Cisco Systems

СЕРИЯ "ПЕРВЫЙ ШАГ"

Беспроводные сети

Первый шаг

Ваш первый шаг в мир беспроводных сетей

- Не требуется никакого опыта работы с беспроводными сетями
- Все объясняется просто и доступно
- Обучение не требует особых усилий

www.williamspublishing.com
www.ciscopress.ru
ciscopress.com

Джим Гейер
Автор и независимый консультант

Беспроводные сети

Первый шаг

Wireless Networks

first-step

Jim Geier

Cisco Press
800 East 96th Street
Indianapolis, IN 46240

Беспроводные сети

Первый шаг

Джим Гейер

Москва • Санкт-Петербур • Киев
2005

ББК 32.973.26-018.2.75
Г29
УДК 681.3.07

Издательский дом "Вильяме"
Зав. редакцией С. Я. *Тригуб*
Перевод с английского и редакция *В.С. Гусева*

По общим вопросам обращайтесь в Издательский дом "Вильяме"
по адресу: info@williamspublishing.com, http://www.williamspublishing.com
115419, Москва, а/я 783; 03150, Киев, а/я 152

Гейер, Джим.

Г29 Беспроводные сети. Первый шаг : Пер. с англ. — М. : Издательский дом "Вильяме", 2005. — 192 с.: ил. — Парал. тит. англ.

ISBN 5-8459-0852-3 (рус.)

В книге приведены основные сведения о беспроводных компьютерных сетях, их компонентах и технологиях. Рассмотрены все разновидности беспроводных сетей — персональные, локальные, региональные и глобальные, рассказано об особенностях их структур, компонентов и методах применения. Особое внимание уделено вопросам безопасности беспроводных сетей, описаны механизмы аутентификации и шифрования.

Книга предназначена для тех, кто лишь приступает к изучению беспроводных сетей. От читателей не требуется какой-либо технической подготовки. Руководители компаний, менеджеры и бизнесмены, инженеры и техники, рядовые пользователи, желающие разобраться в том, как устроены беспроводные сети — все получат пользу от прочтения этой книги.

ББК 32.973.26-018.2.75

Книга подготовлена при участии Региональной сетевой академии Cisco, http://www.academy.ciscopress.ru.

ISBN 5-8459-0852-3 (рус.)
ISBN 1-58-720111-9 (англ.)

Оглавление

Введение 13

Глава 1. Беспроводной мир: введение в концепцию 17

Глава 2. Структура беспроводной системы: как работает беспроводная сеть 37

Глава 3. Основы передачи радио- и световых сигналов: невидимая среда 69

Глава 4. Беспроводные персональные сети: сети для коротких расстояний 85

Глава 5. Беспроводные персональные сети: сети для зданий и кампусов 97

Глава 6. Беспроводные региональные сети: для соединений между зданиями и отдаленными площадками 123

Глава 7. Беспроводные глобальные сети: сети для соединения по всему миру 133

Глава 8. Безопасность беспроводных сетей: способы защиты информации 149

Приложение А. Ответы на вопросы для самопроверки 173

Глоссарий 179

Предметный указатель 187

Содержание

Введение **13**

Для чего была написана эта книга 13
Для кого предназначена эта книга 13
Структура книги 13
Некоторые особенности книги и принятые в ней условные обозначения 14
От издательского дома "Вильяме" 15

Глава 1. Беспроводной мир: введение в концепцию **17**

Классификация беспроводных сетей 17
Беспроводные персональные сети 19
Беспроводные локальные сети 21
Беспроводные региональные сети 22
Беспроводные глобальные сети 24
Устанавливаем границы 25
Области применения беспроводных сетей 26
Основные конфигурации 26
Доступ в Internet 27
Передача речи без проводов 27
Управление запасами 28
Здравоохранение 28
Образование 29
Операции с недвижимостью 30
Коммунальные предприятия 30
Обслуживание в полевых условиях 30
Торговля в полевых условиях 31
Продажа через торговые автоматы 31
Общедоступные сети 31
Службы определения местонахождения 32
Преимущества беспроводной сети 33
Повышение эффективности и точности 33
Повышение надежности 34
Резюме 35
Вопросы для самопроверки 35

Глава 2. Структура беспроводной системы: как работает беспроводная сеть **37**

Компоненты беспроводных сетей 37
Пользователи 38
Компьютерные устройства 38
Платы интерфейса сети 39
Воздушная среда 42
Инфраструктуры беспроводных сетей 43
Контроллеры доступа 44

Применение программного обеспечения, обеспечивающег
о установление соединений 46
Распределительная система 49
Управляющие системы 52
Структура сети 54
Информационнце сигналы 57
Цифровые сигналы 57
Аналоговые сигналы 59
Передача информации через беспроводную сеть 59
Конечные точки информационного потока 59
Ввод, хранение и отображение информации 60
Взаимодействие с воздушной средой 60
Передача беспроводных сигналов 65
Подключение к инфраструктуре проводной сети 65
Резюме 66
Вопросы для самопроверки 66

Глава 3. Основы передачи радио- и световых сигналов: невидимая среда 69

Беспроводные приемопередатчики 69
Что Такое радиосигналы? 70
Параметры радиосигналов 70
Преимущества и недостатки радиочастотных сигналов 71
Искажение радиочастотного сигнала 72
Что такое световые сигналы? 74
Параметры светового сигнала 74
Преимущества и недостатки световых сигналов 75
Искажение световых сигналов 76
Модуляция: подготовка сигналов к передаче 77
Частотная манипуляция 77
Фазовая манипуляция 78
Квадратурная амплитудная модуляция 79
Расширение спектра 79
Мультиплексирование с разделением по ортогональным частотам 80
Сверхширокополосная модуляция 81
Резюме 82
Вопросы для самопроверки 82

Глава 4. Беспроводные персональные сети: сети для коротких расстояний 85

Компоненты беспроводных персональных сетей 85
Пользовательские устройства 85
Радиоплаты интерфейса сети 86
USB-адаптеры 86
Маршрутизаторы 87
Системы на основе беспроводных персональных сетей 87
Дом или небольшой офис 87
Технологии беспроводных персональных сетей 89
Стандарт 802.15 89
Bluetooth 90

IrDA 94
Резюме 95
Вопросы для самопроверки 95

Глава 5. Беспроводные персональные сети: сети для зданий и кампусов 97

Компоненты беспроводных локальных сетей 97
Системы беспроводных локальных сетей 101
Беспроводные локальные сети для домашнего применения 101
Беспроводные локальные сети предприятий 103
Неплановые беспроводные локальные сети 106
Технологии беспроводных локальных сетей 107
Стандарт 802.11 107
Wi-Fi , 117
Что означает Wi-Fi? 118
Защищенный доступ к Wi-Fi 118
HiperLAN/2 119
Преимущества HiperLAN/2 119
Угрожает ли HiperLAN/2 системам стандарта 802.11? 120
Резюме 121
Вопросы для самопроверки 121

Глава 6. Беспроводные региональные сети: для соединений между зданиями и отдаленными площадками 123

Компоненты беспроводных региональных сетей 123
Мосты 123
Направленные антенны 125
Системы беспроводных региональных сетей 127
Системы типа "точка-точка" 127
Системы пакетной радиосвязи 128
Технологии беспроводных региональных сетей 129
Стандарт 802.11 и Wi-Fi 129
Стандарт 802.16 130
Резюме 131
Вопросы для самопроверки 131

Глава 7. Беспроводные глобальные сети: сети для соединения по всему миру 133

Компоненты беспроводных глобальных сетей 134
Пользовательские устройства беспроводных глобальных сетей 134
Радиоплаты интерфейса сети 134
Базовые станции 135
Антенны 136
Системы беспроводных глобальных сетей 137
Беспроводные глобальные сети с сотовой структурой 137
Беспроводные глобальные сети на основе космических технологий 141
Метеорная связь 143
Технологии беспроводных глобальных сетей 144

Резюме 146
Вопросы для самопроверки 146

Глава 8. Безопасность беспроводных сетей: способы защиты информации 149

Угрозы безопасности 149
Мониторинг трафика 150
Неавторизованный доступ 150
Атаки типа "человек посредине" 151
Отказ в обслуживании 153
Шифрование 155
WEP 156
Как работает WEP? 157
Виртуальные частные сети 160
Аутентификация 160
Уязвимость механизма аутентификации стандарта 802.11 160
MAC-фильтры 161
Аутентификация с использованием открытого ключа шифрования 162
Стандарт 802.1x 162
Политика безопасности 164
Стадии оценки 165
Общая политика безопасности 167
Резюме 171
Вопросы для самопроверки 171

Приложение А. Ответы на вопросы для самопроверки 173

Глава 1 173
Глава 2 173
Глава 3 174
Глава 4 175
Глава 5 175
Глава 6 176
Глава 7 176
Глава 8 177

Глоссарий 179

Предметный указатель 187

Об авторе

Джим Гейер (Jim Geier) — основатель и главный консультант компании Wireless-Nets, Ltd. (www.wireless-nets.com), независимой консультационной фирмы, которая помогает компаниям разрабатывать и применять изделия и системы беспроводных локальных сетей. За 20 лет работы он приобрел опыт по анализу, конструированию, разработке программного обеспечения, установке и сопровождению многочисленных систем типа клиент-сервер и беспроводных сетей для предприятий, аэропортов, домов, магазинов, производственных подразделений, складов и больниц по всему миру.

Джим является членом с правом голоса Альянса Wi-Fi, ответственного за сертификацию пригодности к взаимодействию беспроводных локальных сетей стандарта 802.11 (Wi-Fi). Занимал пост председателя Компьютерного сообщества IEEE (IEEE Computer Society), секции Дейтона (Dayton Section), и председателя Международной конференции IEEE по применению беспроводных локальных сетей (IEEE International Conference on Wireless LAN Implementation). Был активным членом Рабочей группы по стандарту IEEE 802.11, ответственным за разработку международных стандартов на бес-.проводные локальные сети. Член консультативных советов нескольких лидирующих компаний, поставляющих беспроводные локадьные сети.

Написал несколько книг, в том числе *Wireless LANs* (SAMS, ISBN: 0672320584), *Wireless Networking Handbook* (MTP, ISBN: 15620563IX) и *Network Reengineering* (McGraw-Hill, ISBN: 007023034X), а также множество статей. Он также главный редактор сайта MobilizedSoftware.com, который своими онлайн-публикациями помогает разработчикам применять мобильные приложения.

Джим имеет степени бакалавра и магистра электротехники и магистра делового администрирования.

Написать письма Джиму можно по адресу: jimgeier@wireless-nets . com.

О технических рецензентах

Джоэл Баррет (Joel Barrett) — специалист по беспроводным технологиям компании Cisco Systems. Сертифицированный сетевой специалист (CCNP) по изделиям Cisco Systems, сертифицированный специалист по проектированию сетей (CCOP), в том числе беспроводных, а также сертифицированный системный инженер (MCSE) по продуктам Microsoft и сертифицированный инженер (администратор сетей) по NetWare. В компании Cisco Джоэл руководит консультативной группой по применению технологии канальной связи в обеспечение мобильности (channels technology advisory team for mobility), консультант виртуальной группы по мобильной связи для предприятий (enterprise mobility virtual team) и участник Программы по руководству внедрением мобильных технологий Cisco на предприятиях (Cisco's enterprise mobility technology leadership program). Является консультантом Форума по беспроводным технологиям (wireless technology forum), а также соавтором и главным техническим редактором книг по технологиям беспроводных локальных сетей: *CWSP Official Study Guide u Managing and Securing a Cisco Structured Wireless-Aware Network*.

Джоэл, его жена, Барбара Курт, сын и две дочери живут близ Атланты, шт. Джорджия. Его персональный Web-сайт располагается по адресу www. brainslap. com/joel.

Д. Эд Лэмпрехт (D. Ed Lamprecht) — руководитель Группы профессиональных услуг компании Monarch Marking Systems, которая занимается, в основном, клиентским программным обеспечением и сетевыми решениями. Имеет 17-летний опыт разработки приложений, операционных систем и программирования сетевых задач. В 1998 г. Эд начал работать в Monarch Marking Systems— компании, специализирующейся на принтерах штрих-кодов и этикеток. С 1996 года Эд занимается разработкой систем сбора данных, обеспечивающих соединения с беспроводной сетью ручных принтеров и терминалов сбора данных для сфер торговли, промышленности, производства и здравоохранения.

В компании Monarch Marking Systems Эд разрабатывал приложения типа клиент/сервер, посещал клиентов с целью анализа и решения проблем и обучал персонал работе с изделиями и беспроводными соединениями. Владеет семью патентами на программное обеспечение для штрих-кодов и ручные принтеры/устройства сбора данных.

Эд вместе со своей женой Мишель и сыном Колином живет в Дэйтоне, шт. Огайо. Если он не занят дома компьютерами и домашней сетью, то моделирует железные дороги, собирает реликвии, относящиеся к железной дороге, играет в гольф, путешествует или проводит время со своей семьей.

Джозеф Рот (Joseph Roth), лейтенант-коммандер (lieutenant commander) ВМС США, сейчас проходит службу как военный профессор и руководитель Группы защиты сетей в аспирантуре ВМС (Naval postgraduate school, NFS). Имеет четыре степени магистра: компьютерных наук (NPS), технологии информационных систем (NPS), государственного управления (университет штата'Мэриленд) и национальной безопасности и стратегических исследований (Высший военно-морской колледж). Джозеф также получил степень бакалавра вычислительной техники в университете им. Джорджа Вашингтона и два сертификата о высшем образовании Кембриджского университета. Имеет многочисленные промышленные сертификаты, включая CCNA, CWNA, Security +, Network + и MCP. Его статьи публиковались в изданиях *InfoWorld u Federal Computer Week*. Джозеф пять лет служил в Европе, был на Балканах и Среднем Востоке.

Посвящения

Мэдисон, Сьерре и Эрику

Благодарности

Я хотел бы поблагодарить моего сына, Эрика Гейера, за помощь в проведении исследований для этой книги. Эрик относится к техническому персоналу моей консультационной компании, Wireless-Nets, Ltd., где он анализирует и исследует технологии беспроводных сетей, проводит анализ беспроводных локальных сетей и разрабатывает тренировочные курсы, основанные на использовании компьютеров.

Эрик— сертифицированный специалист по беспроводным сетям (certified wireless network professional, CWNP) и основатель Web-сайта www.wirelessnetworks4homes.com, посвященного применению беспроводных локальных сетей в домах и небольших офисах.

Введение

Уже несколько десятилетий люди применяют компьютерные сети для обеспечения связи между персоналом, компьютерами и серверами в компаниях, колледжах и городах. Однако наблюдается тенденция ко все более широкому использованию беспроводных сетей. И действительно, сейчас доступны беспроводные интерфейсы, позволяющие использовать сетевые службы, работать с электронной почтой и просматривать Web-страницы независимо от того, где находится пользователь.

Эти беспроводные приложения позволяют людям "расширить" свое рабочее место и получить в результате этого ряд преимуществ. Во время деловых поездок можно, например, отправлять электронные письма в ожидании посадки на самолет в аэропорту. Домовладельцы могут с легкостью использовать общее Internet-соединение для многих ПК и ноутбуков без прокладки кабелей. В этой книге рассказывается о технологиях, позволяющих реализовывать приложения таких типов.

Для чего была написана эта книга

Цель нашей книги — дать основные сведения о применении беспроводных сетей, их компонентах и технологиях. Рассмотренные здесь концепции дадут солидную основу для более подробного изучения в дальнейшем различных тем, относящихся к беспроводным сетям. После прочтения этой книги.вы сможете эффективно продолжить изучение конкретных беспроводных сетей.

Для кого предназначена эта книга

Эта книга написана для тех, кто приступает к изучению беспроводных сетей. От читателей не требуется какой-либо технической подготовки. Исполнительные директора компаний, менеджеры и бизнесмены, инженеры и техники получат пользу от прочтения этой книги. Даже пользователи, желающие разобраться в том, как работает беспроводная сеть, найдут в этой книге много интересного.

Структура книги

В книге рассмотрены все аспекты беспроводных сетей, особое внимание уделяется уникальным особенностям беспроводных систем. В первых трех главах даны основы предмета для лучшего понимания в дальнейшем, из каких узлов собираются сети, описанные в последующих главах. В заключительной главе достаточно подробно проанализированы проблемы безопасности беспроводных сетей.

В главе 1, "Беспроводной мир: введение в концепцию", даны основные определения, относящиеся к беспроводным сетям, и кратко описаны их основные типы. Рассматриваются многие варианты применения беспроводных сетей и обсуждаются получаемые в результате их использования преимущества.

Глава 2, "Структура беспроводной системы: как работает беспроводная сеть", посвящена различным компонентам беспроводных сетей. Рассказано, как в сети распространяются информационные потоки, благодаря чему материал главы является

великолепной основой для понимания в дальнейшем, как работают беспроводные сети различных типов.

В главе 3, "Основы передачи радио- и световых сигналов: невидимая среда", подробно описано, как электромагнитные волны радиодиапазона и световые сигналы могут передавать информацию через воздушную среду. Это основные элементы, делающие сеть беспроводной.

В главе 4, "Беспроводные персональные сети: сети для коротких расстояний", проанализированы компоненты, технологии и конфигурации беспроводных персональных сетей (PAN).

Глава 5, "Беспроводные локальные сети: сети для зданий и кампусов", посвящена компонентам, технологиям и конфигурациям беспроводных локальных сетей (LAN).

В главе 6, "Беспроводные региональные сети: для соединений между зданиями и отдаленными площадками", даны компоненты, технологии и конфигурации беспроводных региональных сетей (MAN).

В главе 7, "Беспроводные глобальные сети: сети для соединения по всему миру", рассмотрены компоненты, технологии, и конфигурации беспроводных глобальных сетей (WAN).

В главе 8, "Безопасность беспроводных сетей: способы защиты информации", описаны потенциальные угрозы беспроводным сетям и возможные контрмеры. При развертывании беспроводных сетей важно помнить о проблемах безопасности, возникновение которых обусловлено природой беспроводных сигналов.

Приложение А, " Ответы на вопросы для самопроверки". В этом приложении приведены ответы на контрольные вопросы, которыми заканчивается каждая глава, и необходимые пояснения.

Глоссарий поможет быстро найти основные англоязычные термины, упоминаемые в книге, и уточнить их значение.

Некоторые особенности книги и принятые в ней условные обозначения

Эта книга имеет некоторые особенности, которые помогут читателю быстрее овладеть представленными в ней темами. Ниже описаны все элементы текста, которые вы найдете в книге.

"В этой главе...". Каждый тематический раздел начинается с перечня целей, которые должны быть достигнуты в результате прочтения материала, а также они указывают, что именно вы должны освоить.

Ключевые термины и глоссарий. Ключевые термины, встречающиеся в книге, выделены полужирным курсивным шрифтом. Эти понятия играют достаточно важную роль в беспроводных сетях. Незнакомые термины или те, которые следует освежить в памяти, читатель найдет в словаре терминов — глоссарии, приведенном в конце книги.

Резюме. Каждая глава заканчивается кратким изложением всего представленного в ней материала, в котором еще раз напоминаются цели главы и обсуждается связь ее содержимого с материалом других глав.

Вопросы для самопроверки. В каждую главу включено несколько обзорных вопросов. Ответив на них, читатель сможет понять, насколько хорошо им усвоены основные идеи и концепции данной главы.

Нетехнические заголовки и пояснения. В заголовках и тексте всей книги авторы по возможности избегали использования технических терминов. Вместо этого внимание концентрировалось на словах, имеющих отношение к обсуждаемой в данный момент концепции.

В иллюстрациях книги использованы следующие пиктограммы для обозначения сетевых устройств и соединений:

От издательского дома "Вильяме"

Вы, читатель этой книги, и есть главный ее критик. Мы ценим ваше мнение и хотим знать, что было сделано нами правильно, что можно было сделать лучше и что еще вы хотели бы увидеть изданным нами. Нам интересно услышать и любые другие замечания, которые вам хотелось бы высказать в наш адрес.

Мы ждем' ваших комментариев и надеемся на них. Вы можете прислать нам бумажное или электронное письмо либо просто посетить наш Web-сервер и оставить свои замечания там. Одним словом, любым удобным для вас способом дайте нам знать, нравится ли вам эта книга, а также выскажите свое мнение о том, как сделать наши книги более интересными для вас.

Посылая письмо или сообщение, не забудьте указать название книга и ее авторов, а также ваш обратный адрес. Мы внимательно ознакомимся с вашим мнением и обязательно учтем его при отборе и подготовке к изданию последующих книг. Наши координаты:

E-mail: info@wi 11 iamspublishing. com
WWW: http://www.williamspublishing.com

Информация для писем из

России: 115419, Москва, а/я 783
Украины: 03150, Киев, а/я 152

В этой главе...

- *S* сходство и отличия персональных локальных региональных и глобальных беспроводных сетей;
- *s* наиболее распространенные сетевые приложения;
- *S* основные преимущества беспроводных сетей.

ГЛАВА 1

Беспроводной мир: введение в концепцию

Беспроводные сети играют важную роль в жизни людей, где бы они ни находились — на работе, дома или в общественном месте. Даже если беспроводная сеть создается с простой целью — обеспечить связь пользователей с источниками информации без использования проводов, нужно вначале разобраться в основных концепциях беспроводных сетей, а потом уже выяснять, как они работают. В этой главе рассмотрены основные определения, относящиеся к беспроводным сетям, и показано, какую пользу они могут принести в том или ином случае.

Классификация беспроводных сетей

Беспроводные сети позволяют людям связываться и получать доступ к приложениям и информации без использования проводных соединений. Это обеспечивает свободу передвижения и возможность использования приложений, находящихся в других частях дома, города или в отдаленном уголке мира. Например, человек, осуществляющий из своего дома поиск информации в Internet, может делать это вдали от шумных детей или сидя перед телевизором вместе со всей семьей. Беспроводные сети позволяют людям получать электронную почту или просматривать Web-страницы там, где им удобно или нравится это делать.

Беспроводные сети соседствуют с нами уже многие годы. Так, к примитивным формам беспроводной связи можно отнести дымовые сигналы американских индейцев, когда они бросали в огонь шкуры бизонов, чтобы передать на большое расстояние какое-то сообщение. Или использование прерывистых световых сигналов для передачи посредством азбуки Морзе информации между кораблями, этот метод был и остается важной формой связи в мореплавании. И, конечно, столь популярные ныне сотовые телефоны, позволяющие людям общаться через огромные расстояния, также можно отнести к беспроводной связи.

Существует множество разновидностей беспроводной связи, но важнейшей особенностью беспроводных сетей является то, что связь осуществляется между компьютерными устройствами. К ним относятся *персональные цифровые помощники* ***(personal digital assistance, PDA),*** ноутбуки, персональные компьютеры (ПК), серверы и принтеры. Компьютерными устройствами считаются такие, которые имеют процессоры, память и средства взаимодействия с какой-то сетью. Обычно сотовые телефоны не относят к числу компьютерных устройств, однако новейшие телефоны и даже головные гарнитуры (наушники) уже обладают определенными вычислительными возможностями и сетевыми адаптерами. Все идет к тому, что скоро большинство электронных устройств будут обеспечивать возможность подключения к беспроводным сетям.

Как и сети, основанные на использовании проводов или *оптических волокон (optical fiber),* беспроводные сети передают информацию между компьютерными устройствами. Эта информация может быть представлена в виде сообщений электронной почты, Web-страниц, записей базы данных, потокового видео или голосовых сообщений. В большинстве случаев беспроводные сети передают *данные (data),* такие как сообщения электронной почты и файлы, но по мере улучшения характеристик беспроводных сетей они способны передавать и видеосигналы, а также обеспечивать телефонную связь.

Беспроводные сети в качестве средства передачи для обеспечения взаимодействия между пользователями, серверами и базами данных используют радиоволны или инфракрасный (ИК) диапазон[1]. Эта среда передачи невидима для человека. Кроме того, действительная среда передачи (воздух) прозрачна для пользователя. Сейчас многие производители интегрируют платы интерфейса сети (network interface card, NIC), так называемые сетевые адаптеры, и антенны в компьютерные устройства таким образом, что они не видны пользователю. Это делает беспроводные устройства мобильными и удобными в применении.

В зависимости от размеров физической зоны, связь в которой они способны обеспечить, беспроводные сети подразделяются на несколько категорий:

- беспроводная персональная сеть (wireless personal-area network, PAN);
- беспроводная локальная сеть (wireless lokal-area network, LAN);
- беспроводная городская сеть (wireless metropolitan-area network, MAN);
- беспроводная глобальная сеть (wireless wide-area network, WAN).

Эти термины являются лишь расширением обобщенных форм проводных сетей (таких как LAN и WAN), использовавшихся задолго до появления беспроводных сетей.

В табл. 1.1 дана краткая характеристика разновидностей таких сетей. Каждый тип беспроводной сети имеет дополняющие другие сети особенности, благодаря чему удовлетворяются различные предъявляемые к сетям требования.

Таблица 1.1. Разновидности беспроводных сетей

Тип	Сфера дейсгвия	Характеристики	Стандарты	Область применения
Персональная беспроводная сеть	В непосредственной близости от пользователя	Средние	Bluetooth, IEEE 802.15, IRDA[2]	Замена кабелей периферийных устройств
Локальные беспроводные сети	В пределах зданий и кампусов	Высокие	IEEE 802.15, Wi-Fi, HiperLAN	Мобильные расширения проводных сетей

[1] *Подробнее об этом в главе 3.* — Прим. ред.

[2] *Стандарт на передачу данных в инфракрасном диапазоне с выводом на печать.* — Прим. ред.

Окончание табл. 1.1

Тип	Сфера действия	Характеристики	Стандарты	Область применения
Региональные беспроводные сети	В пределах города	Высокие	Патентованные, IEEE 802.16, WIMAX	Фиксированная беспроводная связь между зданиями и предприятиями и Internet
Глобальные беспроводные сети	По всему миру	Низкие	CDPD[1] и сотовые системы телефонной связи поколений 2, 2,5 и 3	Мобильный доступ к Internet вне помещений

Беспроводные персональные сети

Беспроводные персональные сети отличаются небольшими расстояниями передачи (до 17м, или 50 футов), что делает их идеальными для развертывания в небольшом помещении или в "персональной зоне" (рис. 1.1). Характеристики беспроводных персональных сетей средние, скорость их передачи не превышает обычно 2 Мбит/с. Во многих ситуациях они с успехом заменяют кабельные сети.

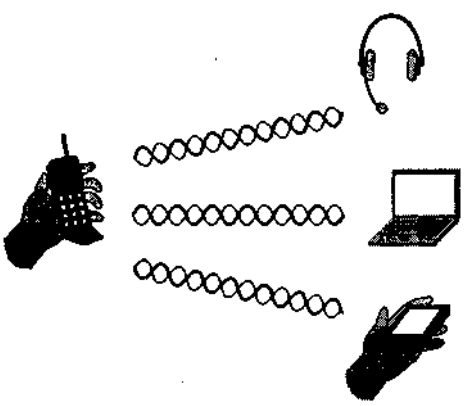

Рис. 1.1. Беспроводные персональные сети обеспечивают взаимодействие компьютерных устройств в непосредственной близости от пользователя

Такая сеть могла бы обеспечивать, например, беспроводную синхронизацию данных на PDA пользователя и на его ПК или ноутбуке. Аналогичным образом может обеспечиваться беспроводное соединение с принтером. Исчезновение путаницы проводов, связывающих компьютер с периферийными устройствами — достаточно серь-

[3] *Стандарт CDPD —- Cellular Digital Packet Data (сотовая система передачи пакетов цифровых данных).* — Прим. ред.

езное преимущество, благодаря которому значительно облегчается начальная установка и последующее, при необходимости, перемещение периферийных устройств.

Малая потребляемая мощность и компактные размеры большинства *приемопередатчиков (transceiver)* беспроводных персональных сетей делают возможной эффективную поддержку небольших пользовательских устройств, снабженных микропроцессорами, а также позволяет компьютерному устройству длительное время работать от одной батареи (или аккумулятора). Это, в свою очередь, избавляет пользователя от необходимости часто подзаряжать аккумулятор. Кроме того, малая потребляемая мощность обусловила успешное внедрение беспроводных персональных сетей в сотовые телефоны, PDA и головные гарнитуры. Телефон может непрерывно взаимодействовать с адресной книгой PDA, так что все номера телефонов в менеджере контактов пользователя оказываются доступны, когда он собирается кому-нибудь позвонить. Можно также использовать наушники во время телефонного разговора или для прослушивания музыки, записанной в цифровом виде на PDA. Благодаря этому во время работы или развлечений можно не опасаться зацепиться за что-нибудь проводами.

Персональные беспроводные сети могут обеспечить взаимодействие ноутбуков и настольных ПК с целью совместного использования подключений к Internet и приложений. Это подходит для сетей, сфера действия которых ограничена одной комнатой. А беспроводные локальные сети эффективнее для организации беспроводных соединений в пределах здания.

В большинстве беспроводных персональных сетей для передачи информации используются радиоволны. Так, спецификация на технологию *Bluetooth* регламентирует работу беспроводных персональных сетей в диапазоне 2,4 ГГц на расстояние до 50 футов со скоростью передачи до 2 Мбит/с. Более того, Институт инженеров по электротехнике и электронике США (Institute of Electrical and Electronics Engineers, IEEE) включил в свой стандарт *802.15 для* персональных беспроводных сеть спецификацию Bluetooth. Эта технология обеспечивает надежное и долговременное решение для соединения компьютерных устройств в небольшой зоне.

В некоторых беспроводных персональных сетях для передачи информации из одной точки в другую используется ИК-излучение. Спецификация Ассоциации передачи данных в ИК-диапазоне (Infrared Data Association, IrDA) регламентирует использование направленных ИК-лучей для передачи информации на расстояние до 1 м (3 футов) со скоростью до 4 Мбит/с. Преимущество такой передачи информации состоит в защищенности ее от радиопомех, но требование нахождения компьютерных устройств на расстоянии прямой видимости по отношению друг к другу накладывает существенные ограничения на размещение компонентов беспроводной сети. Офисная перегородка, например, блокирует распространение ИК-сигнала, из-за чего беспроводные устройства можно использовать лишь в непосредственной близости одно от другого.

О технологиях персональных беспроводных сетей и их компонентах — в главе 4.

Беспроводные локальные сети

Беспроводные локальные сети обеспечивают высокие характеристики при передаче данных внутри и вне офисов, производственных помещений и зданий (рис. 1.2). Пользователи таких сетей обычно используют ноутбуки, ПК и PDA с большими экранами и процессорами, способными выполнять ресурсоемкие приложения. Эти сети вполне удовлетворяют требованиям, предъявляемым к параметрам соединений компьютерными устройствами такого типа.

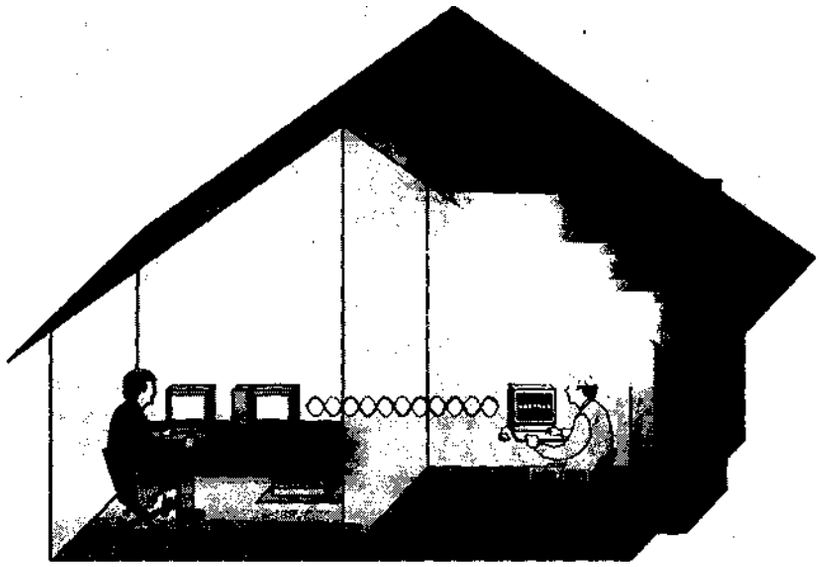

Рис. 1.2. Беспроводные локальные сети обеспечивают взаимодействие компьютерных устройств в пределах здания

В какой-нибудь фирме, например, беспроводная локальная сеть может быть развернута с целью обеспечения доступа к корпоративным приложениям с ноутбуков. В системах такого типа служащий может использовать сетевые службы, находясь в конференц-зале или в других помещениях здания, что позволяет ему эффективно выполнять свои обязанности.

Беспроводные локальные сети легко обеспечивают характеристики, необходимые для бесперебойного выполнения высокоуровневых приложений. Так, пользователи этих сетей могут получать объемные вложения в сообщения электронной почты или потоковое видео с сервера. При скоростях передачи до 54 Мбит/с беспроводные локальные сети способны удовлетворять требования почти всех офисных или бытовых приложений.

По своим характеристикам, компонентам, стоимости и выполняемым операциям эти сети похожи на традиционные проводные локальные сети типа Ethernet.

Вследствие того, что адаптеры беспроводных локальных сетей уже встроены в большинство ноутбуков, многие провайдеры общедоступных беспроводных сетей начали предлагать беспроводные локальные сети для обеспечения мобильного широкополосного доступа к Internet. Пользователи ряда общедоступных беспроводных

сетей в "горячих" зонах доступа, таких как аэропорты или гостиницы, могут отправлять и получать сообщения электронной почты или выходить в Internet за определенную плату (если данное учреждение не обеспечивает бесплатный доступ). Быстрый рост числа общедоступных беспроводных сетей делает Internet доступным для пользователей, находящихся в зонах скопления людей.

Преобладающим для беспроводных локальных сетей является стандарт IEEE *S02.ll,* различные версии которого регламентируют передачу данных в диапазонах 2,4 и 5 ГГц. Основная проблема, связанная с этим стандартом, состоит в том, что в должной мере не обеспечивается взаимодействие устройств, соответствующих его различным версиям. Так, адаптеры компьютерных устройств беспроводных локальных сетей стандарта 802.11a не обеспечивают соединения с компьютерными устройствами, соответствующими стандарту 802.lib. Существуют и другие нерешенные вопросы, связанные со стандартом 802.11, например недостаточная степень безопасности.

Для того чтобы как-то разрешить проблемы, связанные с применением устройств стандарта 802.11, организация "Альянс Wi-Fi" свела все его совместимые функции в единый стандарт, названный *Wireless Fidelity (Wi-Fi).* Если какое-то устройство беспроводных локальных сетей соответствует стандарту Wi-Fi, это практически гарантирует способность его совместной работы с другими устройствами, соответствующими стандарту Wi-Fi. Открытость стандарта Wi-Fi позволяет различным пользователям, применяющим разные платформы, работать в одной и той же беспроводной локальной сети, что чрезвычайно важно для общедоступных беспроводных локальных сетей.

О технологиях беспроводных локальных сетей и соответствующих им уст-

Беспроводные региональные сети

Беспроводные региональные (городские) сети обслуживают зоны, по площади соответствующие городу. В большинстве случаев для выполнения приложений требуется фиксированное соединение, но иногда необходима мобильность. Например, в больнице такая сеть обеспечит передачу данных между основным корпусом и удаленными клиниками. Или энергетическая компания, используя ее в масштабах города, обеспечит доступ к нарядам на работу из различных его районов. Как результат, беспроводные региональные сети соединят существующие сетевые инфраструктуры воедино или позволят мобильным пользователям устанавливать соединения с уже существующей сетевой инфраструктурой.

Поставщики услуг беспроводного Internet (Wireless Internet Service Provider, WISP) предоставляют в распоряжение клиентов беспроводные региональные сети в городах и сельской местности (рис. 1.3) для обеспечения постоянных беспроводных соединений для домашних пользователей и компаний. Подобные сети имеют существенные преимущества перед обычными проводными соединениями (такими как цифровые абонентские линии (Digital Subscriber Line, DSL) и кабельные модемы), когда последние трудно установить. Они эффективны, когда ограничения, связанные с прокладкой проводных соединений, делают невозможным или слишком дорогим их применение.

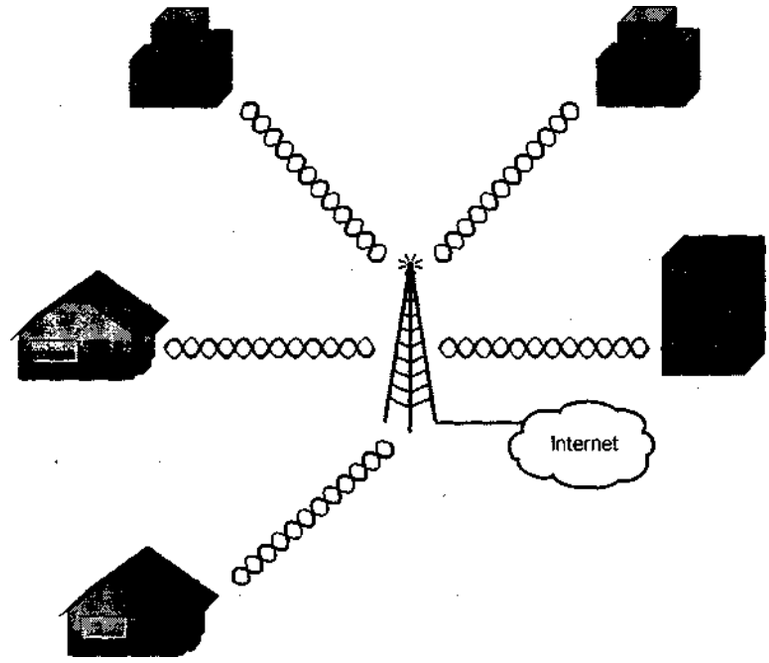

Рис. 1.3. Беспроводные региональные сети являются альтернативой для применения в домашних условиях или в компаниях для получения доступа к Internet

Характеристики беспроводных региональных сетей различны. Соединения между строениями с использованием ИК-технологии могут обеспечивать скорость передачи данных 100 Гбит/с и более, у радиоканалов скорость передачи до 100 кбит/с, но на расстояния свыше 30 км (20 миль). Реальные же характеристики зависят от того, какой именно выбор был сделан среди многих технологий и компонентов.

Рынок предлагает множество патентованных решений для беспроводных региональных сетей, однако промышленность все же ориентируется на стандарты. Некоторые поставщики используют стандарт 802.11 в качестве основы создания беспроводных региональных сетей. Хотя системы этого стандарта оптимальны для удовлетворения требований, предъявляемым к сетям внутри зданий, они могут обеспечивать соединения и в масштабах города с использованием направленных антенн.

Сейчас все большее число компаний предпочитают системы стандарта IEEE 802.16. Это относительно новый стандарт, а соответствующие ему изделия не так давно появились на рынке. Предлагая стандартизированные решения для беспроводных региональных сетей со скоростью передачи порядка нескольких Мбит/с и на приемлемые расстояния, стандарт 802.16 со временем может стать общепринятым для беспроводных региональных сетей.

О технологии и устройствах беспроводных региональных сетей — в главе 5.

Беспроводные глобальные сети

Беспроводные глобальные сети обеспечивают работу мобильных приложений с обеспечением доступа к ним в масштабе страны или даже континента. Руководствуясь экономическими соображениями, телекоммуникационные компании будут развертывать, по-видимому, относительно дорогую инфраструктуру беспроводной глобальной сети, способной обеспечить соединения на больших расстояниях для множества пользователей. Затраты на подобное развертывание могут быть распределены среди всех пользователей, вследствие чего абонентская плата окажется невысокой.

Беспроводные глобальные сети имеют почти неограниченную сферу действия, что обеспечивается за счет кооперации многих телекоммуникационных компаний (рис. 1.4). Доступные соглашения по роумингу между телекоммуникационными операторами делают возможным установление протяженных соединений, обеспечивающих быструю передачу данных мобильным пользователем. Заплатив одному поставщику телекоммуникационных услуг, он может получить ограниченный доступ к ряду служб Internet через беспроводную глобальную сеть практически из любой точки мира.

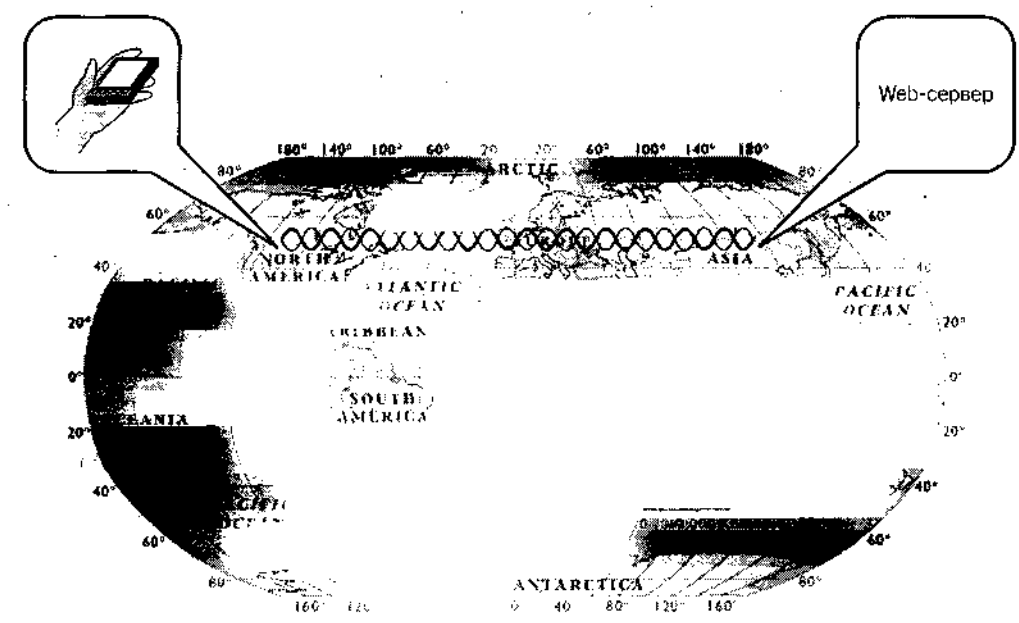

Рис. 1.4. Беспроводная глобальная сеть способна поддерживать мобильные приложения по всему миру

Характеристики беспроводной глобальной сети относительно невысокие, типичная скорость передачи данных составляет 56 кбит/с, иногда до 170 кбит/с. Это аналогично уровню, обеспечиваемому при связи по коммутируемым телефонным линиям посредством модемов. Однако уже созданы специальные Web-порталы, эффективно работающие с потоковой информацией при посредстве компактных устройств и сетей с низкими характеристиками.

Скорость передачи данных в пересчете на одного пользователя беспроводных глобальных сетей относительно невысока, но в общем приемлема для небольших

устройств (сотовых телефонов, PDA), которые имеют пользователи, нуждающиеся в связи через такую сеть. Меньшие размеры экрана и ограниченные вычислительные возможности сотовых телефонов не требуют высоких характеристик от сети. Передача видеоизображения на небольшой экран сотового телефона или PDA может состояться и при меньшей скорости передачи данных.

Приложения, характерные для беспроводных глобальных сетей — это обеспечивающие доступ пользователей к Internet, передачу и прием сообщений электронной почты и доступ к корпоративным приложениям при нахождении пользователя вне дома или офиса. Абоненты могут, например, устанавливать соединения во время поездок в такси или прогулок по городу. Беспроводная глобальная сеть может-осуществляться из мест, откуда нет доступа к сетям других типов, благодаря чему пользователь не регламентирован территориально.

Существует несколько конкурирующих, постепенно развивающихся стандартов по беспроводным глобальным сетям. Один из наиболее старых — это стандарт на *сотовую систему передачи пакетов цифровых данных* ***(Cellular Digital Packet Data, CDPD).*** Эта технология обеспечивает передачу данных через аналоговую систему сотовой телефонной связи со скоростью 19,2 кбит/с. Некоторые компании США все еще предлагают услуги CDPD, но эта система уже выходит из употребления, поскольку телекоммуникационные операторы переходят на системы телекоммуникаций третьего поколения (third generation, 3G), способные передавать данные со скоростями, измеряемыми уже в Мбит/с.

Одна из проблем, связанных с внедрением технологии беспроводных глобальных сетей, состоит в том, что сама по себе она не способна обеспечить связь для пользователей, находящихся в каких-либо помещениях. Поскольку элементы инфраструктуры этих сетей находятся вне помещений, радиосигналы в зданиях значительно ослабляются. В результате пользователи беспроводных глобальных сетей, находящиеся внутри зданий, могут вообще потерять возможность установления соединения или, в лучшем случае, характеристики связи значительно ухудшатся. Некоторые телекоммуникационные компании устанавливают системы беспроводных глобальных сетей внутри зданий, но обходится это дорого и технически не всегда оправданно.

О технологии и устройствах беспроводных глобальных сетей — в главе 7.

Устанавливаем границы

Беспроводные персональные, локальные, региональные и глобальные сети являются взаимодополняющими и удовлетворяют различным требованиям. Однако иногда бывает трудно отличить одну сеть от другой. Например, беспроводная локальная сеть внутри здания может обеспечивать соединение между PDA и ПК одного и того же пользователя, аналогично тому, что выполняет персональная беспроводная сеть.

Четко установить различие между беспроводными сетями разных типов позволяют применяемые технологии и стандарты. Беспроводные персональные сети в основном соответствуют стандарту IEEE 802.15 (или Bluetooth), беспроводные локальные сети — стандарту IEEE 802.11 (или Wi-Fi) и т.д. Главное при развертывании беспроводной сети — это полностью определить предъявляемые к системе требования и выбрать тот ее тип, который наилучшим образом этим требованиям соответствует.

Если говорить о перспективах с точки зрения пользователя, то границы между беспроводными сетями разных типов должны быть стерты. Уже появляются платы интерфейса сети компьютерных устройств, которые поддерживают работу в беспроводных сетях разных типов. Например, у туриста или бизнесмена может быть современный сотовый телефон, обеспечивающий взаимодействие как с беспроводной локальной, так и с беспроводной глобальной сетью. Это обеспечивает бесшовное беспроводное соединение, в ходе которого в здании аэропорта пользователь работает со своей электронной почтой, используя общедоступную беспроводную локальную сеть, а затем по дороге в гостиницу взаимодействует уже с одной из служб, основанных на передаче данных через сотовую сеть.

Области применения беспроводных сетей

Беспроводные сети поддерживают множество приложений, которые выгодны для пользователя тем, что обеспечивают его мобильность и высокую надежность связи в отличие от подверженных сбоям кабельных соединений. Более того, во многих случаях благодаря применению беспроводных сетей достигается существенная экономия средств за счет повышения эффективности труда и уменьшения количества периодов вынужденного бездействия, возникающих при применении проводных сетей. Для использования большинства технологий беспроводных сетей не требуется лицензия, что делает их развертывание простым и экономически выгодным.

Основные конфигурации

В большинстве случаев беспроводная сеть — это просто расширение какой-нибудь уже существующей проводной сети. В этом случае служащий может выполнять определенное задание, находясь в оптимальном для этого месте, а не там, где у него есть доступ к проводной сети. Например, работник склада может использовать беспроводное ручное устройство для сканирования предметов, разгружаемых из грузовика. Это намного эффективнее, чем записывать их номера с последующим введением их в настольный терминал, находящийся где-то в помещении, далеко от погрузочной платформы.

Другая ситуация — специализированная беспроводная сеть, полностью устраняющая необходимость в каких-то проводах. Так, спасательная команда, прибывшая на место авиакатастрофы, может быстро развернуть временную беспроводную сеть непосредственно на месте катастрофы. Все компьютерные устройства спасателей будут напрямую взаимодействовать друг с другом. Это даст им возможность иметь централизованный доступ к важной информации, касающейся катастрофы.

Приложения, доступные через беспроводные сети, могут предоставляться пользователям приватным образом или открыто. Компания или владелец дома, приобретающий и устанавливающий беспроводную сеть для частного пользования, предоставляет ограниченный доступ к такой сети. Как правило, доступ предоставляется только служащим компании или квартиросъемщикам. Для того чтобы только авторизованные пользователи могли подключиться к такой сети и воспользоваться ее услугами, компании обычно применяют меры защиты. С другой стороны, общедоступные сети обеспечивают открытый доступ к своим ресурсам. Например, бизнесмен может воспользоваться общедоступной беспроводной сетью аэропорта для выхода в Internet в ожидании посадки в самолет. Эти "горячие" зоны свободного доступа появились уже во многих аэропортах, гостиницах и даже кафе, т.е. там, где в этом есть потребность.

Доступ в Internet

Одна из основных причин для развертывания беспроводной сети — необходимость совместного использования одного высокоскоростного канала доступа в Internet. При таком типе конфигурирования сети каждый член семьи или небольшой фирмы может использовать одно на всех высокоскоростное соединение, обеспечиваемое кабельным модемом или цифровой абонентской линией (Digital Subscriber Line, DSL). Такая практика общепринята и позволяет экономить средства, поскольку многие одновременно могут получать доступ в Internet, находясь при этом в Любом уголке дома или офиса.

Беспроводная сеть в такой ситуации имеет повышенную гибкость, потому что в любой момент в нее можно ввести новую-рабочую станцию, не заботясь о прокладке кабеля, а также перемещать с места на место включенные в беспроводную сеть ПК, принтеры и серверы.

Компания, имеющая беспроводную сеть, дает возможность служащим с других площадок, а также визитерам с беспроводными компьютерными устройствами быстро подключаться к сети при минимальном конфигурировании. Использование ресурсов Internet при нахождении вне стен своего офиса или дома значительно повышает производительность. Визитер может просто открыть свой ноутбук и получить доступ к электронной почте или нужному ему приложению.

Передача речи без проводов

Весьма привлекательна возможность использования беспроводных сетей для обеспечения передачи голосовых сообщений, особенно когда люди должны постоянно контактировать друг с другом. Действительно, локальная беспроводная сеть, рассчитанная на поддержку речевой связи, может полностью заменить традиционную проводную телефонную систему в отдельном здании (рис. 1.5). Возможность передачи через одну беспроводную сеть как речи, так и данных обеспечивает полную мобильность при низких эксплуатационных расходах.

