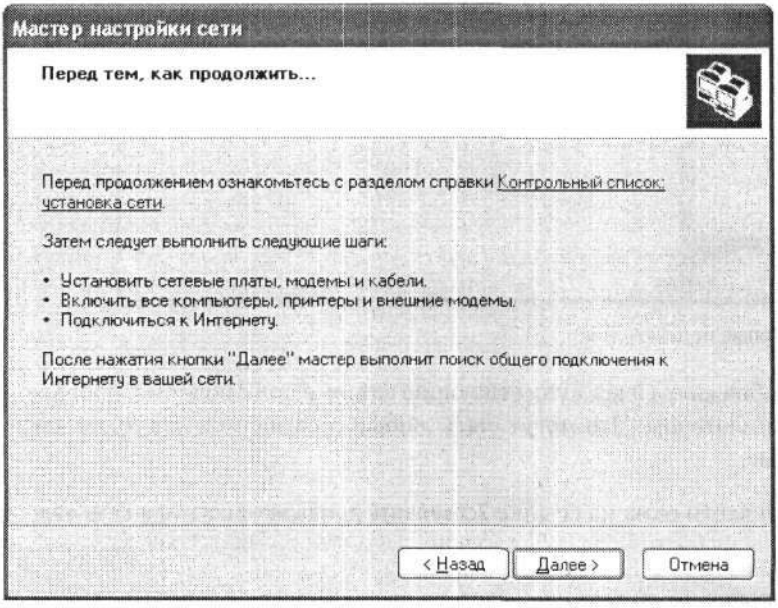

Рис. 13.3. Условия настройки сети

В следующем окне следует указать, каким образом компьютер подключается к Интернету (рис. 13.4). Реально существует всего два варианта. Первый указывает, что компьютер подключен к Интернету с помощью модема, а все остальные сетевые компьютеры пользуются Интернетом, предоставляемым этим компьютером.

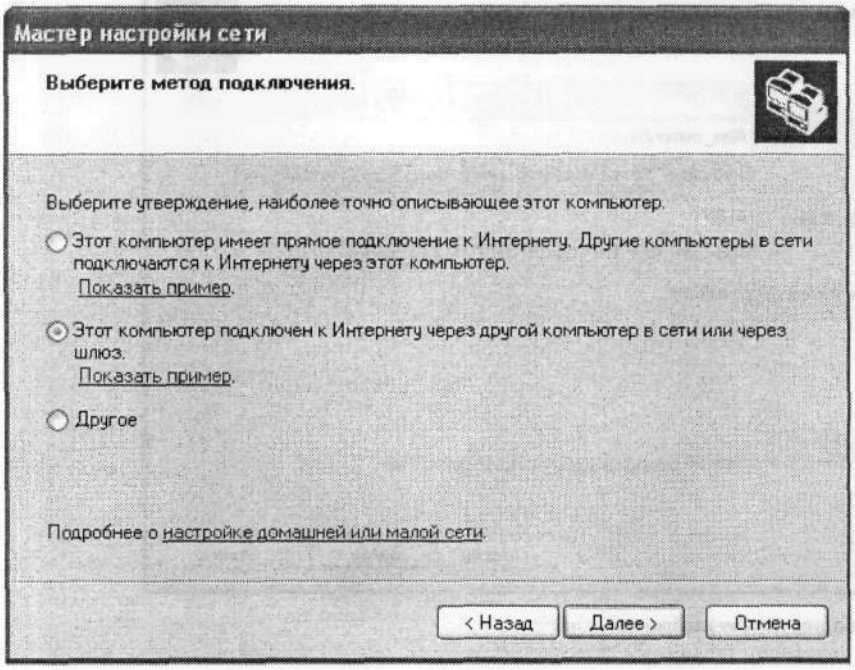

Рис. 13.4. Указываем способ подключения к Интернету

Если компьютер использует чужое подключение к Интернету, например интернет-шлюз или другой сетевой компьютер, установите переключатель в среднее положение.

В зависимости от условий вы можете выбрать один из этих двух вариантов или установить переключатель в положение Другое, чтобы затем более детально указать необходимую информацию. Как правило, в беспроводных сетях чаще всего используется вариант с интернет-шлюзом, хотя может применяться и непосредственное подключение к Интернету (это зависит от важности данного компьютера в сети и развитости самой сети).

Предположим, вы решили установить переключатель во второе положение. После этого нажмите кнопку Далее.

В следующем окне мастер настройки сети попросит вас указать имя компьютера и его краткое описание (рис. 13.5). Желательно выбирать имя, которое однозначно указывало бы другим пользователям сети, чей компьютер они видят или где он находится. В качестве описания компьютера может выступать любой текст, но лучше не набирать слишком много слов, поскольку во многих файловых менеджерах

описание компьютера просто не умещается в выделенный для этого диапазон и поэтому обрезается. Будьте кратки и лаконичны!

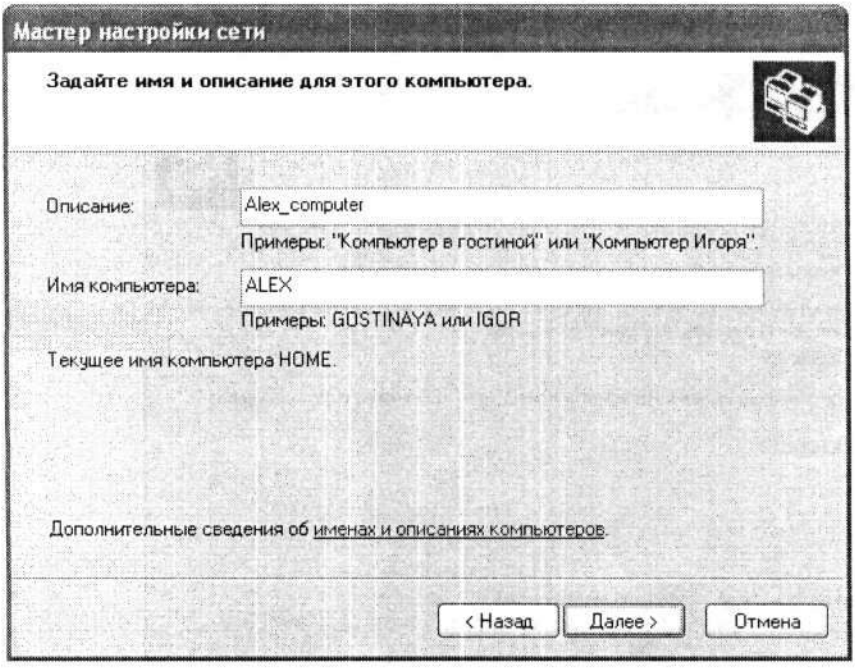

Рис. 13.5. Вводим необходимые данные

Указав необходимые данные, нажмите кнопку **Далее**. Следующий шаг — ввод имени сетевой группы, которую необходимо создать или к которой компьютер нужно присоединить (рис. 13.6). Если вы хотите подключиться к существующей сетевой группе, то нужно ввести правильное имя группы, иначе вместо подключения к сетевой группе вы создадите новую, и весь процесс настройки придется начинать сначала.

В следующем окне мастер настройки сети отобразит всю введенную вами информацию (рис. 13.7). Остается внимательно ее перепроверить и при необходимости изменить. Для этого можно вернуться к предыдущим окнам с помощью кнопки **Назад** и изменить нужные параметры.

Проверив информацию, подтвердите ее нажатием кнопки **Далее**. Начнется непосредственно сам процесс настройки, во время которого мастер произведет необходимые изменения в компонентах операционной системы и пропишет нужные настройки (рис. 13.8). Этот процесс достаточно длительный, поэтому запаситесь терпением и дождитесь его окончания.

Перед завершением работы мастер предложит вам создать диск с аналогичными настройками, который вы при необходимости сможете использовать на другом компьютере, подключенном к сети (рис. 13.9). Такой подход достаточно удобен,

поскольку при этом не нужно запоминать название группы и ответы на другие каверзные вопросы мастера настройки.