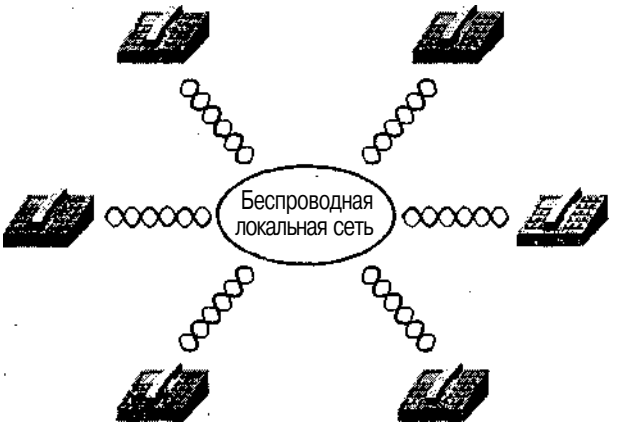

Рис. 1.5. Беспроводная локальная сеть обеспечивает инфраструктуру для телефонной связи в здании

Например, служащие магазина розничной торговли могут определять местонахождение необходимого покупателю товара или проводить инвентаризацию с использованием специальных беспроводных телефонов, включенных в беспроводную локальную сеть. Сеть в магазине должна также поддерживать передачу штрих-кодов, что необходимо в период проведения инвентаризации или определения цены с помощью беспроводных ручных сканеров штрих-кодов. Снижение эксплуатационных расходов достигается за счет того, что компании достаточно развернуть и поддерживать только одну телекоммуникационную систему, обеспечивающую передачу речи и данных.

Аналогичным образом владелец фирмы может обеспечить внутреннюю телефонную связь, развернув беспроводную локальную сеть. Это даст возможность служащим все время иметь при себе телефоны, как при пользовании сотовой связью. Находясь в здании фирмы, они смогут отвечать на звонки в любой момент.

Управление запасами

Многие фирмы с успехом применяют беспроводные локальные сети для управления процессом производства, что снижает эксплуатационные расходы. Поскольку связь между производственным оборудованием и главными управляющими системами осуществляется без использования проводов, компания может реорганизовать сборочный процесс в любое время из любого места, экономя тем самым время и средства.

Благодаря использованию беспроводной локальной сети отслеживаются и обновляются данные инвентаризации в реальном масштабе времени, тем самым существенно повышается их точность и эффективность. В условиях розничной торговли при продаже какого-либо товара беспроводная система управления немедленно обновит инвентаризационные данные. В условиях производства руководство компании может своевременно получать сведения об имеющихся исходных материалах и готовой продукции. Служащие с помощью беспроводных сканеров штрих-кодов могут проверять или изменять цену изделий, а также проверять их количество на складах.

Повышение точности, достигаемое за счет использования беспроводной локальной сети при инвентаризации, вызывает цепную реакцию улучшений. Поскольку информация вводится непосредственно в главный компьютер посредством ручных сканеров, отпадает необходимость в бумагах. Это существенно снижает ошибки персонала, возникающие при вводе данных, и повышает точность финансового учета. Это важно для компаний-производителей, потому что точные финансовые документы позволяют правильно платить налоги, благодаря чему штрафы (и, возможно, судебные процессы) сводятся к минимуму.

Здравоохранение

Все больше больниц развертывают беспроводные сети с целью повышения эффективности эксплуатации и удобства. В большинстве случаев учреждения здравоохранения развертывают беспроводные локальные сети в зонах, где высок "трафик" пациентов, к которым относятся помещения неотложной помощи, палаты с критическими больными, комнаты медсестер, а также кабинеты врачей и зоны ожидания пациентов. Врачебный персонал может использовать мобильные компьютерные устройства для повышения эффективности и тщательности ухода за пациентами.

Центры здравоохранения должны точно вести учет с целью обеспечения высококачественного ухода за больными. Нелепая ошибка может стоить кому-то жизни. По-

этому врачи и медсестры обязаны аккуратно фиксировать результаты анализов, физические данные, фармацевтические предписания и хирургические процедуры. Эта бумажная работа часто перегружает медперсонал, занимая 50-70% его времени. Использование мобильных беспроводных устройств сбора данных, посредством которых последние передаются в централизованную базу данных, существенно повышает точность и степень наглядности данных для тех, кому эта информация необходима.

Врачи и медсестры также становятся максимально мобильными, перемещаясь из палаты в палату и заботясь о больных. Использование электронных медицинских карт с возможностью ввода, просмотра и обновления данных о пациенте из любого помещения больницы повышает точность и оперативность ухода за больными. Это улучшение становится возможным благодаря тому, что каждая медсестра и врач получают компьютер с перьевым вводом данных (планшетный ПК или PDA), подключенный через беспроводную сеть к базе данных, в которой хранится медицинская информация о пациентах.

Лечащий врач может, например, выписать направление на анализ крови, введя запрос в карманный персональный компьютер (КПК). Лаборатория получит направление в электронном виде и направит своего сотрудника к больному, чтобы взять у него кровь на анализ. Лаборатория, выполнив необходимый анализ, введет его результаты в электронную медицинскую карту больного, а врач сможет ознакомиться с ними через свое компьютерное устройство из любого помещения больницы.

Еще одна сфера применения сетей в больницах — это мониторинг лекарств. За счет использования мобильных ручных устройств сканирования и печати кода резко повышается эффективность и точность всех операций с лекарствами: получение, сортировка, распределение, инвентаризация и проверка срока их годности. Однако важнее то, что медперсонал вовремя дает нужное лекарство именно тому пациенту, которому оно назначено.

Образование

Многие колледжи и начальные школы считают целесообразным развернуть на своей территории беспроводную локальную сеть — в основном, для обеспечения мобильного доступа к сетевым приложениям для своих учащихся. Наличие такого доступа расценивается как конкурентоспособное преимущество. Школы стараются увеличить число учеников с ноутбуками, желающих получить доступ в Internet и к школьным ресурсам из любого уголка кампуса (студенческого городка), например из класса, библиотеки, институтского двора или общежития. Быстро получить и отправить электронную почту, просмотреть Web-страницы, воспользоваться специализированными школьными приложениями, узнать свои оценки и посмотреть конспекты лекций — все это дает возможность учащимся рациональнее распределять свое время.

Приобретение и обеспечение работы компьютерных классов — дорогое удовольствие, но необходимое для выполнения учебных заданий. Ученикам часто приходится ждать, пока компьютер освободится. Беспроводная локальная сеть дает ученикам доступ к необходимым им ресурсам через их ноутбуки из любого уголка кампуса и в любое время, даже когда компьютерный класс закрыт. Благодаря этому доступ к сети равномерно распределяется между учениками, повышая тем самым эффективность обучения. При этом учебное заведение может сэкономить средства, выделяемые на содержание компьютерных классов.

Операции с недвижимостью

Агенты по недвижимости большую часть своего рабочего времени проводят вне офиса, общаясь с клиентами. Перед тем как покинуть офис, агент подбирает несколько объектов, которые он собирается показать клиенту, распечатывает информацию о них, а затем объезжает с потенциальным покупателем все отобранные объекты. Если клиенту не понравился ни один из них, агент по недвижимости должен вернуться в офис и взять описания других объектов. Если клиент решит приобрести какую-то собственность, они оба должны вернуться в агентство по недвижимости для оформления сделки.

Беспроводные сети позволяют намного ускорить процесс продажи недвижимости. Агент может использовать компьютер вне офиса для получения информации о предлагаемых объектах, а также с помощью портативных компьютера и принтера подготовить договор и заявку на получение ссуды для подписания их непосредственно в месте продажи.

Коммунальные предприятия

Коммунальные предприятия поддерживают работоспособность весьма протяженных систем, поставляющих электроэнергию и природный газ промышленным предприятиям и населению. Они непрерывно отслеживают работу энергораспределительных систем, линий газоснабжения и водопроводов и по крайней мере раз в месяц контролируют использованные объемы для выставления счетов. Это означает, что служащий перемещается с места на место, посещая дома и офисы компаний, записывает информацию, а затем вводит полученные данные в сервисный или вычислительный центр.

Теперь коммунальные предприятия используют глобальные беспроводные сети, обеспечивающие автоматическое считывание показаний счетчиков и систем слежения. Вместо служащего, фиксирующего показания счетчиков на бумаге и затем вводящего их в компьютер для обработки, счетчики периодически передают данные через беспроводную глобальную сеть коммунальному предприятию. Благодаря этому экономится время и снижаются эксплуатационные расходы, поскольку отпадает необходимость в считывании показаний счетчиков служащим.

Обслуживание в полевых условиях

Персонал, обеспечивающий обслуживание в полевых условиях, проводит большую часть своего времени в дороге, устанавливая или обслуживая системы либо инспектируя строящиеся объекты. Для выполнения своих обязанностей эти люди нуждаются в доступе к документации изделий и технологий их изготовления. Обычно персонал, обеспечивающий обслуживание в полевых условиях, возил с собой несколько тюков документации и часто не имел не только телефонов, но даже электричества.

Иногда служащие были не в состоянии привезти всю нужную документацию на место работ, из-за чего возникали задержки. В дальних командировках эта информация могла поступить адресату слишком поздно. В ожидании ее обновления проходили дни. Возможность доступа к документации через беспроводную сеть наверняка улучшит работу полевого персонала. Служащие, имеющие при себе портативный компьютер, подключенный к офисной беспроводной локальной сети, могут в любой момент найти и получить всю необходимую и свежую документацию.

Торговля в полевых условиях

Будучи в месте расположения клиента, коммивояжер нуждается в доступе к обширной информации о предлагаемых им продуктах и услугах, а также для размещения заказов, фиксации финансового положения и поддержки инвентаризации.

Благодаря беспроводному доступу к главной офисной сети коммивояжер получает доступ к централизованной контактной информации, описанию товаров, вносит предложения, заключает договоры и остается на связи с офисом и другими коммивояжерами. Наличие такой связи делает возможным заключение сделки непосредственно в месте нахождения клиента, вследствие чего возрастает вероятность успешных продаж и сокращается соответствующий цикл.

Продажа через торговые автоматы

Компании, предлагающие напитки и закуски, устанавливают торговые автоматы в гостиницах, аэропортах и офисных зданиях, чтобы увеличить объемы продаж своих продуктов. Служащие компании периодически наполняют автоматы продуктами, но иногда автоматы остаются какое-то время пустыми, поскольку у Компании нет способа узнать, что предлагаемые автоматом изделия закончились.

Беспроводная локальная сеть способна обеспечивать мониторинг запасов путем передачи соответствующих данных от каждого торгового автомата в центральную базу данных, содержимое которой доступно персоналу компании из одной точки. Такой мониторинг позволяет компании заблаговременно наполнять свои автоматы продукцией, поскольку .всегда известен уровень запасов каждого автомата, а также составлять реальные графики работ для людей, пополняющих эти автоматы.

Общедоступные сети

Вследствие широкого распространения ноутбуков, PDA и цифровых телефонов наблюдается рост потребности в мобильном доступе к Internet и корпоративным приложениям. Пользователи хотели бы получать бесшовное, постоянное мобильное подключение с высоким уровнем характеристик и надежности ко всем информационным ресурсам. Беспроводные сети обеспечивают инфраструктуру, обеспечивающую эту потребность в общедоступных местах, вне дома или офиса.

Общедоступная беспроводная сеть является средством, позволяющим подключаться к Internet людям, находящимся в стадии перемещения из одного места в другое. В общем случае доступ к беспроводной локальной сети обеспечивается из мест, в которых наблюдаются скопления людей. Беспроводные регионачьные и глобальные сети, с другой стороны, имеют широкую сферу действия.

Общедоступные беспроводные локальные сети размещаются в таких общественных местах, как гостиницы и рестораны, но могут быть развернуты и в любом другом месте., Так, 90% любителей отдыха на воде регулярно пользуются Internet, находясь дома или на работе. Но многие хотели бы получать доступ к Internet и в то время, когда они, например, на ночь швартуются возле какой-нибудь пристани. В результате пристани для яхт по всему миру развертывают беспроводные локальные сети.

Перечень общедоступных беспроводных сетей можно найти hawww.wi-fihotspotlist.com

Чтобы воспользоваться услугами общедоступной'беспроводной сети, пользователь должен иметь компьютерное устройство, например ноутбук, с платой интерфейса беспроводной локальной сети. Провайдеры общедоступных беспроводных сетей развертывают сейчас, как правило, сети, удовлетворяющие стандарту ШЕЕ 802.1 lb (Wi-Fi). Плата интерфейса сети компьютерного устройства автоматически обнаруживает наличие беспроводной локальной сети и ассоциируется с нею. Для получения доступа в Internet пользователь должен подписаться на эту услугу через Web-сайт, доступный из беспроводной локальной сети. Некоторые общедоступные беспроводные локальные сети бесплатны, но большинство провайдеров за пользование ими взимают какую-то плату.

В других общедоступных беспроводных сетях используются технологии беспроводных региональных сетей, обеспечивающие беспроводные каналы для связи абонентов (в данном случае — домов и офисов) с Internet. Провайдер устанавливает небольшую параболическую антенну на доме или непосредственно в офисе и направляет ее на централизованный концентратор (хаб). Система "точка-несколько точек" обеспечивает соединение "последней мили", необходимое для доступа к Internet в местах, где невозможно использовать кабельный модем или цифровую абонентскую линию.

Службы определения местонахождения

При использовании беспроводных сетей появляется возможность определять местонахождение людей или предметов. Отслеживание перемещающихся объектов позволяет реализовать несколько интересных приложений. Координаты пользователя могут вводиться в серверную программу, обеспечивающую какой-нибудь сервис, основанный на местонахождении. Например, провайдер беспроводной локальной сети может использовать эту концепцию для предоставления соответствующей моменту информации туристам, прибывающим в аэропорт или на железнодорожную станцию. Подобная информация может заключаться в отображении местонахождения туриста на плане маршрута таким образом, что он найдет путь к сектору отправления в аэропорту или в ближайший ресторан.

В больницах *служба определения местонахождения (location-based service)* может быть использована для отслеживания перемещений врачей и медсестер. Это позволит администрации в случае экстренной необходимости направить к больному нужного специалиста.

Системы, реализующие услуги определения местонахождения через беспроводные локальные сети, появляются и на потребительском рынке. Так, весьма полезными они могут оказаться для отслеживания местонахождения детей в парке с аттракционами. Представьте, что ребенок начал гулять по такому парку самостоятельно и потерялся. Благодаря этой системе родители смогут легко найти своего ребенка в толпе отдыхающих. Скрытая в одежде ребенка метка поможет предотвратить такое ужасное преступление, как похищение ребенка.

Торговые пассажи с помощью этой системы могут посылать рекламные сообщения покупателям, имеющим PDA. Система учитывает физическое местонахождение покупателей в магазине и предлагает им соответствующую информацию. В итоге покупатели рациональнее используют свое время, а владельцы магазинов получают большую прибыль.

В описанном случае пользователи могут получить электронный указатель и рекламные сообщения на свои беспроводные PDA после того, как войдут в пассаж. Этот указатель включает карту магазина, на которой четко отмечено местонахождение покупателя. После того как он щелкнет на изображении торгового отдела, ком-

наты отдыха или банкомата, на карте отмечается маршрут к выбранной точке. Если у партнера по покупкам или супруги тоже есть беспроводное устройство, каждый из них может знать, где в данный момент находится другой.

Преимущества беспроводной сети

Люди, проживающие в разных уголках земного шара, получают пользу от беспроводных соединений, проверяя свою электронную почту, просматривая страницы Internet и получая доступ к корпоративным приложениям. Продолжающееся улучшение изделий, в состав которых входит беспроводной интерфейс, позволяет им обходиться без проводов и пользоваться преимуществами мобильности и гибкости. В итоге повышается эффективность, точность и надежность.

Повышение эффективности и точности

Среди основных доводов в пользу развертывания беспроводных сетей отметим такое их преимущество, как повышение производительности. Если выгода очевидна даже'вопреки затратам, связанным с установкой и обслуживанием беспроводной сети, последняя становится привлекательным решением. Несомненная польза от инвестиций служит хорошим стимулом для вложения средств в новые системы.

В офисе

В качестве примера повышения производительности рассмотрим приобретение ноутбуков, снабженных адаптерами стандарта 802.11. Они позволяют служащим получать и отправлять электронные письма и просматривать Web-страницы во время производственных собраний, при этом пользователи могут участвовать в дискуссиях пе мере необходимости, а если ее нет — работать на своем ноутбуке. Хотя этот пример кажется тривиальным, рост производительности может оказаться нешуточным. Если пользователь присутствует на заседаниях три часа ежедневно, но при этом примерно 15 минут каждого часа посвящает работе с электронной почтой или выполняет другие, связанные с Internet задачи, он высвобождает около 45 минут ежедневно для решения иных заданий.

Рост производительности, обусловленный увеличением рабочего дня на 45 минут, позволяет компании сэкономить средства, объем которых зависит от стоимости рабочего часа служащего. Если он получает $50 в час, экономия составит $37,5 в день на одного сотрудника. Небольшая компания с 20-ю служащими сэкономит $750 в день, $15 тыс. в месяц, $180 тыс. в год и т.д. При стоимости оборудования беспроводная сети, составляющей $40 тыс., затраты окупятся уже через три месяца! Даже если учесть стоимость приобретения нового ноутбука для каждого служащего, компания получит положительный эффект менее чем через год.

В дополнение к росту производительности беспроводные сети обеспечивают следующие преимущества при использовании их в офисах:

- пользователи могут продолжать работу в сети во время перестановок мебели и перегородок, что довольно часто случается в корпорациях;
- служащие из других подразделений могут подключаться к серверу компании и работать с приложениями из любой точки здания;
- для экономии средств компания может использовать и другие беспроводные приложения, такие как беспроводны? телефоны.

На складе

Мобильность дает основание для выполнения работы быстрее и меньшим количеством сотрудников. Предположим, партию деталей для автомобилей привезли в дилерский центр. Во время разгрузки служащие с помощью беспроводных ручных сборщиков данных сканируют штрих-коды на каждой коробке. Штрих-код содержит уникальный номер, который автоматически и немедленно посылается в систему управления складом, фиксирующую тем самым получение такой-то детали. Система управления складом через дисплей сборщика данных инструктирует сотрудника, куда нужно положить полученную деталь или, может быть, какому клиенту ее нужно сразу же отгрузить.

Если деталь должна храниться на складе, система напечатает ярлык с указанием места хранения. Или укажет на ярлыке данные о маршруте и погрузке, который сотрудник прикрепит к коробке с деталями, подлежащими отправке клиенту. Теперь можно поместить коробку на отведенное для нее место, будь это складская полка или отправляющийся грузовик.

За счет использования такой системы приема грузов компания может уменьшить складские запасы, немедленно отправляя полученные заказы клиентам. Она также избавляется от бумажной документации и необходимости ввода данных вручную. Что более важно, такая компания быстрее доставляет заказы своим клиентам. В общем, система позволяет компании резко повысить свою эффективность за счет отказа от чреватых ошибками процессов, основанных на бумажном делопроизводстве. Отслеживание заказов на бумаге и ввод данных в систему управления складом через настольный терминал значительно увеличивает вероятность ошибок и требует большего количества служащих.

В больнице

В больнице беспроводная сеть может помочь сохранить жизни больных за счет повышения скорости и точности получения пациентами лекарств. Согласно правительственным инструкциям, больницы должны строго учитывать расход наркотических лекарств, из-за чего администрация применяет усиленные меры контроля, часто с использованием бумажных документов. Беспроводная сеть дает возможность использовать ручные сканеры штрих-кодов, которые на 300% ускоряют процесс сортировки и инвентаризации и делают его более точным.

Кроме того, медсестра может удостовериться в том, что дала лекарство именно тому больному, просканировав и упаковку, и идентификационный браслет пациента. Это значительно снижает вероятность приема больным не предназначенного для него лекарства. Вдобавок такая система может проконтролировать, нет ли у пациента аллергии на прописанное ему лекарство. Беспроводная сеть делает возможным использование приложений такого рода в быстро меняющихся условиях больницы.

Возможны и другие применения беспроводных сетей. Нужно лишь тщательно проанализировать их преимущества и сравнить со стоимостью сетей.

Повышение надежности

Кабели не отличаются высокой надежностью из-за коррозии и возможных повреждений. Причиной выхода из строя проводных сетей чаще всего является неправильная прокладка кабелей или их повреждение. Техники телефонных компаний постоянно сталкиваются с трудностями, обусловленными повреждением телефонных кабелей. На период устранения неполадок (иногда довольно длительный) часть телефонной системы связи выходит из строя.

Неблагоприятная погода (тропический циклон или торнадо) может причинить вред как воздушным, так и подземным кабельным коммуникациям. Из-за чего все проживающие в больших зданиях лишаются доступа к важным приложениям. Хотя проводные сети обычно имеют более высокие характеристики, их подверженность простоям может снизить уровень их надежности до неприемлемого.

Беспроводная сеть существенно уменьшает количество проблем, связанных с физическим повреждением. Коэффициент готовности такой системы гораздо выше, благодаря чему пользователи могут пользоваться ее услугами большую в процентном отношении часть времени. Проводная сеть может оказаться необходимой, если беспроводная не удовлетворяет предъявляемым к сети требованиям, но беспроводная сеть может обеспечить резервирование проводного канала связи. Комбинация проводной и беспроводной линий связи между строениями позволяет создать надежные и вместе с тем высокопроизводительные системы.

Резюме

Беспроводная сеть позволяет обойтись без проводных соединений между компьютерными устройствами, такими как PDA и ноутбуки, и существующими сетями. Это делает компьютерные устройства и их обладателей абсолютно мобильными при взаимодействии с Internet и корпоративными приложениями. Пользователь может оставаться на связи, где бы он ни находился.

Беспроводные сети разных типов обеспечивают работу приложений в домах, офисах, больницах, общественных местах, где пользователи могут получать пользу от мобильного доступа к сетевым службам. Способность беспроводных сетей обеспечивать удобный доступ к мобильным приложениям часто является вполне достаточным аргументом в пользу их выбора. Однако в некоторых случаях компании придется провести тщательный анализ потенциальных улучшений эффективности, точности и надежности, чтобы показать: вложенные в систему средства дадут результат.

Вопросы для самопроверки

Ответы на эти вопросы вы можете найти в приложении А.

1. Каково главное отличие беспроводной сети от обычной беспроводной системы связи?
2. Передачу информации каких типов обеспечивает беспроводная сеть?
3. Назовите основные четыре разновидности беспроводных сетей.
4. Какова максимальная протяженность беспроводной персональной сети?
5. Действительно ли беспроводная персональная сеть потребляет мало энергии от небольших ручных компьютерных устройств?
6. Как называется общепринятый стандарт на беспроводные локальные сети?
7. Какой относительно новый стандарт предложен для беспроводных региональных сетей?
8. Что делает беспроводную глобальную сеть неэффективной для применения пользователями, находящимися в помещениях?
9. Какова общая характерная черта применения беспроводных сетей дома и в небольших офисах?
10. Приведите примеры применения беспроводных глобальных сетей.

В этой главе...

компоненты беспроводной сети;

элементы структуры распространенных беспроводных сетей;

передача информационных потоков через беспроводную сеть.

ГЛАВА 2

Структура беспроводной системы: как работает беспроводная сеть

В беспроводных сетях используются те же компоненты, что и в проводных сетях, однако беспроводные сети должны уметь преобразовывать информацию в форму, пригодную для передачи ее через воздушную *среду* ***(medium).*** Хотя беспроводная сеть непосредственно включает только часть всей инфраструктуры сети, снижение параметров всей сети вызывается, несомненно, ухудшением, вызванным применением беспроводной среды передачи. В этой главе рассматриваются концепции, общие для всех типов беспроводных сетей, в частности, их компоненты и информационные сигналы.

Компоненты беспроводных сетей

Беспроводная сеть состоит из нескольких компонентов, обеспечивающих связь с использованием радиоволн или ИК-излучения, распространяющихся через воздушную среду[1]. Некоторые из них аналогичны используемым в проводных сетях, но имеет смысл рассмотреть все компоненты, применяемые в беспроводной сети (на рис. 2.1 показаны лишь основные).

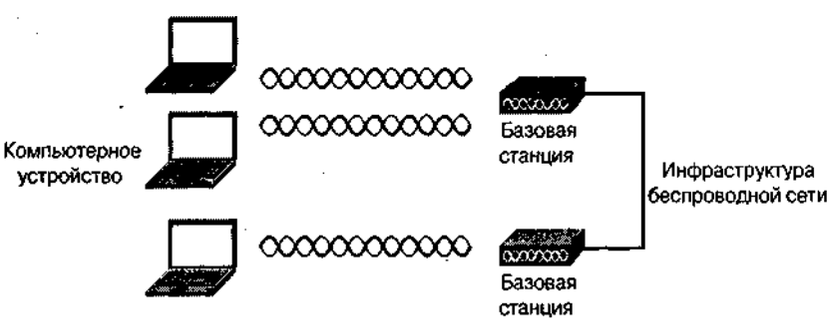

Рис. 2.1. Беспроводные сети включают компьютерные устройства, базовые станции и беспроводную инфраструктуру

[1] Радиоволны и ИК-излучение распространяются и в среде безвоздушной (вакууме), причем с меньшими потерями, поскольку отсутствуют атмосферные осадки. — Прим. ред.

Пользователи

Под пользователем далее понимается все, что может непосредственно пользоваться услугами беспроводной сети. Одним из наиболее распространенных типов пользователя является человек. Например, находящийся в командировке бизнесмен, получающий доступ к Internet через общедоступную беспроводную локальную сеть аэропорта. Однако пользователем может быть и не человек: производственный робот мог бы получать команды через беспроводную сеть от центрального компьютера, контролирующего производственный процесс. Поскольку беспроводная сеть предназначена для обслуживания пользователя, его можно рассматривать в качестве компонента, извлекающего пользу из существования беспроводной сети. Следовательно, пользователи — это важная часть беспроводной сети.

Пользователь начинает,' он же и заканчивает процесс применения беспроводной сети, поэтому к нему применим термин конечный пользователь. Обычно пользователь оперирует *компьютерным устройством* ***(computer device),*** которое, помимо обеспечения взаимодействия с беспроводной сетью, выполняет и другие функции, связанные с конкретными приложениями.

Пользователи беспроводных сетей часто перемещаются по зданию, кампусу или городу. Мобильность — одно из наиболее заметных преимуществ беспроводной сети. Например, свойством мобильности пользуется человек, передвигающийся по какому-то зданию и отправляющий либо получающий электронную почту посредством своего PDA. В данном случае PDA должен обеспечить непрерывное или часто возобновляемое подключение к инфраструктуре беспроводной сети.

Некоторым пользователям необходима лишь портативность компьютерного устройства; соответственно, они остаются на одном месте при работе с беспроводной сетью в определенный промежуток времени. Примером такого использования сети может служить сотрудник, работающий в конференц-зале на включенном в беспроводную сеть ноутбуке. Такой пользователь включает свой ноутбук, заняв свое место в конференц-зале, и выключает его, прежде чем покинуть помещение. Другие пользователи в действительности могут и не менять своего местонахождения, быть стационарными. Это подразумевает, что они работают на одном и том же месте неопределенно долгое время. Примером пользователя такого рода может служить некто, работающий на беспроводном компьютере в офисе. Основное различие между "стационарным" и "портативным" пользователем состоит в том, что первый из них не требует выполнения каких-либо функций роуминга. В некоторых ситуациях реализовать функции роуминга бывает затруднительно.

Компьютерные устройства

Многие типы компьютерных устройств (иногда их называют клиенты) способны работать с беспроводной сетью. Некоторые компьютерные устройства специально сконструированы для пользователей, другие — являются оконечными системами. На рис. 2.2 представлены компьютерные устройства беспроводных сетей.

Рис. 2.2. Компьютерные устройства беспроводных сетей выполняют различные функции

Для обеспечения работы мобильных приложений компьютерные устройства должны быть компактными, чтобы людям было удобно длительное время носить их с собой. Обычно они имеют небольшие экраны, клавиатуры с небольшим числом клавиш и малогабаритные батареи. Обладая мобильностью, они вместе с тем поддерживают лишь некоторые приложения.

Стационарные и переносные компьютерные устройства гораздо больших размеров, снабжены большими экранами и клавиатурами, что делает их удобнее для просмотра Web-страниц и выполнения других приложений, требующих относительно высоких характеристик. Но проблема состоит в их большой массе и неудобстве перемещения с места на место.

Компьютерные устройства беспроводных сетей также включают оконечные системы, такие как серверы, базы данных и Web-узлы. Например, Web-сайт www. cnn. com предлагает новости, с которыми любой желающий может ознакомиться из номера гостиницы через общедоступную беспроводную локальную сеть. Аналогично служащий может через беспроводное соединение взаимодействовать с системой управления складом, действующей как оконечное компьютерное устройство.

Пользователи могут приспособить уже существующие компьютерные устройства для работы в беспроводной сети. Например, установив плату интерфейса беспроводной сети в ноутбук. Некоторые устройства, такие как беспроводные сканеры кодов, способны работать только в беспроводной сети.

Компьютерное устройство имеет также операционную систему, такую как Windows-XP, Linux или MAC OS, которая запускает на выполнение программное обеспечение, необходимое для реализации приложения беспроводной сети. В некоторых случаях операционная система имеет встроенные средства, повышающие ее работоспособность в беспроводных сетях. Так, Windows XP автоматически обнаруживает беспроводную локальную сеть и ассоциируется с нею.

Платы интерфейса сети

Плата интерфейса сети, или *сетевой адаптер (network interface card),* обеспечивает интерфейс между компьютерным устройством и инфраструктурой беспроводной сети. Она устанавливается внутри компьютерного устройства, но приме-

няются и внешние сетевые адаптеры, которые после включения остаются вне компьютерного устройства. На рис. 2.3 представлены образцы беспроводных плат интерфейса сети нескольких типов.

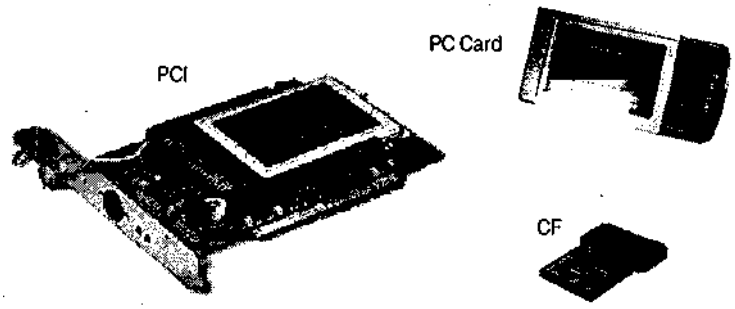

Рис. 2.3. Платы интерфейса беспроводной сети бывают различных типов и форм-факторов

Стандарты на беспроводную сеть определяют, как должна функционировать плата интерфейса сети. Например, плата, соответствующая стандарту IEEE 802.lib, сможет взаимодействовать лишь с беспроводной сетью, инфраструктура которой соответствует этому же стандарту. Поэтому пользователи должны быть внимательными и заботиться о том, чтобы выбранная ими плата соответствовала типу инфраструктуры той беспроводной сети, к которой они желают получить доступ.

Плата интерфейса беспроводной сети характеризуется также форм-фактором, определяющим физические и электрические параметры интерфейса шины, который позволяет плате взаимодействовать с компьютерным устройством. Но чтобы выбрать нужную плату, пользователь должен разбираться в этом. Ниже приведены основные сведения о различных форм-факторах плат беспроводных сетей, предназначенных для внутренней установки.

- **Industry-Standard Architecture** (ISA) — архитектура, соответствующая промышленному стандарту. Шина ISA получила широкое распространение с начала 80-х годов. Хотя ее характеристики были весьма невысокими, почти все производители ПК до недавнего времени устанавливали хотя бы один разъем для шины ISA. Но ее характеристики не могли улучшаться так же быстро, как параметры других компьютерных компонентов, и сейчас уже доступны высокоскоростные альтернативы этой шине. Шина ISA не оказала серьезного влияния на характеристики беспроводных локальных сетей стандарта 802.11Ь. Не стоит приобретать новые карты ISA, поскольку они уже устарели.
- **Peripheral Component Interconnect (PCI).** На сегодня локальная шина соединения периферийных устройств — наиболее популярный интерфейс для ПК, поскольку имеет высокие характеристики. Изначально разработала и выпустила PCI в 1993 г. компания Intel, и эта шина до сих пор удовлетворяет потребностям последних моделей мультимедийных компьютеров. Платы PCI стали первыми, в которых была реализована технология "plug-and-play", значительно облегчающая установку платы интерфейса сети в компьютер. Схем-

ные решения PCI могут распознать совместимые PCI-платы и начать работу с операционной системой компьютера, чтобы выполнить конфигурацию каждой платы. Это экономит время и позволяет избежать ошибок при установке плат неопытными пользователями.

- **PC Card.** Платы конструктива PC Card были разработаны в начале 90-х годов Международной ассоциацией производителей плат памяти для персональных компьютеров IBM PC (Personal Computer Memory Card International Association, PCMCIA). ***PC Card*** представляет собой устройство размером с кредитную карту, содержащее внешнюю память, модемы, устройства подключения к внешним устройствам, а также обеспечивающее совместимость с беспроводной сетью для небольших компьютерных устройств, таких как ноутбуки и PDA. Наиболее широко распространенны и даже более популярны, чем платы для шин ISA или PCI, поскольку используются в ноутбуках и PDA, число которых быстро растет. Можно использовать PC Card и в настольном ПК, воспользовавшись адаптером, преобразующим PC Card в плату PCI, т.е. одна сетевая интерфейсная плата для двух компьютеров. Вы можете брать PC Card в деловую поездку или на работу и использовать ее же в своем настольном ПК в офисе. Некоторые PDA требуют специального устройства (типа "салазки"), монтирующегося под PDA и позволяющего вставлять PC Card. Это лишь один из способов модернизации некоторых устаревших PDA и перевода их таким образом в разряд беспроводных устройств. Однако такой PDA, снабженный салазками и PC Card, прибавляет в габаритах и массе, что делает его менее удобным.
- **Mini-PCI.** Плата типа мини-PCI представляет собой уменьшенную версию стандартной платы PCI для настольных ПК и пригодна для установки в небольшие мобильные компьютерные устройства. Она обеспечивает почти такие же возможности, как и обычная плата PCI, но ее размеры примерно в четыре раза меньше. Плата типа мини-PCI может устанавливаться в ноутбуки (опционально, по желанию покупателя). Серьезным преимуществом платы такого типа (использующей радиоканал) является то, что она оставляет свободным разъем для установки PC Card, в который можно вставить плату расширения памяти или графического акселератора. Кроме того, стоимость беспроводной платы интерфейса сети на основе технологии мини-PCI, как правило, ниже. Однако эти платы тоже имеют недостатки. Для их замены, как правило, приходится разбирать ноутбук, из-за чего можно лишиться гарантии производителя. Применение платы типа мини-PCI может также привести к снижению производительности, поскольку часть обработки (если не всю обработку) они возлагают на компьютер. Несмотря на эти недостатки, платы типа мини-PCI завоевали прочные позиции в мире беспроводных ноутбуков.
- **CompactFlash.** Впервые технология ***CompactFlash (CF)*** была предложена корпорацией SanDisk в 1994г., но беспроводные сетевые интерфейсные платы форм-фактора CF до недавнего времени не производились. Плата CF небольшого размера, весит 15 г (половину унции) и вдвое тоньше PC Card. Ее объем вчетверо меньше, чем у радиоплаты типа PC Card. Отличается низкой потребляемой мощностью, благодаря чему батареи питания служат значительно дольше, чем при использовании устройств с PC Card. Некоторые PDA

поставляются со встроенными интерфейсами CF, т.е. становятся беспроводными, сохраняя при этом малые размеры и массу. Если в компьютере нет разъема под плату CF, то через адаптер ее можно вставить в стандартный разъем, предназначенный для PC Card. У радиоплат типа CF определенно есть будущее, особенно применительно к компактным компьютерным устройствам.

Помимо внутренних плат интерфейса сети выпускается большое количество внешних сетевых интерфейсов, подключаемых к компьютерному устройству через параллельный, последовательный или USB-порт. Они могут быть полезны для стационарных компьютеров, но существенно затрудняют мобильность для большинства беспроводных приложений.

В состав беспроводной платы интерфейса сети должна входить антенна, преобразующая электрические сигналы в радиоволны или оптическое излучение для передачи их через воздушную среду[2]. Конструкции антенн различны: они могут быть внешними, внутренними, постоянными и съемными. Например, антенна для PC Card обычно прикрепляется к краю платы и выступает за пределы ноутбука.

Платы типа мини-PCI снабжаются антеннами, которые располагаются по внешнему краю монитора ноутбука. Некоторые платы интерфейса сети имеют постоянные антенны с определенной диаграммой направленности. Другие позволяют заменять антенну, благодаря чему можно выбрать такую, которая наилучшим образом удовлетворяет условиям применения.

Воздушная среда

Кроме привычных способов использования воздуха, он является также той средой, в которой распространяются сигналы беспроводных систем связи, являющихся главной составляющей беспроводных сетей. Воздух — канал передачи информационных потоков между компьютерными устройствами и беспроводной инфраструктурой. Связь через беспроводные сети можно рассматривать как аналогию общения посредством речи. Если дистанция между собеседниками возрастает, они начинают хуже слышать друг от друга, особенно если рядом что-то шумит.

Информационные сигналы беспроводных сетей также распространяются через воздух, но благодаря своим свойствам могут распространяться на значительно большие расстояния, чем речевые сигналы. Эти сигналы не слышны человеку, поэтому можно усиливать их до более высоких уровней, не опасаясь помешать разговорам. Однако качество связи зависит от наличия препятствий, которые мешают распространению сигналов или рассеивают их, из-за чего уровень сигналов снижается, а дальность их распространения уменьшается.

Дождь, снег, смог и туман — примеры погодных условий, влияющих на условия распространения информационных сигналов беспроводных сетей. Например, сильный ливень может уменьшить дальность связи вдвое. Другие преграды, такие как здания и деревья, могут повлиять на условия распространения и характеристики беспроводной сети. Важность этих проблем возрастает при планировании развертывания беспроводных региональных или глобальных сетей.

Воздушная среда обеспечивает распространение радио- и световых волн, передающихся в беспроводной сети от одной точки к другой. Сигналами такого типа лю-

[2] *Подробнее об этом в главе 3.* — Прим. ред.

ди пользуются уже свыше ста лет, но они все еще представляются несколько загадочными и не вполне понятными большинству профессионалов, занимающихся компьютерной техникой. В главе 3 подробно рассмотрены характеристики сигналов и ухудшение их параметров при распространении через воздушную среду.

Инфраструктуры беспроводных сетей

Инфраструктура беспроводной сети обеспечивает беспроводное взаимодействие пользователей и оконечных систем. Ее могут образовывать базовые станции, контроллеры доступа, программное обеспечение приложений, обеспечивающих установление соединений, и распределительная система. Эти компоненты участвуют в беспроводной связи и выполняют важные функции в конкретных применениях.

Базовые станции

Базовая станция — распространенный компонент инфраструктуры. Она обеспечивает передачу информационных сигналов беспроводных сетей, распространяющихся через воздушную среду, в проводную сеть, ее иногда называют *распределительной системой.* Следовательно, базовая станция обеспечивает доступ пользователей ко множеству сетевых служб, таких как сервисы просмотра Web-страниц, электронная почта и базы данных. Базовая станция часто содержит плату интерфейса беспроводной сети, использующую те же принципы работы, что и плата интерфейса беспроводной сети в компьютере пользователя.

Название базовой станции зависит от выполняемых ею функций. Например, *точка доступа (access point)* — это основная базовая станция беспроводных локальных сетей. Комплект точек доступа беспроводной локальной сети обеспечивает роуминг в пределах здания. Плата интерфейса сети, находящаяся в компьютерном устройстве пользователя, устанавливает соединение с ближайшей точкой доступа, обеспечивая взаимодействие с входящими в инфраструктуру системами и пользователями, ассоциированными с другими -точками доступа. Когда пользователь перемещается в помещение, ближе к которому расположена другая точка доступа, плата интерфейса сети автоматически переключается на связь с нею, поддерживая надежное соединение. Шлюзы и маршрутизаторы локальной сети — это примеры базовых станций с расширенными возможностями, обеспечивающих выполнение дополнительных функций в сети. Шлюз может выполнять такие функции, как контроль доступа и обеспечение взаимодействия приложений, что улучшает обслуживание распределенных сетей общего доступа. *Маршрутизатор (router)* обеспечивает работу нескольких компьютеров через одно широкополосное соединение.

Базовая станция может поддерживать соединения типа "точка-точка" или "точка-несколько точек" (рис. 2.4). Системы типа "точка-точка" способны передавать поток сигналов от одной базовой станции или компьютерного устройства к другой (другому). Такая инфраструктура используется для организации протяженных беспроводных каналов связи. Например, *поставщик беспроводных услуг Internet (wireless Internet service provider, WISP)* может использовать эту систему для передачи сигналов от базовой станции, расположенной в удаленной точке (дом, офис), к базовой станции, находящейся в здании, где развернута сеть.

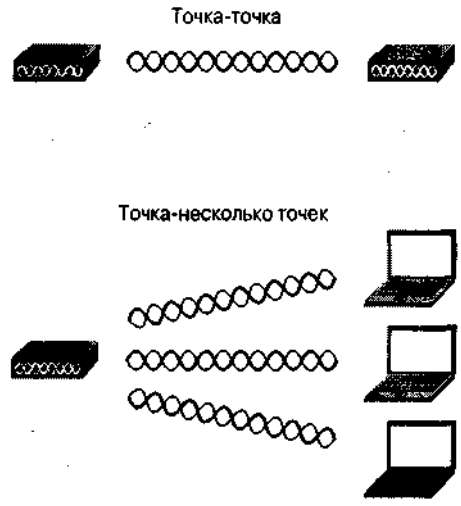

Рис. 2.4. Базовая станция поддерживает различные способы соединений

Как следует из названия, в случае конфигурации "точка-несколько точек" базовая станция может связываться с более чем одним компьютерным устройством или не с несколькими базовыми станциями. Связь такого рода обеспечивает, например, точка доступа, входящая в состав беспроводной локальной сети. Точка доступа представляет собой одно устройство, с которым устанавливают соединения многие компьютерные устройства, чтобы связываться друг с другом и системами, входящими в инфраструктуру беспроводной сети.

Контроллеры доступа

Поскольку существующие стандарты беспроводных сетей не регламентируют способы обеспечения защиты, качества обслуживания (QoS) и осуществления роуминга, для повышения качества сетей производящие их компании предлагают решения, обеспечивающие управление доступом. Ключевым компонентом таких решений является контроллер доступа, обычно представляющий собой аппаратный узел, располагаемый в проводной части сети, между точками доступа и защищаемой частью сети. Контроллеры доступа обеспечивают централизованный надзор за точками доступа с целью регулирования трафика между открытой беспроводной сетью и важными ресурсами. В некоторых случаях функции управления доступом выполняет точка доступа.

Контроллеры доступа имеют широкую сферу применения. Так, в общедоступных беспроводных локальных сетях контроллер доступа регулирует доступ к Internet, выполняя аутентификацию и авторизацию пользователей на основе данных подписки. Аналогичным образом корпорация может применить контроллер доступа, чтобы отправить хакеров на место стоянки автотранспорта компании, вместо того чтобы дать им доступ к важным данным и приложениям.

За счет использования контроллеров доступа снижается потребность в "умных" точках доступа, относительно дорогих и реализующих многие возможности, не соответствующие стандарту 802.11. Обычно поставщики позиционируют эти точки как

рассчитанные для применения на предприятиях. Однако сторонники контроллеров доступа отмечают, что точки доступа стандарта 802.11 должны обеспечивать высокое качество радиосвязи и иметь низкую стоимость. Они также предлагают централизовать функции управления доступом, выполняемые точками доступа, и возложить их на контроллер доступа, обслуживающий все точки доступа. Эти "тонкие"пгочки доступа в основном выполняют требования основного стандарта на беспроводную сеть (такого как IEEE 802.11), и ничего больше.

Развертывая сети с "тонкими" точками доступа, пользователи контроллеров доступа получают следующие преимущества.

- **Снижение стоимости.** Точки доступа с ограниченным набором функций стоят меньше, что снижает стоимость всей системы. Это тем более верно для сетей, в которых используется много точек доступа, таких как сети предприятий. За счет использования "тонких" точек доступа можно сэкономить примерно $400 в пересчете на одну точку доступа. В больших сетях эта экономия значительно превышает дополнительные расходы, вызванные установкой контроллера доступа, который стоит в среднем $5000.
- **Открытость соединений.** "Умные" точки доступа обеспечивают такие преимущества, как повышенные защищенность и производительность по сравнению с соединениями базовых сетей, удовлетворяющих стандартам на беспроводные сети. Однако проблема в том, что во многих случаях эти преимущества реализуются только при условии, что в пользовательских устройствах используется плата интерфейса беспроводной сети, изготовленная тем же производителем, который поставляет точки доступа. Это существенно снижает открытость системы и ограничивает выбор поставщиков. С другой стороны, "тонкие" точки доступа могут легко связываться на основе базового протокола беспроводной сети с платами интерфейса беспроводной сети многих поставщиков, в то время как требуемые улучшения обеспечивает контроллер доступа.
- **Централизованная поддержка.** Одним из преимуществ возложения интеллектуальных функций сети на контроллер доступа является то, что такую систему проще поддерживать в основном за счет снижения числа точек, в которых необходимо осуществлять вмешательство. Если все интеллектуальные функции сети выполняют точки доступа, обслуживающему персоналу приходится взаимодействовать с каждой из них при конфигурировании, мониторинге сети и устранении проблем. Контроллер доступа позволяет возложить на точки доступа выполнение меньшего числа функций, снижая тем самым необходимость работы с ними при выполнении задач поддержки работоспособности сети.

Контроллеры доступа часто обеспечивают контроль доступа, основанный на используемых портах, что позволяет администратору предоставлять доступ к отдельным приложениям каждому конкретному пользователю. Порт, который в действительности представляет собой просто число (например, 80 для http), соответствует отдельному приложению. Например, контроллер доступа может блокировать доступ к порту 80, вынуждая пользователей зарегистрироваться, прежде чем они смогут просматривать Web-страницы. После того как пользователь введет свои пользовательское имя и пароль, контроллер доступа проверит их идентичность на сервере аутентификации. Сетевое приложение могло бы, в качестве альтернативы, использо-

вать с целью аутентификации цифровые сертификаты (digital certificates). Эта функция регулирует доступ пользователя к защищенной сети.

Контроллеры доступа обычно реализуют следующие функции.

- **Аутентификация.** Большинство контроллеров доступа используют для аутентификации пользователей встроенную базу данных, однако некоторые предлагают осуществлять для этого взаимодействие с внешним сервером аутентификации, таким как *Служба удаленной аутентификации пользователей по телефонной сети* ***(Remote Authentication Dial-In User Service, RADIUS)*** и используют *Облегченный протокол службы каталогов* ***(Lightweight Directory Access Protocol, LDAP).*** Для небольших частных сетей подойдет внутренняя база данных. На предприятиях лучшие результаты достигаются при использовании внешних и централизованных серверов аутентификации.
- **Шифрование.** Некоторые контроллеры доступа обеспечивают шифрование данных, передаваемых от клиента к серверу и обратно, используя при этом такой распространенный метод, как ***IPSec.*** Это обеспечивает дополнительную защиту по сравнению с той, которую дают методы, регламентированные стандартами на беспроводные сети. Некоторые из этих особенностей реализуются Web-браузерами.
- **Роуминг через подсети.** Для поддержания роуминга из одной сети в другую контроллеры доступа обеспечивают роуминг через *подсети* ***(subnets)*** без необходимости проведения реаутентификации в системе. В результате пользователь может без перерывов пользоваться сетевыми приложениями, даже если он перемещается по зданию. Это особенно полезно для обширных сетей, когда доступ к сети отдельного пользователя приходится обеспечивать через несколько подсетей.
- **Управление пропускной способностью.** Поскольку пользователи совместно используют полосу пропускания беспроводной сети, важно иметь механизм, не позволяющий отдельным пользователям использовать всю пропускную способность сети. Контроллеры доступа обеспечивают подобную форму управления пропускной способностью за счет назначения профилей пользователей, основанных на требуемых уровнях качества связи. Профиль регламентирует типы предоставляемых услуг, таких как просмотр Web-страниц, электронная почта и потоковое видео, а также ограничения характеристик. Например, неподписанный на сервисы сети визитер, пытающийся воспользоваться услугами общедоступной беспроводной локальной сети, может быть классифицирован как имеющий профиль "визитера", доступ которому может быть разрешен только к информации "горячей" точки. Но абонент может получить и другие права доступа, позволяющие ему использовать широкополосное Internet-соединение.

Применение программного обеспечения, обеспечивающего установление соединений

Доступ к Internet и электронной почте обычно хорошо выполняется через беспроводные сети. Для реализации того и другого необходимо, чтобы браузер и программа электронной почты были установлены на ***клиентском устройстве.*** Пользова-

тели могут время от времени лишаться беспроводного соединения, но протоколы, используемые для выполнения таких, относительно несложных приложений, достаточно устойчивы.

Однако, помимо этих простых приложений, необходимо программное обеспечение для функционирования особых, более сложных приложений, таких как интерфейс между пользовательским компьютерным устройством и оконечной системой, выполняющей приложение или содержащей базу данных. Подобными сложными приложениями могли бы быть программы, осуществляющие управление складом, выполняемые на компьютере IBM AS/400, программа создания моделей, выполняемая на компьютере с операционной системой UNIX, система с временным разделением, базирующаяся на старом мэйнфрейме. К ним относятся базы данных со структурой клиент-сервер, в которых часть или вся программа приложения располагается на клиентском устройстве и взаимодействует с СУБД, такой как Oracle или Sybase. В таких случаях в дополнение к точкам доступа и контроллерам для осуществления связи между пользовательским компьютерным устройством и программой приложения либо базой данных, расположенной на централизованном сервере, важно иметь программное обеспечение, поддерживающее необходимое для работы подобных приложений соединение.