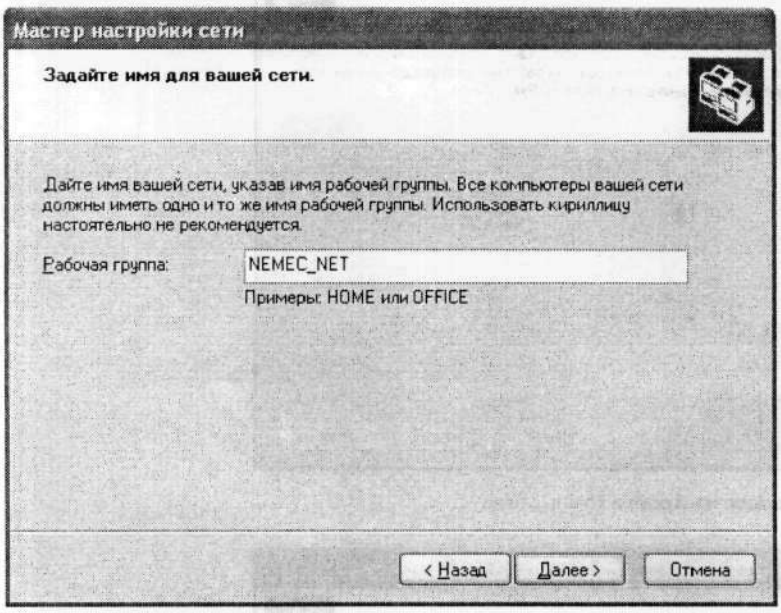

Рис. 13.6. Указываем имя сетевой группы, которую нужно создать или к которой вы хотите подключиться

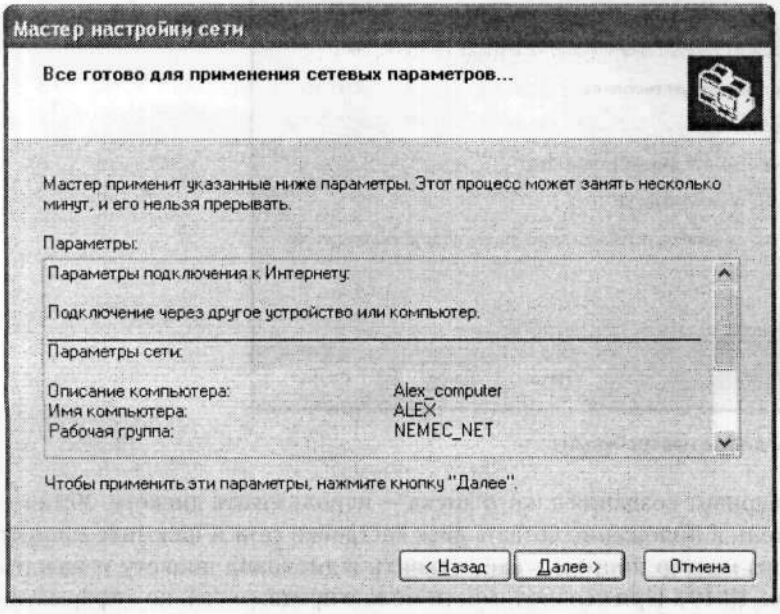

Рис. 13.7. Итоговая информация

Рис. 13.8. Идет процесс настройки компьютера

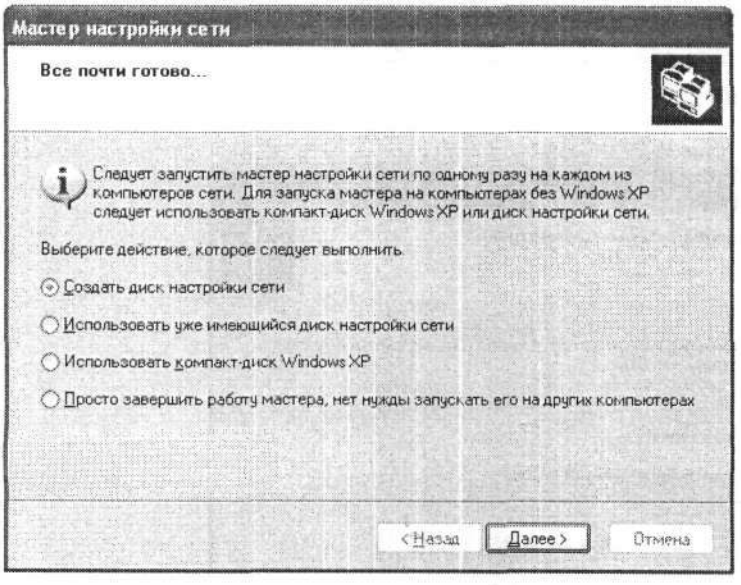

Рис. 13.9. Создаем диск с настройками сети

Самый простой вариант создания такого диска — использовать дискету. Установите переключатель в положение Создать диск настройки сети и нажмите кнопку Далее. После этого мастер попросит вас вставить в дисковод дискету и нажать кнопку Далее (рис. 13.10). При необходимости можно предварительно отформатировать дискету, воспользовавшись кнопкой Форматировать диск.

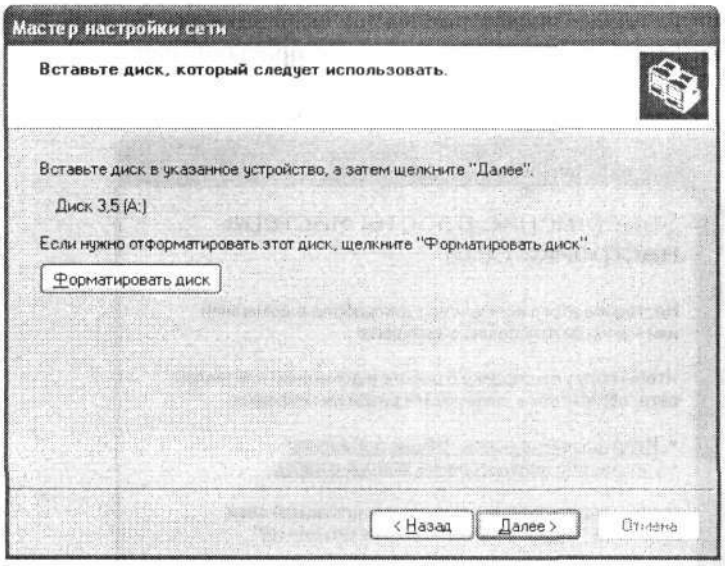

Рис. 13.10. Выполняем совет мастера настройки сети

Мастер установки создаст необходимые конфигурационные файлы и скопирует их на дискету. Это займет совсем мало времени, поскольку объем файлов достаточно незначительный.

Затем на экране появится окно с информацией о том, как следует использовать созданный диск (рис. 13.11).

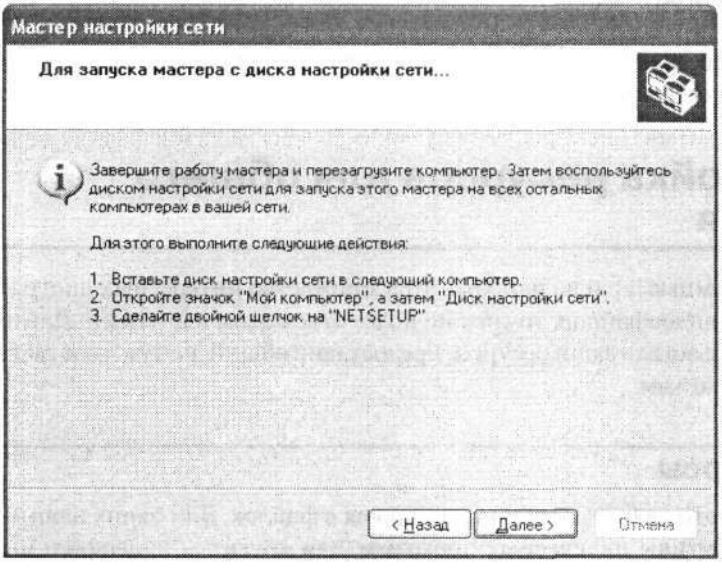

Рис. 13.11. Совет по использованию созданного диска

После нажатия кнопки Далее откроется последнее окно мастера (рис. 13.12). После нажатия кнопки Готово появится сообщение с просьбой перезагрузить компьютер.

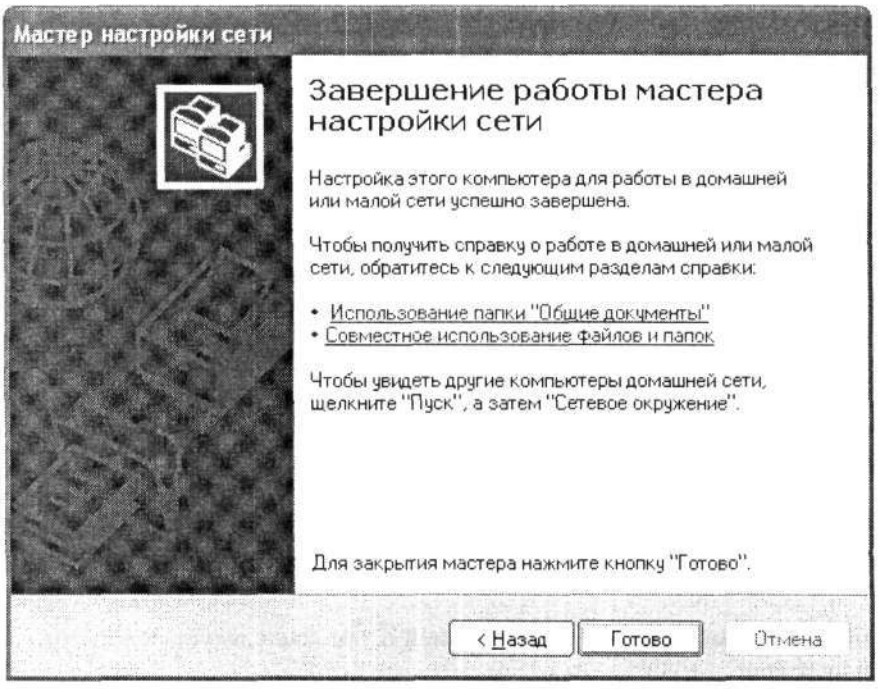

Рис. 13.12. Настройка сети окончена

Если вы настроили все правильно, то после перезагрузки ваш компьютер присоединится к указанной сетевой группе.

13.2. Настройка ресурсов для общего пользования

Если у вас мощный компьютер и на нем хранится множество интересных дистрибутивов, музыки или видеофайлов, то грех не поделиться этим с другими. Дайте им возможность использовать ваши ресурсы, предоставив общий доступ к соответствующим файлам и папкам.

Файловые ресурсы

Файловые ресурсы — это любые данные, хранящиеся в файлах. Для одних ценными являются дистрибутивы интересных программ, для других — видеофильмы и музыка и т. п.

Предоставить доступ к файловому ресурсу очень просто. Найдите в Проводнике объект (папку, диск), к которому вы хотите предоставить общий доступ, щелкните на нем правой кнопкой мыши и в появившемся контекстном меню выберите пункт Общий доступ и безопасность (рис. 13.13).

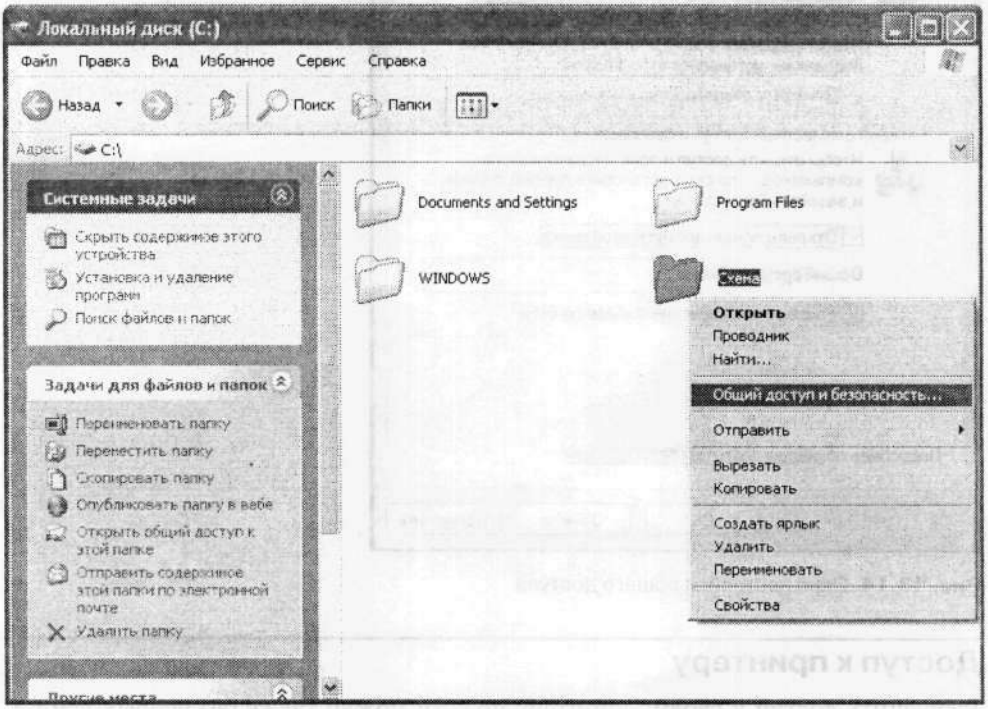

Рис. 13.13. Выбираем пункт Общий доступ и безопасность

В результате откроется окно, изображенное на рис. 13.14.

ПРИМЕЧАНИЕ

При использовании в сети доменной системы в данном окне присутствует большее количество вкладок, в частности, добавляется вкладка Безопасность.

Чтобы открыть доступ к указанному объекту, установите флажок Открыть общий доступ к этой папке. Если вы согласны, чтобы ваш ресурс можно было изменять по сети, например создавать новые файлы или папки, удалять или редактировать, то установите флажок Разрешить изменение файлов по сети. После нажатия кнопки ОК изменения вступят в силу. При этом файловый ресурс, назначенный вами для общего использования, будет отображаться в виде руки, держащей данную папку или диск.

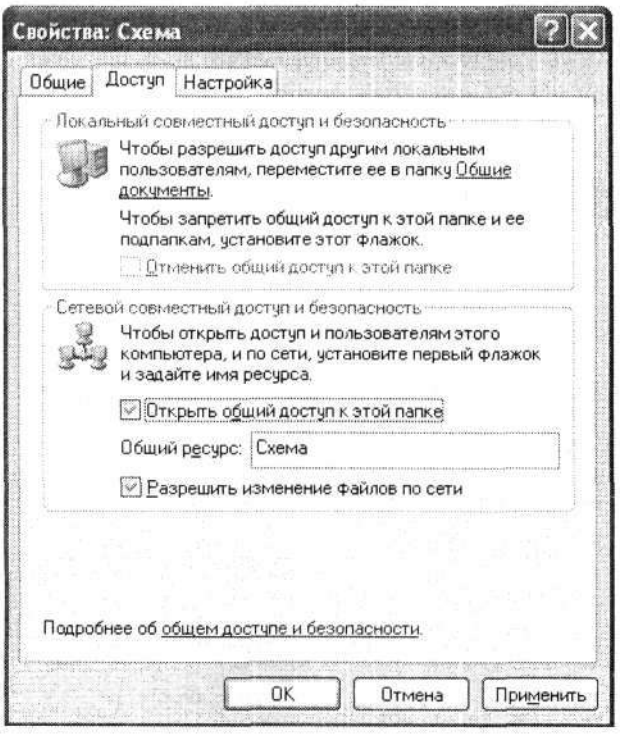

Рис. 13.14. Окно настройки общего доступа

Доступ к принтеру

Разрешить доступ к своему принтеру по сети можно также без особых усилий. Выполните команду Пуск ▸ Панель управления, выберите категорию Принтеры и другое оборудование, затем щелкните на значке Принтеры и факсы. Выберите принтер, к которому вы хотите предоставить общий доступ. При этом в левой части окна будут перечислены действия, которые можно выполнить по отношению к принтеру. В частности, здесь присутствует ссылка Совместный доступ к принтеру, с помощью которой можно настроить доступ к вашему принтеру по сети.

Вы можете также щелкнуть на значке принтера правой кнопкой мыши и выбрать в появившемся контекстном меню пункт Общий доступ (рис. 13.15).

В результате откроется то же окно, что и после щелчка на ссылке Совместный доступ к принтеру (рис. 13.16).

Установите переключатель в положение Общий доступ к данному принтеру и укажите имя, под которым принтер будет отображаться в сети. В принципе, можно оставить имя, заданное мастером по умолчанию, однако зачастую оно не связано ни с типом принтера, ни с его названием. Поэтому лучше самому указать такое имя, чтобы любой сетевой пользователь сразу понимал, о каком принтере идет речь.