Ниже приведены основные типы приложений, обеспечивающих соединения.

- **Эмулятор терминала (therminal emulation).** Программное обеспечение эмуляции терминала выполняется на компьютерном устройстве и заставляет его работать как терминал, обеспечивающий пользователя относительно простым интерфейсом, позволяющим ему взаимодействовать с приложением, выполняемым на другом компьютере. Терминал просто предоставляет пользователю интерфейс и принимает вводимые данные для передачи их программному обеспечению приложения. Например, *эмулятор терминала* ***(terminal emulation)*** VT220 обеспечивает взаимодействие с приложениями, выполняемыми на хосте под управлением UNIX, эмулятор терминала 5250 работает с системами, устанавливаемыми на компьютере IBM AS/400, а эмулятор терминала 3270 позволяет взаимодействовать с мэйнфреймами IBM. Преимущество применения эмуляции терминала состоит в низкой начальной стоимости, а изменения, выполненные приложением, автоматически вступают в силу после регистрации пользователя. Однако беспроводные системы, использующие эмуляцию терминала, могут оказаться неспособными поддерживать непрерывные соединения с унаследованными приложениями, имеющими блокировки по превышению лимита времени (тайм-ауты) и рассчитанными на более надежные проводные сети. Механизм "тайм-аут" автоматически прерывает сеанс связи, если не проявляется какая-либо активность в течение определенного промежутка времени. В результате специалистам отделов информационных технологий (ИТ) приходится тратить много времени, отвечая на звонки конечных пользователей, жалующихся на обрывы связей и незавершенные транзакции. Следовательно, в долговременной перспективе широкое использование эмуляции терминалов может дать отрицательный эффект из-за повышения стоимости эксплуатации.
- **Прямое соединение с базой данных (direct database connectivity).** В случае прямого соединения с базой данных, что иногда называется технологией клиент-

сервер, приложение выполняется на компьютерном устройстве пользователя. При такой конфигурации программное обеспечение на устройстве конечного пользователя выполняет все функции, возложенные на приложение, и обычно взаимодействует с базой данных, размещенной на центральном сервере. Это обеспечивает определенную свободу действий разработчику приложений, поскольку программист полностью контролирует применяемые функции и не ограничен характеристиками унаследованных приложений, выполняемых на центральном компьютере. Прямое соединение с базой данных часто является наилучшим подходом в случаях, когда необходима гибкость при разработке программного обеспечения приложений. Однако сложность заключается в том, что при прямом соединении с базой данных необходимо использовать протокол TCP/IP (Transmission Control Protocol/Internet Protocol — протокол управления передачей/протокол Internet), который лишь отчасти подходит для передачи через беспроводную сеть.

- **Промежуточное программное обеспечение (wireless middleware).** Осуществляет промежуточное соединение между пользовательским компьютерным устройством и программным обеспечением приложения или базой данных, размещенными на сервере (рис. 2.5). Промежуточная программа выполняется на дополнительном компьютере (промежуточном шлюзе), подключенном к проводной сети. Она обрабатывает пакеты, циркулирующие между компьютерными устройствами пользователей и серверами. Это программное обеспечение позволяет создать эффективную и надежную связь в беспроводной сети, поскольку осуществляет подключения к базам данных и взаимодействие с программным обеспечением приложений через более надежную проводную сеть. Иногда эту технологию называют живучая связь (session persistence).

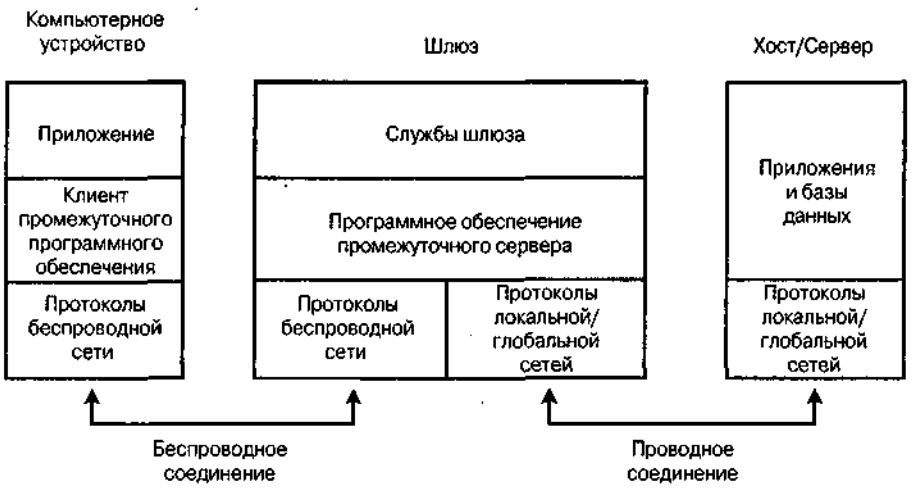

Рис. 2.5. Промежуточное программное обеспечение обеспечивает эффективное взаимодействие приложений компьютерных устройств с хостами и серверами

Промежуточное программное обеспечение характеризуется следующими особенностями.

— **Методы оптимизации.** Многие продукты, относящиеся к классу промежуточного программного обеспечения, выполняют сжатие данных, чтобы уменьшить число пакетов, передаваемых программным обеспечением беспроводному каналу. В некоторых реализациях промежуточного программного обеспечения используются собственные протоколы связи, имеющие преимущество перед традиционными, такими, например, как протокол TCP/IP.

— **Мягкий перезапуск.** В беспроводных сетях передача данных может быть неожиданно прервана на середине. Мягкий перезапуск — это механизм восстановления, способный определить преждевременное завершение передачи. После восстановления соединения промежуточное программное обеспечение возобновляет передачу данных с момента обрыва связи, а не с самого начала. Это позволяет избежать ошибок при выполнении приложений, использующих базы данных.

— **Пакетирование данных.** Некоторые продукты, относящиеся к классу промежуточного программного обеспечения, способны объединять самые маленькие пакеты данных в один большой пакет, передаваемый через беспроводную сеть, благодаря чему снижается стоимость передачи данных через глобальные сети. Поскольку при использовании некоторых служб беспроводной сети с пользователя взимается плата за каждый переданный пакет, за счет пакетирования данных можно снизить суммарную стоимость. •

— **Очистка экрана и восстановление изображения.** Среда разработки некоторых продуктов, относящихся к классу промежуточного программного обеспечения, позволяет разработчикам использовать визуальные средства для формирования и обновления фрагментов окон существующих приложений для более эффективного отображения данных на меньших по размерам дисплеях некоторых беспроводных устройств, не являющихся ПК (PDA, сканеры штрих-кода).

— **Поддержка оконечной системы.** Беспроводное промежуточное программное обеспечение взаимодействует с различными приложениями и базами данных оконечных систем. Если клиентам необходим доступ к приложениям и базам данных многих типов, беспроводное промежуточное программное обеспечение действует как концентратор. Например, пользователь может использовать соединение с промежуточным программным обеспечением для взаимодействия с приложениями, размещенными на платформах AS/400 и UNIX одновременно, запуская у себя программное обеспечение эмуляции соответствующих терминалов.

Распределительная система

Беспроводная сеть редко используется в полном смысле без проводов. Распределительная система, в состав которой часто входят проводные соединения, обычно необходима для объединения в единое целое точек доступа, контроллеров доступа и серверов. В большинстве случаев роль распределительной системы выполняет обычная сеть Ethernet.

Стандарт ШЕЕ *802.3* является основой Ethernet и регламентирует использование протокола CSMA (carrier-sense multiple-access — коллективный доступ с контролем несущей) для обеспечения доступа к совместно используемой среде передачи, такой как провода на основе витых пар, коаксиальные кабели или оптические волокна. На сегодня этот стандарт доминирующий из числа регламентирующих доступ к среде как проводных, так и беспроводных сетей.

Стандарт CSMA управляет доступом к совместно используемой среде таким образом, что в каждый момент времени только одна плата интерфейса сети может передавать информацию. Это похоже на собрание, когда выступающий (в чем-то схожий с платой интерфейса сети) может говорить только в том случае, если остальные молчат. Это дает возможность высказаться каждому участнику собрания в соответствии с регламентом. Если одновременно начинают говорить два или более ораторов, происходит конфликт (коллизия), и каждому придется повторить то, что он уже сказал.

Все компьютерные устройства такой сети должны поочередно использовать среду через хабы Ethernet. Однако коммутатор Ethernet позволяет создать несколько коллизионных доменов, что позволяет одновременно проводить передачу нескольким пользователям, и таким образом повышает производительность. В больших сетях, по размерам превышающих те, которых бывает достаточно для дома или небольшого офиса, для повышения производительности следует обязательно использовать коммутаторы.

В сетях Ethernet для соединения сетевых устройств, таких как точки доступа и другое распределительное оборудование, применяются провода на основе витых пар, коаксиальные кабели и оптические волокна. Десять лет назад, в первых проводных локальных сетях, общепринятым было использование коаксиальных кабелей, но сейчас большинство компаний применяют провода на основе витых пар или оптические волокна. Ассоциации EIA (Electronics Industries Association.— Ассоциация электронной промышленности) и TIA (Telecommunications Industry Associastion — Ассоциация промышленности средств связи) разработали спецификацию на кабель, состоящий из витых пар и получивший название "категория 5" (сокращенно Cat 5), ставший наиболее популярным среди других кабелей на основе витых пар.

Кабель категории 5 содержит четыре неэкранированные витые пары, которые обеспечивают передачу сигналов сети Ethernet на расстояние, немногим меньшее 100 м (примерно 300 футов). При необходимости длина кабеля может быть увеличена за счет использования повторителей, именно этот метод используется для соединения с базовой станцией беспроводной сети, если она находится на расстоянии более 100 м от распределительного шкафа.

Существуют и другие варианты использования кабелей на основе витых пар. Так, все четыре пары усовершенствованного кабеля категории 5 (обозначают как CatSe) можно использовать для коротких соединений в сетях Gigabit Ethernet, обеспечивающих скорость передачи 1000 Мбит/с. Он является обратно совместимым по отношению к кабелю категории 5. Сейчас появились кабели категорий 6 и 7, позволяющие реализовать более широкополосную и на большие расстояния передачу данных в сетях Gigabit Ethernet. Кабель категории 7 выполнен на основе экранированных витых 1 ар, что позволяет с успехом применять его в условиях сильных электромагнитных помех.

Ниже описаны несколько типов сетей Ethernet, обычно выполняющих роль распределительных систем беспроводных сетей, в которых применяются кабели на основе витых пар.

- 10BASE-T. Стандарт 10BASE-T описывает один из физических уровней стандарта 802.3 и регламентирует передачу данных со скоростью 10 Мбит/с. В типичном кабеле сети 10BASE-T бывают задействованы две из четырех пар кабеля категории 5 для передачи и приема данных. С обеих сторон кабель заканчивается разъемами RJ-45, которые несколько больше по размерам обычного телефонного разъема RJ11, применяемого в странах Северной Америки. Лишнюю пару проводов можно использовать для других целей, например, для передачи через кабели Ethernet электропитания (это называется "питание через Ethernet" — Power-ower-Ethernet, PoE). Подобный механизм позволяет какому-нибудь блоку передавать через кабель категории 5 постоянный электрический ток, обеспечивая тем самым электропитание точки доступа через распределительный шкаф. Механизм PoE часто избавляет от необходимости устанавливать новые электророзетки в каждой точке доступа. В случае больших сетей определенно следует рассмотреть возможность использования механизма PoE.
- 100BASE-T. Другой физический уровень стандарта 802.3, 100BASE-T, поддерживает скорость передачи данных 100 Мбит/с. Аналогично сетям Ethernet стандарта 10BASE-T в сетях 100BASE-T используются кабели на основе витых пар. Возможны такие варианты:
  - 100BASE-TX — используются две пары кабеля категории 5;
  - 100BASE-T4 — используются четыре пары устаревшего, низкокачественного кабеля категории 3.

  В большинстве вновь развертываемых сетей используется кабельная разводка стандарта 100BASE-TX. Как и в случае l'OBASE-T, незадействованные пары можно использовать для подачи электропитания. 100BASE-T4 целесообразно использовать, когда необходимо обеспечить передачу данных со скоростью 100 Мбит/с через старую разводку на основе кабелей категории 3, которые широко применялись в начале 90-х годов.
- Оптическое волокно. Оптические кабели стоят намного дороже, чем кабели на основе витых пар, но они могут оказаться экономически более выгодными, поскольку поддерживают скорости передачи порядка Гбит/с и обеспечивают дальность передачи до двух километров. В отличие от традиционного способа передачи электрических сигналов по медным проводам в оптических кабелях передаются световые импульсы по тонким волокнам, выполненным из стекла и/или пластика. Благодаря этому волоконно-оптические кабели не подвержены влиянию электромагнитных помех, что делает их полезными в условиях, когда проблемы возникают из-за электромагнитного излучения. Кроме того, практически невозможны пассивные методы перехвата данных, передаваемых по оптическим кабелям, такие линии защищены намного лучше, чем витые пары. Что касается беспроводных локальных сетей, то оптическое волокно может оказаться приемлемым решением для связи с точками доступа, находящимися на расстоянии более 100м от распределительного шкафа. Но для

создания такой линии связи необходима пара дорогих приемопередатчиков, преобразующих электрические сигналы в световые, и обратно. Одной из проблем, возникающей при работе с оптическими кабелями, является сращивание оптических волокон. Приходится иметь дело со стеклом или пластиком и обеспечивать высокоточное взаимное позиционирование тончайших волокон. Необходим не только особый инструмент, но и специальные навыки. Во избежание трудноразрешимых проблем желательно приобретать уже снабженные наконечниками оптические кабели.

Управляющие системы

Как и в случае сетей других типов, беспроводная сеть предприятия требует эффективного управления, благодаря которому потребности пользователей будут обеспечены в течение всего срока службы сети. Система управления сетью, включающая как людей, так и программные средства, должна обеспечить эти потребности. Ниже рассмотрены функции, выполнение которых возлагается на управляющие системы.

Безопасность

Подсистема безопасности включает механизмы, препятствующие компрометации[3] сетевых ресурсов (таких как базы данных и сообщения электронной почты) или нанесение им ущерба. Это достигается за счет применения жесткой политики безопасности: беспроводная сеть конфигурируется таким образом, чтобы она могла решать проблемы безопасности, связанные с распространением сигналов через беспроводную среду. Например, эта политика может включать меры, предписывающие использование особых методов шифрования, гарантирующих, что злоумышленник не сможет получить и декодировать сообщения электронной почты, пересылаемые между пользовательским компьютерным устройством и точкой доступа. Подробнее о методах защиты сети в главе 8.

Справочный стол

Справочный стол обеспечивает первый уровень поддержки пользователей. Пользователь, испытывающий затруднения с беспроводным соединением, должен знать, как он может обратиться к услугам справочного стола. У пользователей часто возникают проблемы, связанные с привязкой к точкам доступа или плохим качеством связи.

Персонал справочного стола способен решить простые проблемы, связанные с соединением. Например, это может быть оказание пользователю помощи в конфигурировании платы радиоканала и операционной системы, чтобы они соответствовали политике безопасности конкретной беспроводной сети. Для решения более сложных проблем, возникающих у пользователей, справочный стол должен иметь коммуникационный интерфейс, обеспечивающий расширенные функции поддержки, такие как сопровождение.

[3] *Под компрометацией (дискредитацией) в данном случае понимается несанкционированное раскрытие или потеря защищенной информации.* — Прим. ред.

Управление конфигурацией

Под управлением конфигурацией понимается контролирование изменений, происходящих в структуре беспроводной сети и установленной системе. Изменения могут быть такими: установка и ликвидация точек доступа, изменения параметров места доступа, обновление программно-аппаратных средств. Вследствие динамичности, присущей беспроводным сетям, изменения в них происходят намного чаще,. чем в проводных.

Администрации предприятия следует проанализировать все предложения по модификации, которые могут повлиять на производительность или безопасность сети. Анализ необходим компании, чтобы принять во внимание такие важные моменты, как дополнительные расходы и привлекаемые ресурсы. Необходимо провести независимое рассмотрение конструкции, в ходе которого оценить каждое предлагаемое решение, касающееся беспроводной сети, и проверить соответствие общей структурной схеме отдельных элементов. Проверка должна, например, включать пересмотр мест расположения точек доступа, распределение частот радиоканала и установочные параметры системы безопасности.

Мониторинг сети

Под мониторингом сети понимается непрерывное отслеживание различных параметров беспроводной сети, таких как степень использования точек доступа и пользовательский трафик, проходящий через распределительную систему. Это играет ключевую роль в активном управлении беспроводная сетью, позволяющем наращивать число ее пользователей и решать возникающие проблемы до того, как ухудшатся характеристики или безопасность сети.

Персоналу предприятия следует непрерывно оценивать степень загруженности базовых станций, и при изменении пользовательского трафика соответственно менять масштаб беспроводной сети. Базовые станции действуют как измерительные приборы, показывающие, когда необходимо развернуть дополнительные базовые станции, контроллер доступа или увеличить пропускную способность канала, через который осуществляется доступ в Internet. Специфическая проблема беспроводной сети состоит в том, что ее администраторы могут не знать о том, что какая-то базовая станция некоторое время не работала.

В большинстве случаев зоны действия базовой станции перекрываются, и пользователи, скорее всего, привяжутся к другой базовой станции, с ухудшением производительности, если основная точка доступа станет недоступной. Однако средства мониторинга сети немедленно обнаружат бездействие и сообщат об этом служащему, ответственному за работоспособность сети. По возможности компаниям следует интегрировать функции мониторинга беспроводной сети со средствами, традиционно применяемыми в существующих корпоративных сетях, что упрощает ее эксплуатацию.

Отчетность

Подсистема отчетности выдает информацию, относящуюся к различным аспектам эксплуатации беспроводной сети, включая статистику использования, фиксацию нарушений системы защиты и производительность. Эти отчеты необходимы администрации, чтобы она могла эффективно оценивать работоспособность сети

и принимать решения о необходимости тех или иных изменений. Эти отчеты указывают на потенциальные бреши в системе защиты, бездействие точки доступа и степень загрузки. Информация такого рода должна быть доступна для всех, выполняющих функции оперативной поддержки: справочного стола, сопровождения и инженерной поддержки.

Инженерная поддержка

Подсистема инженерной поддержки обеспечивает расширенное техническое сопровождение с целью модернизации беспроводной сети по мере появления новых технологий и решения проблем, связанных с производительностью и безопасностью. Обычно компания или группа сотрудников, которые разрабатывали первоначальный вариант беспроводной сети, выполняют и функции инженерной поддержки. В обязанности этой группы входит рассмотрение и проверка соответствия отдельных конструктивных узлов общей структуре сети. Кроме того, данная группа должна непрерывно отслеживать достижения технологии и изделий, касающиеся беспроводных сетей, и предлагать эффективный переход на новые решения в случае роста степени использования сети.

Сопровождение

Подсистема сопровождения обеспечивает ремонт и конфигурирование беспроводной сети, включая замену поврежденных антенн, организацию каналов в местах доступа и переоценку характера распространения радиоволн. Некоторые задачи сопровождения могут выполняться в результате деятельности группы инженерной поддержки. Например, инженер может посчитать необходимым установить новую точку доступа там, где необходимо создать новую зону действия сети. В этом случае персоналу группы сопровождения придется установить точку доступа там, где укажет инженер.

Важной задачей сопровождения беспроводной сети является периодическая модернизация аппаратно-программного обеспечения точек доступа. Это позволит точкам доступа реализовывать новейшие достижения технологии и ликвидировать дефекты, в результате чего будут достигнуты максимальные на данный момент производительность и защищенность. Следовательно, компаниям необходимо регулярно модернизировать аппаратно-программное обеспечение по мере появления его обновленных вариантов.

Группа сопровождения должна также периодически проверять зоны действия, дабы убедиться в том, что точки доступа способны обслуживать все нужные помещения здания и обеспечивать приемлемый уровень пропускной способности. Это необходимо в том случае, если компания занимается перепланировкой помещений, что ведет к изменению условий распространения радиоволн. Если обнаруживается отклонение от заданных характеристик, группа сопровождения должна сообщить об этом группе инженерной поддержки.

Структура сети

Структура (или архитектура) сети определяет протоколы и компоненты, необходимые для удовлетворения требований выполняемых в ней приложений. Одним из популярных стандартов, на основе которого можно рассмотреть структуру сети, яв-

ляется Эталонная модель взаимодействия открытых систем (Open System Interconnection (OSI) reference model), разработанная Международной организацией по стандартизации (International Standards Organization, ISO). Модель OSI охватывает все сетевые функции, группируя их в так называемые уровни, задачи которых выполняются различными компонентами сети (рис. 2.6). Эталонную модель OSI удобно также использовать при рассмотрении различных стандартов и возможности взаимодействия беспроводных сетей.

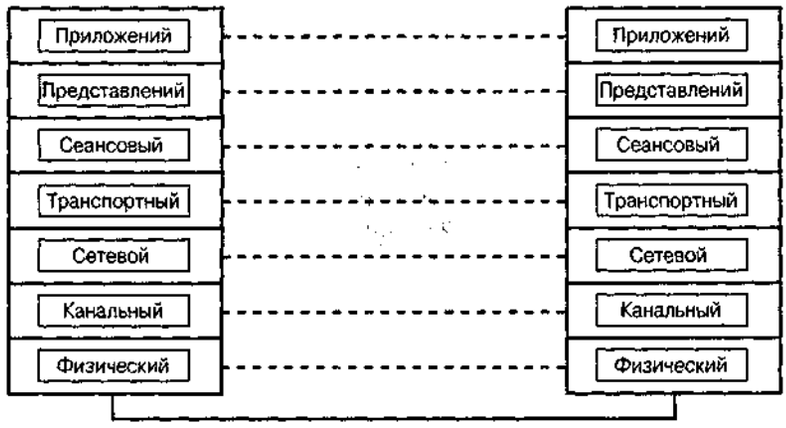

Рис. 2.6. Уровни Эталонной модели OSI представляют все функции, выполняемые сетью

Уровни OSI обеспечивают выполнение следующих функций сети.

- **Уровень 7 — уровень приложений.** Обеспечивает связь пользователей и работу основных коммуникационных служб (передача файлов, электронная почта). Примеры программного обеспечения, выполняемого на этом уровне — простой протокол электронной почты (Simple Mail Transfer Protocol, SMTP), протокол передачи гипертекстовых файлов (Hypertext Transfer Protocol, HTTP) и протокол передачи файлов (File Transfer Protocol, FTP).
- **Уровень 6 — уровень представления данных.** Регламентирует синтаксис передачи данных для уровня приложений и при необходимости осуществляет преобразование форматов данных. Например, этот уровень может преобразовать код, представляющий данные, при обеспечении связи между удаленными системами различных производителей.
- **Уровень 5 — сеансовый уровень.** Устанавливает сеансы связи между приложениями, управляет ими и завершает их. Промежуточное программное обеспечение и контроллеры доступа обеспечивают такую форму связи через беспроводную сеть. Если работа беспроводной сети нарушается из-за помех, задачей сеансового уровня является приостановление связи до момента снижения уровня помех до допустимого.

- **Уровень 4 — транспортный уровень.** Обеспечивает механизмы для создания, сопровождения и должного завершения виртуальных цепей, позволяя более высоким уровням не заботиться о деталях реализации сети. В общем случае эти цепи представляют собой соединения, устанавливаемые между приложениями, выполняемыми на разных концах коммуникационных цепей (например, между Web-браузером ноутбука и Web-страницей сервера). На этом уровне работает, например, протокол управления передачей (Transmission Control Protocol, TCP).
- **Уровень 3 — сетевой уровень.** Обеспечивает маршрутизацию пакетов при их следовании от отправителя к получателю. Механизм маршрутизации обеспечивав^ отправку пакетов в направлении, ведущем к указанной точке назначения. На этом уровне работает протокол Internet (Internet Protocol, IP).
- **Уровень 2 — канальный уровень.** Обеспечивает доступ к среде, а также синхронизацию между объектами сети и контроль ошибок. В беспроводных сетях на этом уровне также осуществляется координация доступа к совместно используемой среде и повторная передача в случае возникновения ошибок при передаче данных от отправителя к получателю. В большинстве разновидностей беспроводных сетей используется общий метод выполнения функций на канальном уровне, независимо от реально используемых средств передачи.
- **Уровень 1 — физический уровень.** Обеспечивает реальную передачу информации через среду. К физическому уровню можно.отнести радиоволны и ИК-излучение.

За счет комбинирования уровней сетевые структуры обеспечивают выполнение необходимых функций, но беспроводные сети непосредственно используют только нижние уровни вышеописанной модели. Например, плата интерфейса сети выполняет функции канального и физического уровней. Другие составляющие, такие как промежуточное программное обеспечение беспроводной сети, обеспечивают выполнение функций, характерных для сеансового уровня. В некоторых случаях добавление беспроводной сети может повлиять только на нижние уровни, но для обеспечения эффективной работы приложений в случае ухудшения характеристик беспроводной сети не стоит забывать и о более высоких уровнях.

Каждый уровень модели OSI обеспечивает потребности вышестоящего уровня. Так, TCP, работающий на транспортном уровне, устанавливает соединение с приложениями, выполняемыми на удаленном хосте, не учитывая то, как нижние уровни обеспечивают синхронизацию и передачу сигналов.

Как следует из рис. 2.6, протоколы на каждом уровне взаимодействуют через сеть с уровнем соответствующего ранга. Однако реальная передача данных происходит на физическом уровне. В результате такая структура обеспечивает процесс расслоения, при котором конкретный уровень вставляет информацию своего протокола во фреймы, размещающиеся во фреймах нижних уровней. Фрейм, пересылаемый на физическом уровне, в действительности содержит фреймы всех верхних уровней. В пункте назначения каждый уровень передает соответствующие фреймы всем вышестоящим уровням, обеспечивая работу протоколов на уровнях одинакового ранга.

Информационные сигналы

Данные являются разновидностью информации, которая посредством сети хранится на подключенных к ней компьютерах. Это означает, что фактически беспроводная сеть передает данные от одного компьютера к другому. Эти данные могут быть сообщениями электронной почты, файлами, Web-страницами, видеофрагментами, музыкой и речью.

Коммуникационная система, а беспроводная сеть одна из них, представляет данные в символьной форме, используя коды, представленные в виде электрических, световых или радиосигналов. Эти сигналы передают информацию от одной точки системы связи к другой. Сигналы могут быть цифровыми или аналоговыми — в зависимости от того, в каком месте системы они в данный момент находятся.

Цифровые сигналы

Цифровые сигналы ***(digitalsignals),*** циркулирующие в компьютере, резко изменяют свою амплитуду (рис. 2.7). Обычно они являются бинарными (принимают два состояния), поэтому общепринято рассматривать такие сигналы как строку двоичных чисел (битов) или двоичных данных. Цифровые цепи компьютера с легкостью хранят и обрабатывают эти цифровые сигналы, представленные в двоичной форме.

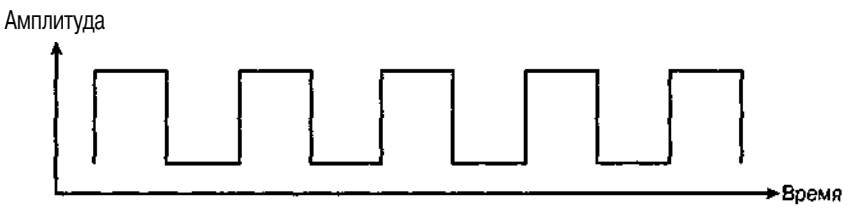

Рис. 2.7. Цифровые сигналы идеальным образом подходят для использования в компьютерах

В двоичной системе счисления для представления всех чисел используются только ноль и единица. Любое число, записанное в привычной десятеричной системе счисления, можно легко преобразовать в двоичное. Однако при использовании некоторых протоколов следует помнить, что двоичные значения во фрейме данных представляют специфичную для данного протокола информацию.

Одним из преимуществ цифровых сигналов является легкость их регенерации. Если сигнал проходит через воздушную среду, он может подвергнуться воздействию шума или помех, которые исказят форму сигнала. Чтобы очистить сигнал и восстановить его, цифровая схема определяет, присутствует ли цифровой импульс в определенный период времени, и создает новый импульс, в точности повторяющий первоначально переданный. Как результат этого — возможность передачи цифровых сигналов на огромные расстояния за счет их периодического возобновления при полном сохранении передаваемой информации. Такое невозможно при использовании аналоговых сигналов.

В обеспечение защиты передаваемой информации часто возникает необходимость в шифровании и последующей дешифровке полученного сигнала в пункте назначения. Этот процесс упрощается при использовании цифровых сигналов, поскольку все, что необходимо сделать — это переставить биты, применив одну из систем шифрования. Когда данные достигают пункта назначения, его компьютерное устройство может использовать определенный ключ и дешифровать данные.

Цифровые сигналы имеют следующие важные особенности:

- **скорость передачи данных** — это скорость, с которой цифровые сигналы передают данные через беспроводную сеть. Следовательно, значение скорости передачи цифровых сигналов позволяет оценить время, необходимое для их передачи из одной точки в другую, а также определить полосу пропускания (пропускную способность), которую среда должна обеспечивать для эффективной передачи сигналов. Скорость передачи данных определяется общим количеством битов, переданных в течение времени, потребовавшемся для их передачи. Общепринятой единицей измерения скорости передачи является количество битов, переданных за одну секунду (бит/с). В качестве примера рассмотрим сигнал, способный передать 1 000 000 бит за одну секунду. Скорость передачи данных составит 1 000 000/1 = 1 000 000 бит/с (или 1 Мбит/с);
- **пропускная способность** аналогична скорости передачи данных. Однако при вычислении пропускной способности обычно исключают биты, соответствующие служебным сигналам, добавляемым коммуникационными протоколами. Стандартов на определение пропускной способности не существует, но обычно при ее определении учитывается только реальная информация, передаваемая по сети. Следовательно, пропускная способность — это более точный метод представления истинной производительности и эффективности сети. Это делает показатель пропускной способности важным при сравнении характеристик беспроводных сетей, поскольку он напрямую связан с производительностью. Чем выше пропускная способность, тем выше производительность. Так, скорость передачи данных беспроводных локальных сетей может составлять 11 Мбит/с, но пропускная способность — только 5 Мбит/с. После вычитания служебных сигналов заголовков фреймов, полей контроля ошибок, фреймов подтверждений и времени, затраченного на повторную передачу вследствие ошибок итоговый объем переданной информации существенно уменьшается. Если число пользователей сети возрастает, растет и конкуренция за совместно используемую среду, что еще больше снижает пропускную способность, поскольку компьютерное устройства (если говорить более точно, платы интерфейса сети) должны дольше находиться в режиме ожидания, прежде чем им будет предоставлена возможность передать данные. Такая задержка, являющаяся, наряду со служебными сигналами, одной из разновидностей "накладных расходов" сети, может существенно снизить ее пропускную способность.

Что касается беспроводных сетей, то в качестве оценки их параметров принято использовать скорость передачи данных в битах. В действительности беспроводная сеть преобразует двоичные цифровые сигналы в аналоговые, а потом уже передает их через воздушную среду.

Аналоговые сигналы

Аналоговый сигнал ***(analog signal,*** рис. 2.8) относится к сигналам, у которых с течением времени изменяется амплитуда. Именно в такой форме распространяются многие сигналы, характерные для природы. Примерами могут служить свет и человеческая речь. Некоторые искусственные сигналы, такие как радиоволны, также являются аналоговыми.

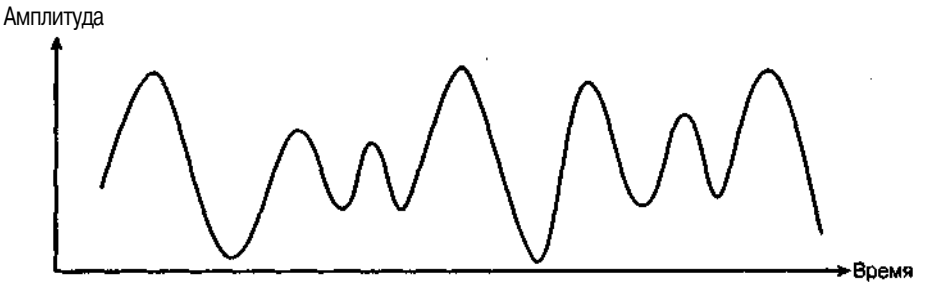

Рис. 2.8. ^налоговые сигналы передают информацию через воздушную среду

На заре электрической связи большинство систем обрабатывали сигналы в аналоговой форме, возможно потому, что входная информация поступала от людей. Параметрами аналогового сигнала являются амплитуда, измеряемая в единицах напряжения или мощности, и частота, измеряемая в количестве циклов изменения амплитуды за единицу времени (эта единица измерения называется *герц).*

В беспроводных сетях обычно передаются аналоговые сигналы в диапазоне 2,4 ГГц, который относится к диапазону радиоволн. Существует несколько методов описания амплитуды беспроводных сигналов. Подробнее об аналоговых сигналах беспроводных сетей в главе 3.

Передача информации через беспроводную сеть

Обычно причиной развертывания беспроводной сети является необходимость передачи информации от одной точки к другой без использования проводов. По мере прохождения потока информации через сеть он меняет свою форму, чтобы поток мог оптимальным способом пройти через сеть. Практически во всех беспроводных сетях поддерживается выполнение особых функций, относящихся к процессу передачи информации — доступ к среде и контроль ошибок.

Конечные точки информационного потока

Как правило, поток информации начинается с пользователя и заканчивается пользователем. Бизнесмен отправляет сообщение электронной почты из аэропорта, врач просматривает медицинские показатели больного через PDA, работник склада создает несколько записей в запоминающем устройстве в ходе инвентаризации.

Изначально информация может быть просто в мозгу человека, затем он преобразует ее в речь или текст, а компьютерное устройство сохраняет ее в виде данных. Ее-

ли пользователем является человек, информация имеет аналоговую форму. При обмене данными пользователями, не являющимися людьми (роботы, компьютерные устройства), информация представлена в виде цифровых сигналов.

Ввод, хранение и отображение информации

Итак, информация передается от пользователя компьютерному устройству, что предполагает ввод ее с помощью клавиатуры, малой клавишной панели, микрофона или видеокамеры. К новейшим методам ввода информации относится также использование для этого движений глаз и излучений мозга. Эта информация представляется в виде аналоговых сигналов.

Прежде чем компьютерное устройство сможет сохранить информацию, система должна преобразовать аналоговую информацию в цифровую, необходимую для компьютерных устройств. Эту задачу выполняют аналого-цифровые преобразователи (АЦП). Специальные схемы осуществляют выборку значений аналогового сигнала, амплитуда полученных в результате импульсов представляется в виде двоичных чисел. Аналогично цифро-аналоговые преобразователи (ЦАП) преобразуют переданные цифровые сигналы в аналоговые с целью представления ее в виде, удобном для пользователя.

В компьютерном устройстве информация представляется в виде данных за счет использования специальных кодов. Так, Американский стандартный код обмена информацией (American standard code for information interchange, ASCII) представляет символы латинского алфавита в виде чисел. Компьютер хранит эти числа в виде данных. Например, ASCII-код (в шестнадцатеричной фирме) прописной буквы A — это число 41, строчной h— 68. В большинстве компьютеров ASCII-кодирование используется для представления чисел в двоичной форме, т.е. только с помощью нулей и единиц. Видео- и аудиоинформация кодируется в виде символов.

Взаимодействие с воздушной средой

После того как компьютерное устройство получит от пользователя задание передать информацию через беспроводную сеть, оно "договаривается" о соединении с удаленным компьютером, подключая для этого функции транспортного и сеансового уровней. После установления соединения устройство передает данные в цифровой форме плате интерфейса беспроводной сети. Эта плата обычно передает фрейм, содержащий информацию, соответствующую указанному стандарту, например ШЕЕ 802.11, плате интерфейса беспроводной сети, находящейся на удаленном компьютерном устройстве или в точке доступа.

Передающая плата интерфейса беспроводной сети, прежде чем передать данные с помощью антенны, преобразует их в радиочастотный или световой сигнал. Для этого необходимо осуществить модуляцию: сигнал преобразуется из цифровой формы в аналоговую. Модулированный сигнал распространяется через среду передачи и достигает платы интерфейса беспроводной сети приемного устройства, где он подвергается демодуляции и обработке, а затем полученные данные передаются на более высокие структурные уровни.

Доступ к среде

Важным аспектом передачи данных через беспроводную сеть является *доступ к среде (medium access)*. Это — функция канального уровня, здесь происходит своего рода суммирование протоколов, которым должны следовать все платы интерфейса

беспроводной сети. Благодаря этим протоколам обеспечивается координация передачи данных платами интерфейса беспроводной сети, особенно если в каждый момент времени только одна из них может вести передачу. При отсутствии такого механизма в сети все время происходили бы коллизии.

Как и в случае проводных сетей, наиболее распространенным протоколом доступа к среде для беспроводных сетей является CSMA. Для обеспечения распределенного доступа к совместно используемой среде CSMA использует метод "слушай, прежде чем говорить". При использовании этого протокола каждая плата интерфейса беспроводной сети имеет возможность принимать сигналы от других устройств.

Если узел А (рис. 2.9) имеет данные, подлежащие передаче, вначале он проверяет, пытаясь принять сигналы, не передает ли данные какой-то другой узел. Если среда свободна — не принимаются никакие сигналы — то узел А передает один фрейм данных. Если узел А обнаруживает сигналы какого-то другого узла, он воздерживается от передачи и выжидает некоторое время, а потом вновь "прослушивает" канал. Операция обнаружения сигналов других узлов выполняется до тех пор, пока узел А не передаст фрейм данных.

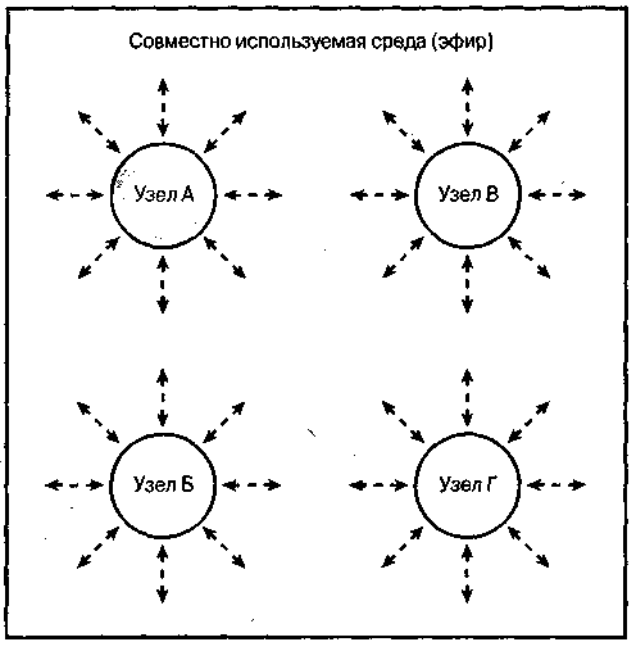

Рис. 2.9. Узел А — часть гипотетической беспроводной сети, в которой каждый узел может передавать данные

Но даже при использовании протокола CSMA может произойти коллизия, хотя передающий узел и будет прослушивать канал, прежде чем приступить к передаче данных. Причина этого — ненулевое время распространения сигнала между узлами. Сигнал, передаваемый конкретным узлом, не блокирует передачу других до тех пор, пока сигнал не достигнет всех остальных узлов.

Допустим, узел Б начинает передавать сигнал. Узлу А тоже необходимо передать фрейм. Он прослушивает среду и решает, что она свободна, поскольку из-за задержки на распространение сигнал узла Б еще не достиг узла А. В результате узел А обнаруживает, что среда не занята, и начинает передачу. В следующий момент происходит коллизия между двумя переданными фреймами, что приводит к ошибкам при приеме обоих фреймов данных. Оба узла вынуждены повторно передавать фреймы.

CSMA обеспечивает асинхронный доступ к среде: для конкретной платы интерфейса сети не гарантируется, что в течение определенного промежутка времени она получит доступ к среде и сможет передать данные. Следовательно, передача пакетов при использовании протокола CSMA не идет с постоянной скоростью. Это вызывает проблемы при передаче информации в реальном масштабе времени, например речи или видеосигналов, поскольку сеть может оказаться не в состоянии передавать фрагменты информации настолько регулярно, чтобы обеспечить надлежащее качество. В таких случаях для улучшения параметров сети повышают ее производительность и применяют функции обеспечения высокого качества связи (QoS).

Контроль ошибок

При распространении сигналов через воздушную среду некоторые биты могут быть получены с ошибками. Их вызывают шум и помехи в месте развертывания беспроводной сети. Поэтому плата интерфейса беспроводной сети использует механизмы контроля ошибок, позволяющие выявить и исправить ошибки, возникающие при передаче символов.

Шум, обусловленный излучением солнца и различными устройствами, приводит к искажению сигналов, распространяющихся в беспроводных сетях; этот шум постоянен. Но *уровень шума (noise floor)* часто бывает достаточно низким, поэтому приемные устройства оказываются в состоянии выделить из него информационные сигналы. При передаче на большие расстояния вследствие затухания уровень информационного сигнала может снизиться до уровня, сравнимого с уровнем шума, и тогда происходят ошибки в приеме двоичных разрядов.

Шум, вызывающий изменение значений битов при передаче информации в беспроводной сети, обычно бывает гауссовым и/иди вызывается импульсными помехами. Теоретически амплитуда гауссова шума одна и та же во всем спектре частот, а ошибки происходят независимо одна от другой. Наиболее вреден импульсный шум, характеризующийся длинными интервалами его отсутствия, после которых появляется шумовой сигнал высокой амплитуды.. Такой шум возникает по естественным причинам (например, из-за молний), а также генерируется рукотворными устройствами. Именно импульсный шум вызывает появление большинства ошибок в цифровых системах связи, причем ошибок, зависимых одна от другой и следующих группами. Такое искажение сигналов получило название *"пакет ошибок"*.

Методы контроля ошибок позволяют значительно снизить их число при передаче. Ошибки в передаче отдельных разрядов чисел по-прежнему происходят при распространении фреймов данных через воздушную среду, но механизмы контроля ошибок исправляют их. Поэтому для высокоуровневых протоколов и пользователей передача информации через среду представляется происходящей как бы без ошибок.

Используются в основном два метода контроля ошибок: автоматический запрос на повторение (automatic repetition query, ARQ) и прямое исправление ошибок (forward error correction, FEC). При применении механизма ARQ, функционирую-

щего на канальном уровне, принимающая сигнал плата интерфейса беспроводной сети выявляет ошибки и использует цепь обратной связи, чтобы послать передающей сигнал плате интерфейса беспроводной сети, передающей сигнал, запрос на повторную передачу фреймов, полученных с ошибками. Возможны два основных события, которые должны произойти, чтобы могла быть осуществлена. коррекция ошибок механизмом ARQ. Во-первых, принятый фрейм должен быть проверен приемником на предмет возможных ошибок, а во-вторых, отправитель должен быть уведомлен о необходимости повторной передачи фреймов, принятых с ошибками. В некоторых протоколах, таких как 802.11, получатель посылает отправителю подтверждение, если принятый фрейм не содержит ошибок. Не получив такого подтверждения, отправитель должен послать фрейм повторно. Существует два подхода к повторной передаче неудовлетворительных блоков:

- ARQ по типу "остановиться и ждать";
- непрерывный ARQ.

ARQ по типу "остановиться и ждать"

При способе передачи "остановиться и ждать" передающая плата интерфейса сети передает блок данных, затем останавливает передачу и ждет от принимающей платы интерфейса сети подтверждение, был ли конкретный фрейм принят или нет. Если передающая сторона получает отрицательное подтверждение, предыдущий фрейм передается повторно. При получении положительного подтверждения передающая плата интерфейса сети отправляет следующий фрейм. Эта форма контроля ошибок применяется в устройствах стандарта 802.11.

Одним из преимуществ метода ARQ по типу "остановиться и ждать" является то, что при его использовании не требуется много памяти для приемной или передающей платы интерфейса сети. Исходящий фрейм запоминается только на стороне отправителя (на случай его повторной передачи). С другой стороны, этот метод неэффективен, если задержка на распространение между отправителем и получателем становится слишком большой. Например, данные, передаваемые по спутниковому каналу связи, обычно имеют задержку, связанную с подтверждением приема, порядка нескольких сотен микросекунд. Следовательно, для поддержания разумной эффективности передачи данных приходится использовать блоки большого объема. Проблема в том, что с увеличением объема данных растет и вероятность появления ошибки в каждом блоке, т.е. чем чаще происходит повторная передача, тем ниже результирующая производительность.

Непрерывный ARQ

Одним из способов повышения пропускной способности протяженных каналов является метод непрерывного ARQ. Передатчик посылает блоки данных непрерывно, до тех пор пока приемная плата интерфейса сети не обнаружит ошибку. Обычно передающая плата интерфейса сети передает определенное количество фреймов, при этом она регистрирует, какие именно фреймы передала. Если на приемной стороне обнаруживается дефектный блок, она посылает сигнал передающей плате интерфейса сети с запросом на передачу такого фрейма. Когда получатель посылает сигнал с требованием повторной передачи определенного фрейма, несколько после-

дующих фреймов могут оказаться уже переданными из-за задержки на распространение между отправителем и получателем.

Передающая плата интерфейса сети может повторно передавать фреймы при использовании непрерывного ARQ по-разному. Один из вариантов таков: отправитель извлекает ошибочный фрейм из памяти передатчика и повторно пересылает его, а также все последующие фреймы. Этот метод называется "возврат на эн" (go-back-n), и он может оказаться эффективнее, чем метод ARQ "остановиться и ждать", поскольку обеспечивает более действенное использование полосы пропускания канала. Проблема возникает в том случае, если п — число фреймов, которые передатчик посылает после ошибочного фрейма, плюс один — становится большим, метод теряет свою эффективность. Это обусловлено тем, что при повторной передаче только одного ошибочного фрейма приходится пересылать и остальные, переданные без ошибок, из-за чего снижается производительность.

Мбтод "возврат на эн" хорош для приложений, когда приемник имеет память небольшого объема, потому что все, что необходимо — это окно на прием единичного размера (т.е. способность запоминать один фрейм), поскольку предполагается, что фреймы не придется располагать по порядку. Когда приемная плата интерфейса сети отбрасывает фрейм с ошибками — посылает отрицательное подтверждение, ей не приходится в ожидании повторной передачи запоминать последующие фреймы для возможного изменения их порядка, поскольку они также будут переданы повторно.

Альтернативой методу непрерывной передачи с "возвратом на эн" является метод, при котором селективно осуществляется повторная передача только ошибочного фрейма и возобновление нормальной передачи с момента, непосредственно предшествующего получению уведомления о плохом блоке данных. Это — подход селективного повторения, который производительнее, чем метод "возврат на эн", поскольку передающая плата интерфейса сети повторно пересылает только ошибочный блок данных. Однако приемник должен быть в состоянии запоминать несколько фреймов данных, если их необходимо обрабатывать в определенном порядке. Приемник буферизирует данные, полученные после того как был отправлен запрос на повторную передачу ошибочного фрейма, и делает это до тех пор, пока поврежденный фрейм не будет передан повторно.

Все типы автоматического запроса на повторение основаны на выявлении ошибок и повторной передаче данных. В общем случае ARQ — наилучший способ коррекции пакетов ошибок, поскольку искажения такого типа обычно накладываются на небольшую долю фреймов и многочисленные повторные передачи выполнять не приходится. Так как ARQ-протоколам изначально присуща обратная связь, используются *полудуплексные* ***(half-duplex)*** или *полнодуплексные* ***(full-duplex)*** линии связи — ведь связь при использовании методов ARQ осуществляется в двух направлениях. Если доступны только *симплексные* ***(simplex)*** линии связи, методы ARQ использовать невозможно, поскольку приемник не сможет сообщить передающей плате интерфейса сети об ошибочных блоках данных.

При использовании метода FEC, альтернативного по отношению к ARQ, приемной платой интерфейса сети автоматически осуществляется исправление максимально возможной доли ошибок, возникающих при передаче данных на физическом уровне, без обращения к передающей плате интерфейса сети. Это возможно, поскольку передающая плата интерфейса сети включает в передаваемые данные достаточное число избыточных битов на случай, если некоторые из них будут утеряны из-

за ошибок. Метод FEC удобен для линий симплексной связи и в случаях, когда затруднена передача данных в обратном направлении (в сторону передающей платы интерфейса сети).

Рассмотрим вариант беспроводной передачи данных для управления космическим зондом, выведенным на орбиту Плутона. За время, пока передающая плата интерфейса сети получит отрицательное подтверждение от зонда и его достигнут повторно переданные данные, зонд скорее всего потерпит аварию, причина чего в слишком большой задержке распространения. Большинство беспроводных сетей развернуты на Земле, но задержки распространения и здесь могут оказаться достаточно большими для того, чтобы метод FEC оказался неприемлемым.

Хотя способность метода FEC исправлять ошибки без обращения к передающей плата интерфейса сети кажется весьма привлекательной, более распространенным методом контроля ошибок остается ARQ. Это обусловлено в основном тем, что ошибки обычно объединяются в кластеры, поскольку вызываются импульсным шумом. Из-за этого приходится корректировать большое число ошибок, а это метод FEC выполнить не в состоянии без значительного увеличения уровня избыточности.

Во многих системах связи используется комбинация методов FEC и ARQ. В этом случае устройства физического уровня пытаются исправить небольшое число ошибок и тем самым избежать необходимости повторной передачи данных. Если по методу FEC удается исправить все ошибки, механизм ARQ не задействуется для повторной передачи фрейма данных. Если ошибок слишком много, в игру вступает ARQ и отправитель повторно посылает такой фрейм.