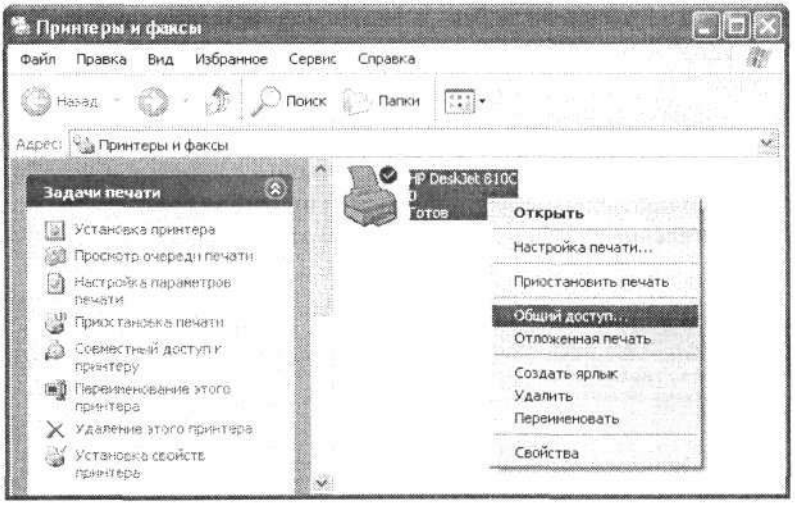

Рис. 13.15. Выбираем пункт Общий доступ

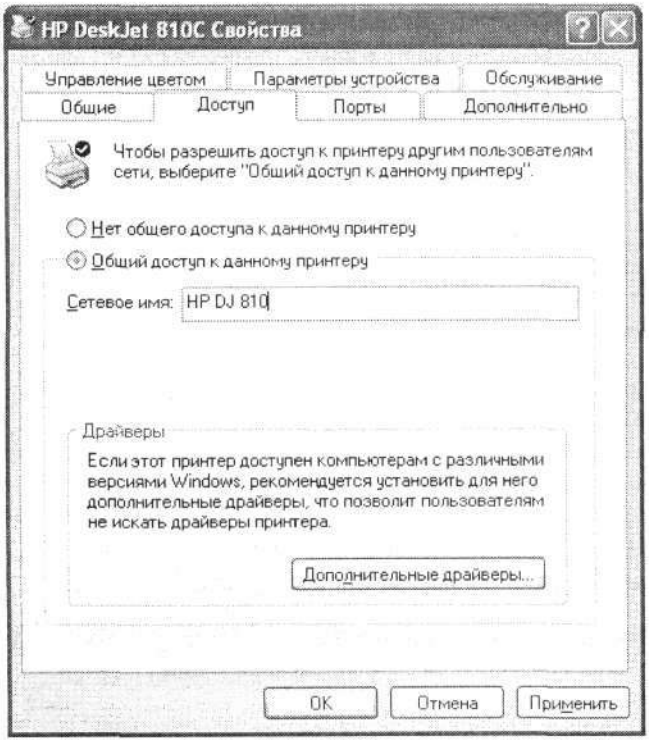

Рис. 13.16. Окно настройки общего доступа к принтеру

Операционная система Windows XP предлагает дополнительно установить драйверы принтера для разных операционных систем. Это позволяет подключать принтер

к компьютеру, на котором установлена любая операционная система, не заботясь об инсталляции нужных драйверов. Все необходимые данные предоставляет операционная система Windows XP, управляющая работой компьютера, к которому подключен принтер.

Такая возможность достаточно удобна, и ею обязательно следует воспользоваться. Для этого в окне настройки общего доступа к принтеру (рис. 13.16) нажмите кнопку Дополнительные драйверы. В результате откроется окно, показанное на рис. 13.17.

Рис. 13.17. Окно Дополнительные драйверы

По умолчанию драйверы устанавливаются только для операционных систем Windows XP и Windows 2000, работающих на платформе Intel. Чтобы установить дополнительные драйверы для остальных систем, указанных в списке, достаточно установить соответствующие флажки. После нажатия кнопки OK системе может понадобиться диск с драйверами, поставляемый в комплекте с принтером. Переписав необходимые файлы, система подготовит себя к выполнению запросов разных операционных систем, работающих на разных процессорных платформах.

Значок принтера, предоставленного в общее использование, примет вид руки, держащей принтер.

13.3. Подключение сетевых ресурсов

Обычно подключение к сетевым ресурсам происходит чаще, чем предоставление их для общего использования. В этом нет ничего странного, поскольку однажды

предоставленный в общее использование ресурс остается таким на протяжении очень длительного времени, особенно если эти ресурсы находятся на сервере. Подключение же к сетевым ресурсам может происходить по десять раз в день.

Подключение к файловому ресурсу

Подключение к файловому ресурсу с использованием операционной системы Windows XP практически не отличается от аналогичного подключения в другой системе, например в Windows 2000.

Выполните команду Пуск ▸ Сетевое окружение и найдите нужный ресурс, предназначенный для общего использования. Если в дальнейшем вы хотите максимально быстро получать доступ к этому ресурсу, то лучшим способом сделать это является назначение ему сетевого диска.

Щелкните правой кнопкой мыши на нужном объекте и в появившемся контекстном меню выберите пункт Подключить сетевой диск (рис. 13.18).

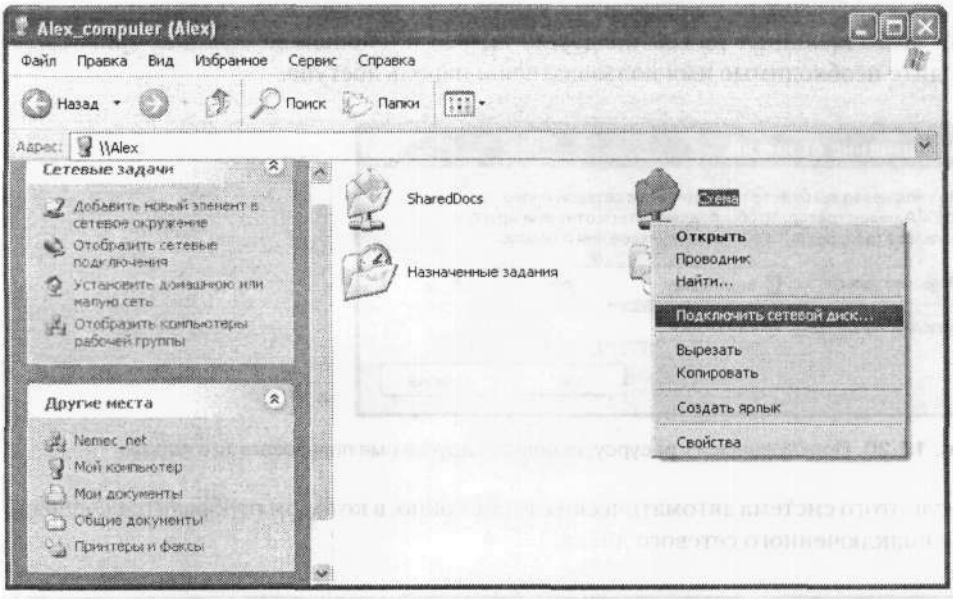

Рис. 13.18. Выбираем пункт Подключить сетевой диск

В результате откроется окно, в котором можно указать любую доступную букву диска, который будет ассоциироваться с выбранным сетевым ресурсом (рис. 13.19). Чтобы сделать этот ресурс доступным постоянно, можно настроить подключение его каждый раз, когда вы входите в сеть. Для этого установите флажок Восстанавливать при входе в систему.

Кстати, вы можете подключиться к этому ресурсу с использованием других имени пользователя и пароля и таким образом, возможно, получить большие права.

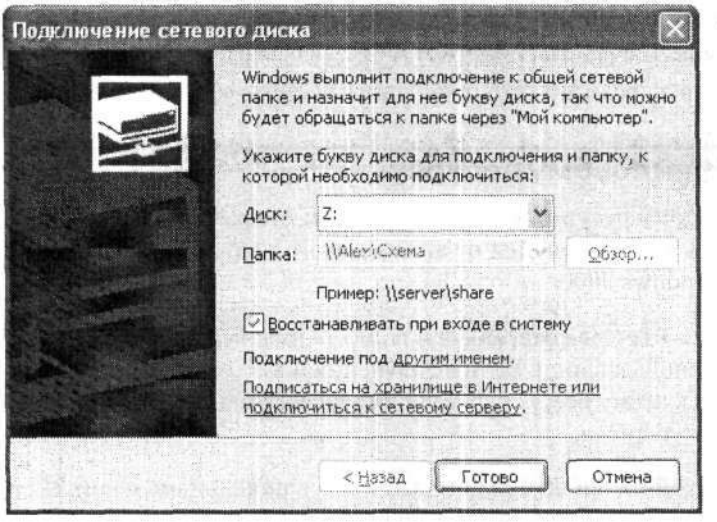

Рис. 13.19. Указываем букву сетевого диска для общего ресурса

Для этого щелкните на ссылке другим именем и в появившемся окне (рис. 13.20) введите необходимые имя пользователя и пароль доступа.

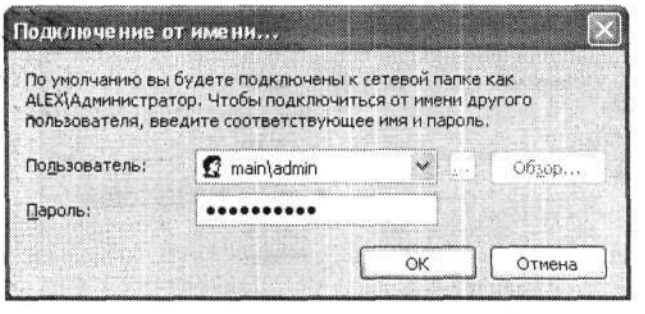

Рис. 13.20. Подключаемся к ресурсу, используя другие имя пользователя и пароль

После этого система автоматически откроет окно, в котором отобразится содержимое подключенного сетевого диска.

Подключение к сетевому принтеру

Подключение к сетевому принтеру — стандартная процедура, с легкостью выполняемая в любой операционной системе, в том числе Microsoft Windows XP.

Подключиться к сетевому принтеру можно разными путями, например с помощью стандартного Мастера установки принтера. Однако рассмотрим более быстрый способ.

Выполните команду Пуск ▸ Сетевое окружение и щелкните в левой части появившегося окна на ссылке Отобразить компьютеры рабочей группы. Зайдите на нужный

компьютер, щелкните правой кнопкой мыши на принтере, к которому вы хотите подключиться, и в появившемся контекстном меню выберите пункт Подключить (рис. 13.21).

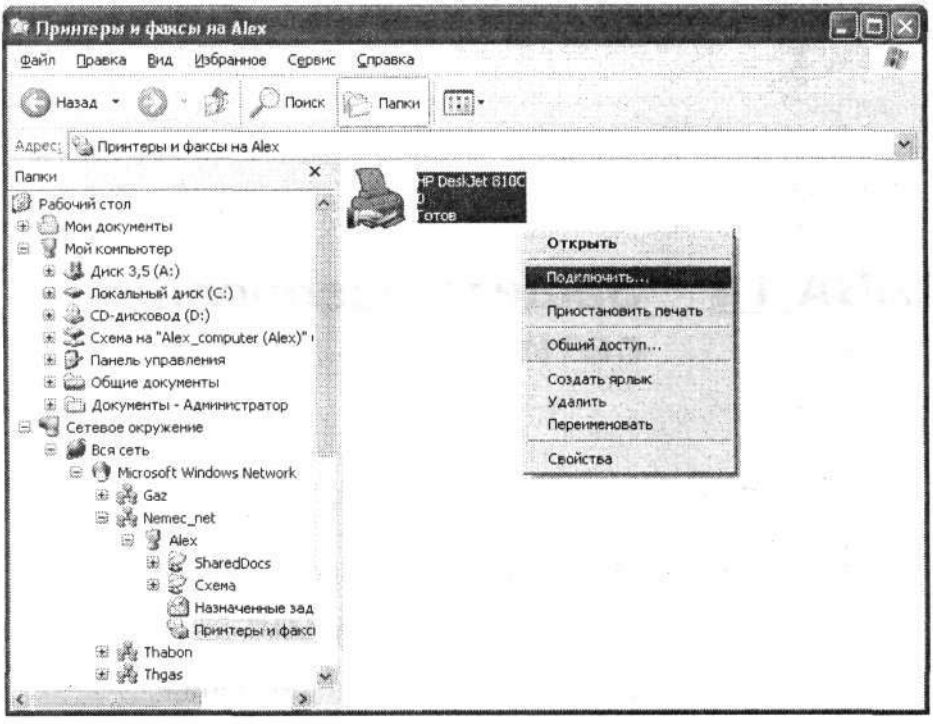

Рис. 13.21. Подключаем сетевой принтер, выбрав пункт Подключить

Дальнейшие действия по подключению система выполнит самостоятельно. В итоге, выполнив команду Пуск ▸ Панель управления, выбрав категорию Принтеры и другое оборудование и щелкнув на значке Принтеры и факсы, вы увидите подключенный принтер.

ГЛАВА 14 Защита беспроводной сети

- ❑ Отключение трансляции SSID
- ❑ Создание списка MAC-адресов
- ❑ Выбор уровня шифрования
- ❑ Снижение мощности передатчика

Создателей и администраторов сети всегда волнует и будет волновать проблема защиты используемых в сети данных. Вне зависимости от ценности этих данных безопасность сети должна стоять на первом месте.

По умолчанию беспроводное оборудование не использует никаких дополнительных механизмов защиты и является абсолютно открытым для внешних атак. Поэтому после создания сети необходимо в первую очередь выполнить действия, которые позволят максимально защитить ее.

Рассмотрим настройку системы безопасности сети при использовании следующего оборудования:

- беспроводной USB-адаптер D-Link DWL-G122;
- беспроводной PCI-адаптер OvisLink WL-8000PCI;
- точка доступа D-Link DWL-2100AP.

14.1. Отключение трансляции SSID

Идентификатор сети (SSID) является уникальным показателем, описывающим сеть. Фактически это имя сети, которое должны знать все, кто собирается к ней подключаться. Поэтому прежде чем отключить транслирование идентификатора сети, обязательно сообщите его всем пользователям вашей сети, в том числе потенциальным.

По умолчанию точка доступа сообщает идентификатор сети всем беспроводным устройствам, находящимся в радиусе ее действия. При сканировании эфира беспроводной клиент может обнаружить точку доступа и ее SSID, после чего подключиться к ней, настроив необходимые параметры.

Соответственно, не зная SSID-точки доступа, подключиться к ней будет сложно, хотя с помощью специализированного программного обеспечения это возможно.

Отключение трансляции SSID нельзя считать полноценным способом защиты сети. Однако таким образом вполне можно отсеять некоторую часть начинающих «любителей бесплатного сыра», поэтому рекомендуется все-таки использовать эту возможность.

Практически все точки доступа позволяют отключить вещание SSID. Для этого необходимо зайти в настройки устройства и изменить значения соответствующих параметров.

Запустив утилиту конфигурирования точки доступа D-Link DWL-2100AP, перейдите на вкладку Wireless (Беспроводная сеть). Чтобы запретить транслирование идентификатора сети, выберите из раскрывающегося списка SSID Broadcast (Транслирование SSID) значение Disable (Запретить).

14.2. Создание списка MAC-адресов

При работе с практически любой точкой доступа можно создавать списки исключений, содержащие MAC-адреса беспроводных устройств, которым позволено подключаться к данной точке доступа.

Вы можете легко создать список MAC-адресов, которые однозначно идентифицируют подключаемые устройства. Это позволит обеспечить дополнительную защиту сети от атак. Учтите, что такая защита может остановить только неопытных вредителей, не имеющих на вооружении нужных утилит. С помощью специальных утилит можно достаточно легко подменить свой MAC-адрес перехваченным, после чего через точку доступа проникнуть в сеть.

Чтобы создать такой список адресов, запустите утилиту конфигурирования точки доступа. В открывшемся окне перейдите на вкладку Filters (Фильтры) и в области IEEE802.11f Access Setting (Настройка доступа для устройств IEEE802.11g) установите флажок Access Control (Контроль доступа) (см. рис. 11.15). Затем задайте этому параметру значение Accept (Принимать), чтобы указать точке доступа, что устройства с указанными MAC-адресами могут к ней подключаться.

Придерживаясь указанного шаблона, введите в поле ACL MAC Address необходимый MAC-адрес, после чего нажмите кнопку Add (Добавить). При вводе адреса желательно не ошибаться, поскольку это может привести к тому, что к точке доступа не сможет подключиться «свой» компьютер.

14.3. Выбор уровня шифрования

Современное беспроводное оборудование позволяет использовать для шифрования протоколы WEP, WPA и WPA2. Протокол WEP поддерживает все существующее оборудование, даже самое «древнее». Иногда именно «древность» оборудования становится причиной использования данного протокола. Протокол WEP представляет собой самый простой и неэффективный способ шифрования данных. Дело в том, что он использует для шифрования статичный ключ, а множество специализированных программ без особого труда способны проанализировать передаваемые данные и определить такой ключ. Конечно, ключ может иметь разную длину, вплоть до 256 бит, однако этот факт влияет лишь на время взлома, а не на его качество.