Передача беспроводных сигналов

Воздушная среда не предполагает использования каких-либо активных компонентов в беспроводной сети. На вид и эффективность беспроводных информационных сигналов влияют несколько пассивных элементов. Так, при распространении через среду сигналы могут затухать из-за погодных условий, находящихся на их пути материальных объектов, а также из-за потерь, вызванных большим расстоянием между передающей и приемной платами интерфейса сети. Кроме того, сигналы, передаваемые через воздушную среду, подвержены *многолучевому* ***(multipath)*** распространению, воздействию помех и других факторов. Подробнее об ухудшении качества сигналов по мере их распространения через среду — в главе 3.

Подключение к инфраструктуре проводной сети

В состав базовой станции, такой как точка доступа, входят как плата проводного, так и плата беспроводного интерфейса сети, а также программное обеспечение, взаимодействующее с этими двумя сетями. Когда "беспроводной" пользователь связывается с другим "беспроводным" пользователем, базовая станция просто перенаправляет фрейм данных, полученный от одного пользователя, другому. В данном случае станция действует как повторитель. Альтернативный вариант — перенаправление базовой станцией фрейма данных в свою проводную часть, если получатель расположен в проводной части сети.

Получая фрейм данных, плата беспроводного интерфейса сети, размещенная в базовой станции, преобразует аналоговый радио- или световой сигнал в цифровую форму и выполняет процедуру обнаружения ошибок, чтобы полученный в результа-

те фрейм данных не содержал ошибочных двоичных разрядов. Если есть ошибки, механизм контроля ошибок посылает плате беспроводного интерфейса сети запрос на повторную передачу фрейма данных. Позаботившись об ошибочных фреймах, плата беспроводного интерфейса базовой станции или перенаправит фрейм, или направит его в проводную часть базовой станции.

Плата интерфейса беспроводной сети обычно реализует технологию Ethernet, обеспечивающую непосредственное взаимодействие с системой предприятия. Базовая станция обычно соединяется с беспроводной и проводной сетями на физическом и канальном уровнях. В состав некоторых базовых станций входит также маршрутизатор, выполняющий функции сетевого уровня.

В ходе передачи по проводам сигналы остаются в цифровой форме, но системы различных типов могут преобразовывать цифровые сигналы в форму, более подходящую для передачи через конкретную среду. Сигналы могут быть вновь преобразованы в аналоговые, если их необходимо передать через другой беспроводной канал, например спутниковый, чтобы они могли попасть в пункт назначения.

Резюме

Беспроводные сети включают компоненты, позволяющие выполнять мобильные и портативные приложения. Конечными точками беспроводной сети являются пользователи, которые применяют компьютерные устройства, разработанные для выполнения конкретных приложений. Платы интерфейса беспроводной сети и базовой станции являются ключевыми компонентами, обеспечивающими связь через воздушную среду. Для роуминга в масштабах здания или города распределительная система, такая как Ethernet, обеспечивает соединения между базовыми станциями и взаимодействие пользователей с серверами и приложениями, размещенными в проводной сети.

Функции сети описывает семиуровневая эталонная модель OSI, но беспроводные сети реализуют лишь те из них, которые относятся к двум нижним уровням — физическому и канальному. В число этих функций входят обеспечение доступа к среде передачи, контроль ошибок и формирование радио- или световых сигналов для передачи их через среду. Однако при развертывании беспроводной сети важно убедиться в том, что протоколы более высоких уровней реализуют свои возможности, направленные на нейтрализацию ухудшений, вносимых беспроводной сетью.

Вопросы для самопроверки

Ответы на эти вопросы вы можете найти в приложении А.

1. Платы интерфейса беспроводной сети с каким форм-фактором наилучшим образом подходят для миниатюрных беспроводных компьютерных устройств?
2. Приведите примеры факторов, отрицательно влияющих на передачу коммуникационных сигналов через воздушную среду.
3. Каково основное назначение базовой станции?
4. Каковы основные особенности промежуточного программного обеспечения беспроводной сети?

5. На каких уровнях эталонной модели OSI работает беспроводная сеть?
6. В чем состоит отличие между пропускной способностью и скоростью передачи данных?
7. Компьютерное устройство хранит данные в аналоговой форме. Справедливо ли это утверждение?
8. В какую форму должна преобразовывать сигналы плата интерфейса беспроводной сети, прежде чем передать их через воздушную среду?
9. Какой протокол доступа к среде является общепринятым для беспроводных сетей?
10. Объясните, как работает механизм контроля ошибок ARQ.

В этой главе...

какие основные параметры радио- и световых сигналов влияют на их распространение через воздушную среду;

как беспроводные сети изменяют форму представления информации для передачи ее через среду.

ГЛАВА 3

Основы передачи радио- и световых сигналов: невидимая среда

Основное различие между беспроводной и проводной сетями состоит в использовании различных сред передачи. В проводных сетях используются медные кабели, по которым с помощью электрического тока и передается информация. В беспроводная сетях используются радиочастотные и световые сигналы, передающие информацию через воздушную среду. В данной главе мы продолжим рассмотрение концепций, общих для беспроводных сетей всех типов, с упором на радиочастотные и световые сигналы.

Беспроводные приемопередатчики

Беспроводной приемопередатчик состоит из приемника и передатчика. В передатчике в ходе процесса, получившего название *модуляция* ***(modulation),*** электрические цифровые сигналы, поступившие из компьютера, преобразуются в радио- или световые волны, которые по своей сути являются аналоговыми сигналами. Затем эти сигналы усиливаются и подаются на *антенну* ***(antenna).*** В пункте назначения приемник выделяет из шумов относительно слабые сигналы и демодулирует их, преобразуя затем в данные, приемлемые для компьютера пункта назначения. Элементы, показанные рис. 3.1, составляют то, что принято называть приемопередатчиком, который реализуется аппаратно и является частью платы интерфейса беспроводной сети.

Рис. 3.1. В беспроводной сети сигналы подвергаются процессам усиления и модуляции

Что такое радиосигналы?

Радиосигналы (RF signals) — это электромагнитные волны, которые система связи использует для передачи информации через воздушную среду от одной точки к другой. Такие сигналы используются уже много лет. Именно благодаря им мы можем слушать радиопередачи и смотреть телевизионные трансляции. В действительности радиосигналы являются более распространенным средством передачи данных, чем беспроводные сети.

Параметры радиосигналов

Радиосигнал передается от антенны передающей станции к антенне приемной. Сигнал, подаваемый на антенну, характеризуется амплитудой, частотой и фазой (рис.3.2). За счет изменения этих параметров можно посредством радиосигналов передавать информацию.

Амплитуда определяет интенсивность радиочастотного сигнала. Мерой амплитуды является мощность, которая аналогична затраченным усилиям человека, преодолевающего на велосипеде определенное расстояние. Мощность — это количество энергии, необходимой для преодоления сигналом определенного расстояния. Если мощность возрастает, то увеличивается и дальность связи.

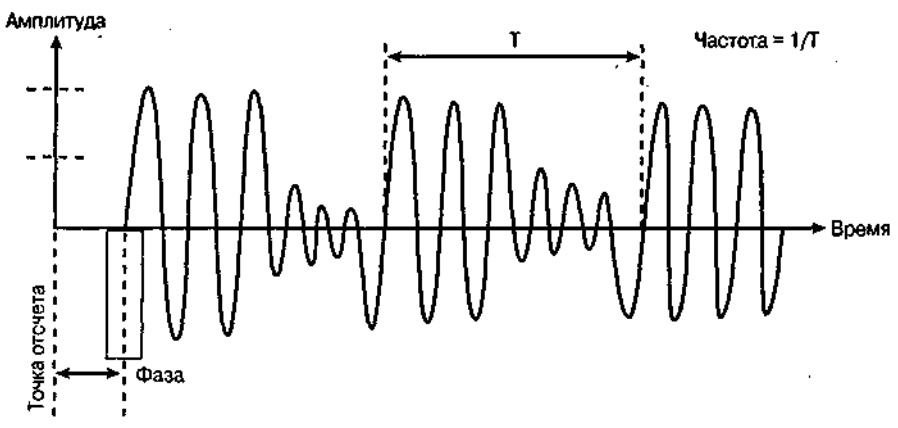

Рис. 3.2. Основными параметрами радиочастотного сигнала являются амплитуда, частота и фаза

Поскольку радиосигнал распространяется через воздушную среду, его амплитуда уменьшается. В случае отсутствия препятствий радиосигналы испытывают то, что инженеры называют *потери в свободном пространстве,* они являются одной из причин затухания сигнала. Кроме того, амплитуда сигнала уменьшается экспоненциально по мере увеличения расстояния между передатчиком и приемником. Экспоненциальное затухание модулированного сигнала вызывает атмосфера, если он распространяется достаточно далеко от антенны. Следовательно, сигнал должен обладать достаточной мощностью для того, чтобы преодолеть нужное расстояние и иметь после этого уровень, достаточный для выделения его из шумов приемным устройством.

Однако способность приемника улавливать сигнал зависит и от наличия других радиочастотных сигналов. Чтобы проиллюстрировать это, представим двух людей, Эрика и Серину, которые разделены расстоянием примерно в 7 м (20 футов) и пытаются разговаривать. Серина, выполняя роль передатчика, говорит достаточно громко, чтобы Эрик, приемник, мог слышать каждое ее слово. Если их ребенок, Мэдисон, громко кричит, Эрик может пропустить несколько слов. В данном случае эффективная связь невозможна из-за помехи со стороны ребенка. Или Эрик и Серина должны подойти ближе друг к другу, или Серина должна говорить еще громче. Это хорошая аналогия того, как передатчики и приемники беспроводной системы используют для связи радиочастотные сигналы.

Частота ***(frequency)*** свидетельствует о том, сколько раз в секунду сигнал повторяет сам себя[1]. Единица измерения частоты — герц (Гц), значение частоты соответствует числу циклов, происходящих в течение секунды. Например, беспроводная локальная сеть стандарта 802.lib работает на частотах порядка 2,4 Гбит/с; это означает, что количество циклов колебаний составляет примерно 2 400 000 000 в секунду.

Фаза соответствует тому, насколько далеко сигнал отстоит от какой-то исходной точки[2] Традиционно принято считать, что каждый цикл сигнала соответствует повороту фазы на 360 градусов. Например, сдвиг фазы сигнала может составлять 90 градусов, это означает, что сдвиг фазы равен четверти (90/360 = 1/4) от полного цикла сигнала. Изменение фазы может быть использовано для передачи информации. Так, сдвиг фазы сигнала на 30 градусов можно представить как двоичную 1, а сдвиг фазы на 60 градусов — как двоичный 0. Важным преимуществом представления данных в виде сдвигов фазы является снижение влияния затухания сигнала при его распространении через среду. Затухание обычно влияет на амплитуду, а не на фазу сигнала.

Преимущества и недостатки радиочастотных сигналов

Преимущества радиочастотных сигналов по сравнению со световыми (табл. 3.1) делают их эффективными для применения в большей части беспроводных сетей. Большинство стандартов беспроводных сетей, таких как 802.11 и Bluetooth, регламентируют применение именно радиочастотных сигналов.

Таблица 3.1. Преимущества и недостатки радиочастотных сигналов

Преимущества	Недостатки
Относительно большая дальность связи, до 35 км, при условии прямой видимости	Меньшая пропускная способность, порядка Мбит/с
Высокая работоспособность в условиях слабого и сильного тумана; только сильный дождь ухудшает характеристики	Подверженность помехам со стороны внешних систем, использующих радиоволны
Не требуется лицензия (только для систем стандарта 802.11)	Низкая защищенность, поскольку радиоволны распространяются за пределы строений

[1] Дополним это весьма вольное объяснение определением из "Политехнического словаря": частота колебаний — количественная характеристика периодических колебаний, равная отношению числа циклов колебаний ко времени их совершения. — Прим. ред.

[2] А вот определение, которое дает "Политехнический словарь": фаза — величина, определяющая состояние колебательного процесса в каждый момент времени. — Прим. ред.

Искажение радиочастотного сигнала

Радиочастотные сигналы подвержены искажениям, которые обусловлены помехами и многолучевым распространением. Они влияют на связь между отправителем и получателем, часто снижая ее характеристики и вызывая недовольство пользователей.

Помехи

Помехи ***(interference)*** возникают, когда приемной станции одновременно достигают два сигнала, предположительно одной и той же частоты и фазы. Это похоже на то, как если бы человек пытался одновременно слушать двух говорящих. В подобной ситуации приемная плата интерфейса беспроводной сети делает ошибки при декодировании информации.

Федеральная комиссия связи США (Federal Communication Commission, FCC) регламентирует использование большинства частотных диапазонов и типов модуляции, чтобы системы не создавали взаимных помех. Однако избежать их все равно не удается, особенно если системы работают в диапазонах, не подлежащих лицензированию. Пользователи могут свободно устанавливать и использовать не подлежащее лицензированию оборудование, в том числе беспроводные локальные сети, не координируя с кем-либо его использование и не беспокоясь о создаваемых им помехах.

На рис. 3.3 схематично представлены различные формы помех. Внутренние помехи возникают тогда, когда внешние сигналы мешают распространению радиосигналов беспроводной сети. Эти помехи могут вызывать ошибки в информационных разрядах передаваемого сигнала. Приемник обнаруживает ошибки, в результате осуществляется повторная передача, а пользователь, возможно, замечает задержку связи. Сильные внутренние помехи могут возникать, если неподалеку работает другая радиосистема на той же частоте и с тем же типом модуляции. Примером могут служить две беспроводные локальные сети, работающие в одних и тех же нелицензируемых диапазонах и развернутые неподалеку одна от другой.

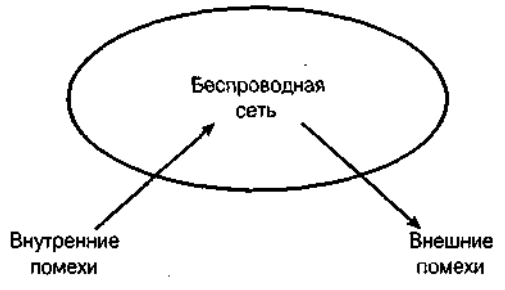

Рис. 3.3. Помехи могут быть внутренними и внешними

Другими источниками внутренних помех могут быть беспроводные телефоны, микроволновые печи и устройства стандарта Bluetooth. Если используются радиочастотные устройства таких типов, пропускная способность беспроводной сети может существенно снизиться — вследствие повторных передач и возрастания в сети конкуренции за право доступа к среде. Поэтому развертывание сети следует тщательно планировать и учитывать при этом другие радиоустройства, которые могут создавать помехи беспроводной сети.

Одним из наилучших способов борьбы с радиочастотными помехами является удаление их источников. Например, в компании могут запретить использование беспроводных телефонов, работающих в том же частотном диапазоне, что и беспроводная сеть. Однако, невозможно полностью ограничить использование потенциальных источников помех, например, устройств стандарта Bluetooth. Если помехи становятся серьезной проблемой, следует выбрать беспроводную сеть, работающую в частотном диапазоне, в котором не возникает конфликтов.

Внешние помехи возникают тогда, когда сигналы радиочастотной системы создают помехи другим системам. Как и в случае внутренних помех, сильные внешние помехи могут возникнуть, если беспроводная сеть находится в непосредственной близости от другой системы. Поскольку мощность сигналов, передаваемых в беспроводной сети, относительно невелика, внешние помехи редко вызывают какие-то проблемы.

Многолучевое распространение

Многолучевое распространение происходит тогда, когда один и тот же радиосигнал приходит к узлу назначения (точке доступа) различными путями (рис. 3.4). Одна его часть достигает точки назначения, распространяясь по прямой, другая — отразившись от поверхности стола, а затем от потолка. Поэтому часть сигнала проходит больший путь до приемника, т.е. испытывает дополнительную задержку.

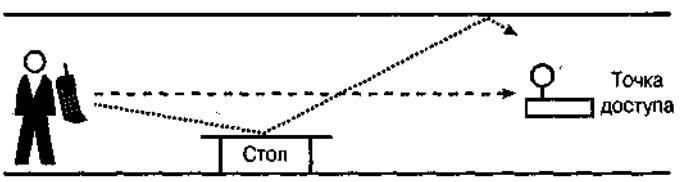

Рис. 3.4. Препятствия могут вызывать отражения сигнала в различных направлениях

Многолучевое распространение приводит к тому, что информационные символы, представленные в виде радиосигнала, смазываются (рис. 3.5). Поскольку информация, подлежащая передаче, заключена именно в форме сигнала, приемник делает ошибки при выделении информации из сигналов. Если задержки достаточно велики, пакеты принимаются с ошибками, особенно при большой скорости передачи данных. А приемник не в состоянии различать символы и правильно интерпретировать их соответствующие биты. При многолучевом распространении приемная станция в процессе контроля ошибок обнаруживает значительное их количество. В результате передающая станция вынуждена повторно передавать фреймы.

При многолучевом распространении и, как следствие, повторных передачах пользователи ощущают снижение характеристик сети. Например, сигналы стандарта 802.11 в домах и офисах могут испытывать задержку порядка 50 не, в то время как заводизготовитель ориентируется на задержку в 300 не. Следовательно, многолучевое распространение не будет представлять серьезной проблемы при домашнем использовании беспроводных сетей и в офисах. Но на заводах станки и металлическое стеллажи имеют множество поверхностей, от которых радиочастотные сигналы отражаются и вследствие этого распространяются совершенно беспорядочно. Поэтому на складах, заводах и в других помещениях, где есть различные металлические препятствия, проблема многолучевого распространения может оказаться весьма серьезной.

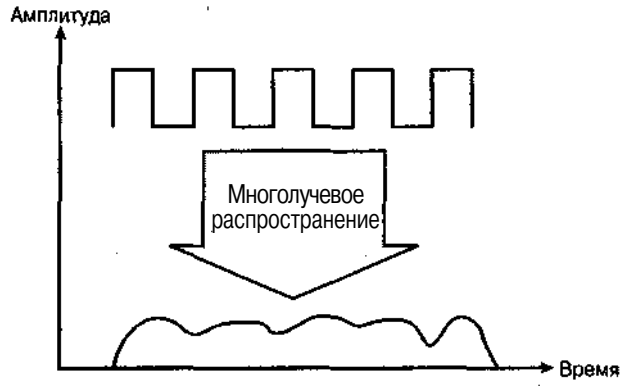

Рис. 3.5. Смазывание сигналов из-за многолучевого распространения ведет к появлению ошибок

Что же делать, если такие сложности возникли? Оставим в стороне вариант освобождения здания от столов и стеллажей. Для обеспечения отказоустойчивости системы применяют метод диверсификации (разнообразия). В данном случае диверсификация может быть осуществлена за счет использования двух антенн для каждой радиоплаты интерфейса сети с тем, чтобы усилить разницу между сигналами, принимаемыми разными антеннами, и обрабатывать лучший из них. Антенны должны быть физически удалены от радиостанции, чтобы одна из них наверняка была меньше подвержена многолучевому распространению. Иными словами, смешанный сигнал, принимаемый одной антенной, должен быть ближе к оригиналу, чем сигнал, достигающий другой антенны. Приемник использует методы фильтрации сигнала и программное обеспечение принятия решений, чтобы выбрать для демодуляции лучший из двух сигналов. В действительности возможен и обратный вариант: когда не приемник, а передатчик выбирает лучшую антенну, излучающую в другом направлении.

Что такое световые сигналы?

Световые сигналы начали применять в системах связи намного раньше, чем радиочастотные. Сотни лет назад для передачи кода между кораблями на море использовали фонари. И до сих пор световыми устройствами пользуются во многих аэропортах как резервным средством связи с самолетами, у которых отказала радиоаппаратура.

Однако беспроводные сети на основе световых сигналов распространены не так широко, как сети, применяющие радиосигналы. Световые сигналы обычно удовлетворяют потребностям специальных приложений, таких как каналы связи между зданиями и в персональных сетях небольшого радиуса действия. В некоторых беспроводных локальных сетях и продуктах, предназначенных для применения внутри зданий, при передаче информации между компьютерами используется лазерное излучение.

Параметры светового сигнала

Световые сигналы являются аналоговыми по своей сущности и имеют очень высокую частоту, применение электромагнитных волн этого диапазона не регламентируется FCC. В большинстве беспроводных сетей, применяющих для беспроводной

передачи сигналов свет, используется ИК-излучение с длиной волны 900 нм. Это соответствует частоте 333 333 ГГц, что намного выше частоты радиосигналов и несколько ниже частотного диапазона, воспринимаемого человеческим глазом.

Существуют два основных способа световой передачи — это направленное и рассеянное ИК-излучение (рис. 3.6). Рассеянное лазерное излучение отражается от стен и потолка, а направленное излучение фокусируется в определенном направлении. В большинстве "лазерных" локальных сетей применяется рассеянное лазерное излучение, а модемы и PDA в зданиях используют направленное ИК-излучение.

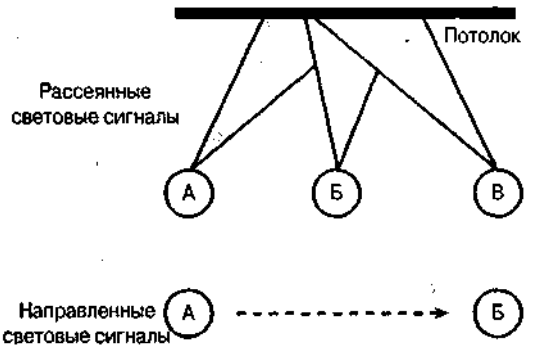

Рис. 3.6. В беспроводных сетях используют как рассеянные, так и направленные световые сигналы

ИК-излучение имеет очень широкую полосу частот, однако при рассеянном излучении сигнал сильно затухает. Поэтому во избежание при передаче большого числа ошибок используется низкая скорость передачи данных (менее 1 Мбит/с). Кроме того, при этом методе область размещения беспроводных компонентов ограничена высотой потолков — примерно 13м (40 футами), что и определяет геометрию распространения. Преимущество таких сетей в легкости их развертывания и дешевизне компонентов.

При использовании направленного излучения (иногда этот метод называют "оптика свободного пространства") мощность светового сигнала возрастает аналогично тому, как это происходит при использовании направленной радиоантенны. Благодаря этому радиус действия маломощных лазерных систем возрастает до 1,6 км при скоростях передачи данных порядка Гбит/с.

Как и в случае радиочастотных сигналов, амплитуда световых волн уменьшается по мере увеличения расстояния между передающей и приемной станциями. Радиус действия ИК-систем может изменяться от нескольких метров при использовании PDA до полутора километров при направленном ИК-излучении. Это существенно меньше, чем при использовании радиочастотных систем.

Преимущества и недостатки световых сигналов

Характеристики световых сигналов делают их эффективными для применения в специализированных приложениях, когда требуется чрезвычайно высокая пропускная способность сети. Так, компания может установить ИК-канал связи между двумя соседними зданиями, чтобы обеспечить высокоскоростное резервирование сервера через беспроводную сеть (табл. 3.2).

Таблица 3.2. Преимущества и недостатки световых сигналов

Преимущества	Недостатки
Очень высокая пропускная способность, порядка нескольких Гбит/с	Изменчивые характеристики, снижающие надежность, в случае смога, тумана, дождя, снега и других явлений, нарушающих прозрачность атмосферы
Высокая степень защищенности, обусловленная узостью лазерного луча	Относительно небольшой (около 1,6 км) радиус действия
Не требуется лицензия	Функционирование только при условии прямой видимости и отсутствии преград, таких как здания, деревья и телефонные столбы
Чрезвычайно высокая помехозащищенность от сигналов внешних радиосистем	Проблемы, связанные с разъюстировкой, обусловленной покачиванием зданий

Искажение световых сигналов

При использовании световых сигналов возникают определенные трудности. Искажения, вызванные помехами и препятствиями, ограничивают эксплуатационные характеристики беспроводных сетей, использующих световые сигналы.

Помехи

Световые сигналы не подвержены воздействию помех со стороны источников радиочастотных сигналов, таких как беспроводные телефоны и микроволновые печи. FCC не регламентирует применение световых сигналов — вероятность того, что применяющие их системы станут мешать одна другой, очень мала. Частоты электромагнитных волн ИК-диапазона намного превышают частоты радиоволн и никак на них не влияют, поэтому FCC и не ограничивает их применение.

Однако, помехи от других источников света, могут иногда создавать проблемы. Так, при установке ИК-систем передачи, ориентированных в восточном или западном направлении, они могут быть подвержены влиянию помех со стороны восходящего или заходящего солнца, находящегося низко над горизонтом. В некоторых случаях эта помеха может оказаться столь серьезной, что передача данных через ИК-канал окажется вообще невозможной. При установке таких систем следует следовать рекомендациям производителя по ориентации антенн.

Затухание из-за препятствий и погодных условий

Препятствия, такие как здания, горы и деревья, могут обусловить существенное затухание света при распространении его через атмосферу. Многие из этих объектов состоят из материалов, интенсивно поглощающих или рассеивающих свет. Поэтому следует позаботиться о том, чтобы на участке между конечными точками ИК-системы связи не было каких-либо препятствий.

Даже если препятствия на пути светового луча отсутствуют, затухание все же воз-, можно из-за меняющихся погодных условий. Так уже через час после сильного тумана небо может полностью очиститься, что весьма затруднит расчет энергетического потенциала линии связи ИК-диапазона, особенно если она должна обеспечить передачу данных на предельно большие расстояния. Разработчик должен быть уверен, что затухание, вызванное погодными условиями, не приведет к нарушению связи.

Модуляция: подготовка сигналов к передаче

За счет модуляции данные, полученные из сети, преобразуются в радио- или световые сигналы таким образом, что они становятся пригодными для передачи через воздушную среду. В названный процесс входит преобразование цифровых сигналов, характерных для компьютеров, в аналоговые. Частью этого процесса является также наложение информационного сигнала на носитель, представляющий собой электромагнитную волну определенной частоты. Чтобы носитель мог передавать какую-то информацию, посредством модулирующего сигнала изменяют его параметры, поскольку передавать информационный сигнал в его естественной форме непрактично. Представим, что Брайен хотел бы сказать что-то, не используя проводную связь, из Дейтона, расположенного от нас на расстоянии примерно 100 км. Один из способов — использовать мощные усилитель и громкоговорители. Однако при этом будут оглушены все жители Дейтона. Более приемлемый вариант — промодулировать голосом Брайена радиочастотный или световой *несущий сигнал,* или *несущую* ***(carrier signal),*** который не воспринимается органами слуха человека и может передаваться через воздух. Информационный сигнал может изменять амплитуду, частоту или фазу несущей, а усиление несущего сигнала не беспокоит людей, поскольку его частота находится за пределами диапазона слышимости человека[3].

Именно это и происходит при модуляции. Модулятор смешивает сигнал, поступающий от источника информации, такого как голос или данные, с несущим сигналом. Приемопередатчик подает модулированный усиленный сигнал в антенну. Модулированный сигнал покидает антенну и распространяется через воздушную среду. Антенна приемной станции улавливает сигнал и подает его на демодулятор, который выделяет из модулированного сигнала сигнал информационный.

Одной из простейших форм модуляции считается амплитудная: в этом случае представление данных осуществляется за счет изменения амплитуды сигнала. Амплитудную модуляцию часто используют в световых системах. Включение света означает, что передается бит данных со значением 1, выключение —- передачу бита данных, имеющего значение 0. На самом деле световой сигнал кодируется более сложным образом, но основная идея остается той же— для передачи данных используют включение и выключение света[4]. Это равносильно тому, как если бы люди в темной комнате использовали для передачи данных фонари, кодируя информацию путем их включения и выключения.

В радиочастотных системах применяются более сложные методы модуляции, некоторые из которых рассмотрены ниже.

Частотная манипуляция

Частотная манипуляция, ЧМн ***(frequency-shift keying, FSK),*** осуществляется за счет небольших изменений несущей частоты. Как показано на рис. 3.7, значения битов информационного сигнала, равные 1 или 0, представляются в виде положительного или отрицательного сдвига частоты несущего сигнала. Под отрицательным сдвигом частоты подразумевается ее уменьшение, под положительным — увеличение на определенную небольшую величину. Приемник определяет этот сдвиг, осуществляя тем самым демодуляцию сигнала.

[1] *Точнее, из-за того, что электромагнитные волны любой частоты не воспринимаются органами чувств человека. Кроме того, их коэффициент затухания существенно ниже, чем акустических волн.* — Прим. ред.

Для передачи данных используют очень короткие световые импульсы. — Прим. ред.

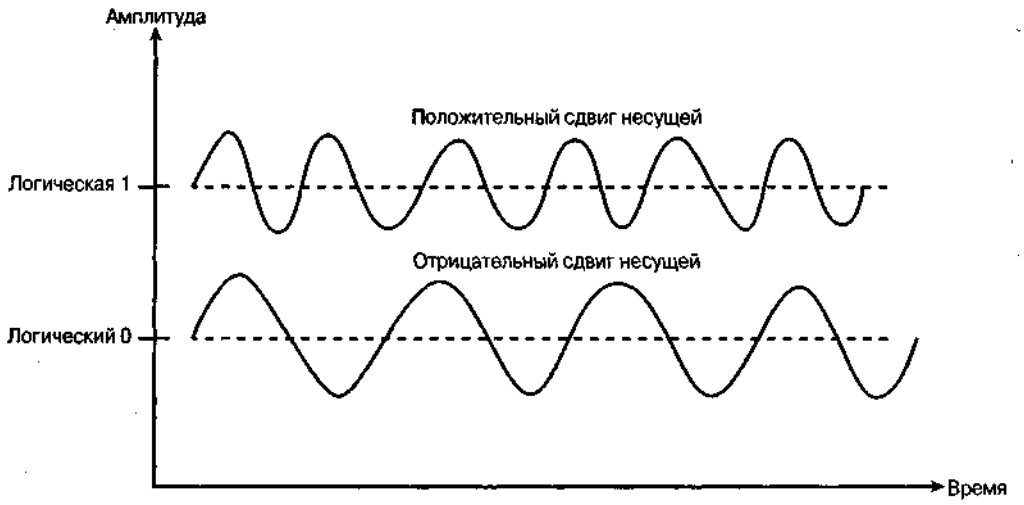

Рис. 3.7. При частотной манипуляции для передачи информации используется сдвиг частоты несущего сигнала

Фазовая манипуляция

Фазовая манипуляция, ФМн ***(phase-shift keying, PSK),*** происходит за счет небольших изменений фазы несущего сигнала. При ФМн для передачи данных используются изменения фазы, в то время как частота остается постоянной. Фазовый сдвиг может быть как положительным, так и отрицательным относительно фазы опорного сигнала (рис. 3.8). Приемник способен обнаруживать эти сдвиги фазы и получать в результате соответствующие биты данных.

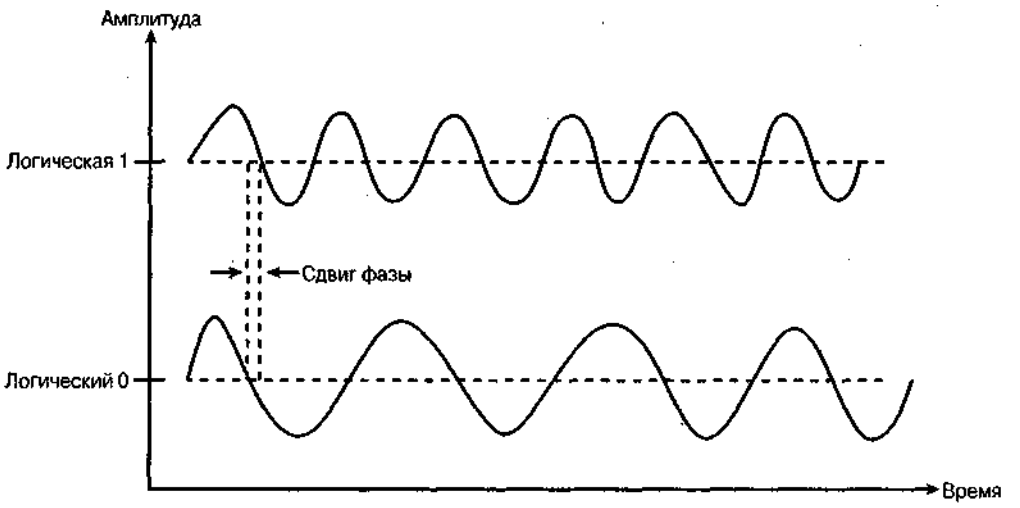

Рис. 3.8. При использовании ФМн для передачи информации используются сдвиги фазы

Квадратурная амплитудная модуляция

Квадратурная амплитудная модуляция ***(quadrature amplitude modulation, QAM)*** предполагает одновременное изменение как амплитуды, так и фазы несущей для представления совокупности данных, называемой символом (рис. 3.9). Преимущество модуляции такого типа заключается в ее способности представлять большую группу символов в виде одной комбинации изменений амплитуды и фазы. Действительно, некоторые системы, при подобной модуляции, используют до 64 комбинаций фазы и амплитуды, позволяющих представить 6 бит данных в виде одного передаваемого символа. Это делает возможным применение QAM в таких стандартах, как 802.На и 802.1 lg, регламентирующих передачу данных с повышенными скоростями.

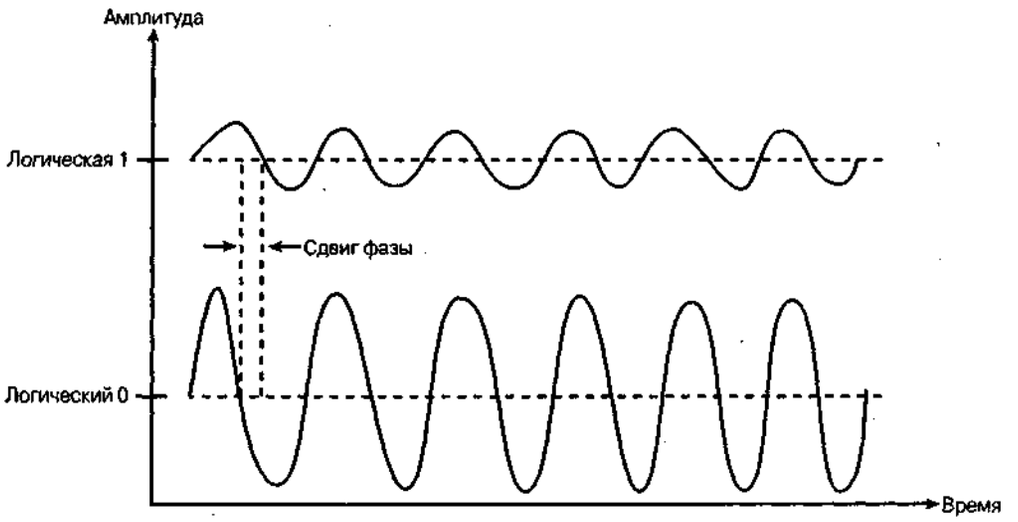

Рис. 3.9. В случае использования квадратурной амплитудной модуляции для передачи информации используют изменения частоты и фазы

Расширение спектра

Помимо модуляции цифровым сигналом аналоговой несущей с использованием ЧМн, ФМн и квадратурной амплитудной модуляции, в некоторых беспроводных сетях применяется расширение спектра модулированной несущей за счет специальных регулятивных правил. Этот процесс, получивший название *расширение спектра* ***(spread spectrum),*** существенно снижает возможность возникновения внешних и внутренних помех. Поэтому регулятивные правила обычно не требуют от пользователей систем с расширением спектра получения лицензии.

Технология расширения спектра, первоначально разработанная для военного ведомства предполагает распределение мощности сигнала в широком диапазоне частот (рис. 3.10). Компоненты, обеспечивающие расширение спектра радиочастот, реализуют или технологию расширения спектра методом прямой последовательности, или технологию скачкообразного переключения частоты. При использовании первой из них несущая модулируется цифровым кодом со скоростью передачи битов намного большей, чем полоса частот информационного сигнала. При скачкообраз-

ном изменении частота носителя резко изменяется от одного значения к другому в пределах определенного диапазона. На рис. 3.11 и 3.12 показано, как изменяется частота при методе прямой последовательности и скачкообразном изменении соответственно.

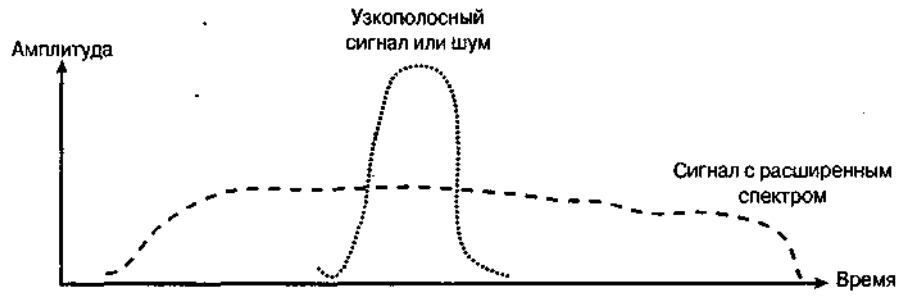

Рис. 3.10. При расширении спектра используется широкая полоса спектра радиочастот

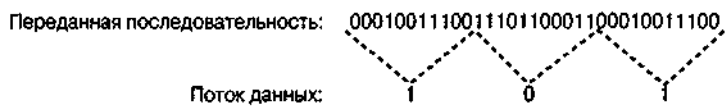

Рис. 3.11. Метод прямой последовательности— один из способов расширения спектра

Большинство систем расширения спектра работают в частотных диапазонах, выделенных Федеральной комиссией связи США (FCC) для промышленного, научного и медицинского применения (Industrial, Scientific and Medicine, ISM). Решение о том, что эти же диапазоны могут быть использованы для беспроводных локальных сетей, было принято FCC в 1975 г. Диапазоны ISM расположены вблизи частот 902 МГц, 2,4 ГГц и 5,7 ГГц. Радиочастотные системы, работающие в диапазонах ISM, должны использовать методы модуляции с расширением спектра, выходная мощность их передатчиков не должна превышать 1 Вт. Потребители, приобретающие продукты диапазонов ISM, не обязаны приобретать лицензию FCC. Благодаря этому можно беспрепятственно устанавливать или перемещать беспроводные сети. Однако, поскольку диапазоны ISM открыты для всех, следует позаботиться об отсутствии помех со стороны других устройств, работающих в этих же диапазонах.

Мультиплексирование с разделением по ортогональным частотам

В некоторых системах используется не технология расширения спектра, а *мультиплексирование с разделением по ортогональным частотам (Orthogonal Frequency Division Multiplexing, OFDM)*. При применении OFDM сигнал, модулированный при посредстве ЧМн, ФМн или квадратурной амплитудной модуляции, делится по многим поднесущим, занимающим определенный канал (рис. 3.13). Технология OFDM очень эффективна, поскольку позволяет передавать данные с повышенной скоростью и минимизировать проблемы, связанные с многолучевым распространением.

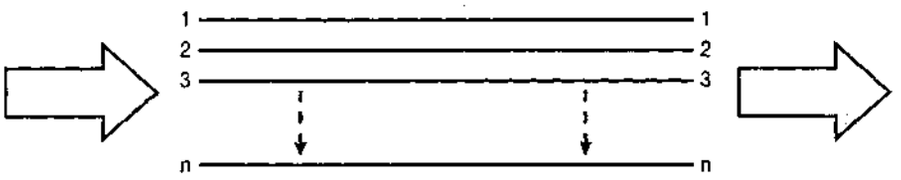

Рис. 3.13. Технология OFDM позволяет одновременно передавать множество данных за счет их распараллеливания

Технология OFDM все чаще используется для высокоскоростной передачи данных. Она не только составная часть стандартов 802.Ha и 802.llg на беспроводные локальные сети, но и основа европейских стандартов HiperLAN/2 на беспроводные локальные сети. Кроме того, технология OFDM поддерживает общемировой стандарт ADSL (Asymmetric Digital Subscriber Line — асимметричная цифровая абонентская линия), т.е. стандарт высокоскоростной проводной телефонной связи.

Сверхширокополосная модуляция

Сверхширокополосная модуляция (ultrawideband, UWB) играет все большую роль в сфере беспроводных сетей, эта технология идет на смену системам с расширением спектра и OFDM. Первоначально ее использовали военные, но сейчас она проходит процедуру необходимых разрешений и утверждений с целью применения ее на коммерческой основе. Хотя внедряется она довольно медленно, но в будущем технология UWB может стать преобладающей для многих типов беспроводных сетей.

Технология UWB основана на использовании для передачи данных маломощных радиосигналов, представляющих собой очень короткие импульсы; спектр частот таких сигналов очень широк. Передаются миллионы импульсов; ширина спектра таких сигналов может составлять несколько ГГц. Соответствующий приемник преобразует импульсы в данные, прослушивая легкоузнаваемую последовательность импульсов, переданную передатчиком.

Первоначально для UWB использовалась скорость передачи от 40 до 600 Мбит/с, но со временем скорости могут быть повышены (при возрастании мощности). UWB-системы могут работать при очень низких уровнях мощности, составляющих примерно одну десятитысячную от таковой сотовых телефонов. Это делает технологию UWB удобной для использования в самых маленьких устройствах, таких как сотовые телефоны, PDA и даже наручных часах, которые пользователь может постоянно носить.

Поскольку системы UWB работают при такой низкой мощности, они почти не влияют на работу других устройств и создают меньше помех, чем обычные радиочастотные системы. Кроме того, поскольку они используют относительно широкий спектр, существенно снижается влияние помех со стороны других систем.

Возможны проблемы, вызванные помехами от высокомощных UWB-систем. FCC планирует пересмотреть рекомендации по технологии UWB в ближайшем будущем, а членам комиссии придется внимательно изучить проблемы, возникающие при применении высокомощных систем. До тех пор применение LTWB-устройств разрешается только при небольшом радиусе действия.

Резюме

Именно благодаря использованию радиочастотных и световых сигналов стало возможным создание беспроводных сетей, представляющих собой средство передачи информации через воздушную среду. Ухудшение качества передачи вызывается в основном помехами, поэтому при развертывании сети следует уделить этому вопросу самое пристальное внимание. Различные методы модуляции — ЧМн, ФМн, квадратурная амплитудная модуляция — используются в сочетании с технологией расширения спектра или OFDM при создании приемопередатчиков, которые можно считать основными узлами плат интерфейса беспроводной сети.

Вопросы для самопроверки

Ответы на эти вопросы вы можете найти в приложении А.

1. Действительно ли радиочастотные сигналы обеспечивают меньший радиус действия, чем световые?
2. Какие метеоусловия существенно влияют на распространение радиочастотных сигналов?
3. Каким образом помехи вызывают появление ошибок в беспроводных сетях?
4. Каковы источники радиочастотных помех?
5. Правда ли, что многолучевое распространение влияет на системы с высокой скоростью передачи данных в системах диапазона 2,4 ГГц сильнее, чем на низкоскоростные?
6. Что понимается под ЯК-системами, использующими рассеянный свет?
7. На каких максимальных дальностях передачи можно использовать направленные ИК-системы?
8. Как модуляция влияет на передачу информации через воздушную среду?
9. Какие параметры сигнала изменяются'для представления информация при квадратурной амплитудной модуляции?
10. Нужна ли пользователю лицензия для использования систем с расширением спектра?

В этой главе...

специфические приложения беспроводных персональных сетей;

компоненты и стандарты беспроводных персональных сетей;

реализация различных систем на основе беспроводных персональных сетей.

ГЛАВА 4

Беспроводные персональные сети: сети для коротких расстояний

Беспроводные персональные сети удовлетворяют требованиям, предъявляемым к беспроводным соединениям для реализации связи на относительно небольших расстояниях, например, между сотовым телефоном и ноутбуком. В большинстве случаев дальность действия сети не превышает 9 м (30 футов). Это делает беспроводные персональные сети применимыми для реализации многих решений, но в большинстве случаев они используются для замены кабелей сопряжения или просто для передачи информации от одного пользователя к другому.

В этой главе даны определения основных компонентов беспроводной персональной сети, показано, как эти компоненты взаимодействуют при формировании различных систем, и рассмотрены несколько технологий, основанных на использовании радио- и ИК-сигналов.

Компоненты беспроводных персональных сетей

В беспроводных персональных сетях применяются как технологии, основанные на использовании радиоволн, так и технологии, базирующиеся на ИК-излучении. И те и другие производители используют в устройствах различных типов.

Пользовательские устройства

Беспроводные персональные сети не требуют для работы высокоемких батарей питания, что делает их идеальными для применения в небольших пользовательских устройствах, таких как наушники, сотовые телефоны, PDA, игровые устройства, GPS-блоки', цифровые камеры и ноутбуки. Некоторые из устройств перечисленных типов показаны на рис. 4.1. Например, беспроводная персональная сеть позволяет слушать музыку через наушники, беспроводным способом соединенные с PDA, или переслать телефонную книгу со своего ноутбука в сотовый телефон. Во всех случаях беспроводная персональная сеть позволяет обойтись от проводов, часто мешающих пользователям.

GPS — сокр. от Global Positioning System (глобальная система навигации и определения положения). — Прим. ред.

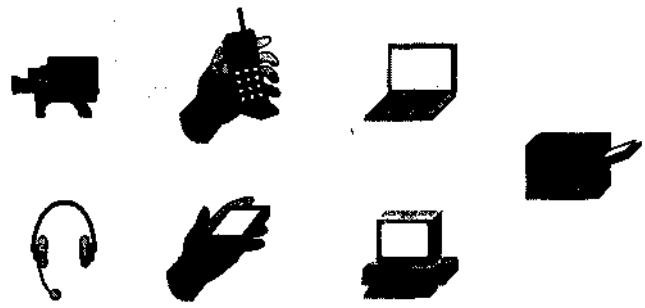

Рис. 4.1. Пользовательские устройства многих типов работают через беспроводную персональную сеть

Радиоплаты интерфейса сети

Радиоплаты интерфейса сети (radio NICs) для беспроводных персональных сетей выпускаются в двух форм-факторах — PC Card и Compact Flash (CF). Если у вас есть, например, ноутбук, его можно наделить способностью работать в беспроводной персональной сети, просто установив в него CF. Многие из новейших PDA и ноутбуков имеют один или несколько интерфейсов беспроводной персональной сети. Это делает названные беспроводные устройства изначально подготовленными к соединению с другими устройствами, такими как принтеры, PDA и сотовые телефоны, если они также имеют интерфейс беспроводной персональной сети. Большие по габаритам PC Card реже используются в беспроводных персональных сетях, в основном потому что для устройств беспроводных персональных сетей хорошо подходят лишь малогабаритные узлы.

USB-адаптеры

Несколько компаний предлагают USB-адаптеры для беспроводных персональных сетей (рис. 4.2), называемые также *беспроводными заглушками (wireless dangle)*. Например, вы можете приобрести USB-Bluetooth-адаптер и подключить его к USB-порту своего компьютера. Это позволит осуществлять синхронизацию ПК с другими устройствами, способными устанавливать Bluetooth-соединения. Bluetooth — это спецификация, разработанная для приемопередатчиков радиодиапазона, обеспечивающих небольшой радиус действия.

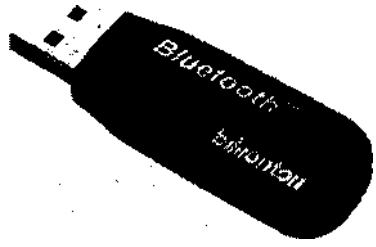

Рис. 4.2. Беспроводные USB-Bluetooth-адаптеры позволяют ПК и ноутбукам взаимодействовать с другими Bluetooth-устройствами

PDA, использующие технологию Bluetooth, могут без помощи проводов взаимодействовать с Bluetooth-ПК и синхронизироваться с ними без необходимости помещения PDA в устройство синхронизации. Но через Bluetooth USB-соединение работает медленнее, чем при подключении к USB-порту ПК через проводной интерфейс. Обусловлено это тем, что беспроводной USB-адаптер работает через последовательный порт ПК, который передает информацию медленнее, чем USB-порт. Беспроводное решение может оказаться более удобным, но процесс синхронизации займет вдвое больше времени.

Маршрутизаторы

В большинстве случаев беспроводная персональная сеть просто заменяет кабельные соединения, но некоторые поставщики предлагают снабженные интерфейсом Bluetooth маршрутизаторы, обеспечивающие беспроводное подключение к Internet. Из-за малого радиуса действия эти маршрутизаторы беспроводных персональных сетей применяются в основном в офисах и в домашних условиях. Чтобы удовлетворить более высоким требованиям, некоторые маршрутизаторы беспроводных персональных сетей поддерживают также интерфейсы беспроводных локальных сетей, таких как сети стандарта 802.11.

Системы на основе беспроводных персональных сетей

Системы на основе беспроводных персональных сетей обычно предназначаются для отдельных пользователей, но некоторые обеспечивают поддержку сразу нескольких. Рассмотрим некоторые конфигурации систем беспроводных персональных сетей.

Дом или небольшой офис

Многие различные конфигурации систем на основе беспроводных персональных сетей применяются в домашних условиях или в небольших офисах.

Синхронизация

Чаще всего беспроводные персональные сети используются для синхронизации PDA и сотовых телефонов с ноутбуками или ПК. На рис. 4.3 показано, как взаимодействуют компоненты системы такого типа. Когда пользователь нажимает на кнопку синхронизации портативного устройства, радиоплата интерфейса сети этого устройства пересылает соответствующие данные радиоплате интерфейса сети ноутбука или ПК. Аналогичным образом ноутбук или ПК пересылает данные портативному устройству. В большинстве случаев беспроводное соединение осуществляет "удлинение" последовательного порта RS-232 до ручного устройства.