Протоколы WPA и WPA2 представляют собой более новую спецификацию. Этот способ шифрования на сегодняшний день является наиболее предпочтительным, поскольку позволяет оперировать динамичными ключами, а значит, фактически исключает возможность взлома ключа, который может меняться каждые 10 тысяч пакетов.

Как бы там ни было, точка доступа обязательно должна использовать протокол шифрования, вне зависимости от того, в каком режиме она функционирует.

Для настройки протокола безопасности воспользуемся утилитой конфигурирования, которая поставляется в комплекте с точкой доступа. Запустив данную утилиту, перейдите в ее окне на вкладку Security (Безопасность) (см. рис. 11.14).

На данной вкладке можно выбрать необходимый протокол и настроить параметры шифрования и подключения к точке доступа.

Если вы планируете использовать протокол WEP (например, при использовании устаревших беспроводных адаптеров, неспособных работать с более универсальным протоколом), установите флажок Authentication (Аутентификация) и выберите из соответствующего раскрывающегося списка значение Open (Открытый), Shared (Разделенный) или Both (Оба режима). Из раскрывающегося списка Encryption (Шифрование) выберите значение Enable (Разрешить). Именно эти параметры отвечают за настройку протокола WEP.

После выбора одного из упомянутых значений необходимо выбрать ключ шифрования, указав его длину, тип и непосредственно символьное наполнение. При работе точка доступа может использовать четыре разных ключа шифрования, к которым можно обращаться в любое время. При этом одновременно может использоваться только один, выбранный в данный момент, ключ.

Чтобы выбрать нужный ключ, достаточно задать в поле Active Key Index (Индекс активного ключа) номер ключа и настроить его (если вы не сделали этого ранее). Если вы выбрали тип ключа ASCII, то при вводе самого ключа старайтесь использовать редко употребляемые словосочетания. При этом не забывайте, что ключ имеет фиксированную длину, например 5 или 13 символов (в зависимости от выбранной длины ключа).

Если для работы в сети вы используете достаточно новое оборудование, которое поддерживает новейшие протоколы шифрования, то обязательно воспользуйтесь этим и настройте параметры протокола WPA. Для этого на вкладке Security (Безопасность) установите флажок Authentication (Аутентификация) и выберите из соответствующего раскрывающегося списка значение WPA-EAP или WPA-PSK. В результате появится дополнительная вкладка — IEEE802.11g WPA, на которой вы сможете настроить некоторые параметры протокола (рис. 14.1).

Если в вашей беспроводной сети установлен сервер аутентификации RADIUS, тогда лучше выбрать для параметра Authentication (Аутентификация) значение WPA-EAP, поскольку это лучшая на данный момент степень защищенности сети. Далее укажите IP-адрес и порт RADIUS-сервера. Из раскрывающегося списка Cipher Type (Тип шифра) выберите необходимый вариант: TKIP или AES.

Напомню, что шифр TKIP обеспечивает динамическую генерацию ключа и проверку целостности пакетов с возможностью их шифрования с помощью разных ключей, что на порядок выше свойств протокола WEP. Шифр AES является представителем последнего достижения шифрования и обладает самым мощным алгоритмом шифрования, поддерживающим ключ длиной 256 бит[1].

---

[1] Этот тип шифрования относится к спецификации протокола WPA2.

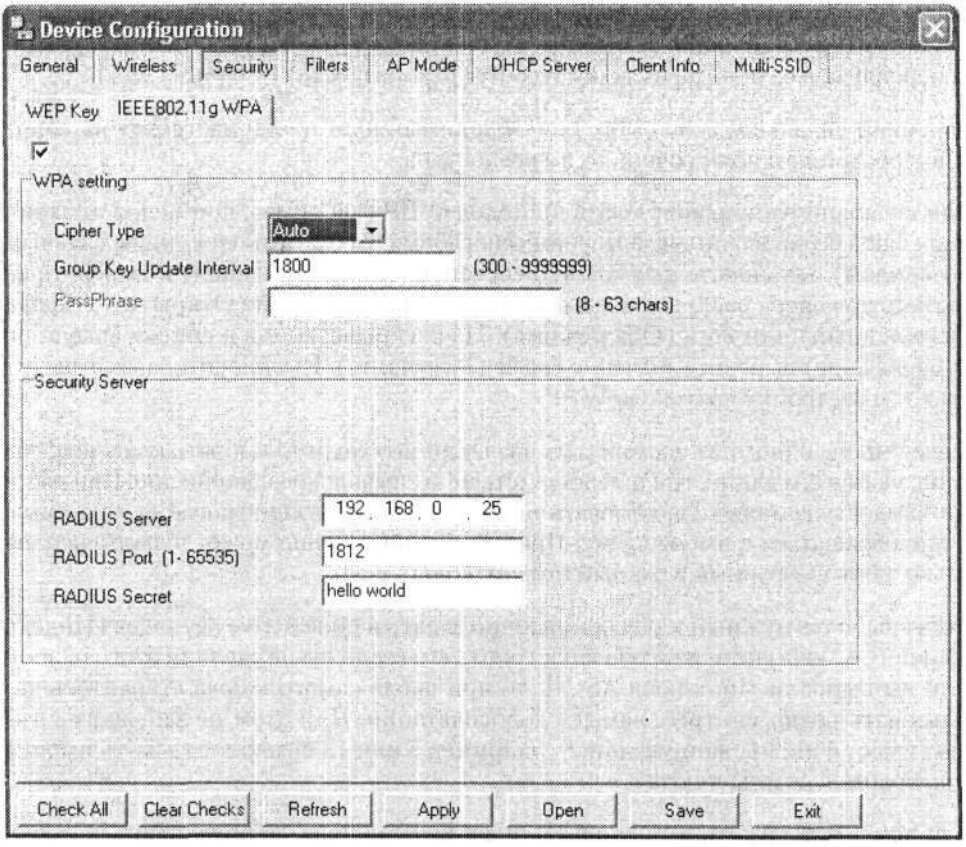

Рис. 14.1. Настраиваем протокол WPA с использованием сервера аутентификации RADIUS

Если вы не можете решить, какой тип шифра выбрать, то лучше предоставить выбор самой точке доступа, задав параметру Cipher Type (Тип шифра) значение Auto (Автоматический выбор).

Если в вашей беспроводной сети не планируется использование RADIUS-сервера, но вы все-таки хотите воспользоваться возможностями протокола WPA, то выберите из раскрывающегося списка Authentication (Аутентификация) пункт WPA-PSK. При этом вам также необходимо будет определиться с типом шифра и указать фразу шифрования (рис. 14.2).

14.4. Снижение мощности передатчика

Как известно, каждое беспроводное устройство передает данные с помощью приемника и передатчика радиоволн. От мощности передатчика зависит радиус беспроводной сети, а от чувствительности приемника — качество восприятия сигнала. Поскольку радиоволны — вещь неконтролируемая и никогда нельзя предугадать, кто может их принимать, неплохим вариантом защиты сети является подбор мощности

передатчика вполне достаточной для покрытия всей радиосети. При этом вы отсекаете недоброжелателей, которые могут «пристроиться» к вашей сети, находясь, например, за стенкой соседнего дома или в машине на стоянке, расположенной рядом с офисом.

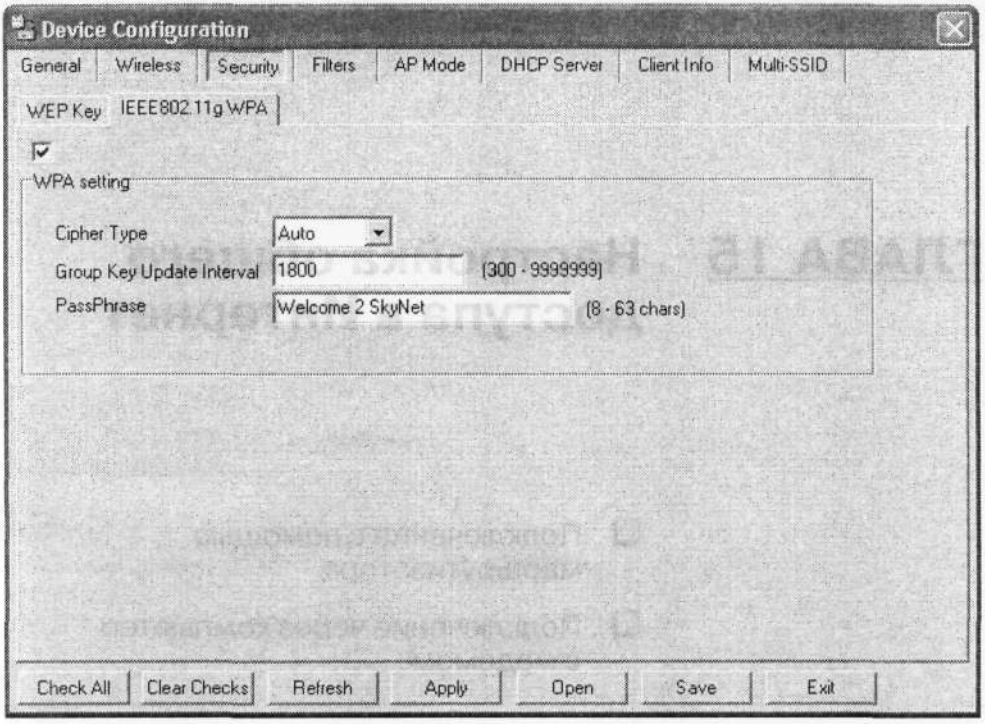

Рис. 14.2. Настраиваем протокол WPA без сервера аутентификации RADIUS

Другое преимущество такого предприятия — экономия энергии, что немаловажно для переносных компьютеров и устройств.

Чтобы выбрать уровень мощности сигнала, запустите утилиту конфигурирования точки доступа и перейдите в ее окне на вкладку Wireless (Беспроводная сеть) (см. рис. 11.13). Обратите внимание на параметр Tx Power (Мощность сигнала), которому можно присвоить следующие значения: Full (Полная мощность), Half (Половина мощности), Quarter (Четверть мощности), Eighth (Восьмая часть мощности) или Min (Минимальная мощность).

Сразу устанавливать слишком низкую мощность не стоит, поскольку так можно «обрубить» связь с некоторыми удаленными компьютерами. Уменьшайте мощность постепенно. Не следует устанавливать мощность, которая является пороговой для работы устройства, поскольку в определенных условиях сигнал может ослабнуть, что приведет к отключению некоторых удаленных компьютеров.

ГЛАВА 15 Настройка общего доступа в Интернет

- Подключение с помощью маршрутизатора
- Подключение через компьютер с модемом

Чаще всего после создания локальной сети появляется необходимость подключения ее к Интернету. Дело в том, что рано или поздно пользователи сети поймут, что им чего-то не хватает, а именно — новых возможностей, нового общения и новых развлечений, которые может предоставить Интернет. Кроме того, учитывая сегодняшнюю стоимость подключения к Глобальной сети, не подключаться к ней — просто настоящее кощунство. Хотя, с другой стороны, Интернет — как наркотик, со временем он начинает затягивать...

Настройка общего подключения к Интернету — довольно простая процедура, давно отработанная и проверенная. Конечно, существует множество вариантов подключения (например, с помощью маршрутизатора, xDSL-модема или обычного аналогового модема), однако основные принципы настройки общего доступа в Интернет являются общими.

15.1. Подключение с помощью маршрутизатора

Достаточно часто в локальной сети используется маршрутизатор с подключенным к нему xDSL-модемом. В этом случае управление доступом пользователей к Интернету ложится на аппаратную часть маршрутизатора.

Беспроводной маршрутизатор можно сравнить с точкой доступа, только количество параметров, которые при этом следует настроить, значительно превосходит количество настроек точки доступа.

Для подключения модема к маршрутизатору, как правило, используют один из имеющихся на маршрутизаторе портов: RG-45 или COM-порт. Другим обязательным условием является наличие у маршрутизатора статичного IP-адреса, который в дальнейшем прописывается на компьютерах-клиентах в качестве основного шлюза.

В первую очередь следует настроить на маршрутизаторе DHCP-сервер. Поскольку маршрутизатор сам отвечает за разграничение между пользователями доступа в Интернет, он должен обладать соответствующими механизмами настройки, в качестве которых используются DHCP-сервер и (при необходимости) DNS-сервер.

Параметры маршрутизатора можно настраивать двумя способами.

- Настройка с использованием программного обеспечения, поставляемого в комплекте с маршрутизатором. При этом лучше использовать прямое подключение кабелем RG-45 через сетевую карту компьютера, что гарантирует постоянное подключение к маршрутизатору даже при неверной настройке параметров. Если для подключения к маршрутизатору использовать беспроводной адаптер, то при неверных настройках маршрутизатора подключиться к нему будет практически невозможно.
- Настройка с помощью стандартной утилиты Telnet. В этом случае также рекомендуется использовать прямое кабельное подключение к маршрутизатору через сетевую карту компьютера. Очень часто при использовании утилиты Telnet

количество доступных для изменения настроек маршрутизатора значительно увеличивается. Это связано с тем, что не все параметры удается оформить визуально, в виде элементов управления интерфейса (кнопки, списки, поля ввода и т. д.).

Какой бы способ настройки маршрутизатора вы ни выбрали, обязательно необходимо ознакомиться с инструкцией, в которой описаны возможные значения параметров настройки маршрутизатора. Это значительно облегчит понимание назначения того или иного параметра.

О настройке DHCP-сервера маршрутизатора необходимо обязательно сообщить всем активным устройствам, использующимся в сети: другим маршрутизаторам, мостам, точкам доступа и т. д. Например, при настройке точки доступа D-Link DWL-2100AP в качестве адреса шлюза нужно указать адрес данного маршрутизатора (см. рис. 11.11, поле Gateway (Шлюз)) и снять флажок DHCP-Server (Сервер DHCP) (см. рис. 11.17).

В принципе, этих настроек достаточно, чтобы маршрутизатор начал транслирование в сеть данных, поступающих с модема. При этом компьютером необходимо присваивать адреса так, как рассмотрено при описании настройки DHCP-сервера маршрутизатора. О настройке клиентского компьютера для работы в Интернете читайте в следующем разделе.

15.2. Подключение через компьютер с модемом

Что делать, если в сети не используется беспроводной маршрутизатор или мост? Неужели оставаться без Интернета? Совершенно не обязательно! В этом случае достаточно, чтобы на одном компьютере в сети было настроено обычное подключение к Глобальной сети с помощью аналогового модема. Рассмотрим пример настройки такого подключения на компьютере с установленной операционной системой Windows XP.

Настройка основного компьютера

Как уже упоминалось, операционная система Windows XP обладает специальным механизмом настройки сети, который носит название Мастер настройки сети. Чтобы вызвать окно мастера, выполните команду Пуск ▸ Сетевое окружение и в появившемся окне щелкните на ссылке Установить домашнюю или малую сеть.

Работа с данным мастером подробно описана в разд. 13.1. Остановимся на моментах, отличных от описанных. В окне, изображенном на рис.13.4, установите переключатель в верхнее положение, означающее, что другие компьютеры сети будут использовать подключение к Интернету, настроенное на этом компьютере.

После нажатия кнопки Далее появится окно, содержащее все найденные в системе подключения, среди которых необходимо выбрать подключение к Интернету (рис. 15.1). Отметив нужное подключение, нажмите кнопку Далее.

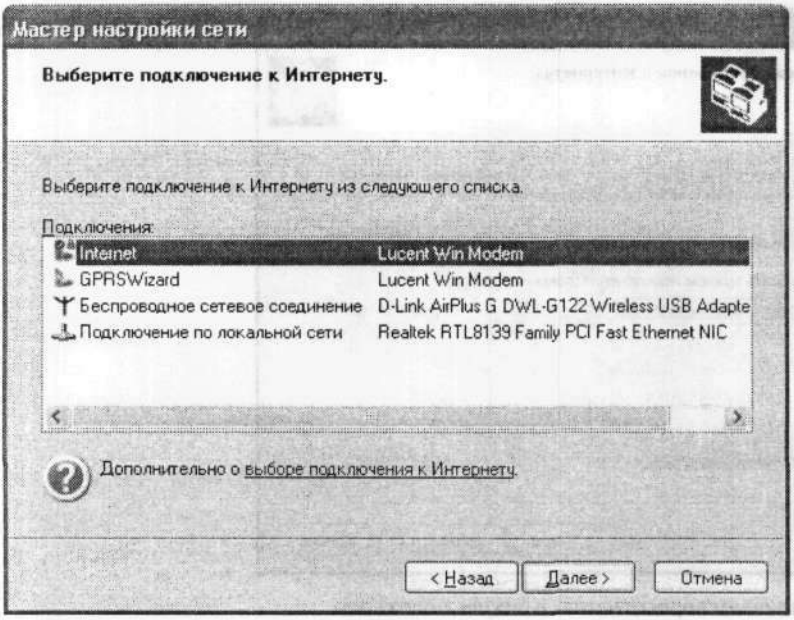

Рис. 15.1. Выбираем подключение к Интернету

Затем необходимо выбрать сетевые подключения, которые будут служить для выхода в Интернет. В рассматриваемом случае это сетевое подключение к беспроводной сети. На компьютере могут быть настроены и другие сетевые подключения, например к проводной части сети, для которой не должен быть установлен доступ в Интернет. Поэтому прежде чем связывать сетевые подключения, в следующем окне мастера необходимо установить переключатель в положение Я выберу сетевые подключения вручную (рис. 15.2).