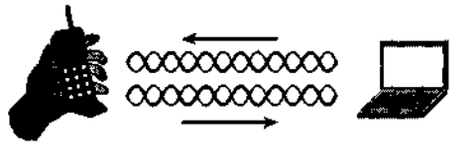

Рис. 4.3. В процессе синхронизации информация передается между двумя устройствами в обоих направлениях

Потоковые мультимедиа-приложения

Большое число приложений беспроводных персональных сетей предназначены для передачи потоковых аудио- и видеосигналов. Например, пользователь может прослушивать потоковые MP3-файлы, хранящиеся на MP3-плейере (рис. 4.4). Многие PDA предоставляют возможность проигрывания аудио MP3-файлов после установки одного из популярных проигрывателей, например RealOne фирмы RealNetworks. При наличии беспроводной персональной сети пользователю не нужно находиться вблизи MP3-плейера и возиться с проводами или при прослушивании музыки быть все время на одном месте. Аналогичная конфигурация включает использование беспроводных наушников и микрофона при разговоре по сотовому телефону, что позволяет высвободить руки. Недостатком такого подхода является то, что при использовании таких беспроводных соединений емкости батарей не хватает на длительную работу.

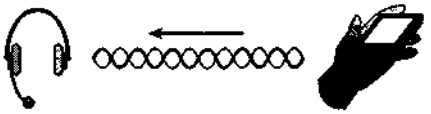

Рис. 4.4. Беспроводная персональная сеть позволяет использовать наушники

Другое преимущество беспроводной персональной сети при использовании потоковых приложений — гибкое соединение между видеокамерой и сервером. Владельцы домов могут, например, разместить Web-камеры в стратегически важных точках для обеспечения своей безопасности. Скрытая камера, размещенная перед входной дверью, позволяет владельцу дома заблаговременно увидеть визитеров на экране и решить, открывать им дверь или нет. В данном случае процедура установки упрощается, поскольку к камере не нужно подводить провода. Электропроводка или батарея, конечно, необходимы для питания камеры, но электророзетки ведь есть в любом доме.

Управление

Беспроводные персональные сети позволяют избавиться от проводов, тянущихся к периферийным устройствам компьютера, таким как беспроводная мышь, клавиатура и телефонная розетка, облегчая перемещение и настройку ПК. Пользователь, например, может использовать полноразмерную клавиатуру, беспроводным способом соединенную с ноутбуком или PDA. Кроме того, беспроводная персональная сеть может помочь уменьшить количество проводов, опутывающих настольный компьютер. Надежность при этом повышается, поскольку исключаются обрывы кабелей и уменьшается вероятность неумышленного нарушения контакта, если кто-то зацепит незакрепленный кабель.

Печать

Беспроводное соединение между ПК и принтером возможно через беспроводную персональную сеть, если они размещены в одной комнате (рис. 4.5). Кабели принтера часто бывают недостаточно длинными, и его приходится устанавливать не там, где удобно, а там, где это возможно. Беспроводная персональная сеть позволяет оптимально разместить принтер.

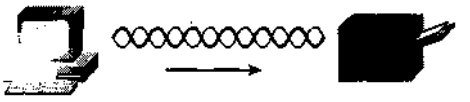

Рис. 4.5. Беспроводная персональная сеть облегчает установку принтера

Соединение с Internet

Пользователь может работать с электронной почтой и просматривать Web-страницы из любой точки комнаты, если беспроводная персональная сеть обеспечивает доступ к Internet. Например, вместо того чтобы сидеть за столом, пользователь может с удобством расположиться в кресле или на диване. Такая свобода делает работу на компьютере намного более приятной. На рис. 4.6 показана конфигурация системы, обеспечивающей такую возможность.

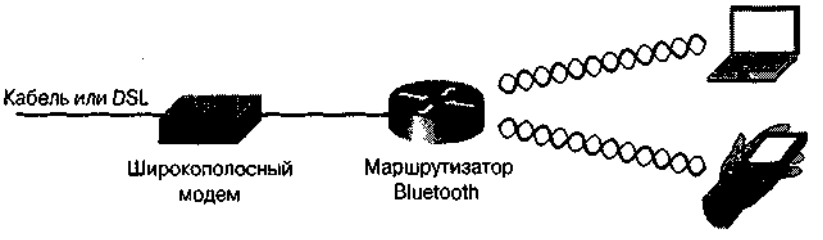

Рис. 4.6. Маршрутизатор беспроводной персональной сети обеспечивает подключение к Internet

Предприятие

Беспроводные персональные сети часто развертываются на промышленных предприятиях, а используемые в сетях приложения и конфигурации системы аналогичны применяемым в домашних условиях и в небольших офисах. Служащие применяют беспроводные персональные сети для синхронизации своих PDA с настольными компьютерами и пользуются преимуществами беспроводного подключения периферийных устройств. Однако для подключения к Internet служащие предприятий используют не маршрутизатор беспроводной персональной сети, а беспроводную локальную сеть.

Площадь предприятия слишком велика, поэтому применение беспроводной персональной сети становится непрактичным — пришлось бы устанавливать слишком много базовых станций.

Технологии беспроводных персональных сетей

Технологии беспроводных персональных сетей основаны на применении как радиоволн, так и ИК-излучения — в зависимости от того, с какой целью развертывается сеть.

Стандарт 802.15

Рабочая группа IEEE по стандартам серии 802.15 занимается разработкой стандартов для беспроводных персональных сетей и координацией их с другими стандартами, такими как стандарт 802.11 на беспроводные локальные сети.

Рабочая группа ШЕЕ по стандартам серии 802.15 состоит, в свою очередь, из следующих групп:

- **802.15.1.** Рабочая группа 1, определяет стандарты на беспроводную персональную сеть, основанную на использовании спецификаций Bluetooth версии 1.1. В основе этой технологии с расширением спектра лежит скачкообразное изменение частоты (FHSS), скорость передачи не превышает 1 Мбит/с. Группа 802.15 опубликовала стандарт 802.15.1 в июне 2002 года; на его основе и осуществляется разработка Bluetooth-устройств.
- **802.15.2.** Группа, отвечающая за разработку этого стандарта, Рабочая группа 2, дает практические рекомендации, способствующие сосуществованию сетей стандартов 802.15 и 802.11. Проблема состоит в том, что обе сети работают в одном и том же диапазоне 2,4 ГГц, поэтому координация между их работой жизненно необходима. Группа проводит оценку возможных помех и предлагает методы противодействия им.
- 802.15.3. Рабочая группа 3 работает над проектами новых стандартов на высокоскоростные беспроводные персональные сети. Скорость передачи может составлять 11, 22, 33, 44 и 55 Мбит/с. Наряду с этими повышенными скоростями передачи стандарты регламентируют применение механизмов обеспечения качества связи (QoS), что делает их хорошей основой для обеспечения работы мультимедийных приложений. Эта группа занимается также снижением стоимости и потребляемой мощности. Проект стандарта 802.15.3 уже готов для распространения.
- 802.15.4. Рабочая группа 4 работает над стандартами, предусматривающими низкую скорость передачи данных, но зато при экстремально низком энергопотреблении для малогабаритных устройств, рассчитанных на работу без замены батареи питания в течение месяцев и даже лет. Кандидатами на применение этой технологии могут быть всевозможные датчики, "умные" идентификационные жетоны и системы бытовой автоматизации. Скорость передачи данных составляет 20, 40 и 250 Кбит/с. Проект стандарта 802.15.4 уже можно приобрести.

Подробнее о стандартах 802.15 на http://grouper.ieee.org/groups/802/15

Bluetooth

Технология Bluetooth появилась в 1998 г. в результате совместной деятельности компаний Ericsson, IBM, Intel, Nokia и Toshiba. Они работали над созданием решения, обеспечивающего беспроводное взаимодействие компьютерных устройств. Спецификация Bluetooth, которая не считается стандартом, идеальным образом подходит для дешевых малогабаритных устройств с малой потребляемой мощностью и радиоканалами небольшого радиуса действия. Это делает технологию Bluetooth эффективным решением для соединения между собой малогабаритных устройств в небольших рабочих зонах. Именно поэтому Рабочая группа 802.15 выбрала Bluetooth в качестве основы для стандарта 802.15.1.

Основные особенности

Специальная группа по интересам (Special Interest Group, SIG) Bluetooth опубликовала первую версию спецификации в середине 1999 г. С тех пор она несколько раз дорабатывалась, но технические характеристики остались в основном прежними. Приемопередатчики Bluetooth работают в диапазоне 2,4 ГГц со скоростью до 1 Мбит/с с использованием технологии FHSS. Она предполагает непрерывное скачкообразное изменение частоты во всем отведенном для передачи спектре с частотой 1600 изменений в секунду, что намного быстрее, чем частота изменений, предусмотренная для аналогичной технологии в стандарте 802.11.

Устройства Bluetooth с низким энергопотреблением обеспечивают дальность передачи около 9 м (30 футов). Высокомощные Bluetooth-устройства способны работать на расстояниях до 91 м (300 футов), однако такой режим работы применяется редко.

Модули Bluetooth имеют относительно небольшие форм-факторы. Типичные габариты 10,2 x 14 x 16 мм, поэтому они могут быть легко встроены в различные пользовательские устройства.

Технология Bluetooth способна обеспечивать автоматическое соединение Bluetooth-устройств, находящихся неподалеку одно от другого, но пользователь имеет возможность принять или отклонить возможность соединения с другим пользователем. В случае, если есть сомнения в безопасности, соединение можно отклонить. Возможность шифрования также оговорена в спецификации.

Может ли Bluetooth заменить беспроводные локальные сети?

Технология Bluetooth обеспечивает рабочие характеристики, сходные с таковыми беспроводных локальных сетей. За счет использования высокомощной версии Bluetooth производители в дальнейшем смогут предлагать точки доступа и маршрутизаторы Bluetooth с радиусом действия таким же, какой обеспечивают сети стандарта 802.11. Однако предлагаемые в настоящее время изделия Bluetooth имеют намного меньшую потребляемую мощность и ориентированы на выполнение функций, характерных для беспроводных персональных сетей. Кроме того, продуктам, поддерживающим технологию Bluetooth, было бы трудно завоевать существенную долю рынка, поскольку уже достаточно широко распространены изделия стандарта 802.11.

В чем уступает технология Bluetooth изделиям стандарта 802.11, так это в радиусе действия и производительности. Компоненты сетей 802.11 могут обеспечивать скорость передачи до 54 Мбит/с, Bluetooth — в лучшем случае 1 Мбит/с. Этого может оказаться вполне достаточно в большинстве случаев замены кабельных соединений (например, для обеспечения взаимодействия наушников и PDA), но для просмотра Web-страниц с использованием широкополосного соединения или создания корпоративной сети нужны более высокие характеристики. Кроме того, радиус действия устройств стандарта 802.11 в условиях офиса обычно составляет примерно 90 м (300 футов), что намного превышает возможности Bluetooth. Для организации беспроводной сети на основе технологии Bluetooth на достаточно обширной площади пришлось бы развертывать слишком много точек доступа. Поэтому весьма маловероятно, что продукты технологии Bluetooth вытеснят с рынка изделия стандарта 802.11. Магазины электроники торгуют в основном изделиями стандарта 802.11 (Wi-Fi), предназначенными для организации беспроводных персональных сетей, а не устройствами Bluetooth.

Могут ли беспроводные локальные сети заменить Bluetooth?

Вполне возможно, что беспроводные персональные сети стандарта 802.11 окажут большое влияние на объемы продаж Bluetooth-устройств, поскольку их компоненты по своим параметрам соответствуют аналогичным параметрам Bluetooth или превосходят их. Так как изделия Bluetooth пока еще недостаточно широко распространены, у поставщиков сетей стандарта 802.11 есть время для выхода на рынок и беспроводных персональных сетей. Однако для этого необходимо осуществить некоторые модификации. Например, уменьшить габариты компонентов сетей стандарта 802.11, но для этого компании должны наладить выпуск более миниатюрных чипсетов. Компоненты с меньшими габаритами, как правило, потребляют меньше энергии, что делает их пригодными для устройств (типа сотовых телефонов), питающихся от миниатюрных батарей. Поскольку группа 802.15 разрабатывает стандарты для беспроводных персональных сетей на основе технологии Bluetooth, а группа 802.11 сосредоточена на беспроводных локальных сетях, весьма вероятно, что технологии стандарта 802.11 и Bluetooth смогут сосуществовать и дополнять одна другую.

Минимизация помех со стороны Bluetooth

Количество беспроводных устройств растет, и поэтому приходится все больше внимания уделять потенциально возможным взаимным помехам. Результаты тестирования фиксируют существенные взаимные помехи между устройствами Bluetooth и другими системами, работающими в диапазоне 2,4 ГГц, такими как беспроводные локальные сети стандарта 802.11. Проблема возникает из-за того, что устройства Bluetooth и компоненты сетей стандарта 802.11 никогда "не понимали" друг друга и не следовали одним и тем же правилам. Радиостанция Bluetooth может бессистемно начать передачу данных как раз в то самое время, когда станция стандарта 802.11 передает фрейм. Возникает коллизия, из-за которой станция стандарта 802.11 вынуждена передать этот фрейм повторно. Из-за отсутствия какой-либо координации и возникают взаимные радиочастотные помехи между устройствами стандарта 802.11 и спецификации Bluetooth.

Из-за потенциальной возможности возникновения коллизий сети стандарта 802.11 и спецификации Bluetooth не реализуют все свои возможности. Станция стандарта 802.11 автоматически снижает скорость передачи данных и повторно передает фрейм, если случается коллизия. Соответственно и протокол стандарта 802.11 при наличии поблизости устройств Bluetooth вводит задержки. Степень влияния радиочастотных помех зависит от степени использования и близости устройств Bluetooth. Помехи возникают тогда, когда устройства стандарта 802.11 и Bluetooth начинают передавать данные одновременно. Пользователи могут иметь ноутбуки и PDA со встроенным интерфейсом Bluetooth, но помех не будет, если их Bluetooth-устройства не используют Bluetooth для передачи данных.

Приложения Bluetooth, обеспечивающие печать с ноутбука или синхронизацию PDA с настольным компьютером, используют радиоканал в течение коротких периодов времени. В этом случае Bluetooth-устройства не бывают активными настолько долго, чтобы существенно снизить производительность сети стандарта 802.И. На1фимер, пользователь может синхронизировать свои PDA и настольный компьютер по утрам, после прибытия на работу. В другое время его Bluetooth-радиостанция остается неактивной и не вносит какие-либо помехи в течение всего дня.

Наибольшее влияние оказывается, если в компании используется крупномасштабная сеть, посредством которой, например, обеспечивается мобильность врачей и сестер, использующих PDA, в пределах всей больницы. Если сеть Bluetooth достаточно обширна и степень ее использования колеблется от средней до высокой, Bluetooth-система, возможно, будет вызывать множество коллизий в сети стандарта 802.11, размещенной на той же территории. В таком случае сосуществование сетей стандарта 802.11 и Bluetooth окажется затрудненным, и производительность, скорее всего, снизится.

Помимо интенсивности использования Bluetooth-устройств степень влияния помех во многом зависит от близости этих устройств к радиоплатам интерфейса сети и точкам доступа. Мощность, излучаемая Bluetooth-устройствами, обычно ниже, чем в сетях стандарта 802.11. Следовательно, станция стандарта 802.11 должна находиться достаточно близко (на расстоянии около 3 м) к передающему Bluetooth-устройству, чтобы возникли существенные взаимные помехи.

Типичным примером возникновения такой ситуации может служить ноутбук пользователя, в котором Bluetooth используется для поддержания соединений с PDA и принтером, а интерфейс стандарта 802.11 — для доступа к Internet и корпоративным серверам. Возможность возникновения помех в этом случае очень велика, особенно если пользователь работает вблизи границы зоны действия сети стандарта 802.11 (рис. 4.7). Сигнал от Bluetooth-устройств, вероятнее всего, заглушит ослабленный вследствие большого расстояния от точки доступа сигнал стандарта 802.11.

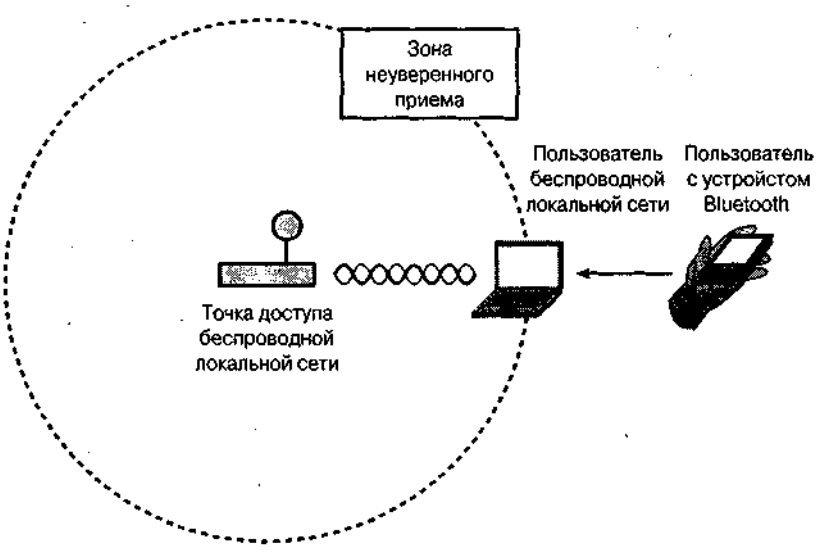

Рис. 4.7. Радиочастотные помехи могут возникать между Bluetooth-устройствами и устройствами беспроводной локальной сети стандарта 802.11

Существует несколько способов, помогающих избежать помех со стороны Bluetooth-устройств.

- **Регулируйте применение радиочастотных устройств.** Одним из способов снижения уровня помех является правильный выбор типов радиочастотных устройств для дома и офиса. Иными словами, следует установить собственные регулятивные правила использования нелицензионных радиочастотных устройств. Экстремаль-

ной мерой был бы полный запрет на использование Bluetooth-устройств, но это непрактично, а в некоторых случаях и невозможно. Например, можно запретить использование Bluetooth-устройств в общедоступных зонах крупного офиса. Что касается личных приложений, то можно выработать политику компании, ограничивающую использование Bluetooth только конкретными приложениями, такими как синхронизация PDA и настольных компьютеров.

Обеспечьте адекватную зону действия сети стандарта 802.11. Сильные, хорошо различимые сигналы во всех зонах действия сети стандарта 802.11 снижают степень воздействия со стороны сигналов Bluetooth. Если сигнал беспроводной локальной сети становится слишком слабым, помехи со стороны сигналов Bluetooth становятся более проблематичными. Проведите исследование уровня сигналов в зоне развертывания сети и определите места размещения точек доступа.

Перейдите в диапазон 5 ГГц. Если ни одна из вышеназванных мер не решила проблему, рассмотрите возможность использования беспроводной локальной сети, работающей в диапазоне 5 ГГц, например сети стандарта 802.11a. Вы можете полностью избавиться от помех в этом диапазоне — по крайней мере, в обозримом будущем.

Подробнее о спецификации Bluetooth и соответствующих ей изделиях на `www.bluetooth.com`.

IrDA

Основной конкурент технологии Bluetooth — технология, продвигаемая *Ассоциацией по средствам передачи данных в инфракрасном диапазоне* ***(infrared data association,*** ассоциация ***IrDA).*** Соответствующий стандарт был разработан и опубликован в 1993 г. Ассоциация IrDA получила право на создание стандарта, регламентирующего последовательную передачу данных на небольшие расстояния. Основные требования, предъявляемые к этой технологии — дешевизна, низкое энергопотребление, возможность взаимодействия с другими сетями. Технологию IrDA начали применять намного раньше, чем Bluetooth. И действительно, уже несколько лет многие ноутбуки и сотовые телефоны снабжаются IrDA-интерфейсом.

Основные особенности

Основой технологии IrDA является ИК-излучение, которое неспособно преодолевать стены и другие препятствия. Это ограничивает радиус действия IrDA-устройств пространством, свободным от препятствий. Поэтому IrDA-устройства пригодны только для создания приложений типа "точка-точка", например для синхронизации PDA и ПК. Преимуществом технологии IrDA является то, что при ее применении не приходится беспокоиться о радиочастотных помехах.

Стандарт на передачу данных с использованием технологии IrDA, наиболее подходящий для таких устройств, как MP3-плейеры, для которых необходима потоковая передача информации, обеспечивает скорости передачи данных до 4 Мбит/с. Эта версия стандарта предусматривает радиус действия около 1 м (3 футов). Благодаря переходу на менее энергопотребляющие версии можно существенно продлить срок службы батарей, но радиус действия снизится при этом до 20 см (8 дюймов).

Для того чтобы обеспечивать эффективное взаимодействие с периферийными устройствами компьютера (клавиатурой и мышью), разработана версия стандарта для управляющих устройств, при этом скорость передачи данных снижена до 75 Кбит/с. Но зато хост-компьютер может взаимодействовать одновременно с восемью периферийными устройствами.

Подробнее о спецификации IrDA и соответствующих ей изделиях на www.irda.org.

Резюме

Беспроводные персональные сети призваны обеспечивать установление беспроводных соединений в небольших зонах, по размерам соответствующих комнате. Устройства, снабженные интерфейсом Bluetooth или IrDA, позволяют уменьшить количество соединительных кабелей, благодаря чему возрастает гибкость использования приложений. Можно говорить по сотовому телефону и одновременно что-то делать обеими руками, слушать потоковый аудиоплейер, синхронизовать PDA и компьютер. Приложения многих типов могут использоваться как в домашних, так и в рабочих условиях.

Bluetooth и IrDA — основные технологии, применяемые в беспроводных персональных сетях. Группа 802.15 выбрала Bluetooth в качестве основы для стандарта 802.15.1 на беспроводные персональные сети. Из-за ограниченных радиуса действия и производительности технологии Bluetooth маловероятно, что в будущем она вытеснит беспроводные локальные сети стандарта 802.11.

Вопросы для самопроверки

Ответы на эти вопросы вы можете найти в приложении А.

1. Какие форм-факторы наиболее употребительны для радиоплат беспроводных персональных сетей?
2. Какие приложения получают особенно большой выигрыш от использования беспроводного USB-адаптера (или "беспроводной заглушки")?
3. Когда имеет смысл использовать маршрутизатор в беспроводной персональной сети?
4. Какова зона действия беспроводной персональной сети?
5. Какая группа IEEE использовала Bluetooth в качестве основы при разработке своего стандарта?
6. В каком частотном диапазоне работают Bluetooth-устройства?
7. Какая основная проблема возникает при использовании Bluetooth-устройств в области развертывания беспроводной локальной сети стандарта 802.11?
8. Действительно ли оборудованные интерфейсом Bluetooth устройства все время находятся в состоянии "передача"?
9. Какова наибольшая скорость передачи для устройств IrDA?
10. Каковы преимущества технологии IrDA по сравнению с Bluetooth?

В этой главе...

специфические приложения беспроводных локальных сетей;
компоненты и стандарты беспроводных локальных сетей;
конфигурации беспроводных локальных сетей.

ГЛАВА 5

Беспроводные персональные сети: сети для зданий и кампусов

Беспроводные локальные сети удовлетворяют требованиям, предъявляемым к беспроводным соединениям для реализации связи в зданиях и кампусах. Обладая характеристиками и уровнем защиты, сравнимыми с таковыми проводных сетей, решения на основе беспроводных локальных сетей используются в домашних условиях, небольших офисах, на предприятиях и в общественных местах.

В этой главе описаны основные компоненты беспроводных локальных сетей, показано, как эти компоненты должны взаимодействовать в различных системах, и рассмотрены стандарты 802.11.

Компоненты беспроводных локальных сетей

Беспроводные локальные сети состоят из тех же компонентов, что и традиционные локальные проводные Ethernet-сети, а их протоколы похожи на протоколы Ethernet. Различие между ними в том, что беспроводные локальные сети не нуждаются для своего развертывания в проводах.

Пользовательские устройства

Пользователи беспроводных локальных сетей работают со многими устройствами — ПК, ноутбуки, PDA. Применение беспроводных локальных сетей для соединения между собой ПК эффективно потому, что избавляет от необходимости прокладки кабелей. Ноутбуки и PDA подключаются к беспроводной локальной сети просто в силу своей "портативной природы". Пользовательские устройства могут также иметь специфичное аппаратное обеспечение. Например, в беспроводные локальные сети часто включают сканеры штрих-кодов и устройства слежения за состоянием пациентов.

Радиоплаты интерфейса сети

Основной компонент беспроводной локальной сети — радиоплата интерфейса сети, зачастую реализуемая на основе стандарта 802.11. Эти радиоплаты обычно работают на одном физическом уровне — 802.11a или 802.1 lb/g. Как следствие, радиоплата должна реализовывать версию стандарта, совместимого с беспроводной локальной сетью. Радиоплаты беспроводных локальных сетей, реализующие сразу несколько версий этого стандарта и обеспечивающие поэтому более высокую *способность к взаимодействию* ***(interoperability),*** становятся все более распространенными.

Радиоплаты поставляются в различных форм-факторах: ISA, PCI, PC card, mini-PCI и CF. В ПК обычно используются платы ISA и PCI, а в PDA и ноутбуках PC card, mini-PCI и CF-адаптеры.

Точки доступа

Точка доступа состоит из радиоплаты, обеспечивающей связь с отдельными пользовательскими устройствами беспроводной локальной сети, и проводной платы интерфейса сети, обеспечивающей взаимодействие с *распределительной системой (distribution system),* такой как Ethernet. Системное программное обеспечение точки доступа обеспечивает взаимодействие частей беспроводной локальной сети и распределительной системы точки доступа. Это программное обеспечение дифференцирует точки доступа по степени обеспечения управляемости, установки и функциям безопасности. Пример аппаратного обеспечения точки доступа представлен на рис. 5.1.

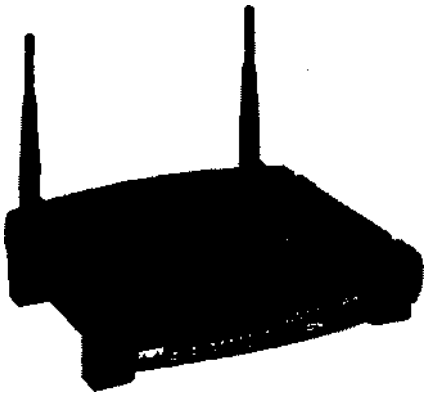

Рис. 5.1. Точка доступа беспроводной локальной сеть соединяет беспроводную локальную сеть с проводными сетями (фото компании Linksys)

В большинстве случаев точка доступа обеспечивает http-интерфейс, позволяющий изменять ее конфигурацию с помощью пользовательского устройства, оборудованного сетевым интерфейсом, и Web-браузера. Некоторые точки доступа также оснащаются последовательным интерфейсом RS-232, благодаря чему их можно конфигурировать через последовательный кабель или пользовательское устройство, осуществляющее эмуляцию терминала и выполняющее программу Telnet (гипертерминал).

Конфигурирование точки доступа

Рассмотрим основные параметры конфигурирования радиотракта для точки доступа Cisco 350, которые применимы и к другим точкам доступа.

Одним из параметров, который нужно выбрать, является идентификатор набора служб (service set identifier, SSID). Этот идентификатор SSID предоставляет имя для конкретной беспроводной локальной сети, к которой привязывается пользователь. С целью обеспечения должного уровня безопасности значение параметра SSID устанавливается отличным от предлагаемого по умолчанию.

В большинстве случаев мощность передатчика точки доступа устанавливается на максимальный уровень, который для США составляет 100 мВт. Это позволяет увеличить радиус действия беспроводной локальной сети. В действительности максимальная эффективная мощность составляет 1 Вт, но меньшая мощность излучения позволяет применять антенны с высоким коэффициентом усиления и в то же время не нарушать установленные ограничения.

В США можно задавать работу точки доступа в одном из 11 -ти разрешенных каналов. Если устанавливается только одна точка доступа, не имеет значения, в каком именно канале она работает. При установке нескольких точек доступа или в случае, когда поблизости и в том же диапазоне работает другая беспроводная локальная сеть, следует выбирать неперекрывающиеся каналы (такие как 1, 6 и 11) для каждой точки доступа, находящейся в зоне действия другой точки доступа.

Как минимум, необходимо активизировать работу протокола шифрования в беспроводной связи (wired equivalent privacy, WEP) для обеспечения хотя бы первичного уровня защищенности. Для этого устанавливается ключ шифрования, необходимый для всех пользовательских устройств, имеющих право взаимодействовать с точкой доступа, позволяющей получать зашифрованные данные. При применении 40-разрядного ключа вводят 10 шестнадцатеричных символов, каждый из которых может принимать значение от 0 до 9 или от A до F. При использовании 104-разрядных ключей потребуется вводить 26 шестнадцатеричных символов. Следует иметь в виду, что 40-разрядные ключи соответствуют 64-разрядной системе шифрования, а 104-разрядные — 128-разрядной системе шифрования в добавок к 24-разрядному вектору инициализации в обоих случаях.

Маршрутизаторы

Судя по названию, маршрутизатор передает пакеты из одной сети в другую, выбирая следующий наилучший канал для передачи пакетов в точку, ближайшую-к месту назначения. Маршрутизаторы используют заголовки пакета *протокола Internet (Internet Protocol, IP)* и таблицы маршрутизации, а также внутренние протоколы для определения наилучшего пути для каждого пакета.

Маршрутизатор беспроводной локальной сети наделяет многопортовый маршрутизатор Ethernet возможностью выполнения функции встроенной точки доступа. Благодаря этому возможно комбинирование сетей Ethernet и беспроводных соединений. Типичный маршрутизатор беспроводной локальной сети имеет четыре порта, точку доступа стандарта 802.11 и зачастую параллельный порт, поэтому он может выполнять и функции сервера печати. Это дает возможность пользователям беспроводной сети получать и отправлять пакеты во многие проводные сети точно так же, как если бы они были подключены к одной из них.

Маршрутизаторы используют *протокол трансляции сетевых адресов (network address translation, NAT),* позволяющий многим'сетевым устройствам совместно использовать один *IP-адрес (IP address),* предоставленный поставщиком (провайдером) *услуг Internet (Internet service provider, ISP).* Эта концепция представлена на рис. 5.2. Маршрутизаторы также применяют *протокол динамического конфигурирования узла (dynamic host configuration protocol, DHCP)* для обслуживания всех устройств, позволяющий предоставлять устройствам отдельные IP-адреса. Совместными усилиями NAT и DHCP делают возможной работу в Internet нескольких сетевых устройств, таких как ПК, ноутбуки и принтеры, с использованием только одного IP-адреса.

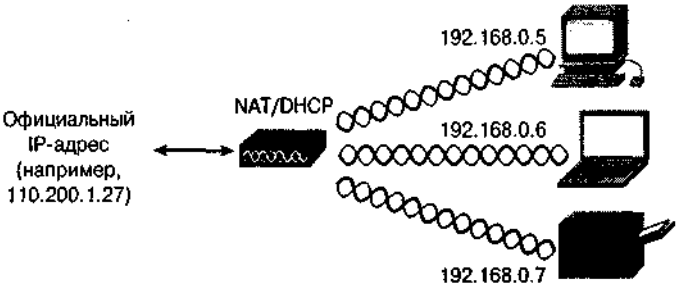

Рис. 5.2. NAT и DHCP— основные протоколы, используемые маршрутизаторами

Маршрутизаторы беспроводных локальных сетей дают существенные преимущества, будучи установленными дома или в небольшом офисе. Например, можно подписаться на услуги, предоставляемые провайдером посредством кабельного модема. В этом случае клиенту выделяется один IP-адрес для маршрутизатора, работающего по протоколу DHCP, а затем маршрутизатор предоставляет IP-адреса с помощью того же протокола DHCP всем клиентам локальной сети. Затем NAT устанавливает соответствие между конкретным клиентом локальной сети и назначенным Internet-провайдером IP-адресом всякий раз, когда клиенту понадобится доступ в Internet. Следовательно, если вы собираетесь предоставлять доступ в Internet более чем одному устройству локальной сети, используя один предоставленный провайдером адрес, вам необходим маршрутизатор. Вместо того чтобы использовать один корпус для маршрутизатора и еще один для точки доступа, оба эти устройства помещают в один корпус. Однако маршрутизаторы редко используют в больших сетях, таких как сети больниц и головных офисов крупных компаний. В подобных случаях рациональнее использовать точки доступа, поскольку в такой сети наверняка есть проводные компоненты с IP-адресами.

Повторители

Точки доступа, для работы которых нужны соединительные кабели, играют основную роль в обеспечении необходимой зоны обслуживания для большинства случаев развертывания беспроводных локальных сетей. Чтобы расширить радиус действия существующей беспроводной локальной сети, в нее вводятся дополнительные точки доступа; второй вариант — воспользоваться беспроводными *повторителями* ***(repeaters).*** Производители предлагают несколько моделей автономных беспроводных повторителей для локальных сетей, но некоторые точки доступа имеют встроенные повторители.

Повторитель просто регенерирует сигналы, распространяющиеся по сети, для увеличения радиуса действия уже существующей сетевой инфраструктуры (рис. 5.3). Повторитель беспроводной локальной сети не имеет физического контакта (осуществляемого с помощью проводов) с какой-либо частью сети. Он принимает радиосигналы от точки доступа, устройства конечного пользователя или другого повторителя и повторно передает полученные фреймы. Это дает возможность повторителю, размещенному между точкой доступа и отдаленным пользователем, функционировать в качестве ретранслятора фреймов, передаваемых от пользователя к точке доступа и обратно.

Поэтому беспроводные повторители представляют собой эффективное решение для преодоления последствий ослабления сигнала, вызванного затуханием радиоволн. Например, повторители могут обеспечить соединение с локальной сетью отдаленной

вующие компоненты и установить беспроводную локальную сеть. Установка и конфигурирование беспроводной локальной сети не представляет трудностей.

Беспроводная локальная сеть для дома или небольшого офиса (рис. 5.4) обычно включает в свой состав один маршрутизатор беспроводной локальной сети, через который и осуществляется широкополосное соединение с Internet (через DSL или кабельный модем). Типичный радиус действия такого маршрутизатора обычно бывает достаточным для обеспечения связи в пределах дома, квартиры или небольшого офиса. Маршрутизатор необходим, если предполагается использование более одного сетевого устройства. НаприМер, если в доме есть беспроводные ПК, ноутбук и принтер, то для обеспечения всех этих устройств сетевыми адресами необходимы протоколы NAT и DHCP.

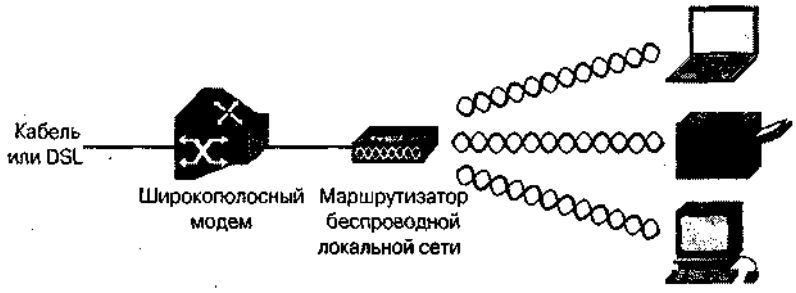

Рис. 5.4. Беспроводная локальная сеть дома или офиса имеет простую конфигурацию

Всего одна точка доступа в доме или небольшом офисе также обеспечит работоспособность сети, но она позволит только одному устройству получить IP-адрес и, соответственно, доступ к Internet. Это обусловлено тем, что большинство точек доступа не работают по протоколам NAT и DHCP. Но комбинация точки доступа и проводного маршрутизатора может заменить маршрутизатор беспроводной локальной сети (рис. 5.5). И это менее дорогостоящее решением, чем приобретение маршрутизатора беспроводной локальной сети, если у вас уже есть точка доступа или проводной маршрутизатор (или и то, и другое).

Рис. 5.5. Комбинация точки доступа беспроводной локальной сети и маршрутизатора Ethernet обеспечивает выполнение тех же функций, что и маршрутизатор беспроводной локальной сети

В точках доступа и маршрутизаторах беспроводной локальной сети установки параметров безопасности, такие как WEP, отключены по умолчанию. Для того чтобы запретить доступ к файлам сети, при установке беспроводной локальной сети нужно активизировать систему ее безопасности.

Беспроводные локальные сети предприятий

Беспроводная локальная сеть предприятия намного сложнее, чем сеть квартиры или небольшого офиса. Основная причина в том, что сети предприятий обычно включают в свой состав множество точек доступа, для соединения которых необходима мощная распределительная система (рис. 5.6). Точки доступа образуют перекрывающиеся радиоячейки (соты), позволяющие пользователю перемещаться в пределах предприятия и иметь доступ к его ресурсам через беспроводную сеть. Такая конфигурация или *режим инфраструктуры* ***(infrastructure mode),*** типична для беспроводной локальной сети, зона обслуживания которой имеет площадь до 1800 м^2.

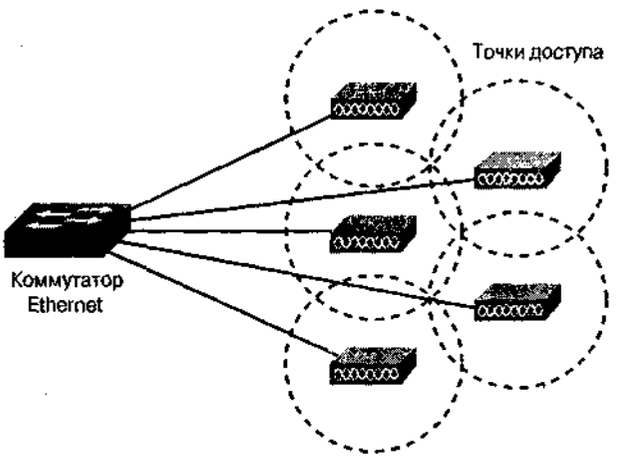

Рис. 5.6. Беспроводная локальная сеть предприятия может быть развернута с использованием множества кабелей, соединяющих точки доступа

Беспроводная локальная сеть больницы может включать сотни точек доступа, разбросанных по всей ее территории. Много коммутаторов Ethernet и кабелей понадобится для того, чтобы это все соединить. Как и в случае других беспроводных локальных сетей предприятий, в больнице, вероятно, уже имеется аппаратное обеспечение, на котором выполняется DHCP. Поэтому на предприятиях используются точки доступа, а не маршрутизаторы беспроводной локальной сети.

Беспроводные локальные сети предприятий также нуждаются в хитроумных механизмах обеспечения безопасности. Гораздо больше внимания должно быть уделено аутентификации и шифрованию, чем в случае применения беспроводной локальной сети дома или в небольшом офисе. Подробнее о безопасности беспроводных локальных сетей — в главе 8.

При развертывании беспроводной лекальной сети на предприятии или в общедоступном месте желательно пригласить специалиста по беспроводным локальным сетям для картирования места работ с целью выявления источников радиочастотных помех, определения оптимальных мест размещения точек доступа и распределения между ними радиочастотных каналов.

Беспроводные локальные сети в больницах

Центры здравоохранения, такие как больницы, госпитали и офисы врачей, должны тщательно вести документацию, без чего невозможно эффективно лечить больных. Элементарная ошибка может стоить кому-то жизни. Поэтому врачам и медсестрам приходится скрупулезно фиксировать результаты анализов, физические данные, назначения лекарств и хирургические вмешательства. Эта бумажная работа перегружает медперсонал, занимая от 50-ти до 70% его рабочего времени. За счет использования мобильных устройств сбора данных, передающих без использования проводов информацию в централизованную базу данных, существенно повышаются точность, степень доступности и наглядности собранных данных.

Врачи и медсестры также становятся "мобильными", могут свободно перемещаться из одной палаты в другую, оказывая помощь пациентам. Благодаря использованию электронных записей о пациентах и возможности ввода, просмотра и обновления данных о них из любого помещения больницы повышается точность и скорость оказания врачебной помощи. Этот результат достигается за счет того, что каждый врач или медсестра получает в свое распоряжение беспроводной компьютер с рукописным вводом — планшетный или PDA, связанный через беспроводную сеть с базой данных, в которой хранится медицинская информация о пациентах.

Так, лечащий врач может выписать больному направление на анализ крови, набрав текст требования на своем карманном компьютере. Лаборатория получит электронный запрос и направит служащего забрать кровь на анализ у пациента. После проведения анализа лаборатория зафиксирует результаты в электронной медицинской карте больного, а врач сможет ознакомиться с ними с помощью своего карманного устройства из любой точки больницы.

Другой вариант использования беспроводных сетей в больницах — отслеживание движения медикаментов. За счет использования ручных устройств считывания и печатания штрих-кодов резко повышается эффективность и точность всех операций, производимых с лекарственными препаратами. Но главное — медперсонал может дать нужное лекарство нуждающемуся в нем больному в нужное время. Если в больнице не используются беспроводная сеть, централизованная база данных и мобильные устройства сбора информации, возможные при этом ошибки трудно исключить.

Беспроводные локальные сети в общественных местах

Общедоступная беспроводная локальная сеть (public wireless LAN) позволяет любому пользователю, имеющему пользовательское устройство с платой интерфейса беспроводной сети, получить доступ к Internet. Общедоступные беспроводные локальные сети развернуты во многих людных местах по всему миру — в аэропортах, торговых центрах, гостиницах. Места, которые постоянно посещают люди, лишь ненадолго задерживаясь в них и сохраняя возможность доступа к сетевым услугам, принято называть *"горячими точками" (hotspots)*.

Найдите ближайшую к вам "горячую точку" на сайте www.wi-fihotspotlist.com/.

Общедоступной беспроводной локальной сетью может пользоваться любой из нас. Она может служить и источником прибыли, потому что владелец "горячей точки" выставляет счета своим абонентам. Однако иногда владельцы таких точек предоставляют доступ к беспроводной сети бесплатно с целью привлечения посетителей.

Беспроводные локальные сети небольших "горячих точек" устроены просто. Например, владелец кафе может установить один маршрутизатор беспроводной локальной сети, позволяющий пользоваться широкополосным Internet-соединением, подобно тому, как это происходит в условиях дома или небольшого офиса. Свободный доступ привлекает посетителей, которые при просмотре Web-страниц и работе с электронной почтой заказывают кофе и какие-то блюда.

Если владелец "горячей точки" намерен получать плату за доступ к сети, в систему беспроводной локальной сети включаются контроллер доступа и узел выставления счетов абонентам (рис. 5.7). Когда пользователь запускает свой Web-браузер, контроллер доступа автоматически перенаправляет его на Web-страницу, на которой ему предлагается зарегистрироваться или подписаться на услуги. Счета абонентам выставляют по различным тарифным планам: поминутно, за день или за месяц пользования. Система выставления счетов отслеживает степень использования сервиса и автоматически снимает нужные суммы с кредитных карт.

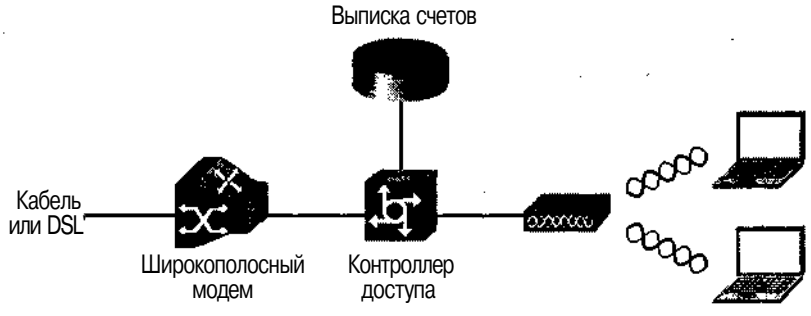

Рис. 5.7. Общедоступные беспроводные локальные сети нуждаются в таких компонентах, которые, в общем-то, не относятся к технологиям беспроводных сетей

В крупных "горячих точках" необходимо устанавливать несколько точек доступа, что делает их сети сравнимыми с беспроводными локальными сетями предприятий. Общедоступные беспроводные локальные сети, охватывающие сразу несколько мест, нуждаются в сложных системах контроля доступа и выписки счетов. Крупная сеть гостиниц может, например, развернуть общедоступные беспроводные локальные сети в сотнях различных мест, а пользователи — подписаться на несколько месяцев предоставления услуг и пользоваться ими из любой гостиницы. Здесь для выполнения функций контроля доступа потребуется централизованный сервер, способный обеспечивать аутентификацию, авторизацию и учет (authentication, authorization and accounting, AAA; принцип трех А).

Общедоступные беспроводные локальные сети в гостиницах

Чтобы обеспечить услугами беспроводного доступа своих постояльцев, гостиницы установили точки доступа в концертных и танцевальных залах, клубах, холлах, бассейнах и гостиничных номерах.

Гостиничная беспроводная локальная сеть позволяет постояльцам во время их пребывания в городе пользоваться следующими услугами:

- просматривать Web-страницы при посещении бассейнов или фитнес-центров;
- получать защищенный доступ к корпоративным сетям из гостиничного номера;
- просматривать в онлайн-режиме расписания встреч и вносить в них необходимые изменения;
- совместно с другими участниками конференции использовать широкополосное Internet-соединение;
- осуществлять из гостиничного номера удаленную печать в бизнес-центре;
- пользоваться видеосвязью для общения с партнерами или членами семьи.

Управляющие и персонал гостиницы также могут извлечь немало пользы из развертывания в ней беспроводной сети. Например, обслуживающий персонал при посредстве беспроводной локальной сети сможет быстрее и эффективнее решать следующие задачи:

- проверять номер гостиницы после освобождения его постояльцем, а результат фиксировать в головном компьютере через PDA стандарта 802.11;
- выполнять скрытую и безопасную проверку того, что дверь номера заперта, огнетушители заряжены, аварийное освещение в порядке и т.д. Вся информация обновляется в реальном масштабе времени, благодаря чему экономится время и исключаются ошибки;
- поддерживать связь с обслуживающим персоналом через беспроводные телефоны, включенные в локальную сеть. Администрация может связываться со служащими в любое время, благодаря чему они быстрее получают и выполняют распоряжения.

Неплановые беспроводные локальные сети

В неплановой (иногда ее называют случайной или специальной) беспроводной локальной сети (ad hoc wireless LAN) отсутствует точка доступа (рис. 5.8). Каждое отдельное пользовательское устройство непосредственно связывается с устройством другого пользователя. Преимущество такой конфигурации состоит в том, что пользователи могут спонтанно и быстро сформировать беспроводную локальную сеть. Неплановые сети также часто называют одноранговыми или пиринговыми сетями (от англ, peer-to-peer).

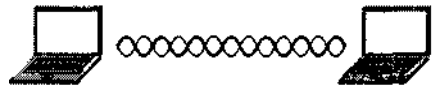

Рис. 5.8. Неплановые беспроводные локальные сети быстро развертываются и приводятся в действие

Неплановая беспроводная локальная сеть позволяет быстро передать файл большого объема коллеге, находящемуся неподалеку в конференц-зале, в случае, если инфраструктура беспроводной локальной сети в нем недоступна. Каждый пользователь просто конфигурирует радиоплату интерфейса сети таким образом, чтобы она могла работать в *режиме неплановой сети* ***(ad hoc mode),*** и нужные соединения осуществляются автоматически. В таких случая пользователи должны удостовериться в том, что их IP-адреса принадлежат одной и той же подсети.

Режим неплановой сети полезен и для поддержания аварийных служб, когда операции должны проводиться в местах, где развертывать проводную сеть для соединения точек доступа непрактично. Члены групп оказания помощи при катастрофах могут, например, быстро установить сетевые соединения между собой во время работы в местностях, где прошел ураган, случилось наводнение или произошло нападение террористов.

Технологии беспроводных локальных сетей

Чаще всего беспроводные локальные сети создают в соответствии со стандартами 802.11 и HyperLAN/2. Их мы и рассмотрим.

Стандарт 802.11

Стандарт IEEE802.il описывает общий *протокол управления доступом к передающей среде* ***(Media Access Control,*** *MAC)* и несколько физических уровней беспроводных локальных сетей. Первая редакция стандарта 802.11 .была принята в 1997 г., но тогда беспроводные локальные сети не нашли широкого применения. Ситуация коренным образом изменилась в 2001-м, когда цены на компоненты резко снизились. Рабочая группа по разработке стандарта IEEE 802.11 активно работает над усовершенствованием стандарта, стремясь улучшить характеристики и защищенность беспроводных локальных сетей.

Стандарт 802.11 регламентирует применение физического уровня с использованием ИК-излучения, однако в настоящее время на рынке отсутствуют продукты, соответствующие этой версии стандарта.

Уровень MAC канального уровня стандарта 802.11

Стандарт 802.11 описывает один уровень MAC, на котором обеспечивается выполнение множества функций с целью обеспечения работоспособности беспроводных локальных сетей стандарта 802.11. Уровень MAC осуществляет управление и поддержку связи между станциями стандарта 802.11 (радиоплатами интерфейса сети и точками доступа), координируя доступ к совместно используемой среде (в данном случае к радиоэфиру). Считающийся "мозгом" сети, уровень MAC стандарта 802.11 управляет физическим уровнем стандарта 802.11, таким как 802.11a, 802.11Ь или 802.1 lg, с целью решения задач по определению занятости или незанятости среды, осуществления передачи и приема фреймов стандарта 802.11.

Прежде чем передать фрейм, станция должна получить доступ к среде, т.е. совместно используемому станциями радиоканалу. Стандарт 802.11 регламентирует две формы доступа к среде: *распределенная функция координации* ***(distributed coordination function, DCF)*** и точечная функция координации (point coordination function, PSF).

Поддержка режима DCF обязательна и основана на протоколе, обеспечивающем *множественный доступ с контролем несущей* и предотвращением коллизий *(Carrier Sense Multiple Access* with Collision Avoidance, CSMA/CA). При работе в режиме DCF станции вступают в конкуренцию за право доступа к среде и пытаются передать фреймы, если в это время никакая другая станция не осуществляет передачу (рис. 5.9). Если какая-то станция передает фрейм, остальные ждут освобождения канала.