После нажатия кнопки Далее появится окно, содержащее список подключений, которые необходимо связать с подключением к Интернету. Установите флажки только беспроводных подключений (рис. 15.3), после чего нажмите кнопку Далее.

В следующем окне вам предложат указать имя и описание данного компьютера. Описание дальнейшей работы с мастером см. в разд. 13.1.

После того как все изменения будут сделаны, вам необходимо будет перезагрузить компьютер.

Настройка компьютера-клиента

В предыдущем подразделе мы рассмотрели, как настроить общее подключение к Интернету, используя для этого модемный ресурс одного компьютера. Чтобы любой другой сетевой компьютер мог использовать общий Интернет, его также нужно настроить.

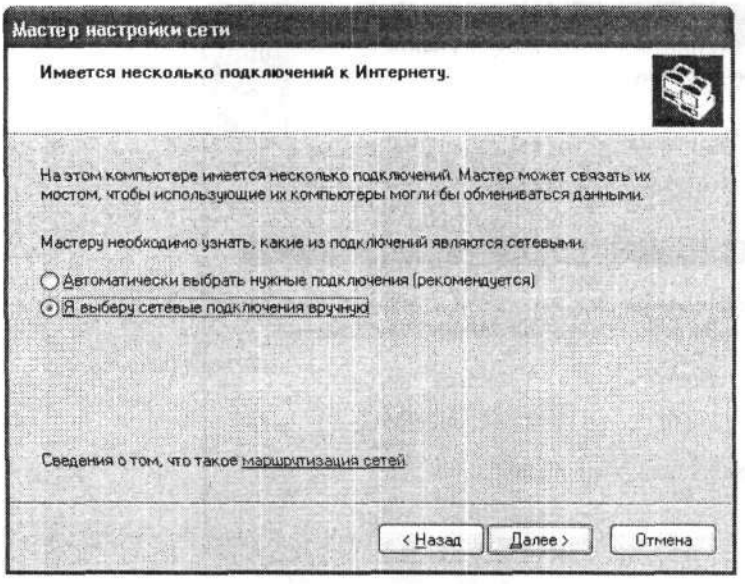

Рис. 15.2. Устанавливаем переключатель в нижнее положение

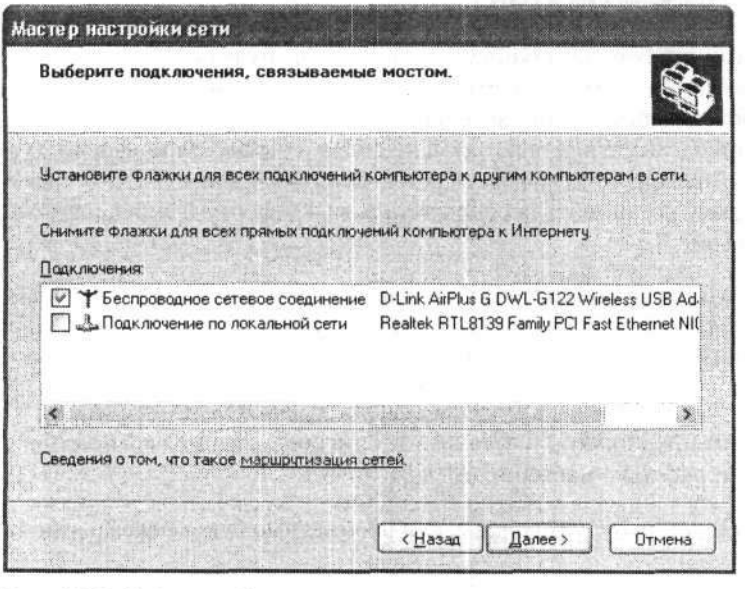

Рис. 15.3. Выбираем беспроводное подключение

При настройке главного компьютера (компьютера, через который все остальные компьютеры сети подключаются к Интернету) ему автоматически присваивается IP-адрес 192.168.0.1 и сетевая маска 255.255.255.0. Поэтому, чтобы клиентский компьютер смог получить доступ в Интернет, ему необходимо присвоить адрес 192.168.0.25.

Выполните команду Пуск ▸ Сетевое окружение и щелкните в левой части появившегося окна на ссылке Отобразить сетевые подключения. В результате откроется окно, содержащее все имеющиеся в системе сетевые подключения. В этом окне щелкните правой кнопкой мыши на значке нужного беспроводного подключения и в появившемся контекстном меню выберите пункт Свойства. Откроется окно свойств данного подключения. На вкладке Общие данного окна отображается список компонентов, которые использует выбранное подключение.

Найдите в списке пункт Протокол Интернета (TCP/IP), отметьте его указателем мыши и нажмите кнопку Свойства. Можно также дважды щелкнуть на данном пункте. Откроется окно свойств протокола TCP/IP (см. рис. 11.1), по умолчанию используемого для передачи данных в сети. Установите переключатель в положение Использовать следующий IP-адрес и в соответствующие поля введите IP-адрес подключения, маску подсети `255.255.255.0` и IP-адрес шлюза (в рассматриваемом случае — `192.168.0.1`).

Если в вашей беспроводной сети настроен DHCP-сервер[1] и вы не планируете присваивать статичный IP-адрес, то выполните следующие действия. В окне свойств протокола TCP/IP установите переключатель в положение Получить IP-адрес автоматически. Затем нажмите кнопку Дополнительно, в результате чего откроется окно с дополнительными параметрами протокола TCP/IP (рис. 15.4). На вкладке Параметры IP в области Основные шлюзы нажмите кнопку Добавить.

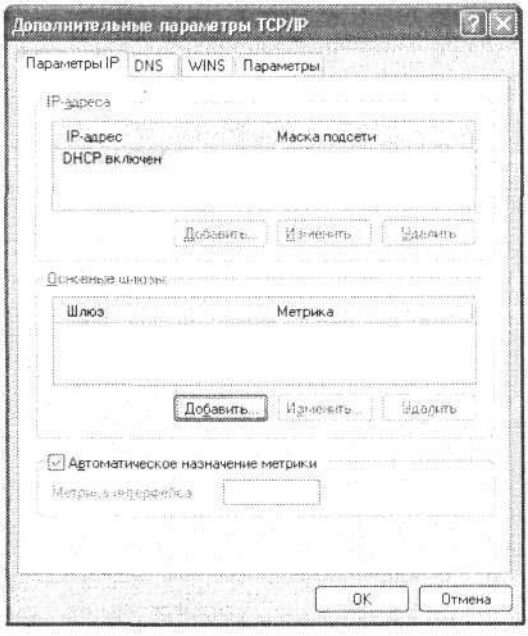

Рис. 15.4. Содержимое вкладки Параметры IP окна дополнительных параметров

[1] DHCP-сервер в этом случае должен быть настроен для выдачи адресов в описываемом диапазоне, например 192.168.0.2–192.168.0.10.

В результате откроется небольшое окно (рис. 15.5), содержащее всего одно поле для ввода. В этом поле наберите адрес шлюза — `192.168.0.1`.

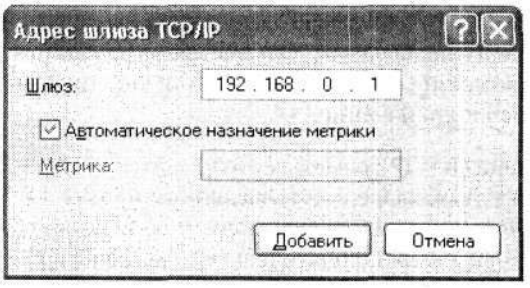

Рис. 15.5. Добавляем адрес шлюза

После этого закройте все окна нажатием кнопки `OK`. Настройка общего Интернета закончена.