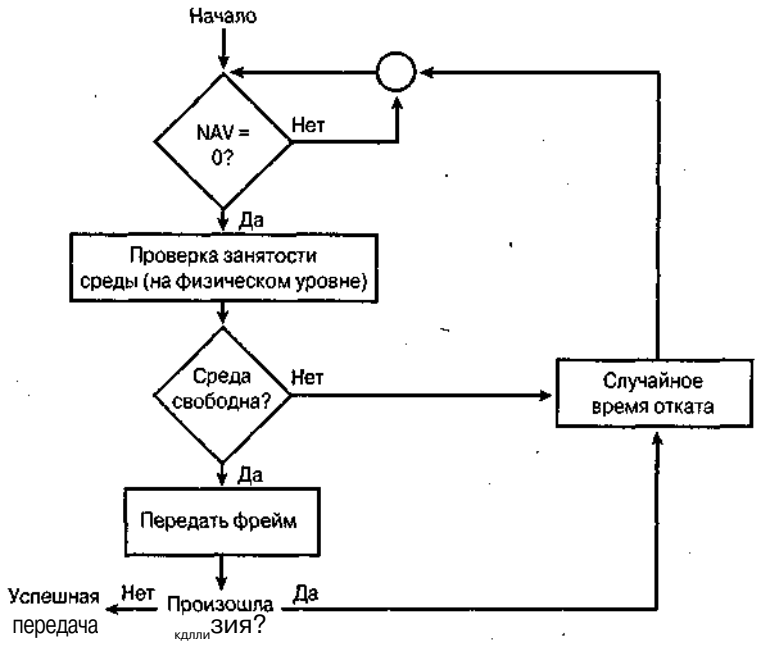

Рис. 5.9. Режим DCFпредполагает распределенную форму доступа к среде

В качестве условия доступа к среде (см. рис. 5.9) уровень MAC проверяет значение своего *вектора распределения сети* (network allocation vektor, NAV), который представляет собой размещенный на каждой станции счетчик, значение которого соответствует времени, необходимому для передачи предыдущего фрейма. Значение NAV должно быть равно нулю, чтобы станция могла попытаться отправить фрейм. Прежде чем послать фрейм, станция вычисляет необходимое для его передачи время на основе объема фрейма и скорости передачи данных в сети. Станция помещает значение, соответствующее названному времени, в *поле продолжительности* (duration field) заголовка фрейма. Когда станция получает фрейм, она проверяет значение в его поле продолжительности и использует его в качестве основы для установки своих NAV. Благодаря этому процессу среда резервируется для использования ее передающей станцией.

Важным аспектом режима DCF является *таймер отката* (back-off timer), который станция использует в случае, если среда передачи оказывается занятой. Если канал используется другой станцией, желающая передать фрейм станция должна находиться в режиме ожидания некоторый случайный промежуток времени и лишь после этого вновь попытаться получить доступ к среде. Благодаря этому исключается возможность того, что несколько станций, намеревающихся передать фреймы,

начнут их отправку одновременно. Из-за случайной задержки разные станции ожидают права на передачу в течение разных периодов времени, поэтому не проверяют среду на занятость в один и тот же момент времени и, обнаружив, что канал свободен, не начинают передачу, создавая тем самым коллизию. Таймер отката существенно снижает число коллизий и, соответственно, повторных передач, особенно когда количество активных пользователей велико.

При использовании локальных сетей на основе радиоканалов передающая станция не может прослушивать среду на предмет возникновения коллизии во время отправки данных, поскольку она не способна использовать свой приемник во время передачи данных. Поэтому приемная станция должна послать *подтверждение* (acknowledgement, ACK) того, что она не обнаружила в полученном фрейме ошибок. Если передающая станция не получит ACK в течение определенного промежутка времени, она предполагает, что произошла коллизия или фрейм был поврежден из-за радиопомех, и передает его повторно.

С целью поддержки оперативной передачи фреймов (например, видеосигналов) стандарт 802.11 опционально предлагает механизм PCF, при использовании которого точка доступа гарантирует конкретной станции доступ к среде путем опроса станции в период, свободный от конкуренции. Станции не могут передавать фреймы до тех пор, пока точка доступа не опросит их на предмет наличия фреймов для передачи. Периоды времени для трафика данных на основе механизма PCF (если это возможно) наступают поочередно с периодами конкуренции.

Точка доступа опрашивает станции в соответствии с опросным листом, затем переходит в режим конкуренции, при котором станции используют механизм DCF. Благодаря этому поддерживаются оба режима работы — синхронный и асинхронный. Однако на рынке пока отсутствуют беспроводные платы интерфейса сети или точки доступа, способные работать в режиме PCF.

Одна из проблем, связанных с PCF, состоит в том, что мало кто из поставщиков поддерживает его в своих продуктах. Поэтому обычно предоставляемые этим механизмом возможности оказываются недоступными для пользователей. Однако в будущем продукты будут поддерживать PCF, поскольку этот механизм позволяет получить необходимое качество обслуживания (QoS).

Далее рассмотрены основные функции, выполняемые на уровне MAC стандарта 802.11.

Сканирование

Стандарт 802.11 регламентирует оба варианта сканирования— активное и пассивное. В ходе этого процесса радиоплата интерфейса сети отыскивает точку доступа. Пассивное сканирование является обязательным, при его осуществлении каждая плата интерфейса сети сканирует отдельные каналы с целью обнаружения наилучшего сигнала от точки доступа. Точки доступа периодически в широковещательном режиме посылают маячковый сигнал (beacon). Радиоплаты интерфейса сети принимают эти маячковые сигналы и принимают к сведению уровень соответствующего сигнала. Эти маячковые сигналы содержат информацию о точке доступа, включая ее идентификатор зоны обслуживания (service set ifentifier, SSID) и поддерживаемую скорость передачи данных. Радиоплата интерфейса сети может использовать эту информацию наряду с данными об интенсивности сигнала для сравнения точек доступа и принятия решения о том, к какой из них следует подключиться.

Опциональное активное сканирование осуществляется похожим способом, за исключением того, что этот процесс инициируется радиоплатой интерфейса сети. Она посылает широковещательный зондирующий фрейм (probe frame), а все точки доступа, находящиеся в радиусе действия, посылают ей ответ на зондирующий фрейм (probe responce). Благодаря активному сканированию радиоплата интерфейса сети может немедленно получить ответы от точек доступа, не дожидаясь передачи маячкового сигнала. Однако при активном сканировании в сети возникают непроизводительные затраты, обусловленные передачей зондирующих фреймов запроса и ответов на них.

Станции, работающие в режиме неплановой сети, в стандарте 802.11 называются *независимой базовой зоной обслуживания* (independent basic service set, IBSS). При работе в этом режиме одна из станций всегда посылает маячковые сигналы, извещая тем самым новые станции о наличии сети. Ответственность за передачу этого маячкового сигнала лежит на каждой станции, ожидающей завершения маячкового интервала (beacon interval) еще некоторое случайное время. Станция передает маячковый сигнал, если по истечении маячкового интервала и некоторого случайного промежутка времени эта станция не получит маячковый сигнал от какой-либо другой станции. Таким образом, ответственность за передачу маячковых сигналов распределяется между всеми станциями.

Аутентификация

Аутентификация — это процесс, в ходе которого проверяется идентичность. Стандарт 802.] 1 регламентирует две ее формы: открытая система аутентификации и аутентификация с совместно используемым ключом. Открытая система аутентификации является обязательной и проводится в два этапа. Радиоплата интерфейса сети инициирует процесс аутентификации, посылая точке доступа фрейм запроса на аутентификацию. Точка доступа отвечает фреймом ответа на запрос об аутентификации, содержащий разрешение или отказ в аутентификации, что указывается в поле кода состояния (status code) тела фрейма.

Аутентификация с совместно используемым ключом является опциональной и осуществляется в четыре этапа. Процесс основан на определении того, имеет ли аутентифицируемое устройство правильный WEP-ключ.' Радиоплата интерфейса сети начинает его, посылая точке доступа фрейм запроса на аутентификацию. Точка доступа, поместив текст вызова (challenge text) в тело фрейма ответа, посылает его радиоплате интерфейса сети. Радиоплата интерфейса сети использует свой WEP-ключ для шифрования текста вызова и посылает его назад точке доступа в другом фрейме аутентификации. Точка доступа дешифрует текст вызова и сравнивает его с первоначальным. Если оба текста эквивалентны, точка доступа предполагает, что радиоплата интерфейса сети имеет корректный ключ. Точка доступа завершает последовательность обменов путем отправки радиоплате интерфейса сети фрейма аутентификации с разрешением или отказом. Многие хакеры знают, как можно преодолеть барьер, создаваемый посредством аутентификаций с совместно используемым ключом, поэтому полагаться на такую систему защиты, если нужно обеспечить высокий уровень безопасности, не стоит.

' *WKP (wired equivalent privacy) — защищенность, эквивалентная таковой проводных сетей.* — Прим. ред.

Привязка

После завершения процесса аутентификации радиоплата интерфейса сети должна привязаться к точке доступа, только после этого она сможет посылать фреймы данных. *Привязка* ***(association)*** необходима для обмена важной информацией между радиоплатой интерфейса сети и точкой доступа, например, о поддерживаемых скоростях передачи данных. Радиоплата интерфейса сети инициирует процесс привязки путем отправки фрейма с запросом на привязку, содержащим такие данные, как SSID и поддерживаемая скорость передачи данных. Точка доступа отвечает, отправляя фрейм ответа на запрос о привязке, содержащий идентификатор ассоциации и другую информацию по точке доступа. После того как радиоплата интерфейса сети и точка доступа завершат процесс привязки, они могут передавать одна другой фреймы данных.

WEP

Если опциональный режим WEP доступен, плата интерфейса беспроводной сети, прежде чем передать какой-либо фрейм, шифрует его тело (но не заголовок) с использованием общего ключа. Приемная станция, получив фрейм, дешифрует его с помощью общего ключа. Стандарт 802.11 не регламентирует метод распределения ключа, что делает беспроводные локальные сети стандарта 802.11 уязвимыми для подслушивания. Однако версия 802. Hi этого стандарта повышает степень защищенности за счет введения в стандарт механизмов 802.11x и более надежного шифрования.

RTS/CTS

Опциональные механизмы определения готовности к передаче (request to send) и готовности к приему (clear to send) позволяют точке доступа контролировать процесс использования среды передачи станциями, у которых активизирована функция RTS/CTS. При использовании большинства радиоплат интерфейса сети пользователи могут устанавливать максимальный объем фрейма, при превышении которого радиоплата интерфейса сети активизирует режим RTS/CTS. Например, при задании объема фрейма, равного 1000 бит, режим RTS/CTS будет использован для всех фреймов объемом свыше 1000 бит. За счет использования режима RTS/CTS смягчаются проблемы скрытого узла (когда две или более радиоплаты интерфейса сети не могут слышать одна другую, хотя и привязаны к одной точке доступа).

Если радиоплата интерфейса сети активизировала режим RTS/CTS, она, прежде чем посылать фрейм данных, отправляет точке доступа фрейм RTS. Точка доступа отвечает на него фреймом CTS, указывая тем самым, что радиоплата интерфейса сети может послать фрейм данных. Одновременно с отправкой фрейма CTS точка доступа предлагает значение поля продолжительности заголовка фрейма, которое удерживает другие станции от передачи, чтобы станция, передавшая фрейм RTS, могла передать и свой фрейм данных. Это позволяет избежать коллизий, вызванных проблемой скрытого узла. Обмен фреймами RTS/CTS сопровождает передачу каждого фрейма данных, объем которого превышает порог, установленный на соответствующей радиоплате интерфейса сети.

Режим энергосбережения

Режим энергосбережения является опциональным. При переходе в этот режим пользователь получает возможность отключать радиоплату интерфейса сети, если ему не нужно передавать данные, с целью экономии энергоресурса батареи питания. При переходе в режим энергосбережения радиоплата интерфейса сети сообщает

точке доступа о своем желании перейти в "спящий" режим через бит состояния, располагаемый в заголовке каждого фрейма. Точка доступа учитывает, что та или иная радиоплата интерфейса сети желает перейти в режим энергосбережения, и буферизирует пакеты, предназначенные для "спящей" станции.

Чтобы все же сохранить возможность получения предназначенных для нее пакетов данных, "спящая" плата интерфейса сети должна периодически "просыпаться" (в определенные моменты времени) и принимать регулярно посылаемый точкой доступа маячковый сигнал. В этих маячковых сигналах содержится информация о том, имеет ли точка доступа предназначенные для спящей станции буферизированные фреймы, ожидающие доставки. Радиоплата интерфейса сети, по адресу которой поступили фреймы, должна запросить их у точки доступа. После получения фреймов радиоплата интерфейса сети может вернуться в "спящий" режим.

Фрагментация

Опциональная функция фрагментации позволяет станциям стандарта 802.11 делить пакеты данных на более мелкие фреймы. Это делается во избежание необходимости повторной передачи больших фреймов при наличии радиопомех. Ошибки в передаче отдельных разрядов, возникающие из-за радиопомех, скорее всего повлияют на один фрейм. Непроизводительные расходы, вызванные повторной передачей одного фрейма, окажутся значительно меньшими, чем при повторной передаче большого пакета данных. Как и в случае использования механизма RTS/CTS, пользователи могут устанавливать максимальный объем фрейма, при превышении которого станция активизирует механизм фрагментации'. Если объем фрейма оказывается больше заданного, радиоплата интерфейса сети разбивает пакет на несколько фреймов, при этом объем каждого будет меньше порогового.

Физические уровни стандарта 802.11

Несколько физических уровней стандарта 802.11 удовлетворяют различным требованиям, предъявляемым к сети разными приложениями. Ниже кратко описан каждый из физических уровней стандарта 802.11

Изначальный 802.11

Первоначальный стандарт 802.11, ратифицированный в 1997г., включает физические уровни, на которых выполняется *расширение спектра путем скачкообразного переключения частоты* ***(Frequency Hopping Spread Spectrum, FHSS)*** и *высокоскоростная передача с расширением спектра методом прямой последовательности* ***(high-rate direct sequence spread spectrum, HR-DSSS).*** Скорость передачи данных достигает 2 Мбит/с, связь осуществляется в диапазоне 2,4 ГГц' При использовании технологии FHSS широкополосные сигналы занимают весь диапазон 2,4 ГГц, отведенный для таких целей. Можно настроить точки доступа, работающие в режиме FHSS, на 15 различных схем переключения частоты, чтобы они не создавали взаимных помех. Благодаря этому до 15 точек доступа могут эффективно работать в режиме FHSS водной и той же зоне. Поскольку текущая версия стандарта 802.11 с режимом FHSS обеспечивает максимальную скорость передачи данных лишь 2 Мбит/с, немногие компании предлагают решения на основе FHSS для беспроводных локальных сетей, предназначенных для развертывания внутри помещений. Сейчас доступны более быстродействующие сети на основе стандартов 802.11a, 802.11Ь и 802.1 lg. Кроме того, механизм FHSS не спосо-

бен взаимодействовать с другими физическими уровнями стандарта 802.11. Однако сети на основе FHSS представляют собой хорошее решение для систем типа "точка-несколько точек", предназначенных для развертывания вне помещений. Это обусловлено тем, что технология FHSS более устойчива к воздействию радиопомех, уровень которых вне помещений может оказаться весьма высоким.

Системы DSSS стандарта 802.11 также обеспечивают скорость передачи всего лишь 2 Мбит/с, но зато совместимы с новейшим физическим уровнем,802.lib. Поэтому пользователь, в ноутбуке которого установлена радиоплата интерфейса сети стандарта 802.11 DSSS, может взаимодействовать с точками доступа стандарта 802.lib. Однако такая ситуация маловероятна, поскольку радиоплаты интерфейса сети стандарта 802.11 DSSS уже не продаются.

802.11a

В конце 1999 г. IEEE выпустила стандарт 802.11 а, регламентирующий передачу данных в диапазоне 5 ГГц с использованием технологии мультиплексирования с разделением по ортогональным частотам (orthogonal frequency division multiplexing, OFDM), при этом обеспечивается скорость передачи данных до 54 Мбит/с. Однако продукты, реализующие эту технологию, не были доступны до 2000 г., в основном из-за трудностей, возникающих при разработке электронных схем, работающих в этом диапазоне.

Устройства стандарта 802. На работают в диапазоне 5 ГГц, обеспечивая скорость передачи данных до 54 Мбит/с при радиусе действия до 90 м, который зависит от действительной скорости передачи данных. Точки доступа и радиоплаты интерфейса сети стандарта 802.На появились на рынке в конце 2001-го, поэтому доля установленного оборудования, соответствующего этому стандарту, пока незначительна по сравнению с количеством сетей стандарта 802.11Ь. Рекомендуется тщательно изучить проблемы совместимости, которые могут возникнуть при развертывании сети стандарта 802.11 а.

Важным преимуществом стандарта 802.На является то, что он предлагает повышенную пропускную способность благодаря использованию 12-ти отдельных, неперекрывающихся каналов. Это хороший выбор при необходимости поддержки многих, сконцентрированных в небольшой зоне пользователей и высокопроизводительных приложений, таких как потоковое видео. Помимо более высоких характеристик, чем у систем стандарта 802.11Ь, сети стандарта 802.11а имеют и более высокую пропускную способность, чем сети 802.1 lg.

Другим преимуществом стандарта 802. Па является то, что диапазон 5 ГГц используется еще недостаточно широко, что позволяет пользователям достигать высокой производительности. Большинство создающих помехи устройств, таких как микроволновые печи и беспроводные телефоны, работают в диапазоне 2,4 ГГц. Поскольку потенциал радиопомех в диапазоне 5 ГГц ниже, развертывание беспроводной локальной сети оказывается менее рискованным.

Потенциальная проблема сетей стандарта 802.11 а— их ограниченный радиус действия, что обусловлено главным образом их работой в диапазоне более высоких частот (5 ГГц). При работе на скоростях до 54 Мбит/с радиус действия в большинстве случаев ограничен величиной 90 м. Для того чтобы обеспечить работу сети в пределах заданной зоны, приходится устанавливать больше точек доступа, чем при использовании устройств стандарта 802.11Ь.

Однако, если сравнить работу сетей стандартов802.lib и 802.Па, то окажется, что пользователь сети 802.11а имеет возможность передавать данные с более высокой скоро-

стью нате же расстояния, что и пользователь сети стандарта 802.11Ь, прежде чем он потеряет возможность установления соединения. Но при этом пользователь сети стандарта 802.11Ь может продолжать работу при низкой скорости передачи данных — 1 или 2 Мбит/с — при больших расстояниях, чем характерные для сетей стандарта 802.11а.

Несомненную сложность представляет то, что стандарты 802. Па и 802.11b/g несовместимы. Так, пользователь, компьютерное устройство которого оборудовано радиоплатой стандарта802.lib, не может привязаться к точке доступа, соответствующей стандарту 802.11 а, и наоборот. Производители решают эту проблему, предлагая многорежимные радиоплаты, поддерживающие оба стандарта — 802. Паи 802.11Ь.

Модулятор стандарта 802. На преобразует двоичный сигнал в аналоговую форму, используя различные методы модуляции в зависимости от того, какая скорость передачи данных была выбрана. Например, при работе со скоростью 6 Мбит/с подуровень среды передачи (physical layer medium dependent, PMD) использует двоичную относительную фазовую манипуляцию (differential binary phase shift keying, DBPSK), при которой осуществляются сдвиги фазы центральной частоты передачи, отображающие различные комбинации двоичных разрядов. При более высоких скоростях передачи (54 Мбит/с), используется квадратурная амплитудная модуляция (quadrature amplitude modulation, QAM). В этом случае биты данных представляются путем изменения центральной частоты передачи, а также изменения амплитуды сигналов в дополнение к сдвигам фазы.

802.11Ь

Наряду со стандартами 802. И а IEEE ратифицировал стандарт 802.11Ь, представляющий собой расширение изначального стандарта 802.11, основанного на расширении спектра методом прямой последовательности в диапазоне 2,4 ГГц. Скорость передачи при этом достигает 11 Мбит/с. Точки доступа и радиоплаты интерфейса сети стандарта 802.11Ь начали появляться на рынке с 1999 г., поэтому значительное количество установленных к настоящему времени сетей соответствуют стандарту 802.11Ь.

Важным преимуществом стандарта 802.11Ь является то, что соответствующие ему устройства обеспечивают относительно большой радиус действия. Можно рассчитывать, что в большинстве случаев применения внутри помещений дальность связи превысит 270 м. Повышенный радиус действия поззоляет устанавливать существенно меньшее количество точек доступа при развертывании беспроводной локальной сети в том же здании, где могла бы быть установлена сеть стандарта 802.11а.

Недостаток стандарта 802. 1ib в том, что можно выбрать только три неперекрывающихся канала в диапазоне 2,4 ГГц. Стандарт 802.11 определяет 14 каналов (в США разрешены к применению только каналы с 1-го по 11-й), на работу в которых могут быть сконфигурированы точки доступа, но каждый из каналов передачи занимает примерно треть от всего диапазона 2,4 ГГц. Многие компании используют только неперекрывающиеся каналы 1, 6 и И, чтобы точки доступа не создавали взаимные помехи. Это ограничивает общую пропускную способность сетей стандарта802.lib, поэтому они хорошо подходят лишь для выполнения приложений среднего уровня производительности, таких как электронная почта и просмотр Web-страниц.

Другим недостатком сетей стандарта 802.11Ь является их потенциальная подверженность помехам со стороны других радиоустройств. Например, беспроводной телефон, работающий в диапазоне 2,4 ГГц, может создавать серьезные помехи для беспроводной локальной сети стандарта802.lib, из-за чего пользователи ощущают

ухудшение ее характеристик. Микроволновые печи и другие устройства, работающие в диапазоне 2,4 ГГц, также могут создавать помехи.

Устройства стандарта 802.11Ь используют технологию DSSS для рассеяния сигнала фрейм данных по подканалам диапазона 2,4 ГГц, ширина каждого из которых составляет 22 МГц. Это приводит к повышению помехоустойчивости связи по сравнению с тем, когда передача сигнала осуществляется в узкой полосе частот. Поэтому FCC позволяет не приобретать лицензию на использование устройств, работающих с расширением спектра.

Модулятор стандарта802.1ib преобразует расширенный двоичный сигнал в аналоговую форму, используя различные методы модуляции в зависимости от того, с какой скоростью осуществляется передача данных. Например, при работе со скоростью 1 Мбит/с на уровне PMD используется двоичная относительная фазовая манипуляция (differential binary phase shift keying, DBPSK). В действительности этот метод не так сложен, как его название. Модулятор просто сдвигает фазу центральной частоты передачи, чтобы в потоке данных можно было отличить двоичную 1 от двоичного 0.

Для передачи со скоростью 2 Мбит/с PMD использует относительную квадратурную фазовую манипуляцию (differential quadrature phase shift keying, DQPSK), которая аналогична DBPSK, за исключением того, что используются четыре возможных сдвига фазы для представления каждых двух битов данных. Благодаря этому хитроумному процессу можно передавать поток данных со скоростью 2 Мбит/с при использовании той же полосы пропускания, которая необходима для передачи со скоростью 1 Мбит/с в случае применения других методов модуляции. Похожие методы используются и при передаче данных с более высокими скоростями — 5,5 и 11 Мбит/с.

802.11 д

ШЕЕ ратифицировал стандарт 802.1 Ig в 2003 г. Он совместим со стандартом 802.11Ь и регламентирует повышенную скорость передачи (54 Мбит/с в диапазоне 2,4 ГГц). При этом используется мультиплексирование с разделением по ортогональным частотам (orthogonal frequency division multiplexing, OFDM).

Сильной стороной стандарта 802.1lg является то, что он обратно совместим со стандартом802.1ib. Компании, уже развернувшие сети стандарта802.11Ь, в общем случае могут модернизировать точки доступа, чтобы обеспечить их совместимость с устройствами стандарта802.llg, просто за счет модернизации программно-аппаратных средств. Это эффективный способ перевода сети компании на новый уровень. Но существующие клиентские устройства стандарта 802.11Ь при работе в сети стандарта 802.1lg требуют введения механизмов защиты, которые ограничивают характеристики беспроводной локальной сети в целом. Это обусловлено тем, что устройства стандарта 802.11Ь из-за различия в используемых методах модуляции не могут определить, когда устройства стандарта 802.1 Ig осуществляют передачу. Поэтому оба типа устройств должны объявлять о своем намерении использовать среду передачи, используя понятный для обоих тип модуляции.

Недостатки стандарта 802.1ib, такие как подверженность потенциальным радиопомехам и наличие только трех неперекрывающихся каналов, присущи и сетям стандарта 802.1 Ig, поскольку они работают в том же диапазоне 2,4 ГГц. Поэтому сети стандарта802.1lg имеют ограниченную пропускную способность по сравнению с сетями стандарта 802.Па.

2,4 или 5 ГГц?

При развертывании беспроводных локальных сетей компании должны решить, какие использовать точки доступа и платы интерфейса сети — рассчитанные на работу в диапазоне 2,4 ГГц, 5 ГГц или в обоих диапазонах. Не так давно проблема выбора частотного диапазона не возникала, поскольку были доступны изделия только стандарта 802.lib, работавшие в диапазоне 2,4 ГГц. Теперь появились как изделия стандартов 802.11g и 802.1ib, работающие в диапазоне 2,4 ГГц, так и продукты стандарта 802.11a, рассчитанные на работу в диапазоне 5 ГГц. Это может вызвать некоторое замешательство при решении вопроса о развертывании беспроводной локальной сети. Какие же факторы нужно учитывать при принятии столь важного решения?

При рассмотрении всех "за" и "против" систем, работающих в диапазонах 2,4 и 5 ГГц, вначале следует четко сформулировать предъявляемые к сети требования. Это даст солидную основу для правильного выбора ее компонентов. Без учета конкретных требований выбор может оказаться неверным.

Требования, которые нужно учитывать при выборе между диапазонами 2,4 и 5 ГГц, перечислены ниже.

- **Географическое расположение.** Беспроводную локальную сеть диапазона 2,4 ГГц можно беспрепятственно развернуть почти в любой стране мира, однако на использование сетей диапазона 5 ГГц могут накладываться ограничения. Например, в США разрешено их использование, в других станах может быть запрещено. Возможно, придется использовать сеть диапазона 2,4 ГГц независимо от того, какие требования вы к ней предъявляете.
- **Характеристики.** Ширина предоставляемого для целей связи частотного спектра в диапазоне 5 ГГц намного больше. Каждый из 12-ти неперекрывающихся каналов этого диапазона занимает полосу частот шириной 20 МГц. Это позволяет добиться существенно более высоких рабочих характеристик, чем при использовании диапазона 2,4 ГГц. Весь диапазон 2,4 ГГц имеет ширину лишь 80 МГц, что позволяет разместить в нем лишь три неперекрывающихся канала. Если необходимы высокие характеристики сети, имеет смысл использовать диапазон 5 ГГц.
- **Размер помещения.** По мере роста частоты радиус действия обычно уменьшается. Поэтому системы диапазона 5 ГГц, как правило, имеют меньший радиус действия, чем таковые диапазона 2,4 ГГц. При развертывании беспроводной локальной сети диапазона 5 ГГц потребуется установить больше точек доступа, что приведет к повышению стоимости системы. Следовательно, можно сэкономить на установке беспроводной локальной сети в больших помещениях, выбрав систему диапазона 5 ГГц, при условии, что высокая производительность не является основным требованием, предъявляемым к сети. Однако следует иметь в виду, что в некоторых ситуациях радиус действия систем диапазона 5 ГГц может оказаться сравнимым или даже более высоким, чем у систем диапазона 2,4 ГГц.
- **Радиочастотные помехи.** Беспроводные локальные сети, работающие в диапазоне 2,4 ГГц, могут подвергаться воздействию помех со стороны беспроводных телефонов, микроволновых устройств и других беспроводных локальных сетей. Сигналы помех снижают производительность сети стандарта802.lib, периодически блокируют доступ пользователей и точек доступа к совместно

используемой среде передачи. Если невозможно снизить уровень помех до приемлемого уровня, следует развертывать систему диапазона 5 ГГц, который относительно свободен от источников помех. Сейчас на рынке предлагаются несколько моделей телефонов, работающих в диапазоне 5 ГГц, но помех с их стороны вполне можно избежать, поскольку стандарт 802.11a предусматривает использованиемногихнеперекрывающихсяканалов.

- **Возможность взаимодействия сетей.** Системы диапазонов 2,4 и 5 ГГц напрямую несовместимы, и пока немногие пользователи и точки доступа работают в диапазоне 5 ГГц. Следовательно, имеет смысл развернуть сеть диапазона 2,4 ГГц, если нет возможности контролировать, какие именно платы интерфейса сети пользователи применяют в своих PDA и ноутбуках. Это положение особенно актуально для университетов и беспроводных локальных сетей, развертываемых в "горячих точках" и общедоступных местах. Характер выполняемых приложений также может склонить чашу весов в пользу диапазона 2,4 ГГц, поскольку большинство пользователей имеют компьютерные устройства, оборудованные более распространенными платами стандарта 802.11Ь. Однако поставщики уже предлагают двухдиапазонные радиоплаты интерфейса сети и точки доступа, благодаря чему снижаются проблемы взаимодействия сетей. Те пользователи, компьютерное устройства которых оборудованы двухдиапазонными радиоплатами, могут привязываться как к точке доступа диапазона 2,4 ГГц (стандарты 802.1 lb/g), так и к точке доступа диапазона 5 ГГц (стандарт 802.11a). Поскольку все больше пользователей оборудуют свои устройства двухдиапазонными радиоплатами, проблема обеспечения взаимодействия сетей постепенно потеряет свою актуальность.
- **Безопасность.** Безопасность беспроводных локальных сетей — объект пристального внимания многих компаний. Если минимизировать распространение радиоволн за пределы контролируемой зоны внутри здания, беспроводная сеть становится более защищенной, поскольку снижается вероятность подслушивания и атак хакеров, направленных на отказ в обслуживании (DoS). Следовательно, системы диапазона 5 ГГц могут обеспечить больший уровень безопасности, чем системы диапазона 5 ГГц, за счет меньшего радиуса действия.

Из вышеизложенного следует, что в большинстве случаев для выполнения стандартных офисных приложений больше подходит диапазон 2,4 ГГц. Изделия этого диапазона недороги и способны обеспечивать выполнение большинства наиболее распространенных приложений. Однако в некоторых ситуациях выгоднее перейти на диапазон 5 ГГц, например, если вокруг много источников радиопомех и необходимо выполнять мультимедийные приложения.

Wi-Fi

Альянс Wi-Fi (Wi-Fi Alliance), который начал свою работу под именем "Ассоциация контроля совместимости с беспроводным Ethernet" или просто "ассоциация WECA" (wireless ethernet compatibility alliance, WECA), является международной некоммерческой организацией, занимающейся маркетингом и проблемами взаимодействия компонентов беспроводных локальных сетей стандарта 802.11. Альянс Wi-Fi — это группа, раскручи-

вающая бренд "Wi-Fi", под который подпадают все разновидности беспроводных сетей, соответствующие стандарту 802.11 (802.11a, 802.11Ь и 802.1 lg), а также все стандарты такого типа, которые появятся в будущем. Альянс Wi-Fi также продвигает технологию *защищенного доступа к Wi-Fi* ***(Wi-Fi Protected Access, WPA),*** связующее звено между многократно раскритикованным механизмом WEP и стандартом защиты 802.111.

Альянс Wi-Fi преследует следующие цели:

- обеспечивать по всему миру сертификацию, побуждающую производителей придерживаться стандартов 802.11 при разработке компонентов беспроводных локальных сетей;
- способствовать сбыту сертифицированных Wi-Fi изделий для применения их в домашних условиях, небольших офисах и на предприятиях;
- Ш тестировать и сертифицировать изделия Wi-Fi с целью обеспечения взаимодействия сетей.

Что означает Wi-Fi?

Сертификация Wi-Fi — это процесс, благодаря которому обеспечивается возможность взаимодействия компонентов беспроводных локальных сетей, таких как точки доступа и радиоплаты, выполненные в различных форм-факторах. Для получения сертификата на свои изделия компания должна стать членом Альянса Wi-Fi.

Альянс руководствуется утвержденными программами тестирования для сертификации изделий на предмет обеспечения взаимодействия с другими сертифицированными Wi-Fi-компонентами. После того как изделие успешно протестировано, его производитель получает право использовать логотип "Сертифицировано Wi-Fi" для каждого отдельного изделия, а также на его упаковке и инструкции по применению.

Сертификация Wi-Fi дает клиентам уверенность в том. что они приобрели компоненты беспроводной локальной сети, соответствующие требованиям обеспечения взаимодействия с изделиями многих других производителей. Логотип "Wi-Fi" на изделии означает, что оно соответствует требованиям тестирования на совместимость и наверняка сможет совместно работать с Wi-Fi-сертифицированными изделиями других поставщиков.

Защищенный доступ к Wi-Fi

Механизм WEP не обеспечивает достаточного уровня безопасности для большинства приложений, выполняемых в беспроводных локальных сетях предприятий. Поскольку в нем используется статический ключ, WEP легко взломать, используя уже имеющиеся программные средства. Это побуждает менеджеров информационных технологий использовать более динамичные формы WEP.

Однако эти улучшенные механизмы защиты являются патентованными, что затрудняет обеспечение их поддержки клиентскими устройствами от других поставщиков. Поэтому Альянс Wi-Fi предпринял значительные усилия для эффективной стандартизованной защиты беспроводных локальных сетей, определив механизм WPA как обеспечивающий взаимодействие сетей. При использовании WPA сетевая среда, образуемая радиоплатами интерфейса сети разных типов стандарта 802.11, может пользоваться преимуществами расширенных форм шифрования.

WPA 1.0 является вариантом изначальной, нератифицированной версии стандарта 802ЛИ, который включает механизмы временного протокола целостности ключа (temporal key integrity protocol, TKIP) и 802. Их. Комбинация этих двух механизмов позволяет обеспечивать шифрование с изменяющимся ключом и взаимную аутентификацию, которая бывает иногда совершенно необходима для беспроводных локальных сетей.

Для аутентификации WPA 1.0 использует комбинацию открытой аутентификации и аутентификации в соответствии с механизмом 802. Их. Вначале беспроводной клиент аутентифицируется точками доступа, которые разрешают клиенту посылать фреймы точке доступа. Затем WPA выполняет аутентификацию на уровне пользователя с помощью механизма 802. Их. Выполняя эту процедуру, WPA 1.0 взаимодействует с сервером аутентификации предприятия. Если никакой сервер аутентификации недоступен, как это бывает в домашних сетях и сетях небольших офисов, то WPA 1.0 может работать в так называемом режиме предварительного совместно используемого ключа (pre-shared key mode).

Стандарт 802,Hi обратно совместим с WPA1.0, однако 802.Hi включает также опционально используемый усовершенствованный стандарт шифрования (advanced encryption standard, AES). Для применения AES необходимы сопроцессоры, которыми большинство точек доступа на сегодняшний день не оборудованы, поэтому AES больше подходит для вновь развертываемых сетей. Новый стандарт WPA 2.0 использует AES.

HiperLAN/2

Стандарт HiperLAN/2, за которым стоит стандарт на высокопроизводительную локальную радиосеть (high performance radio LAN), представляет собой стандарт на беспроводную локальную сеть, разработанный Подразделением широкополосного доступа к сетям по радиоканалу (broadband radio access networks (BRAN) division) Европейского института стандартизации электросвязи (European Telecommunications Standards Institute, ETSI). Этот стандарт регламентирует применение эффективной, высокоскоростной технологии беспроводных локальных сетей, которая удовлетворяет всем требованиям принятых в Европе регулятивных правил распределения спектра.

Стандарт HiperLAN/2 использует физический уровень, похожий на таковой стандарта IEEE 802. Па, на котором передача осуществляется со скоростью 54 Мбит/с в диапазоне 5 ГГц при посредстве мультиплексирования с ортогональным частотным разделением сигналов (orthogonal frequency division multiplexing, OFDM). Основное отличие HiperLAN/2 заключается в использовании протокола, ориентированного на соединение, и временного мультиплексирования (time-division multiplexing, TDM) в качестве основы для обеспечения возможности обмена данными между пользователями. Этот метод передачи эффективен для мультимедийных приложений, в том числе передачи речи и видео.

Преимущества HiperLAN/2

Однако сходство между HiperLAN/2 и 802.11a заканчивается на уровне MAC[2]. В то время как стандарт 802. Па использует для передачи пакетов технологию CSMA/CA, HiperLAN/2 применяет МДВР — множественный доступ с временным разделением

[2] *MAC (media access control) — подуровень канального уровня, задающий методы доступа к среде, формат кадров, способ адресации.* — Прим. ред.

каналов (time division multiple access, TDMA). Проблема, связанная с использованием CSMA/CA, состоит в том, что станции вынуждены находиться в режиме ожидания неопределенно долгие промежутки времени, это называется *асинхронный доступ*. При работе в таком режиме не существует каких-либо регулярных временных отношений, касающихся доступа к среде передачи. Поэтому нет гарантированной возможности для конкретной станции передать пакет в течение определенного времени. Из-за отсутствия регулярного доступа к среде снижается эффективность такой системы, что отрицательно сказывается на передаче речи и видеоинформации.

Напротив, в HiperLAN/2 за счет использования технологии TDMA доступ к сети осуществляется на регулярной основе. Системы TDMA динамически назначают каждой станции временной интервал (time slot), учитывая необходимость для станции передать данные. Поэтому станции осуществляют передачу через регулярные промежутки времени в течение выделенных для них временных интервалов, благодаря чему среда используется эффективнее и улучшается поддержка речевых и видеоприложений.

Системы HiperLAN/2 имеют ряд привлекательных особенностей по сравнению с системами стандарта 802.11. Первая и, наверное, наиболее важная состоит в повышенной скорости передачи. И системы стандарта 802.11, и HiperLAN/2 отличаются максимальной скоростью передачи, оцениваемой величиной 54 Мбит/с, но она не соответствует реальной скорости передачи информации между станцией и точкой доступа.

Истинная максимальная пропускная способность HiperLAN/2 составляет 42 Мбит/с, а максимально возможная пропускная способность систем стандарта 802. На примерно лишь 18 Мбит/с. Технология HiperLAN/2 значительно опережает системы 802.11a, если говорить о производительности каждой точки доступа.

Уникальная особенность технологии HiperLAN/2 — это возможность взаимодействия с другими высокоскоростными сетями, включая сотовые третьего поколения (3G), системы с асинхронным режимом передачи (asynchronous transfer mode, ATM) и другими сетями, основанными на использовании протокола Internet. Это может оказаться серьезным преимуществом, когда речь зайдет об интеграции беспроводных локальных сетей с сотовыми системами связи и глобальными сетями (WAN).

Угрожает ли HiperLAN/2 системам стандарта 802.11?

Вопреки смелым предсказаниям относительно массового производства и применения изделий HiperLAN/2, появившимся во второй половине 2002 года, очень немногие продукты такого рода (если они вообще есть) доступны для потребителей. И действительно, в результате тщательного поиска в Internet не была найдена информация о каких-либо продуктах HiperLAN/2, предлагаемых потребителям. По-видимому, HiperLAN/2 не продвигается на рынок с ощутимой скоростью.

Во многом это связано с жесткими регулятивными правилами, и многие приверженцы технологии HiperLAN/2 отказываются от ее продвижения. Кроме того, рабочая группа 802.1 lh занимается пересмотром стандарта 802.11, чтобы сделать его более применимым в Европе, где только и могла бы, наверное, доминировать технология HiperLAN/2.

По существу 802.1lh— это стандарт 802.Па с двумя дополнительными (для Европы) особенностями. Первой из них является механизм контроля мощности передачи (transmit power control, TPC), благодаря которому становится возможным автоматический контроль мощности передачи с целью снижения взаимных помех, возникающих при работе вблизи других систем. Вторая особенность — это динамиче-

ский выбор частоты (dynamic frequency selection, DFS), за счет чего станция прослушивает канал, прежде чем занять его. Это еще один механизм уклонения от помех, наличия которого ETSI требует для сетей, устанавливаемых в Европе.

Сейчас стандарт 802.11 определенно лидирует на мировом рынке и является наилучшим выбором для развертывания беспроводной локальной сети. Это делает системы 802.11 единственной альтернативой для развертывания сегодня беспроводных локальных сетей. С учетом отсутствия продуктов HiperLAN/2 возникают сомнения, что этот стандарт сможет стать доминирующим на рынке беспроводных локальных сетей.

Резюме

К числу компонентов беспроводных локальных сетей относятся радиоплаты интерфейса сети, точки доступа, маршрутизаторы, повторители и антенны, с помощью которых становится возможным выполнение беспроводных приложений в зданиях и на территориях кампусов. Эти компоненты являются строительными блоками, позволяющими создавать беспроводные локальные сети в жилых домах, небольших офисах, на предприятиях и в общедоступных местах. Размеры этих сетей могут существенно разниться — от одной точки доступа в квартире или небольшом офисе до сотен точек доступа в больших зданиях. Беспроводная локальная сеть может включать также только двух пользователей, напрямую связывающихся между собой в режиме неплановой сети.

Стандарт 802.11 относится к наиболее распространенным во всем мире, он регламентирует передачу данных со скоростью до 54 Мбит/с в диапазоне 2,4 или 5 ГГц. Wi-Fi дает гарантию совместимости компонентов беспроводных локальных сетей, предлагаемых разными производителями. HiperLAN/2 — это европейский стандарт, который вряд ли составит конкуренцию стандарту 802.11.

Вопросы для самопроверки

Ответы на эти вопросы вы можете найти в приложении А.

1. Какой компонент беспроводной локальной сети чаще других используется в домашних условиях и небольших офисах?
2. В чем разница между точкой доступа и маршрутизатором беспроводной локальной сети?
3. Когда имеет смысл применять повторитель в беспроводной локальной сети?
4. Как радиоплата беспроводной локальной сети определяет, к какой точке доступа нужно привязываться?
5. Является ли WEP обязательным механизмом шифрования?
6. В каком частотном диапазоне работают устройства стандарта 802.11а?
7. Сколько неперекрывающихся каналов доступны в беспроводных локальных сетях стандарта 802.11Ь?
8. Верно ли, что устройства стандарта 802.1 lg работают со скоростью до 54 Мбит/с и совместимы с сетями 802.11Ь?
9. Какие частоты стандарта 802.11 доступны почти во всем мире?
10. Что обеспечивает Wi-Fi?

В этой главе...

специфические приложения беспроводных региональных сетей;

технологии и компоненты беспроводных региональных сетей;

реализация систем беспроводных региональных сетей различных типов.

ГЛАВА 6

Беспроводные региональные сети: для соединений между зданиями и отдаленными площадками

Беспроводные региональные сети удовлетворяют потребность в соединениях в масштабах мегаполиса, например в городах, сельской местности. Обычно эти сети обеспечивают стационарные соединения для стационарных пользователей.

Сети характеризуются быстрой окупаемостью инвестиций, поскольку компании могут обойтись без лизинга или прокладки дорогих медных либо оптических кабелей. На практике иногда бывает и вовсе невозможно проложить проводную сеть между двумя точками, когда действуют, скажем, ограничения на землеустроительные работы. В таких случаях компания может использовать компоненты беспроводной региональной сети для передачи данных между головным офисом и расположенной неподалеку оптовой базой.

Ощутима и экономия средств за счет использования беспроводной региональной сети, которая окупает себя уже в течение года или двух лет. Это определенно стимулирует компании создавать коммуникации между зданиями, разбросанными по городу.

В данной главе рассмотрены примеры компонентов беспроводных региональных сетей, показано, как они должны соединяться между собой при формировании систем, а также описаны различные стандарты.

Компоненты беспроводных региональных сетей

Компоненты беспроводных региональных сетей обычно поставляются парами, поскольку они должны обеспечивать фиксированное беспроводное соединение между двумя точками. Рассмотрим основные компоненты беспроводных региональных сетей.

Мосты

Мост ***(bridge)*** — это устройство, обеспечивающее соединение двух сетей, в которых используются одинаковые или различные протоколы уровня управления передачей данных (или канального уровня, это второй уровень Эталонной модели взаимодействия открытых систем OSI). Эта концепция представлена на рис. 6.1.

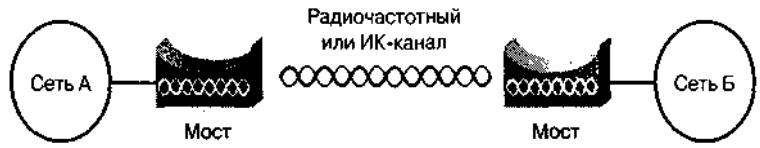

Рис. 6.1. Мосты служат для соединения двух сетей

Беспроводные мосты обычно располагаются на каждом конце канала "точка-точка", например, при обеспечении соединения между двумя зданиями. Мост имеет проводной порт, соединенный с сетью, и беспроводной порт, который взаимодействует с приемопередатчиком. Мост получает пакеты с одного порта и передает их на другой. Мост не начинает ретрансляцию до тех пор, пока не получит весь пакет. Благодаря этому станции по обеим сторонам моста могут передавать пакеты одновременно, не опасаясь возникновения коллизий.

Некоторые мосты передают каждый полученный пакет противоположному порту независимо от того, предназначен ли он станции, расположенной в другой сети. Самообучающийся мост (а такие мосты используются чаще) проверяет адрес назначения каждого пакета с целью выяснения, должен ли он передать пакет в другую сеть, руководствуясь при этом таблицей решений, которую сам же постепенно и создает. Это повышает эффективность, поскольку мост не станет передавать пакет в другую сеть, если выяснится, что получатель пакета находится с той же стороны моста, что и отправитель. Самообучающиеся мосты также проверяют записи в таблицах адресов, удаляя те из них, которые не используются в течение указанного периода времени,

Мосты сети "прозрачны" для пользователя. Пакеты пересылаются через мост автоматически. Пользователь не замечает, что его пакеты проходят по каналу, соединяющему два разных места.

Мосты или точки доступа?

Точки.доступа беспроводным способом соединяют между собой многих пользователей и обеспечивают их работу в проводной сети. Так, несколько пользователей, компьютерные устройства которых оборудованы платами интерфейса сети стандарта 802.11, могут привязаться к одной точке доступа, включенной в сеть Ethernet. Каждый из них будет иметь доступ к сети Ethernet и другим пользователям. Точка доступа в этом случае похожа на мост, но она позволяет взаимодействовать с сетью многим пользователям. Мост же обеспечивает взаимодействие только двух сетей.

Беспроводной мост можно использовать внутри помещения. Например, мост беспроводной локальной сети может обеспечить взаимодействие сети Ethernet напрямую с конкретной точкой доступа. Это может оказаться необходимым в случае, если несколько устройств, расположенных в труднодоступной части здания, взаимодействуют между собой через Ethernet. Мост беспроводной локальной сети включается в эту сеть Ethernet и использует протокол 802.11 для связи с точкой доступа, находящейся в пределах досягаемости. Таким образом, мост обеспечивает беспроводное соединение для "кластера" пользователей (фактически сети) с точкой доступа.

Базовые мосты для связи Ethernet с беспроводной сетью

Мост для связи Ethernet с беспроводной сетью (рис. 6.2) подключается напрямую к одному компьютерному устройству через порт Ethernet и затем обеспечивает беспроводное соединение с точкой доступа. Это делает полезным применение моста в таких

случаях, когда какое-то устройство, например принтер, ПК или игровая видеоприставка, имеет порт Ethernet, но не снабжено платой интерфейса беспроводной сети. В некоторых случаях бывает невозможно оборудовать его платой интерфейса беспроводной сети, что делает применение базового моста (basic bridge) единственным способом обеспечения работы в беспроводном режиме. Как правило, в подобной ситуации оказываются владельцы принтеров и игровых видеоприставок.

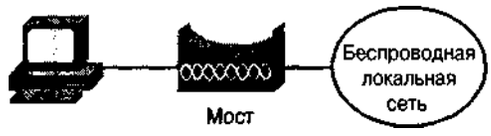

Рис. 6.2. Базовый мост соединяет ПК с беспроводной локальной сетью

Мосты рабочих групп

Мосты рабочих групп (рис, 6.3) обеспечивают соединения беспроводных сетей с большими проводными сетями Ethernet. Мост рабочей группы действует как беспроводной клиент беспроводной сети, взаимодействуя затем с проводной сетью. Его проводная часть подключается к коммутатору Ethernet, который соединяет многие устройства. Мост рабочей группы обеспечивает более надежное и высокоуровневое управление, чем базовый мост, а за дополнительную плату даже выполняет некоторые функции защиты.

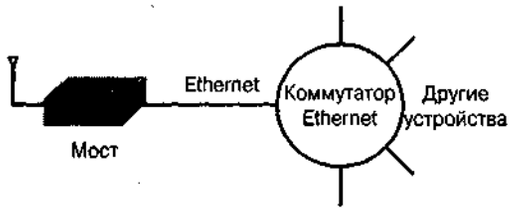

Рис. 6.3. Мост рабочей группы подключается к стандартным проводным сетям

Направленные антенны

Антенна — важный элемент беспроводной региональной сети. В отличие от беспроводных сетей других типов большинство антенн региональных сетей являются *направленными* ***(directional antennae),*** поскольку им приходится работать при повышенных дальностях связи. На рис. 6.4 показано, как распространяются радиоволны от направленной антенны. Это противоположно случаю использования всенаправленной антенны, которая передает радиоволны во всех направлениях.

Антенны разных типов имеют различную ширину диаграммы направленности в горизонтальной и вертикальной плоскостях. Так, всенаправленная антенна имеет ширину диаграммы направленности в горизонтальной плоскости 360 градусов, а в вертикальной — от 7-ми до 80 градусов. Полунаправленная антенна может иметь ширину диаграммы направленности в вертикальной плоскости 20 градусов, в горизонтальной — 50 градусов. В общем случае, чем уже диаграмма направленности, тем больше расстояние, на котором передаваемая мощность сохраняет постоянство.

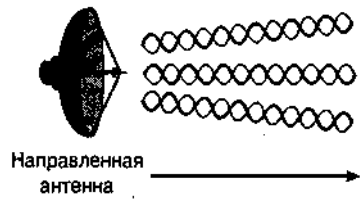

Рис. 6.4. Направленная антенна максимизирует интенсивность радиосигнала в одном направлении

Полунаправленные антенны

Существует несколько типов антенн, обеспечивающих полунаправленное излучение. Например, микрополосковая направленная антенна (patch antenna) может обеспечивать по крайней мере удвоенный радиус действия по сравнению со всенаправленной антенной. Она с легкостью монтируется на стене здания, обеспечивая эффективную связь в обширной области. Популярная антенна типа "волновой канал Яги", предложенная японским изобретателем Хидетсугу Яги (Hidetsugu Yagi), относится к полунаправленным и более других подходит для применения на больших расстояниях.

Полунаправленные антенны эффективно увеличивают амплитуду сигнала (это увеличение характеризуется *коэффициентом усиления антенны)* — примерно в 10 раз. Чаще всего их применяют в беспроводных локальных сетях, обеспечивающих соединения на протяженных пространствах. Например, в университетах антенна Яги может использоваться для обеспечения связи в обширных зонах вне помещений кампуса. Беспроводные региональные сети обычно нуждаются в обеспечении связи на гораздо больших расстояниях и требуют применения антенн с высоким коэффициентом усиления.

Остронаправленные антенны

Остронаправленные антенны имеют очень узкую диаграмму направленности, что обеспечивает большой радиус действия. Чтобы получить высокую степень направленности, нужна параболическая антенна, фокусирующая энергию радиоволн в одном направлении. Антенны таких типов стоят дороже, чем всенаправленные или полунаправленные, однако затраты оправдываются, когда необходимо решение, обеспечивающее связь на больших расстояниях.

Многие остронаправленные антенны используют параболическое зеркало для фокусирования энергии радиоволн в одном направлении. Такое зеркало имеет узкую диаграмму направленности в вертикальной и горизонтальной плоскостях — от 4-х до 25 градусов. Благодаря этому хорошо фокусируются радиоволны и существенно повышается радиус действия.

Однако параболическая антенна может быть повреждена вследствие неблагоприятных погодных условий, например, сильных ветровых нагрузок, особенно если при ее монтаже были допущены ошибки. Поэтому безопаснее применять остронаправленные сетчатые антенны, имеющие в параболическом зеркале отверстия.

Кроме того, и полунаправленные, и остронаправленные антенны можно применять только в случае, если между передающей и приемной антеннами нет препятствий. В некоторых случаях радиочастотные сигналы все же могут проходить через де-

ревья и здания, но при использовании ЯК-излучения никаких преград быть не должно. Радиочастотные и ИК-сигналы испытывают также периодические затухания, вызванные перемещающимися объектами, например, проходящими поездами или автомобилями. Планирование развертывания беспроводных региональных сетей особенно затруднено в условиях города, поскольку многочисленные здания препятствуют распространению сигналов между конечными точками систем.

Эффект поляризации

Поляризация антенны во многом зависит от ориентации ее относительно горизонтальной и вертикальной плоскостей. Так, вертикальной поляризации сигнала, которая чаще применяется в беспроводных локальных сетях, можно добиться за счет размещения антенны перпендикулярно поверхности земли. Горизонтальную поляризацию получают при размещении антенны параллельно поверхности земли. Чтобы энергия, передаваемая от одной антенны к другой, была максимальной, обе они при прочих равных условиях должны использовать одну поляризацию. Если одна из них использует вертикальную поляризацию, а другая — горизонтальную, то ни передачи энергии, ни связи не будет.

Системы беспроводных региональных сетей

Беспроводные региональные сети обеспечивают соединения между строениями и пользователями в пределах города или кампуса. Существует несколько способов конфигурации таких систем, в большинстве случаев пучки радиоволн или ИК-излучения передаются от одной точки к другой посредством направленных антенн.

Системы типа "точка-точка"

Решения типа "точка-точка" основаны на использовании радиочастотных или ИК-сигналов и полунаправленных либо остронаправленных антенн для увеличения радиуса действия до размеров кампуса колледжа или города. При использовании радиосистем с остронаправленными антеннами радиус их действия может достигать 50 км (30 миль). На рис. 6.5 представлена система беспроводной региональной сети типа "точка-точка".

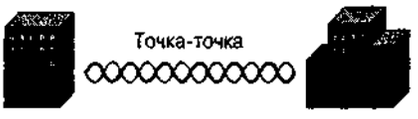

Рис. 6.5. Беспроводная региональная сеть типа "точка-точка" напрямую соединяет две точки системы

В медицинском центре сеть типа "точка-точка" может быть использована для создания канала связи между головным госпиталем и отдаленной клиникой, находящейся в том же городе. Эта система не отличается такой же гибкостью, как решения типа "точка-несколько точек". Но если нужно обеспечить связь только между двумя площадками, она вполне приемлема, поскольку стоимость *системы "точка-точка " (point-to-point system)* ниже, чем систем типа "точка-несколько точек".

Системы типа "точка-несколько точек"

Типичный канал типа "точка-несколько точек" (рис. 6.6) использует центральную всенаправленную антенну, которая обеспечивает один приемопередатчик для связи нескольких отдаленных станций. Например, всенаправленная антенна может быть установлена на здании в центре города, а на других зданиях размещают направленные антенны, ориентированные на центральную. В этом случае центральный приемопередатчик принимает и повторно передает сигналы.

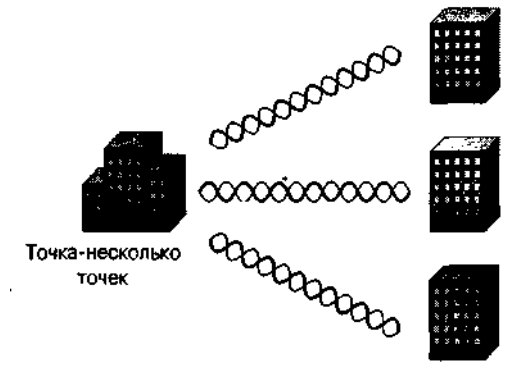

Рис. 6.6. Беспроводная региональная сеть типа "точка-несколько точек" обеспечивает соединение пользователей через централизованный приемопередатчик

Серьезным преимуществом сетей этого типа является то, что они упрощают добавление новых каналов связи. На самом деле это может оказаться менее дорогостоящим вариантом, чем использование систем "точка-точка", если имеется несколько площадок, для которых нужно обеспечить связь между собой или с центральной площадкой. Например, система "точка-несколько точек" выгодна для компании, головной офис которой и несколько складов и производственных предприятий расположены в одном и том же городе. Это же относится к развертыванию беспроводной региональной сети в сельской местности.

Системы пакетной радиосвязи

Системы пакетной радиосвязи (рис. 6.7) используют специальные беспроводные маршрутизаторы, которые перенаправляют содержащиеся в пакетах данные к месту назначения. Каждый пользователь такой системы должен иметь радиоплату интерфейса пакетной сети, способную передавать данные ближайшему беспроводному маршрутизатору. Этот маршрутизатор передает данные следующему маршрутизатору. Эти переходы от одного маршрутизатора к другому выполняются до тех пор, пока пакет не поступит в место назначения. Такие сети с ячеистой топологией не новы. Радиооператоры компании Amateur Ham используют их десятилетиями, а такие компании, как Metricom, развертывали системы подобного типа в городах уже десять лет назад.

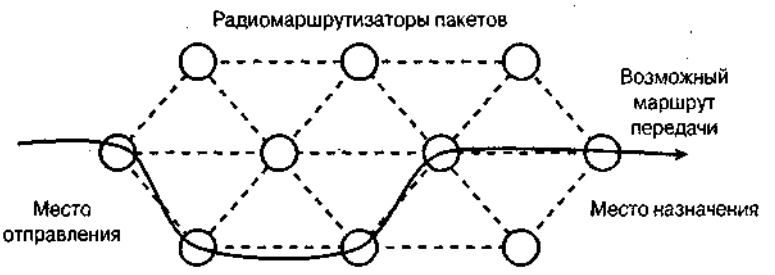

Рис. 6.7. Системы пакетной радиосвязи передают пакеты данных от отправителя к получателю

Городские власти, развернув систему пакетной радиосвязи, обеспечат беспроводную связь с целью поддержки приложений в масштабах всего города. Необходимая инфраструктура может быть создана за счет установки маршрутизаторов в стратегически важных точках города. Связь между маршрутизаторами обеспечивается без помощи проводов. Каждый маршрутизатор осуществляет прием и передачу (переключение) пакетов с целью доставки их к месту назначения.

Эта форма связи обладает высокой живучестью. Если один из маршрутизаторов выходит из строя вследствие удара молнии или умышленного повреждения, протоколы динамической маршрутизации автоматически обновляют таблицы маршрутизации на каждом маршрутизаторе таким образом, что пакеты обходят поврежденный маршрутизатор.

Технологии беспроводных региональных сетей

При установке многих беспроводных региональных сетей используются патентованные технологии, а их работа осуществляется в лицензируемых диапазонах. Лицензирование позволяет избежать взаимных помех, поскольку при этом гарантируется использование близлежащими системами разных частот. Даже если конечным пользователям и приходится проходить процесс лицензирования, он не занимает много времени, поскольку выполняется только один раз. Однако компоненты для лицензируемых частотных диапазонов стоят дорого. Поэтому компании предпочитают использовать стандартное оборудование, что снижает как первоначальные затраты, так и эксплуатационные расходы. Если производитель перестает поддерживать какой-то продукт, компания при модернизации сети может перейти на изделия другого производителя. Следовательно, благодаря стандартизации увеличивается долговечность систем.

Стандарт 802.11 и Wi-Fi

Многие компании развертывают беспроводные региональные сети, используя при этом стандарты беспроводных локальных сетей и Wi-Fi (подробное описание см. в главе 5). Разница между ними состоит в том, что в беспроводных региональных сетях используются направленные антенны для создания каналов типа "точка-точка" между фиксированными точками системы. В состав аппаратного обеспечения входят беспроводные мосты, соответствующие стандартам на беспроводные локальные сети.

За счет использования аппаратного -обеспечения беспроводных локальных сетей в региональных сетях достигается снижение затрат, однако стандарт 802.11 имеет ограничения на число поддерживаемых пользователей, особенно если им необходима гарантированная полоса пропускания. Кроме того, при использовании систем стандарта '802.11 для обеспечения связи в обширных зонах часто возникают серьезные проблемы, связанные с помехами, поскольку передача осуществляется в нелицензируемом диапазоне. Конкуренты могут установить сеть стандарта 802.11, которая будет создавать помехи для вашей сети, и пользователи последней будут периодически ощущать снижение производительности. Решения этой проблемы не существует, поскольку не существует законов, регулирующих подобные ситуации.

Стандарт 802.16

Рабочая группа IEEE 802 инициировала создание рабочей группы IEEE 802.16, задачей которой является разработка стандартов на беспроводной широкополосный доступ с целью получения высокоскоростного, с высокой пропускной способностью, недорогого, масштабируемого решения для расширения магистральных волоконно-оптических линий связи. Первый стандарт IEEE *802.16,* опубликованный, в апреле 2002г., определяет беспроводной радиоинтерфейс для беспроводных региональных сетей (wireless MAN air interface). Предполагается, что системы такого рода обеспечат доступ к сетям в домашних условиях, небольших офисах и бизнес-центрах, став альтернативой традиционным проводным соединениям.

При стоимости базовой станции менее $20 тыс. системы стандарта 802.16 становятся экономически выгодными при обслуживании до 60 клиентов, имеющих скоростные соединения Т-1 (1,5 Мбит/с). Это также привлекательная альтернатива для Internet-провайдеров с ограниченными средствами, осуществляющих беспроводной роуминг (WISP). Кроме того, 802.16 может обеспечить приемлемое решение для соединения "горячих точек" беспроводной локальной сети между собой.

Стандарт 802.16 поддерживает структуру "точка-несколько точек", рабочий диапазон 10-66 ГГц, данные передаются со скоростью до 120 Мбит/с. При работе в этом диапазоне необходимо, чтобы устройства находились в зоне прямой видимости относительно друг друга, поэтому крыши зданий являются наилучшим местом расположения базовых станций и станций абонентов. Базовые станции подключаются к проводной широкополосной сети передачи данных и могут передавать данные без проводов на расстояние до 50 км (30 миль) многим (возможно, сотням) стационарно установленным абонентским станциям.

Для обеспечения доступа на более низких частотах в ситуациях, когда устройства не находятся в пределах прямой видимости, IEEE в январе 2003 г. опубликовал стандарт 802.16а, включающий поддержку ячеистой структуры. Устройства стандарта 802.16а работают на лицензируемых и нелицензируемых частотах в диапазоне 2-11 ГГц, применяя технологию мультиплексирования с ортогональным частотным разделением сигналов (orthogonal frequency division multiplexing, OFDM).

Уровень MAC стандарта 802.16 поддерживает спецификации многих лицензируемых и нелицензируемых физических уровней. На уровне MAC каждая базовая станция динамически распределяет частоты для восходящего и нисходящего каналов абонентских станций, использующих технологию множественного доступа с временным разделением каналов МДВР (time division multiple access, TDMA). Это кардинально отли-

чается от уровня MAC стандарта 802.11, поскольку его текущие реализации используют механизмы обнаружения несущей, которые не обеспечивают эффективного контроля за использованием полосы пропускания радиоканала.

Следующая задача рабочей группы по стандарту 802.16 — это обеспечение портативности и мобильности для устройств данного стандарта. В марте 2002 г. была создана исследовательская группа по стандарту 802.16e, призванному обеспечить мобильный широкополосный беспроводной доступ (mobile broadband wireless access). Этой группе предстоит решить множество различных проблем мобильности, включая обеспечение соединений для средств передвижения, перемещающихся в зоне действия базовой станции.

Резюме

В беспроводных региональных сетях используются, в основном, мосты с направленными антеннами для обеспечения соединения между двумя сетями, развернутыми в городской зоне. Системы типа "точка-точка" служат для непосредственного соединения двух площадок, а системы типа "точка-несколько точек" позволяют взаимодействовать нескольким площадкам через центральный приемопередатчик. Многие компании используют патентованные технологии при создании беспроводных региональных сетей. Стандарты, такие как 802.11 и Wi-Fi, позволяют использовать менее дорогие решения, но при этом сеть может оказаться подверженной воздействию радиочастотных помех. Однако новый стандарт 802.16 позволит вскоре разворачивать эффективные стандартизованные беспроводные региональные сети.

Вопросы для самопроверки

Ответы на эти вопросы вы можете найти в приложении А.

1. Почему беспроводные региональные сети позволяют быстро окупить инвестиции?
2. Верно ли, что самообучающиеся мосты повторно передают все полученные пакеты?
3. В чем основное отличие между мостом и точкой доступа?
4. Приведите пример полунаправленной антенны.
5. Если говорить о диаграмме направленности, то в чем состоит основная разница между полунаправленной и остронаправленной антеннами?
6. Приведите пример остронаправленной антенны.
7. Какая поляризация эффективнее для антенны приемника, если в антенне передатчика использована вертикальная поляризация?
8. В чем преимущество использования систем типа "точка-несколько точек" по отношению к системам "точка-точка" в случае, когда необходимо обеспечить соединения для нескольких площадок?
9. В чем преимущество использования пакетной радиосвязи в беспроводных региональных сетях?
10. Какие стандарты используются при создании беспроводных региональных сетей?

В этой главе...

приложения для беспроводных глобальных сетей;

технологии и компоненты беспроводных глобальных сетей;

реализация систем беспроводных глобальных сетей различных типов.

ГЛАВА 7

Беспроводные глобальные сети: сети для соединения по всему миру

Беспроводные глобальные сети удовлетворяют потребность в соединениях, которые осуществляются на огромных расстояниях, например, между странами и континентами. В большинстве случаев эти сети обеспечивают установление соединений для пользователей, находящихся вне дома, офиса и не имеющих доступа к беспроводным локальным сетям, обеспечивающим доступ вне помещений. Глобальные сети обеспечивают связь для пользователей, находящихся вне помещений, но пропускная способность при этом значительно меньше, чем при работе беспроводных сетей внутри помещений.

Преимущество беспроводных глобальных сетей состоит в большом радиусе действия и экономии от масштаба (снижение средних затрат по мере увеличения объема выпуска), благодаря чему стоимость подписки для абонентов довольно низкая. Недостатком является ограниченность используемого спектра частот, из-за чего снижаются производительность и безопасность. Но для развертывания на больших площадях глобальные сети практичнее, чем беспроводные локальные. Хоть какая-то пропускная способность все же лучше, чем отсутствие таковой вообще.

Например, беспроводная глобальная сеть позволяет абоненту проверять свою электронную почту во время визитов к клиентам в другом городе. Это позволяет пользователям быстрее реагировать на изменение ситуации, чем в случае, когда они проверяют свою почту после возвращения в номер гостиницы. Относительно низкая производительность беспроводной глобальной сети все же позволяет адекватно выполнять приложения такого типа.

Беспроводная глобальная сеть обеспечивает также доступ к Internet из отдаленных мест. Так, турист может направить спутниковую антенну, смонтированную на его рекреационном автомобиле[1], и получить доступ к Internet. Это дает ему возможность общаться с семьей и пользоваться преимуществами Internet, даже находясь в отдаленных местах.

В данной главе приведены примеры компонентов беспроводных глобальных сетей, проанализировано, как эти компоненты взаимодействуют между собой при формировании различных систем, а также описаны различные технологии.

[1] *Специализированный автомобиль или прицеп для любителей автотуризма, разделенный на функциональные секции — кухню, спальню, гостиную, туалет, душ и т. п.* — Прим. ред.

Компоненты беспроводных глобальных сетей

Беспроводные глобальные сети позволяют выполнять мобильные и стационарные приложения. Состав компонентов зависит от используемой технологии и конфигурации беспроводной глобальной сети. Например, спутниковая беспроводная глобальная сеть создается на основе иных компонентов, чем система, основанная на применении сотовой связи.

Пользовательские устройства беспроводных глобальных сетей

Пользователи глобальных сетей применяют небольшие портативные устройства. Это обусловлено тем, что доступ к сети возможен из очень обширных зон, и пользователи должны иметь эти устройства при себе. Например, коммивояжеру не составит особого труда носить небольшой PDA или мобильный телефон и получать электронную почту, когда он едет из аэропорта в гостиницу. На рис. 7.1 представлены пользовательские устройства различных типов, часто применяемые в беспроводных глобальных сетях.

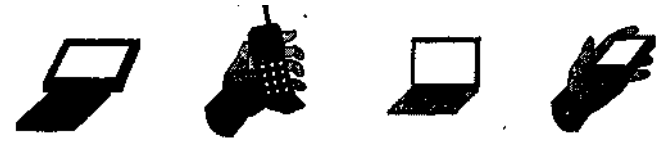

Рис. 7.1. Пользовательские устройства беспроводных глобальных сетей имеют компактные размеры

Для стационарных ПК использование беспроводных глобальных сетей нехарактерно, однако такие варианты возможны. Необходимость снабжения пунктов продажи (POS) на отдаленных площадках (например, во временных концертных залах) может потребовать использования беспроводной глобальной сети. Поставщик, продающий футболки, может обрабатывать кредитные карты через беспроводную глобальную сеть в Internet-центре обработки данных.

Радиоплаты интерфейса сети

Некоторые мобильные телефоны имеют встроенные радиостанции беспроводной глобальной сети. Телекоммуникационные компании, такие как Verizon и Sprint, обеспечивают соединения через беспроводную глобальную сеть с речевыми службами. Существуют различные беспроводные глобальные сети, поэтому у пользователей появляется возможность приобрести мобильный телефон, взаимодействующий с беспроводной глобальной сетью такого типа, которая им больше подходит.

Для обеспечения взаимодействия ноутбука или PDA с беспроводной глобальной сетью нужно приобрести соответствующую радиоплату интерфейса сети (рис. 7.2). Эти платы могут выглядеть так же, как платы для беспроводных персональных и локальных сетей, однако в них применяется одна из нескольких несовместимых технологий.

Рис. 7.2. Радиоплаты интерфейса беспроводной сети для ноутбуков и PDA

Приобретая аппаратное обеспечение, поставщик обычно продает и доступ к сервису, для взаимодействия с которым предназначена плата. Телекоммуникационные компании тратят значительные средства на закрепление за собой частотного спектра и установку аппаратного обеспечения на огромных площадях. Поэтому провайдеры беспроводных глобальных сетей взимают плату за свои услуги. В этом коренное отличие от развертывания беспроводных локальных сетей в "горячих точках", когда гостиницы и аэропорты считают выгодным предоставлять бесплатный доступ пользователям к сети, поскольку для их развертывания не нужны крупные капитальные вложения.

Покупая радиоплату интерфейса беспроводной локальной сети, убедитесь в том, что она соответствует типу беспроводной глобальной сети, развернутой там, где вы собираетесь ею пользоваться.

При пользовании спутниковой беспроводной глобальной сетью необходима аппаратура спутникового терминала. Мобильные версии спутниковых терминалов снабжены компактными параболическими зеркальными антеннами и электронной аппаратурой, которая помещается в небольшом кейсе. Интерфейс беспроводной глобальной сети такого типа стоит довольно дорого. Спутниковые терминалы пригодны и для стационарных установок, таких как дома и рекреационные автомобили.

Базовые станции

Базовые станции беспроводных глобальных сетей обычно располагаются вне помещений. Хорошо знакомые многим мачты сотовой связи (рис. 7.3) установлены во многих городах и сельской местности. По аналогии с беспроводными локальными сетями эти станции используют провода для подключения к распределительной системе, обеспечивающей необходимую коммутацию и интерфейс Internet. В большинстве случаев эти антенные мачты устанавливаются вне помещений с целью обеспечения максимальной зоны действия. Однако и в некоторых крупных общественных зданиях (торговых пассажах, аэропортах) устанавливают базовые станции сотовой сети для обслуживания большого числа абонентов.

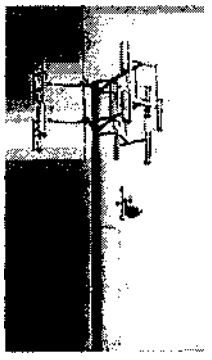

Рис. 7.3. Мачты сотовой связи часто используются для размещения базовых станций беспроводной глобальной сети

Другая форма базовой станции беспроводной глобальной сети — это *спутник (satellite)* на орбите, который, по сути, является повторителем в небе. На земле пользователь направляет параболическую антенну на спутник, тот принимает сигнал и повторно передает его на наземную станцию (рис. 7.4). Важным преимуществом такого подхода является то, что необходимая инфраструктура размещается на земле. Но при этом операторам приходится выкладывать миллионы долларов за установку спутниковой системы, способной передавать трафик компьютерной сети. Из-за этого пользователям дорого обходится такой сервис.

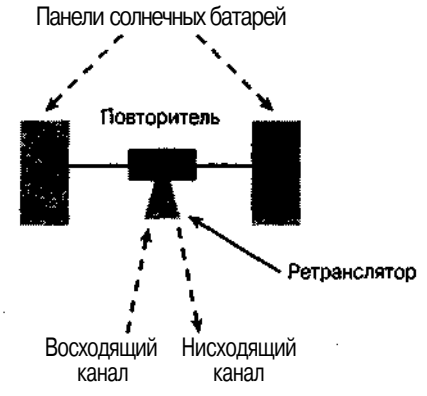

Рис. 7.4. На спутниках находятся ретрансляторы, принимающие и передающие радиосигналы, их электропитание осуществляется от солнечных батарей

Антенны

Базовые станции беспроводных глобальных сетей и пользовательские устройства используют антенны различных типов, их выбор зависит от типа беспроводной глобальной сети. В сотовых системах антенна пользовательского устройства обычно

всенаправленная. На мачтах сотовой связи, как правило, размещают несколько направленных антенн, которые обеспечивают большую дальность связи.

Абоненты спутниковой связи пользуются параболическими антеннами (рис. 7.5). Приемопередатчик, расположенный в фокусе, принимает и передает радиосигналы. Так, если сигнал отправляется передающей стороной приемопередатчика, то благодаря параболической антенне большая часть его мощности передается в одном направлении.

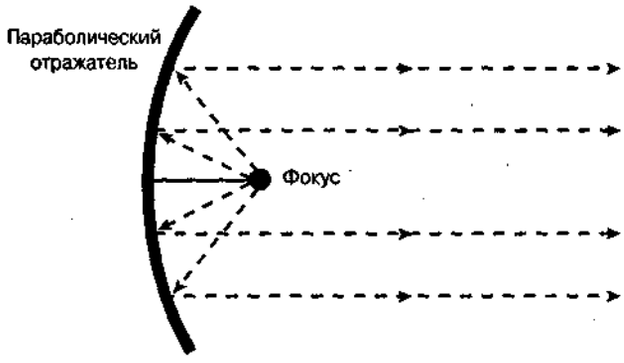

Рис. 7.5. Зеркальная антенна имеет параболический отражатель, который фокусирует сигнал для передачи его в нужном направлении

Независимо от того, под каким углом радиосигнал падает на "тарелку", покидает ее он всегда в одном направлении, что обусловлено ее параболической формой. Когда антенна принимает сигнал, из-за ее параболической формы принятый сигнал фокусируется на приемнике, размещенном в фокусе антенны.

Системы беспроводных глобальных сетей

Большинство беспроводных локальных сетей являются сотовыми, но некоторые используют спутники. Рассмотрим подробнее оба типа.

Беспроводные глобальные сети с сотовой структурой

Сотовая система (рис. 7.6) состоит из мачт, концентраторов, коммутаторов речевых сигналов и шлюзов данных. Мачта сотовой системы принимает сигналы пользовательских устройств и передает информацию пользователям. Коммутатор речевых сигналов подключает пользовательское устройство к проводному или беспроводному устройству другого пользователя через телефонную распределительную систему. Эта часть системы поддерживает обычные телефонные разговоры пользователей.

Компонент, который превращает эту систему в беспроводную глобальную сеть — это шлюз данных. В данном случае шлюз способен выполнять протоколы передачи данных таким образом, что пользователи получают возможность просматривать Web-страницы, получать и отправлять сообщения электронной почты и использовать корпоративные приложения.

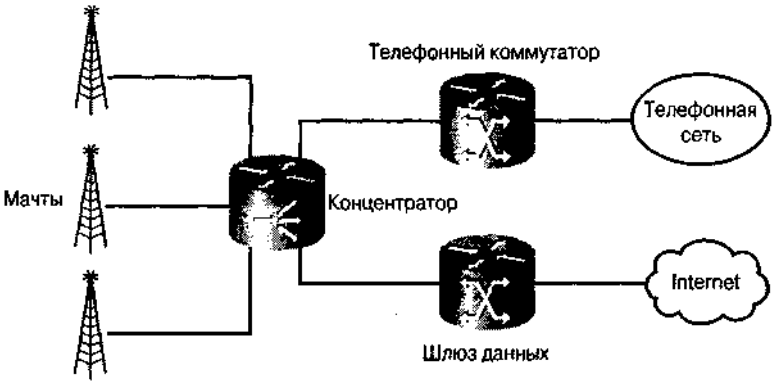

Рис. 7.6. Сотовые системы включают шлюзы данных, благодаря чему обычные службы передачи речи получают возможность устанавливать соединения с беспроводной сетью

Передача текстовых сообщений — весьма популярный сервис беспроводной глобальной сети, базирующейся на системе сотовой связи. Пользователи общаются путем набора коротких текстовых сообщений и отправки их другим пользователям, аналогично тому, как это происходит при использовании приложений для ПК, обеспечивающих мгновенный обмен сообщениями. Однако, поскольку устройства беспроводной глобальной сети малы по размерам, важно, чтобы пользователи имели возможность сохранять сообщения типа "Я сейчас в дороге и позвоню тебе позже" и посылать их путем нажатия одной кнопки. Некоторые устройства беспроводной глобальной сети также способны захватывать изображения в цифровой форме и видеофрагменты, которые также можно переслать через сеть.

Сотовые системы первого поколения

Когда появились первые мобильные телефоны, в беспроводных коммуникациях использовались только аналоговые сигналы. Первые системы сотовой телефонной связи принято называть системами первого поколения, или *сотовыми системами 1G (1G cellular).* Когда кто-то разговаривал по телефону такой системы, его речь передавалась с использованием частотной модуляции (ЧМ), при которой в соответствии с речевым сигналом изменялась только частота несущей. В этих системах использовалось ограниченное число каналов, в которых для передачи управляющих сигналов, необходимых для настройки и поддержания телефонных разговоров, применялась частотная манипуляция (ЧМн).

Несмотря на случающиеся хрипы и шипения, системы первого поколения хорошо подходят для осуществления телефонных разговоров, но мало пригодны для передачи компьютерных данных. Как и при передаче речи, данные должны быть представлены в виде аналоговых сигналов. Пользователи обеспечивают взаимодействие ПК и сотовой системы с помощью модема, преобразующего цифровые сигналы, поступающие с компьютерного устройства, в аналоговую форму (такую как ЧМн или ФМн), которая подходит для передачи через узкополосный, шириной лишь 4 кГц, канал речевой связи. Поэтому скорость передачи данных очень низкая, около 20-30 кбит/с.

Системам первого поколения не хватает пропускной способности для поддержки механизмов аутентификации и шифрования. Пропускной способности цифрового канала управления, использующего ЧМн, хватает только для поддержки телефонных разговоров. Ее недостаточно для передачи имен пользователей и паролей для службы аутентификации или координации процесса шифрования. Это и понятно, ведь системы первого поколения создавались для передачи речи, а не данных.

Одно время системы первого поколения использовались почти на всей территории США. На сегодняшний день они применяются лишь в малонаселенных местностях, где нет смысла обновлять инфраструктуру сети, чтобы она могла обеспечивать работу новейших цифровых систем.

Сотовые системы второго поколения

Не так давно стали доступны цифровые сотовые системы, позволяющие использовать как речевые, так и управляющие каналы для передачи цифровых сигналов. Первая фаза внедрения этих полностью цифровых систем известна как сотовые системы второго поколения, или *сотовые системы 2G (2G* ***cellular).*** Сейчас большинство телекоммуникационных операторов предлагают услуги на основе систем 2G, периодически улучшая их характеристики.

Благодаря использованию цифровых сигналов для передачи речи стало возможным внедрение более эффективных методов модуляции. Это, в свою очередь, сделало возможным поддержку большего числа телефонных разговоров и передачу данных с использованием полосы частот меньшей ширины. Системы второго поколения поддерживают работу различных служб — передачи коротких сообщений, аутентификации и обновления программного обеспечения, обеспечивающего проведение телефонных разговоров — без использования проводов.

Усовершенствованные версии систем 2G (иногда называемые системами 2.5G) используют улучшенные методы модуляции, благодаря чему повышается скорость передачи данных и эффективность использования спектра. Так, протокол GPRS (general packet radio services — пакетная радиосвязь общего назначения) обеспечивает высокоскоростную передачу данных через глобальную систему для сетей GSM (global system for mobile communications — глобальная система связи с подвижными объектами). Максимальная скорость передачи данных по протоколу GPRS составляет 171,2 кбит/с. Но для пользования услугами GPRS нужны специальные мобильные телефоны. Кроме того, перспективная технология мобильной радиосвязи (enhanced data rates for global evolution, EDGE) позволяет расширить возможности GSM за счет использования восьмиуровневой ФМн, при которой каждый переданный символ представляет 3 бита данных. В результате максимальная скорость передачи данных повышается до 474 кбит/с.

Сотовые системы третьего поколения

Многие телекоммуникационные операторы начинают внедрять так называемые сотовые системы третьего поколения, или *сотовые системы 3G (3G* ***cellular).*** Универсальная система мобильной связи (universal mobile telecommunications system, UMTS) способна передавать данные со скоростью 2 Мбит/с вне помещений, до 384 Кбит/с в городских условиях и до 144 Кбит/с в сельской местности. Поэтому системы 3G могут поддерживать мультимедийные приложения.

Специалисты в области беспроводных сетей задаются таким вопросом: могут ли системы 3G вытеснить технологию беспроводных локальных сетей стандарта 802.11 (Wi-Fi)? При высоких скоростях передачи данных вне помещений системы 3G представляют собой альтернативу для беспроводных локальных сетей. Однако сети стандарта 802.11 продолжают повышать свои характеристики, которые и сейчас значительно превышают таковые систем 3G. Например, стандарт 802. Па регламентирует передачу данных со скоростью 54 Мбит/с, что намного больше скорости, присущей системам 3G. Кроме того, стоимость развертывания беспроводной локальной сети намного ниже.

Однако беспроводные локальные сети не пригодны на обширных пространствах, поскольку требуют слишком развитой инфраструктуры. Технология 3G позволяет использовать существующие мачты систем сотовой связи и распределительные системы. Затраты на модификацию сотовых систем первого и второго поколений до систем 3G все еще высоки, но это наиболее подходящий метод для обеспечения беспроводных соединений на больших площадях.

Таким образом, системы 3G и системы беспроводных локальных сетей дополняют одна другую. Это побуждает группы стандартизации и производителей искать пути для плавной интеграции систем сотовой связи третьего поколения и беспроводных локальных сетей. И уже сейчас доступны мобильные телефоны и PDA, применяющие обе эти технологии. Благодаря этому пользователь, выходя из зоны действия беспроводной локальной сети, автоматически начинает работу в сотовой системе связи. Однако до сих пор не разработаны стандарты, описывающие такую форму роуминга, что вынуждает пользователя тщательно выбирать поставщика услуг, поддерживающего работу телефона и PDA пользователя.

Служба коротких сообщений (SMS)

Одним из наиболее востребованных сервисов беспроводных глобальных сетей является служба коротких сообщений (short massage service, SMS). Она представляет собой систему передачи текстовых сообщений, способную одновременно передавать две сотни символов. SMS — это беспроводной вариант широко известных приложений обмена текстовыми сообщениями, работа которых обеспечивается многими Internet-провайдерами. Дополнительные возможности применения SMS, характерные для беспроводных глобальных сетей, перечислены ниже.

- **Распределение содержимого.** SMS — эффективное средство распределения всевозможных обновлений для пользовательских устройств. Так, пользователь может загрузить новую мелодию звонка и фоновую заставку на свой телефон при посредстве SMS. Кроме того, служба SMS позволяет пользователям делать запросы к базам данных и получать новости. Например, вы можете узнать о последних чрезвычайных происшествиях, получая SMS-сообщения.
- **Предупреждения.** Многие операторы рассылают пользователям различные предупреждения: о поступлении речевой почты, счет спортивного состязания, текущий биржевой курс и др. Это позволяет пользователю получать свежую информацию о том, что произошло в сфере его интересов.

- **Интерактивное взаимодействие.** В некоторых телевизионных шоу предполагается взаимодействие зрителей и гостей с помощью SMS. Благодаря этому телезрители могут участвовать в передаче.
- **Интеграция приложений.** Разработчики могут интегрировать службу SMS во многие корпоративные приложения. Так, систему управления продажами, позволяющую агентам по продаже товаров отслеживать клиентов и продукты, можно дополнить службой SMS. Такое дополнение механизма рассылки предупреждений весьма полезно: агенты по продаже товаров могут получать извещения о том, что какой-то продукт поступил в продажу.

На многих Web-сайтах используется язык гипертекстовой разметки для беспроводной связи (wireless markup language, WML), с помощью которого осуществляется преобразование обычных Web-страниц в формат, более пригодный для чтения с помощью малогабаритных устройств, таких как PDA или сотовый телефон. WML также уменьшает объем изображений, чтобы компенсировать меньшую скорость передачи, характерную для беспроводных технологий.

Подробнее о приложениях, обеспечивающих мгновенный обмен сообщениями, на сайте Instant Messaging Planet (www. instantmessagingplanet. com).

Беспроводные глобальные сети на основе космических технологий

Помимо наземных систем сотовой связи средства для соединения пользователей через сеть на обширных пространствах предоставляют системы космического базирования.

Спутники

Спутники для вещательного телевидения и других коммуникаций используются уже несколько десятилетий. Но подключать абонентов к Internet спутниковые системы начали совсем недавно (рис. 7.7). Скорости передачи данных вполне приемлемые, при загрузке — до 1,5 Мбит/с.

Некоторые спутниковые системы поддерживают двусторонний обмен данными, позволяя пользователям посылать данные на спутник (и в обратном направлении). Например, мобильное устройство пользователя может передать на спутник запрос на просмотр Web-страницы. Спутник передает эти данные на соответствующую наземную станцию, которая затем перешлет Web-страницу через спутник пользователю. Отдельные спутниковые системы поддерживают только нисходящий канал связи. Пользовательское устройство может затребовать Web-страницу через другую сеть, например телефонную, после чего спутник передаст страницу пользователю.

За счет размещения активных радиоповторителей на искусственных спутниках Земли можно обеспечить широковещание и связь типа "точка-точка" на больших участках земной поверхности. Возможность широковещания спутникового повторителя уникальна. При должном выборе диаграммы направленности антенны спутника он может обеспечивать вещание в строго определенной области.

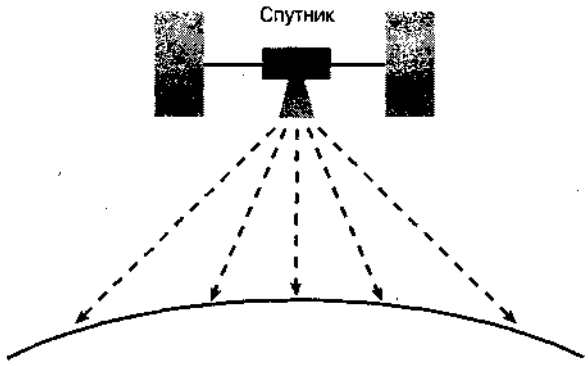

Рис. 7.7. Спутниковая система резко расширяет область действия беспроводной глобальной сети

В зависимости от решаемых задач спутники размещаются в различных точках геостационарной орбиты. Для обеспечения глобальной области действия необходимы, как минимум, три спутника. Однако для того чтобы уровень радиосигналов был примерно постоянным, спутников должно быть четыре. Это также дает некоторую свободу в их позиционировании.

Спутниковые телекоммуникационные системы используют наиболее подходящие для этих целей частотные диапазоны, в которых обеспечиваются высокий выход по энергии, минимальные искажения сигнала при его распространении и минимальная восприимчивость к шуму и помехам. К сожалению, для наземных систем наиболее привлекательны те же частоты. Космос интернационален, поэтому контроль за распределением частот работы спутников осуществляет Международный союзтелекоммуникаций (Internationaltelecommunicationsunion, ITU).

Полоса частот от 450 МГц до 20 ГГц наиболее приемлема для каналов связи типа Земля-космос-Земля. Нет смысла устанавливать каналы связи, работающие на частотах свыше 20 ГГц, с наземными терминалами, расположенными в климатических зонах с большим количеством осадков, если необходим высокий коэффициент готовности.

При работе во всех частотных диапазонах для нисходящего канала используются низшие частоты спектра, поскольку к нему предъявляются строжайшие ограничения по мощности. Такие частоты менее чувствительны к затуханию радиоволн в свободном пространстве, чем радиоволны более высоких частот восходящего канала. Потери проще компенсировать для восходящего канала, поскольку наземные станции могут обеспечивать большую излучаемую мощность.

Спутник выполняет роль повторителя сигнала. Сигналы передаются на него по восходящему каналу и в режиме широковещания возвращаются на Землю по нисходящему каналу. Устройства, выполняющие подобные функции, принято называть ретрансляторами. Спутниковый ретранслятор является аналоговым и обслуживает каналы наземных систем связи. Он может принимать, усиливать и повторно передавать сигналы наземных терминалов, а также выполнять функции ретрансляции для одного или нескольких радиотелекоммуникационных каналов.

Период обращения низкоорбитальных спутников, имеющих круговую, полярную или наклонную орбиту, меньше чем 24 часа. Поэтому с поверхности Земли заметны их перемещения. Эти орбиты удобны для наблюдения за происходящими на Земле процессами, а также используются для связи в высоких северных и южных широтах.

Особый интерес для линий передачи данных общего пользования представляет геостационарная орбита. Спутник, выведенный на эту орбиту, имеет период обращения 24 часа и высоту над поверхностью Земли около 35 880 км (22 300 миль). Он все время находится над одной и той же точкой экватора, поэтому наземному наблюдателю спутник кажется неподвижным.

На самом деле это не так. Даже если орбита спутника в точности круговая и высота выдержана с высокой точностью, из-за природных явлений (таких как слабые гравитационные поля Луны и планет Солнечной системы, а также из-за давления, вызванного излучением Солнца) наблюдается его небольшой дрейф. Последствия этого медленного и малоощутимого дрейфа время от времени корректируются с помощью ракетных двигателей малой тяги, управляемых с Земли.

Поскольку радиосигналы преодолевают довольно большое расстояние (около 22 300 британских статутных миль[2] от наземного терминала до геостационарной орбиты), при передаче сигнала между наземным терминалом и спутником получается задержка около 100 мс. Это означает, что на пути Земля-спутник-Земля задержка составит уже 200 мс. Это делает спутниковую систему неудобной для использования с протоколами (например, 802.11), ожидающими ответа после передачи каждого пакета информации и лишь после этого передающими следующий пакет. Поэтому многие сетевые протоколы, требующие регулярных подтверждений от получателя, неэффективно работают в условиях спутниковой связи.

Метеорная связь

Миллиарды микроскопических метеоров попадают в земную атмосферу. Они падают в любое время и во всех уголках мира. Когда метеоры на большой высоте проникают в атмосферу, они ионизируют газ. Если метеордостаточно крупный, этот газ выглядит как падающая звезда.

При метеорной связи радиосигналы отражаются от метеорных следов (рис. 7.8). Это позволяет создавать протяженные (с дальностью действия до 2400км (1500 миль) беспроводные каналы передачи без каких-либо затрат на запуск и обслуживание спутников.

Системы метеорной связи направляют радиоволны диапазона 40-50 МГц, модулированные сигналом данных, в направлении ионизированного метеорами газа. Радиосигналы, отразившись от ионизированного газа, направляются обратно к Земле. Надежность метеорной связи высока, однако она может гарантировать скорость передачи от 300 до 2400 бит/с. Это очень мало, даже по сравнению с телефонными модемами.

Однако стоимость оборудования для метеорной связи настолько низка по сравнению со спутниковыми системами, что не очень требовательные к производительности сети приложения, такие как передача телеметрических сигналов, вполне могут использовать метеорную связь. Посредством метеорной связи, например, можно передавать данные об уровне снежного покрова в отдаленных горных местностях в центр мониторинга.

[2] *Одна статутная британская миля равна 1,609 км.* — Прим. ред.

Рис. 7.8. Системы метеорной связи используют метеорные следы для отражения сигналов обратно к Земле

Технологии беспроводных глобальных сетей

В беспроводных глобальных сетях используются технологии, обеспечивающие в основном модуляцию речи и данных. Как отмечалось в главе 2, за счет модуляции осуществляется преобразование цифровых сигналов, используемых для представления информации внутри компьютеров, в радио- или световые сигналы. В беспроводных глобальных сетях применяются только радиосигналы, разработанные с целью эффективного обслуживания многих пользователей. За каждым пользователем закрепляется отдельный канал, что принципиально отличает эти сети от беспроводных локальных сетей, в которых все пользователи делят между собой один канал. Благодаря этому значительно снижаются помехи для пользовательского устройства и базовой станции беспроводной глобальной сети.

Рассмотрим методы модуляции подробнее.

Доступ с частотным уплотнением

При *доступе с частотным уплотнением* ***(Frequency division multiple access, FDMA)*** широкий диапазон частот делится на узкие поддиапазоны, и каждый пользователь передает речь и данные в предоставленном ему поддиапазоне. Все пользователи передают свои сигналы одновременно (рис. 7.9).

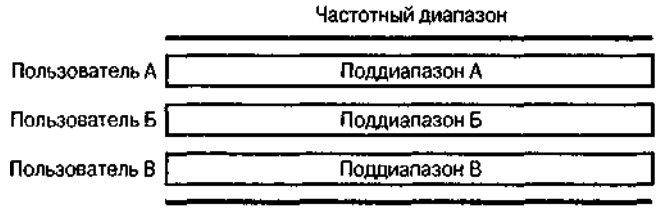

Рис. 7.9. FDMA обеспечивает одновременную передачу, поскольку каждому пользователю выделяется своя часть частотного спектра

Обычные сотовые системы связи используют технологию FDMA для отправки данных.

Множественный доступ с временным разделением каналов

Множественный доступ с временным разделением каналов (time division multiple access, TDMA) обеспечивает разделение сигналов пользователей за счет того, что в каждый момент времени передачу может осуществлять только один из них (рис. 7.10). Каждому пользователю для передачи выделяется определенный временной интервал. Некоторые старые телекоммуникационные операторы используют TDMA для передачи речи и данных через беспроводные глобальные сети. Например, в линиях связи T-1 по технологии TDMA осуществляются соединения нескольких пользователей с помощью одного канала.

Рис. 7.10. При использовании технологии TDMA пользователи могут осуществлять передачу только в отведенные для них промежутки времени

Многостанционный доступ с кодовым разделением каналов

Аналогично технологии TDMA, *многостанционный доступ с кодовым разделением каналов (code division multiple access, CDMA)* позволяет одновременно передавать несколько сигналов (рис. 7.11). Но разница в том, что все пользователи технологии CDMA могут одновременно осуществлять передачу во всем частотном диапазоне и не испытывают воздействия помех, поскольку каждый из них модулирует свой сигнал, используя отличный от других код. Преимуществом технологии CDMA является то, что каждое пользовательское устройство может соединяться со многими базовыми станциями, поскольку используются различные коды. Благодаря этому повышаются производительность и надежность. Сотовые системы преимущественно используют беспроводные сети с технологией CDMA.

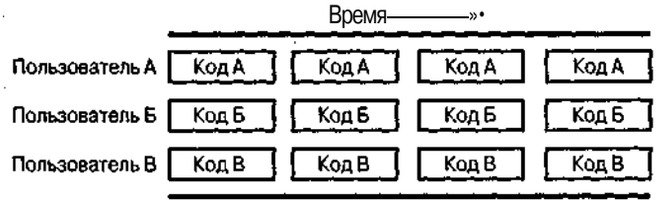

Рис. 7.11. При использовании CDMA каждому пользователю выделяется свой код, благодаря чему передача осуществляется одновременно и без создания взаимных помех

Множественный доступ с пространственным разделением

При применении технологии множественного доступа с пространственным разделением (space division multiple access, SDMA) на устройстве каждого пользователя фокусируется свой пучок излучения. Обычно эта технология применяется в спутниковых системах. Некоторые системы SDMA относятся к числу адаптивных, т.е. радиолуч отслеживает перемещения пользователя. Другие системы требуют повторной привязки пользователя к следующему лучу, если он вышел из зоны действия предыдущего.

Некоторые устройства беспроводных глобальных сетей способны работать в нескольких режимах или частотных диапазонах, поддерживая несколько технологий связи. Так, в одном мобильном телефоне могут поддерживаться режимы TOMA и CDMA. Телефон автоматически переходит от использования одной технологии к другой — в зависимости от того, какая сеть в данный момент доступна.

Резюме

В состав беспроводных глобальных сетей входят мачты сотовой связи, параболические антенны, спутники и телекоммуникационная инфраструктура. Для выполнения большинства приложений беспроводных глобальных сетей требуется установление соединений вне помещений, но некоторые беспроводные глобальные сети развертываются и внутри помещений, таких как аэропорты и конференц-залы. Инфраструктура беспроводной глобальной сети стоит дороже, чем у других беспроводных сетей, но глобальные сети способны обеспечивать связь в масштабах стран и континентов. Наиболее распространенными формами современных беспроводных глобальных сетей, обеспечивающих умеренную производительность, являются сотовая и спутниковая системы. Метеорная связь обходится дешевле, но скорость передачи при этом весьма низкая.

Вопросы для самопроверки

Ответы на эти вопросы вы можете найти в приложении А.

1. Пользовательские устройства каких типов чаще других применяются в беспроводных глобальных сетях?
2. Почему операторы беспроводных глобальных сетей всегда взимают плату за свои услуги?
3. Почему нужно быть особенно внимательным при покупке беспроводной радиоплаты интерфейса сети для пользовательского устройства, предназначенного для работы в беспроводной глобальной сети?
4. Каковы преимущества спутниковой системы?
5. Сотовые системы какого поколения обеспечивают передачу данных со скоростью 2 31бит/с?
6. Системы беспроводных глобальных сетей какого типа наиболее распространены?

7. Какая из двух сотовых систем обеспечивает более высокие скорости передачи данных — GPRS или UMTS?
8. В чем состоит основная проблема метеорной связи?
9. Верно ли, что при использовании технологии доступа с частотным уплотнением пользователи должны поочередно передавать сигналы?
10. За счет чего при использовании технологии CDMA обеспечивается отсутствие взаимных помех?

В этой главе...

сущность проблем, связанных с безопасностью;

методы их решения;

основы технологий и стандарты шифрования и аутентификации.

ГЛАВА 8

Безопасность беспроводных сетей: способы защиты информации

Безопасность жизненно важна для беспроводных сетей, так как коммуникационные сигналы при их распространении через радиоэфир доступны для перехвата. Компании и индивидуальные пользователи должны осознавать потенциально существующие проблемы и принимать контрмеры. В этой главе рассмотрены угрозы безопасности и способы защиты беспроводных сетей за счет использования *шифрования* ***(encryption)*** и *аутентификации* ***(authentication)***.

Угрозы безопасности

Существует несколько форм угрозы безопасности беспроводных сетей (рис. 8.1). Так, *хакеры* ***(hackers)*** могут похитить информацию компании, получив неавторизованный доступ к ее приложениям, и даже нарушить работу сети.

Рис. 8.1. Угрозы безопасности беспроводной сети включают пассивный мониторинг, неавторизованный доступ и отказ в обслуживании (DoS)

Мониторинг трафика

Опытный хакер или даже случайный *снупер*[1] *(snooper)* может легко отследить пакеты незащищенной беспроводной сети, используя такие программные средства, как AirMagnet и AiroPeek, полностью раскрывающие содержимое пакетов данных беспроводной сети. Например, снуперы, находясь в нескольких сотнях метров от здания, в котором функционирует беспроводная локальная сеть, в силах отследить все транзакции, выполняемые в беспроводной части сети. Конечно, основная угроза состоит в том, что в результате атаки кто-то может овладеть важной информацией — узнать имена пользователей, пароли, номера кредитных карт и т.д.

Решение этой проблемы состоит в применении, к&к минимум, шифрования информации, передаваемой между беспроводным клиентским устройством и базовой станцией. В процессе шифрования биты данных изменяются с помощью секретного ключа. Поскольку ключ секретный, хакер не может дешифровать данные. Поэтому за счет использования эффективных механизмов шифрования можно повысить защищенность данных.

Неавторизованный доступ

Аналогично проведению мониторинга выполняемых в сети приложений некто может без особых усилий, если не приняты должные меры предосторожности, получить доступ к корпоративной беспроводной сети, находясь вне помещения, где она развернута. Кто-то может, например, сидя в припаркованном неподалеку автомобиле, привязаться к одной из расположенных в здании базовых станций. Если не обеспечена должная защита, такой человек получает доступ к серверу и приложениям, выполняемым в корпоративной сети. Это равносильно появлению незнакомца в вашем доме или офисе.

К сожалению, многие компании развертывают свои беспроводные сети, используя конфигурацию базовых станций, установленную по умолчанию и не обеспечивающую нужного уровня защиты, что предопределяет беспрепятственное взаимодействие с сервером приложений. Вас, наверное, удивит это, но 30% точек доступа беспроводных сетей среднестатистического города не применяют никаких мер безопасности. Это значит, что кто угодно может получить доступ к жестким дискам или воспользоваться соединением с Internet.

Операционная система Windows XP позволяет легко устанавливать взаимодействие с беспроводными сетями, особенно с общедоступными локальными. Когда ноутбук привязывается к беспроводной локальной сети, его владелец получает доступ к любому другому ноутбуку, привязавшемуся к той же беспроводной локальной сети. Если не применен персональный брандмауэр, кто угодно может ознакомиться с содержимым жесткого диска любого такого ноутбука, а это огромная угроза безопасности данных.

Если даже в точках доступа задействованы механизмы защиты, существенную угрозу представляет возможность подключения к *подставной точке доступа (rogue access point)*. Такая точка представляет собой неавторизованную точку доступа, включенную в сеть (рис. 8.2). Какой-нибудь служащий может приобрести точку дос-

[1] *От англ, snoop — тот, кто подглядывает, подсматривает, сует нос в чужие дела.* — Прим. ред.

тупа и установить ее в своем офисе, не понимая, каковы последствия этого для безопасности сети. Хакер также может разместить точку доступа в здании, умышленно подключив незащищенную точку доступа к корпоративной сети.

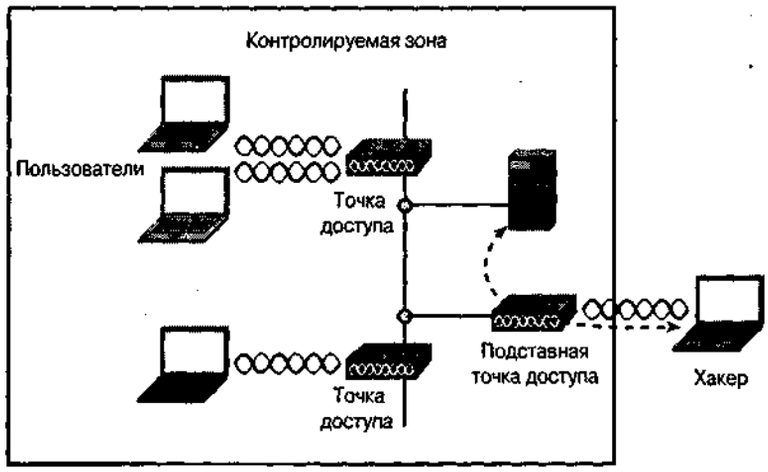

Рис. 8.2. Подставная точка доступа предоставляет открытый порт для хакеров

В подставной точке доступа, как правило, не активизируется система шифрования, и она будет представлять собой открытую дверь для любого, кто захочет получить доступ к корпоративной сети, находясь вне здания. Поэтому компании должны постоянно проверять наличие подставных точек доступа. Эта проблема актуальна независимо от того, установлена беспроводная сеть или нет. Кто-то может подключить подставную точку доступа и к полностью проводной сети Ethernet.

Для противодействия неавторизованному доступу в беспроводной сети используется взаимная аутентификация, осуществляемая между клиентскими устройствами и точками доступа. Аутентификация — это подтверждение идентичности пользователя или устройства. В беспроводной сети должны применяться методы, позволяющие базовой станции удостовериться в идентичности клиента, и наоборот. Это позволяет удостовериться в "законности" пользователя и в том, что он устанавливает соединение с легитимной точкой доступа. Кроме того, точки доступа должны проходить процедуру аутентификации на коммутаторах, что исключает появление в сети подставных точек доступа.

Атаки типа "человек посредине"

Благодаря использованию механизмов шифрования и аутентификации повышается безопасность беспроводной сети, однако опытные хакеры отыскивают слабые места, зная, как работают протоколы сети. Определенную опасность представляют атаки типа "человек посредине" (man-in-the-middle attacks): хакер размещает фиктивное устройство между легальным пользователями и беспроводной сетью (рис. 8.3). Например, при осуществлении стандартной атаки типа "человек посредине" используется протокол преобразования адресов (address resolution protocol, ARP), используемый во всех сетях TCP/IP. Хакер, вооруженный необходимыми программными средствами, может, воспользовавшись ARP, получить контроль над беспроводной сетью.

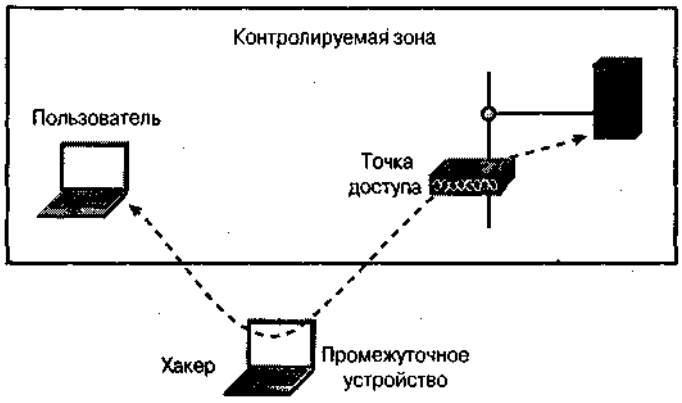

Рис. 8.3. Промежуточное устройство позволяет провести атаку типа "человек посредине"

ARP позволяет выполнять важную функцию путем отправки проводной или беспроводной платой интерфейса сети запроса с целью выявления физического адреса платы интерфейса сети в месте назначения. Физический адрес платы — это то же самое, что MAC-адрес, который присвоен плате ее производителем и отличается от адреса любого другого компонента сети, т.е. он уникален. MAC-адрес — это аналог почтового адреса вашего дома. Подобно тому как кто-то должен знать адрес вашего дома, чтобы послать вам письмо, так передающая плата интерфейса сети должна знать MAC-адрес получателя. Эта плата распознает и реагирует только на физический MAC-адрес.

Прикладные программы, нуждающиеся в передаче данных, должны иметь IP-адрес получателя, а передающая плата интерфейса сети использует протокол ARP для выявления соответствующего физического адреса. Она получает нужный ей адрес, рассылая широковещательные ARP-пакеты, в которых объявляется IP-адрес платы интерфейса сети получателя. Все станции слышат этот запрос, и станция с соответствующим IP-адресом должна возвратить пакет ответа по протоколу ARP, содержащий ее MAC- и IP-адреса.

Затем передающая станция включает этот MAC-адрес в передаваемый фрейм в качестве адреса получателя, а также сохраняет соответствующие MAC- и IP-адреса, помещая их в таблицу на некоторый период времени (до тех пор, пока станция не получит другой ARP-ответ от станции, имеющей этот IP-адрес).

Проблема, связанная с протоколом ARP, состоит в том, что он представляет опасность для системы защиты из-за возможности спуфинга[2]. Так, хакер может ввести в заблуждение станцию, посылая ей через подставное сетевое устройство фиктивный ARP-ответ, содержащий IP-адрес легитимного сетевого устройства и MAC-адрес подставного. Это приведет к тому, что все легитимные станции сети автоматически обновят свои ARP-таблицы, внеся в них ложные данные. В результате станции будут передавать пакеты подставному устройству, а не легитимной точке доступа или маршрутизатору. Это и есть классическая атака типа "человек посредине", в результате которой хакер получает возможность управлять сеансами связи пользователя. Он получит пароли, важные данные и даже сможет взаимодействовать с корпоративными серверами, как если бы он был легитимным пользователем.

[1] *От англ, spoofing — имитация соединения, получение доступа обманным путем.* — Прим. ред.

Для предотвращения атак с использованием спуфинга ARP поставщики (например, компания OptimumPath) предлагают защищенный ARP (secure ARP, SARP). Этот усовершенствованный ARP обеспечивает специальный защищенный туннель между каждым клиентом и беспроводной точкой доступа или маршрутизатором, который игнорирует все ARP-ответы, не связанные с клиентом, находящимся на другом конце этого туннеля. Следовательно, только легитимные ARP-ответы будут служить основанием для обновления ARP-таблиц. Станции, применяющие протокол SARP, не подвержены спуфингу.

Однако для использования протокола SARP на каждом клиентском устройстве нужно установить специальное программное обеспечение. Поэтому SARP не подходит для общедоступных "горячих точек". Но предприятия могут установить SARP на своих клиентских устройствах, обезопасив тем самым свою сеть от атак типа "человек посредине".

Отказ в обслуживании

Атака типа "отказ в обслуживании" (denial ofservice, DoS) — это нападение, в результате которого беспроводная сеть приходит в негодность или ее работа блокируется. Возможность такой атаки должен учитывать каждый, развертывающий беспроводную сеть. Следует обязательно подумать о том, что произойдет, если сеть станет недоступной на неопределенный период времени.

Серьезность DoS-атаки зависит от того, к каким последствиям может привести выход из строя беспроводной сети. Например, хакер может сделать недоступной беспроводную локальную сеть, развернутую в доме, но результатом этого будет лишь беспокойство домовладельца. А вот отказ в обслуживании беспроводной системы инвентаризации предприятия приведет к существенным финансовым потерям.

Одной из разновидностей DoS-атак является метод грубой силы (brute-force attack). Массовая рассылка пакетов, для которой задействуются все ресурсы сети, в результате чего она прекращает работу — • это вариант DoS-атаки, выполненной методом грубой силы. В Internet можно найти программные средства, позволяющие хакерам вызывать интенсивную передачу пакетов в беспроводная сетях. Хакер может провести DoS-атаку методом грубой силы путем отправки бесполезных пакетов серверу с других компьютеров сети. Это вызывает существенные непроизводительные расходы в сети и не позволяет использовать ее пропускную способность легитимным пользователям.

Другим способом приостановки работы большинства беспроводных сетей, особенно тех, в которых используется *метод обнаружения несущей (carrier sense access)* является использование мощного радиосигнала, заглушающего все остальные и делающего таким образом точки доступа и радиоплаты бесполезными. Протоколы, такие как 802.lib, очень "вежливые" и позволяют сигналу DoS-атаки иметь доступ к среде передачи столь долго, сколько захочется хакеру.

Однако попытка проведения атаки на сеть с использованием мощного радиосигнала может оказаться весьма рискованной для хакера. Поскольку для проведения такой атаки мощный передатчик должен располагаться в непосредственной близости от помещения, в котором развернута беспроводная сеть, ее владелец может обнаружить хакера, используя средства обнаружения, входящие в состав сетевых анализаторов. После того как источник преднамеренных помех будет найден, его владельцу придется прекратить атаку и даже, возможно, сесть на скамью подсудимых.

Иногда отказ в обслуживании беспроводной сетью возникает вследствие непреднамеренных действий. Так, сети стандарта 802.11Ь работают в переполненном спектре частот, а такие устройства, как беспроводные телефоны, микроволновые печи и устройства Bluetooth, могут вызвать существенное снижение производительности сетей этого стандарта. Помехи же могут вообще воспрепятствовать работе сети.

Кроме того, превосходной целью для DoS-атак могут служить некоторые механизмы защиты сети. Например, механизм защищенного доступа к Wi-Fi (Wi-Fi protected access, WPA) уязвим для атак типа "отказ в обслуживании". WPA использует математический алгоритм для аутентификацию пользователей сети. Если какой-то пользователь попытается получить к ней доступ и пошлет два пакета неавторизованных данных в течение одной секунды, WPA сочтет, что стал объектом атаки, и прекратит работу сети.

Наиболее эффективный способ противодействия атакам типа "отказ в обслуживании" — это изоляция вашего компьютера в тщательно охраняемой комнате и отключение его от всех сетей, включая Internet. Но это невозможно в отношении беспроводных сетей. Правительство США использует этот метод для защиты своих наиболее важных данных, но это решение неприемлемо для предприятий и домашнего применения, где можно получить существенные выгоды от развертывания беспроводной сети.

Наиболее действенной защитой от DOS-атак является разработка и соблюдение строгих правил безопасности. Такие действия, как установка и обновление брандмауэров, постоянно обновляемые антивирусные средства, установка свежих "заплат", ликвидирующих бреши в системе безопасности, использование длинных паролей и отключение неиспользуемых сетевых устройств должны стать повседневной практикой для всех компаний и домовладельцев.

Можно защитить беспроводную сеть от атак типа "отказ в обслуживании", обеспечив сопротивляемость зданий проникновению в них радиосигналов извне. Вот некоторые рекомендации, следуя которым можно уменьшить поток радиосигналов в помещение:

- если внутренние стены имеют металлические стойки и косяки, заземлите их;
- установите термоизолирующие, покрытые медной или металлической пленкой окна;
- вместо жалюзи и занавесок можно стекла металлизировать;
- для внутренних и наружных стен используйте краски с примесью металлов;
- проведите тестирование, чтобы определить степень просачивания сигнала наружу. Отрегулируйте мощность передатчика таким образом, чтобы полностью устранить утечку сигнала или снизить его уровень до тех значений, при которых можно будет легко выявить хакера;
- используйте направленные антенны, посылающие сигнал внутрь помещений.

Универсального способа противодействия DoS-атакам всех типов не существует. Поэтому, если в результате атаки сеть все же вышла из строя, следует обеспечить переход к пакетной обработке. Или работайте с бумажными документами, если приложения невозможно использовать в результате серьезной DoS-атаки. Вы ведь не хотите, чтобы из-за потенциальной уязвимости беспроводной сети ваша компания разорилась?

Шифрование

Шифрование изменяет биты каждого пакета данных с тем, чтобы злоумышленник не смог их декодировать и узнать, например, номера кредитных карт. Незашифрованные данные называют открытым текстом (plaintext), который легко декодировать, используя средства для пассивного прослушивания сети. В процессе шифрования открытый текст превращается в зашифрованный, а его декодировать можно только с помощью секретного ключа.

Многие методы шифрования, такие как метод WEP стандарта 802.11, гарантирующий *защищенность, эквивалентную таковой проводных сетей (wired equivalent privacy, WEP),* являются симметричными. Это означает, что для шифрования и дешифрования используется один и тот же ключ (рис. 8.4).

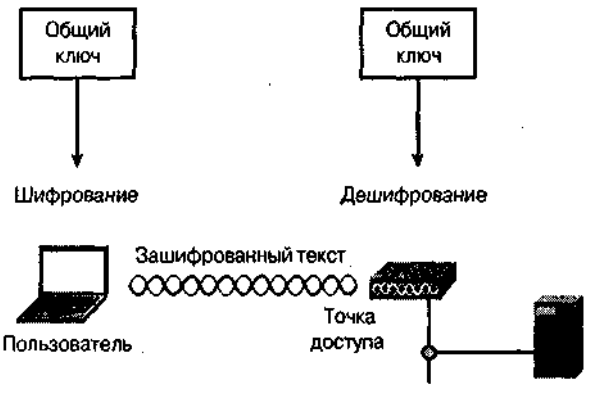

Рис. 8.4. При симметричном шифровании используется общий ключ

Например, радиоплата интерфейса сети может использовать ключ xyz для шифрования пакета данных, а точка доступа с помощью ключа xyz выполнит его дешифрование. Для этого требуется, чтобы передающая и приемная станция доверяли одна другой, что и бывает в случае применения частной беспроводная сети, такой, например, как беспроводная сеть предприятия. Однако нет смысла применять симметричные ключи в общедоступных сетях, поскольку его может получить любой абонент, в том числе и хакер.

Для того чтобы симметричное шифрование было эффективным, следует минимизировать повторное использование ключа за счет его частой замены, желательно при передаче каждого фрейма. Это увеличивает время, необходимое хакеру для проникновения в сеть, и затрудняет (или делает вообще невозможным) нарушение системы защиты сети. Поэтому механизмы симметричного шифрования должны дополняться эффективными методами распределения ключей.

Криптография с открытым ключом основана на использовании асимметричных ключей, один из которых является секретным, а другой — открытым. Как следует из названия, секретный ключ доступен только его владельцу, в то время как открытый ключ известен каждому. Это позволяет создать более эффективные механизмы шифрования и аутентификации, поскольку упрощаются методы распределения открытого ключа.

Важным требованием, предъявляемым к методам шифрования с открытым ключом, является следующее: пара "секретный ключ — открытый ключ" должна быть равноправной с криптографической точки зрения. Например, передающая станция может зашифровать данные с помощью открытого ключа, тогда приемная станция воспользуется своим секретным ключом, чтобы расшифровать данные. Противоположный вариант также возможен. Передающая станция зашифровывает данные с помощью своего секретного ключа, а приемная станция, воспользовавшись открытым ключом, расшифровывает данные.

Если целью является шифрование данных, передающая станция будет использовать открытый ключ для шифрования данных перед их передачей (рис. 8.5). Приемная станция воспользуется соответствующим открытому секретным ключом для дешифровки полученных данных. Каждая станция скрывает свой секретный ключ от других, чтобы не подвергать опасности несанкционированного дешифрования зашифрованную информацию. Поэтому описываемый процесс позволяет любой станции использовать всем известный ключ для отправки зашифрованных данных любой другой станции.

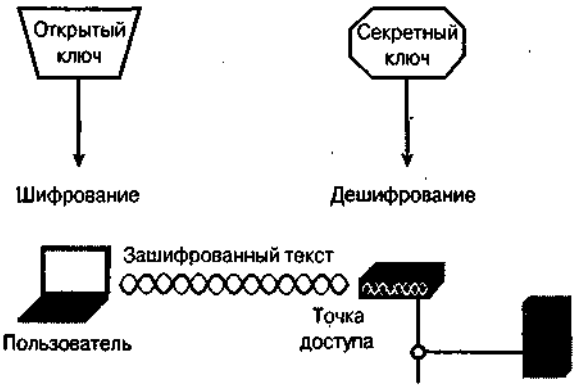

Рис. 8.5. Шифрование с открытым ключом позволяет всем отправителям зашифрованных данных использовать публично объявленный ключ

Криптография с открытым ключом эффективна для шифрования данных, поскольку открытый ключ свободно передается каждому, кто желает передать зашифрованные данные определенной станции. Станция, генерирующая новый секретный ключ, может передать соответствующий ему открытый ключ по сети любому, не опасаясь за свои шифруемые данные. Открытый ключ может быть размещен на Web-сайте или передан в незашифрованном виде через сеть.

WEP

WEP — это опциональный стандарт шифрования и аутентификации стандарта 802 11, применяемый на уровне MAC; его поддерживают радиоплаты интерфейса сети и точки доступа многих производителей. При развертывании беспроводной сети следует четко знать, какие возможности предоставляет WEP для повышения ее защищенности.

Как работает WEP?

Если пользователь активизирует механизм WEP, то до момента передачи плата интерфейса сети шифрует полезную нагрузку (тело фрейма и биты контроля) каждого фрейма стандарта 802.11. Контроль осуществляется с помощью циклического избыточного кода (cyclical redundancy check, CRC). При передаче используется поточный механизм шифрования RC4, обеспечиваемый системой защиты RSA[3]. Приемная станция (например, точка доступа или другая радиоплата интерфейса сети) дешифрует полученный фрейм. Следовательно, WEP стандарта 802.11 шифрует только данные, передаваемые между станциями стандарта 802.11. Как только фрейм поступает в проводную часть сети, как это бывает при передаче его от одной точки доступа к другой, WEP уже не работает.

Будучи частью процесса шифрования, WEP готовит последовательность ключей (задавая начальное число последовательности псевдослучайных чисел) путем связывания совместно используемого секретного ключа, применяемого пользователем передающей станции, с генерируемым случайным образом 24-разрядным вектором инициализации (initialization vector, IV). Таким образом вектор инициализации продлевает срок жизни секретного ключа, поскольку станция может изменять IV при передаче каждого фрейма. WEP вводит получившееся начальное число в генератор псевдослучайных чисел, который производит ключевой поток, равный длине полезной нагрузки фрейма, дополненной 32-разрядным контрольным признаком целостности (integrity check value, ICV), который представляет собой контрольную сумму. Приемная станция повторно вычисляет эту контрольную сумму и сравнивает ее с суммой, полученной от передающей станции. Благодаря этому можно определить, подвергались ли данные в процессе передачи какой-либо фальсификации. Если вычисленный приемной станцией ICV не соответствует содержащемуся во фрейме, приемная станция отбрасывает такой фрейм или сообщает об этом пользователю.

WEP регламентирует применение общего секретного ключа для шифрования и дешифрования данных. В случае использования WEP приемная станция должна использовать для дешифрования тот же самый ключ. Следовательно, каждая радиоплата интерфейса сети и точка доступа должны быть сконфигурированы вручную с одним и тем же ключом.

До начала передачи WEP комбинирует ключевой поток с полезной нагрузкой/ICV в ходе поразрядного выполнения операции "исключающее ИЛИ", в результате которой и получается зашифрованный текст (зашифрованные данные). WEP включает вектор инициализации в чистом (незашифрованном) виде в первые несколько разрядов тела фрейма. Приемная станция использует этот вектор инициализации совместно с общим секретным ключом, который "знает" приемная станция пользователя, для дешифрования части фрейма, содержащей полезную нагрузку.

В большинстве случаев передающая станция использует новый вектор инициализации при передаче каждого фрейма (хотя этого и не требует стандарт 802.11). При передаче сообщений, имеющих стандартное начало (например, адрес отправителя в электронном письме), начало каждой зашифрованной полезной нагрузки будет эквивалентным, если используется один и тот же ключ. После шифрования данных начальные фрагменты этих фреймов будут одинаковыми. Хакеры, анализируя их, могут взломать алгоритм

[3] ***Схема*** *RSA-шифрования — алгоритм асимметричного шифрования с открытым ключом. Назван по фамилиям авторов: Rivest — Shamir — Adelman (Рои Райвест, Ади Шамир и Леонард Эйдельман), разработавших эту схему шифрования в 1978 г.* — Прим. ред.

шифрования. Поскольку вектор инициализации различен для большинства фреймов, WEP устойчив против атак такого типа. Быстрая смена вектора инициализации также улучшает способность WEP противостоять утечкам конфиденциальной информации.

Проблемы, связанные с WEP

Но все равно WEP остается уязвимым, потому что используются относительно короткие векторы инициализации и неизменные ключи. По сути, проблемы, связанные с применением WEP, обусловлены использованием алгоритма шифрования RC4. Используя всего лишь 24-разрядный вектор инициализации (IV), WEP рано или поздно воспользуется тем же IV для другого пакета данных. В большой, активно используемой сети это повторение IV может произойти в течение часа или около того, что приводит к передаче фреймов, имеющих очень похожие ключевые потоки. Если хакер наберет достаточно фреймов, основанных на одном и том же IV, он сможет определить совместно используемые ими значения, т.е. ключевой поток или совместно используемый секретный ключ. А это, в свою очередь, приведет к тому, что хакер сможет расшифровать любой из фреймов стандарта 802.11.

Статическая природа совместно используемого секретного ключа усугубляет эту проблему. Стандарт 802.11 не предлагает каких-либо функций, обеспечивающих обмен ключами между станциями. Поэтому системные администраторы и пользователи применяют одни и те же ключи на протяжении недель, месяцев и даже дней. Это и дает возможность преступникам достаточно времени для мониторинга использующих механизм WEP сетей и проникновения в них.

Когда можно использовать WEP?

Несмотря на недостатки WEP, его следует применять для обеспечения хотя бы минимального уровня безопасности. Многие имеют открытые беспроводные сети, в которых используются анализаторы протокола, такие как AiroPeek и AirMagnet. Такие люди могут выявить беспроводные сети, в которых не используется WEP, а затем с помощью ноутбука получить доступ к ресурсам незащищенной сети.

Однако, за счет активизации механизма WEP, такая возможность существенно минимизируется, особенно это актуально для домашних сетей или сетей небольших фирм. WEP — хороший способ сдерживать любопытных. Но настоящие хакеры, воспользовавшись слабостями WEP, смогут получить доступ к сети даже с активизированным механизмом WEP, особенно это касается активно используемых сетей.

Временный протокол целостности ключа

Стандарт 802. Hi позволяет повысить защищенность беспроводных локальных сетей. Одно из нововведений — временный протокол целостности ключа (temporal key integrity protocol, TKIP), который первоначально назывался WEP2. Протокол TKIP — это частное решение, основанное на использовании временного 128-разрядного ключа, совместно используемого клиентами и точками доступа. TKIP комбинирует временный ключ с MAC-адресом клиентского устройства, а затем добавляет относительно длинный 16-октетный вектор инициализации для создания ключа, посредством которого будут шифроваться данные. Эта процедура гарантирует, что каждая станция будет использовать различные ключевые потоки для шифрования данных.

TKIP использует RC4 для шифрования, что аналогично применению WEP. Основное отличие от WEP состоит в том, что TKIP изменяет временные ключи после

передачи каждых 10 тыс. пакетов. Это дает динамический метод распределения, благодаря чему значительно повышается безопасность сети.

Преимущество применения TKIP состоит в том, что компании, уже имеющие основанные на механизме WEP точки доступа и радиоплаты интерфейса сети, могут модернизировать их до уровня TKIP с помощью относительно простых, встраиваемых "заплаток". Кроме того, оснащенное только WEP оборудование сможет взаимодействовать с TKIP-устройствами, используя WEP. Однако, по мнению многих экспертов, TKIP — это временное решение, и необходимы более сильные методы шифрования.

Помимо временного решения TKIP, стандарт 802.1 П содержит протокол улучшенного стандарта шифрования (advanced encryption standard, AES)>, который обеспечивает более надежное шифрование. Протокол AES использует алгоритм шифрования Rine Dale[4], который обеспечивает существенно более надежное шифрование, чем заменяемый им алгоритм RC4. Многие криптографы считают, что AES вообще невозможно взломать. Кроме того, стандарт 802.111 будет включать AES как опциональный, используемый поверх TKIP. Поэтому организация коммерческого подразделения Национального института стандартов и технологий США (U.S. Commerce Department's National Institutes of Standards and Technology, NIST) выбрала AES для замены устаревшего Стандарта шифрования данных (Data encryption standard, DES). Сейчас AES является федеральным стандартом обработки информации. Он определен как алгоритм шифрования для использования правительственными организациями США для защиты важных, но несекретных сведений. Министр торговли одобрил принятие AES в качестве официального правительственного стандарта в мае 2002 г.

Проблема, связанная с AES, состоит в том, что для его реализации требуется большая вычислительная мощность, чем та, которой обладают большинство точек доступа, предлагаемых сегодня на рынке. Поэтому компаниям для применения AES придется модернизировать аппаратное обеспечение своих беспроводных локальных сетей, чтобы оно поддерживало производительность, необходимую для применения алгоритма AES. Трудность заключается в том, что для работы AES необходим сопроцессор (дополнительное аппаратное обеспечение). Фактически это означает, что ради применения AES компаниям придется заменить имеющиеся у них точки доступа и клиентские платы интерфейса сети.

Защищенный доступ к Wi-Fi

Стандарт на защищенный доступ к Wi-Fi (Wi-Fi protected access, WPA), предложенный Альянсом Wi-Fi, обеспечивает модернизацию WEP за счет одновременного использования метода шифрования с динамическим ключом и взаимной аутентификации. Большинство поставщиков беспроводных сетей сейчас поддерживают WPA. Клиенты WPA используют различные ключи шифрования, которые периодически меняются. Из-за этого взломать алгоритм шифрования намного сложнее.

По сути, WPA 1.0 представляет собой текущую версию стандарта 802.11 i, который включает механизмы TKIP и 802.1x. За счет комбинации этих двух механизмов обеспечивается шифрование с динамичным ключом и взаимная аутентификация, т.е. то, что необходимо для беспроводных локальных сетей. WPA 2.0 полностью совместим со стандартом 802.1 П.

По другим источникам, алгоритм Rijndael (читается "рейн-долл") разработан бельгийскими криптографами Джоаном Дименом (Joen Daemer) и Винсентом Риджменом (Vincent Rijmen). — Прим. ред.

Виртуальные частные сети

Находясь в аэропорту или гостинице, обратите внимание на *виртуальные частные сети* ***(virtualprivate network,*** *VPN).* Даже при сегодняшней недостаточной надежности, они обеспечивают эффективные средства сквозного (end-to-end) шифрования. Виртуальные частные сети эффективны также в тех случаях, когда клиенты перемещаются в зонах действия сетей различных типов, поскольку их работа осуществляется поверх разнородных уровней соединения сетей.

Аутентификация

В беспроводной сети важно использовать взаимную аутентификацию. Благодаря ей можно решить многие проблемы, связанные с безопасностью, например, успешно противостоять атакам типа "человек посредине". При взаимной аутентификации беспроводной клиент и беспроводная сеть доказывают свою идентичность друг другу (рис. 8.6). В ходе этого процесса используется сервер аутентификации, такой как RADIUS (remote authentication dial-in user service — служба дистанционной аутентификации пользователей по коммутируемым линиям, протокол RADIUS).

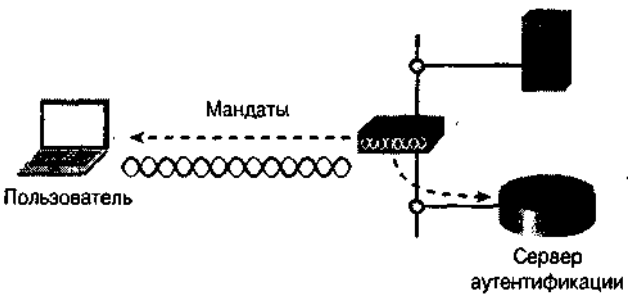

Рис. 8.6. При аутентификации проверяется идентичность пользователя и клиентского устройства по "мандатам"— паролю и цифровому сертификату

Уязвимость механизма аутентификации стандарта 802.11

WEP обеспечивает только метод аутентификации радиоплаты интерфейса сети точкой доступа, обратная операция не выполняется. Поэтому хакер может перенаправить данные по иному пути, обойдя тем самым другие механизмы защиты. Чтобы пресечь такую возможность, в беспроводных сетях должна применяться не односторонняя, а взаимная аутентификация.

Когда беспроводной клиент переходит в активное состояние, он начинает искать среду передачи по маячковым сигналам, рассылаемым точками доступа. По умолчанию точка доступа рассылает в широковещательном режиме маячковые сигналы, содержащие идентификатор зоны обслуживания (service set identifier, SSID) точки доступа, а также другие параметры. Точка доступа разрешает привязку только в том случае, если SSID клиента соответствует SSID точки доступа. Это и является основной (хотя и слабой) формой аутентификации.

Уязвимость этого процесса обусловлена в основном тем, что SSID посылается в незашифрованном виде, а это делает его видимым для программ наблюдения[5] за беспроводными пакетами. Поэтому хакер может легко обнаружить SSID в маячковом фрейме и аутентифицироваться в беспроводной сети. Если даже точка доступа не установлена в режим широковещательной передачи SSID (для некоторых точек доступа опционально предусмотрена такая возможность), программы наблюдения все равно смогут получить SSID из фреймов запроса на ассоциирование (привязку), посылаемых клиентскими устройствами точке доступа.

Стандарт 802.11 по умолчанию предлагает форму аутентификации, получившую название *"система открытой аутентификации"*. При работе в этом режиме точка доступа гарантирует выполнение любого запроса на аутентификацию. Клиент просто посылает фрейм запроса на аутентификацию, а точка доступа дает в ответ "добро". Это позволяет любому, знающему корректный SSID, привязаться к точке доступа.

Стандарт 802.11 также регламентирует (опционально) аутентификацию с совместно используемым ключом, которая является более совершенной формой аутентификации. Процесс ее выполнения осуществляется в четыре этапа:

1) клиент посылает фрейм запроса на аутентификацию;
2) точка доступа отвечает фреймом, содержащим строку текста, называемую "текст вызова" (challenge text);
3) клиент шифрует текст вызова, используя общий ключ шифрования WEP, а затем посылает зашифрованный текст вызова обратно точке доступа, которая дешифрует этот текст, используя общий ключ, и сравнивает результат с посланным ею текстом вызова;
4) если тексты совпадают, точка доступа аутентифицирует клиента.

Этого вполне достаточно с точки зрения аутентификации, но проблема состоит в том, что совместно используемый ключ аутентификации доказывает лишь то, что клиент имеет корректный WEP-ключ.

MAC-фильтры

Некоторые беспроводные базовые станции предлагают фильтрацию на уровне управления доступом к среде (MAC-уровне). В случае применения MAC-фильтрации точка доступа проверяет MAC-адрес источника каждого получаемого ею фрейма и отказывается принимать фреймы с MAC-адресом, не соответствующим ни одному из особого списка, программируемого администратором. Следовательно, MAC-фильтрация обеспечивает простейшую форму аутентификации.

Однако MAC-фильтрация имеет и слабые места. Например, при WEP-шифровании значение поля фрейма, содержащего MAC-адрес, не шифруется. Это позволяет хакеру пронаблюдать за передачей фреймов и выявить действующие MAC-адреса. Или он может воспользоваться свободно распространяемым программным обеспечением для замены MAC-адреса своей радиоплаты интерфейса сети на такой, который соответствует действующему MAC-адресу. Это позволит хакеру прикинуться законным пользователем сети и "обмануть" точку доступа в период, когда легальный пользователь в сети отсутствует.

[5] *Профессионалы такие программы называют снифферами (от англ, sniffer).* — Прим. ред.

Кроме того, поддерживать механизм MAC-фильтрации в сети со многими пользователями — весьма утомительное занятие. Администратор должен внести запись с MAC-адресом каждого пользователя в таблицу и производить в ней изменения по мере появления в сети новых пользователей. Например, служащему другой компании может понадобиться доступ к беспроводной локальной сети предприятия во время визита. Администратору придется определить MAC-адрес компьютерного устройства визитера и ввести его в систему, только после этого посетитель сможет получить доступ к сети. Фильтрация на уровне MAC-адресов приемлема в домашних сетях и сетях небольших офисов, но такой подход нежелателен для администраторов беспроводных сетей предприятий, поскольку в основе лежит "ручное" программирование.

Аутентификация с использованием открытого ключа шифрования

В дополнение к средствам защиты информации от хакеров станции могут использовать метод криптографии с открытым ключом для аутентификации их другими станциями или точками доступа (рис. 8.7). Это может оказаться необходимым до того, как точка доступа или контроллер позволит определенной станции начать взаимодействие с защищенной частью сети. Аналогичным образом и клиент может аутентифицировать точку доступа. Станция аутентифицирует сама себя путем шифрования строки текста в пакете с помощью секретного ключа. Приемная станция дешифрует текст с помощью открытого ключа передающей станции. Если дешифрованный текст совпадает с каким-то предопределенным текстом, например, именем станции, приемная станция считает передавшую ей фрейм станцию легитимной. В данном случае шифрование определенной строки текста выполняет роль цифровой подписи.

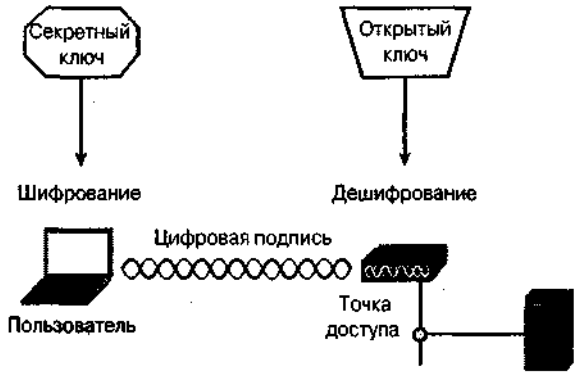

Рис. 8.7. Криптография с открытым ключом позволяет осуществить аутентификацию

Стандарт 802.1x

За счет использования стандарта 802.1x можно заложить основы для эффективной системы автоматической аутентификации и контроля трафика пользователей защищенной сети, а также применять динамически изменяемые ключи шифрования. Стандарт 802.1x применяет расширяемый протокол аутентификации (extensible authentication protocol, EAP) к проводной и беспроводной частям сети и поддержи^

вает методы взаимной аутентификации, такие как "говорящая карта" (token card), Kerberos[6], одноразовые пароли (one-time passwords), сертификаты (certificates) и аутентификацию с открытым ключом (public key authentication).

Как осуществляется аутентификация по стандарту 802.1 x?

В соответствии со стандартом 802.1x связь начинается с того, что проситель (supplicant), т.е. беспроводное клиентское устройство, пытается соединиться с аутентификатором (беспроводной базовой станцией). Базовая станция отвечает просителю, предоставляя ему порт для передачи только EAP-пакетов серверу аутентификации, расположенному в проводной части базовой станции. Но блокирует весь остальной трафик, такой как пакеты HTTP, DHCP и POP3, до тех пор, пока не удостоверится в идентичности клиента с помощью одного из.серверов аутентификации (например, сервера RADIUS). После успешной аутентификации базовая станция открывает порт клиента для всего остального трафика, учитывая при этом права доступа и руководствуясь указаниями сервера аутентификации.

Чтобы досконально разобраться в том, как осуществляется процесс аутентификации в соответствии со стандартом 802.1x, рассмотрим следующие этапы взаимодействия между различными участниками этого процесса:

1) клиент посылает стартовое EAP-сообщение, начинающее серию обменов сообщениями с целью аутентификации клиента. Это аналогично тому, как если бы группа посетителей подошла к центральным воротам тематического парка и руководитель группы (клиент) спросил у привратника, могут ли они войти;
2) базовая станция отвечает сообщением, содержащим запрос на EAP-идентификацию. Продолжая аналогию с тематическим парком, можно сказать, что привратник спрашивает у руководителя группы, как его зовут, и просит предъявить водительские права[7];
3) клиент посылает пакет с EAP-ответом, содержащий необходимые данные для сервера аутентификации. Руководитель группы в нашем примере должен сообщить свое имя и предъявить водительские права; привратник передает эти данные менеджеру экскурсий (серверу аутентификации), который и определяет, имеет ли группа право на экскурсию;
4) сервер аутентификации использует особый алгоритм аутентификации для проверки идентичности клиента. Проверка может осуществляться с использованием цифровых сертификатов или других механизмов аутентификации EAP. В нашем примере это аналогично проверке подлинности водительских прав руководителя группы и сличению фотографии в правах с личностью руководителя. Предположим, что руководитель "авторизован", т.е. оказался тем, за кого он себя выдает;
5) сервер аутентификации посылает базовой станции сообщение с разрешением или отказом. В нашем примере разрешение означает, что менеджер экскурсий тематического парка дает команду привратнику пропустить группу;

[6] *Цербер — название технологии аутентификации и шифрования с открытым ключом, созданной в середине 80-х годов в Массачусетсом технологическом институте (M1T) на базе стандарта DES. — 4*

[7] *В США водительские права во многих случаях заменяют паспорт.* — Прим. ред.

6) базовая станция посылает клиенту пакет с сообщением об успешной аутентификации. Привратник сообщает руководителю, что его группа может войти в парк (но он не пропустит группу, если менеджер экскурсий запретит ей посещение парка);
7) если сервер аутентификации принимает клиента, базовая станция должна перевести выделенный ему порт в авторизованное состояние и обеспечить передачу дополнительного трафика. Это аналогично тому, как если бы привратник автоматически открыл ворота и пропустил в парк только членов группы, получившей право на экскурсию.

Основной протокол стандарта 802.1x обеспечивает эффективную аутентификацию независимо от того, применяете вы WEP-ключи стандарта 802.1x или не используете шифрование вообще. Однако большинство основных поставщиков беспроводных сетей предлагают патентованные версии управления динамическими ключами, используя стандарт 802.1x как механизм их распределения. Будучи сконфигурированным на реализацию обмена динамическими ключами, сервер аутентификации стандарта 802.11 может вернуть базовой станции ключи для сеанса связи, отправляя ей сообщение об успешной аутентификации клиента.

Базовая станция использует ключи сеанса связи для создания, подписания и шифрования с помощью EAP-ключей сообщений, посылаемых клиенту сразу же вслед за сообщением об успешной аутентификации. Клиент может использовать содержимое сообщения с ключами для определения подходящих ключей шифрования. В типичных ситуациях применения стандарта 802.1x клиент может автоматически и часто изменять ключи шифрования с целью минимизации риска того, что злоумышленник получит достаточно времени для взлома текущего ключа.

Типы аутентификации

Отметим, стандарт 802.1x не регламентирует сами механизмы аутентификации. При использовании этого стандарта необходимо выбрать тип EAP. Это может быть протокол защиты транспортного уровня (transport layer security, EAP-TLS), EAP tunneled transport layer security (EAP-TTLS) или облегченная EAP-аутентификация Cisco (lightweight EAP, или LEAP), который и определяет, как будет проводиться аутентификация. Программное обеспечение, поддерживающее аутентификацию конкретного типа, размещается на сервере аутентификации и в операционных системах или в прикладных программах клиентских устройств.

Политика безопасности

Одним из первых шагов, которые следует предпринять для обеспечения безопасности сети — это сформулировать эффективные принципы политики и соответствующий процесс законоприменения. Необходимо тщательно проанализировать требования, предъявляемые к безопасности сети, и обеспечить адекватный уровень защиты. Например, обязательное использование шифрования. WEP применим для дома или небольшого офиса, но для корпоративных приложений следует использовать более действенные методы, такие как WPA. Эффективные методы взаимной аутентификации (LEAP или EAP-TLS) также будут полезны при выполнении корпоративных приложений.

Стадии оценки

После развертывания беспроводной сети следует выполнить аттестацию ее безопасности, которая должна подтвердить, что беспроводная локальная сеть соответствует политике безопасности, принятой в компании. В большинстве ситуаций необходимо знать, эффективны ли применяемые в сети механизмы защиты. Не возлагайте особых надежд на конструкцию системы. Обязательно проведите тестирование и убедитесь в том, что сеть достаточно защищена от неавторизованного пользователя, который может атаковать ресурсы компании.

На практике компании должны периодически, на регулярной основе, пересматривать политику безопасности. Только так можно гарантировать, что произведенные в беспроводной локальной сети изменения не сделали ее уязвимой для хакеров. Для менее важных сетей достаточно пересматривать политику безопасности раз в год, но для сетей, оперирующих важной информацией, это нужно делать раз в квартал или чаще. К таким сетям относятся сети финансовых учреждений, системы маршрутизации почтовых сообщений и системы управления процессом производства.

Пересмотр существующей политики безопасности

Прежде чем приступить к аттестации безопасности, следует ознакомиться с политикой компании по безопасности беспроводных сетей. Это даст точку отсчета для определения того, подчиняется ли компания собственным правилам. Кроме того, вы должны быть способны оценить и сделать соответствующие рекомендации относительно изменения этой политики. Определите, оставляет ли политика возможность рассерженному на администрацию служащему получения доступа к ресурсам компании.

Так, политика должна описывать адекватные методы аутентификации и шифрования в предположении, что WEP стандарта 802.11 взломан, а также обязывать всех служащих согласовывать с отделом информационных технологий компании вопросы приобретения и установки базовых станций. Очень важно, чтобы все базовые станции имели такие параметры конфигурации, которые соответствуют политике и обеспечивают должный уровень безопасности. Кроме того, следует добиться, чтобы политика безопасности была эффективно доведена до служащих компании.

Пересмотр существующей системы

Чтобы разобраться в структуре системы и параметрах конфигурирования базовых станций, рекомендуется поговорить с персоналом отдела информационных технологий и ознакомиться с соответствующей документацией. Следует выяснить, имеются ли в конструкции какие-либо изъяны, из-за которых система может оказаться уязвимой для атак хакеров.

Узнайте как можно больше об имеющихся средствах поддержки сети и выполняемых ею функциях, чтобы выявить возможные проблемы. Например, во многих компаниях базовые станции конфигурируются при посредстве проводной опорной сети Ethernet. В ходе этого процесса пароли, передаваемые для открытия соединения с определенной базовой станцией, передаются по проводной сети в незашифрованном виде. Поэтому хакер, пользуясь аппаратурой контроля, подключенной к сети Ethernet, может легко получить пароли и переконфигурировать базовые станции.

Опрос пользователей

Обязательно побеседуйте с некоторыми служащими, чтобы определить, осведомлены ли они о политике безопасности, касающейся сферы их деятельности. Например, знают ли пользователи, что они должны согласовывать вопросы приобретения и установки базовых станций с соответствующим подразделением компании? Если даже принятая в компании политика требует этого, еще не факт, что каждый служащий знает о такой политике. Кто-нибудь может купить базовую станцию в ближайшем магазине, торгующем офисным оборудованием, и включить ее в корпоративную сеть, чтобы обеспечить беспроводную связь в своем офисе. Не лишним было бы проверить, пользуются ли служащие персональными брандмауэрами.

Проверка конфигурации беспроводных устройств

Выполняя аттестацию, пройдитесь по помещениям, в которых установлены базовые станции, и воспользуйтесь имеющимися средствами для определения их конфигураций. Если в компании централизованно поддерживается программное обеспечение на местах, вы сможете определить параметры конфигурации с одной консоли, подключенной к проводной части сети. Это покажет, какие механизмы защиты действительно применяются и обеспечивают ли они проведение эффективной политики безопасности. Например, политика требует, чтобы физический порт консоли был недоступен, но во время тестирования может выявиться, что порты большинства базовых станций доступны. Это подтвердит их несоответствие политике, что дает возможность хакеру перезагрузить базовую станцию с установками, сделанными по умолчанию производителем, при которых не обеспечивается никакая защита. Кроме того, следует проанализировать встроенное программное обеспечение каждой базовой станции и проверить, обновлялось ли оно. Во встроенных ранних версиях программного обеспечения могут не применяться свежие "заплаты", ликвидирующие уязвимость системы защиты.

Необходимо также исследовать физические особенности установки базовых станций. Обходя помещения, посмотрите, как установлены базовые станции, обращая внимание на их физическую доступность', типы и ориентацию антенн, характер распространения радиоволн в тех помещениях, которые не контролируются физически с точки зрения безопасности. Базовые станции должны быть смонтированы так, чтобы к ним был затруднен физический доступ посторонним и они были незаметны.

Базовая станция, размещенная, например, на книжном шкафу, может быть заменена хакером на другую, с полностью отключенными опциями защиты. Или хакер может подключить ноутбук к порту консоли и перезапустить базовую станцию. Однако, если базовые станции смонтированы под облицовочной плиткой и находятся вне поля зрения служащих, для доступа к ним злоумышленнику придется воспользоваться лестницей, а это может быть замечено охраной или служащими.

Выявление подставных базовых станций

Проблема, с трудом поддающаяся решению, но из-за которой может резко снизиться защищенность сети, возникает, когда служащий устанавливает персональную базовую станцию в офисе. В большинстве случаев эти станции не соответствуют политике безопасности, в результате чего в корпоративной сети появляется открытый, незащищенный порт. Хакер может использовать средства наблюдения за сетью, которые предупредят его о том, что такая возможность появилась. Поэтому составной частью проверки на безопасность должно стать сканирование с целью обнаружения

подобных станций. Администрации многих компаний удивились бы, узнав, как много таких станций было обнаружено. Наиболее эффективный метод обнаружения подставных базовых станций — пройтись по помещениям с аппаратурой наблюдения. Кроме того, компании должны периодически сканировать сеть для выявления подставных базовых станций в проводной части сети. Многие беспроводные сети с централизованными системами управления позволяют это сделать. ,

Испытание на проникновение

Помимо охоты за подставными станциями, попробуйте пойти дальше — и попытайтесь получить доступ к корпоративным ресурсам, используя обычные средства, доступные хакерам. Например, можно ли использовать AirSnort для взлома сети через WEP? Или привязаться к базовой станции, находясь вне контролируемого компанией периметра? Конечно, задача упростится, если отключить механизм WEP. Но при наличии сильных механизмов шифрования и аутентификации вряд ли удастся проникнуть в собственную сеть.

Анализ брешей в системе безопасности

Информация, полученная в ходе тестирования, послужит основой для выводов по текущей ситуации с безопасностью сети в компании или организации, а также выявит потенциальные бреши в системе. Они могут быть связаны с политикой безопасности, структурой сети, оперативной поддержкой и другими аспектами, снижающими уровень защиты, такими как наличие неавторизованных базовых станций и возможность проникновения в сеть. Вам придется перенять манеру мышления хакера и найти все слабые места, облегчающие посторонним проникновение в беспроводную сеть, доступ через нее к ресурсам компании или даже осуществление контроля над ними.

Рекомендуемые усовершенствования

После выявления всех уязвимых мест следует проанализировать и описать методы, позволяющие решить проблему. Начать следует с выработки рекомендаций по улучшению политики безопасности, в которых должно быть указано, какие меры необходимо предпринять компания ради повышения защищенности своей беспроводной сети. Это основа для поиска технических и процедурных решений, благодаря которым можно будет повысить степень защищенности, сети до необходимого уровня.

Общая политика безопасности

Какая бы сеть ни использовалась, применяемая политика должна защищать ее ресурсы от неавторизованного использования.

Размещение авторизованных пользователей за брандмауэром

Рассмотрим возможность создания беспроводной демилитаризованной зоны (demilitarized zone, DMZ) за счет размещения брандмауэра между беспроводной и корпоративной сетями (рис. 8.8). При таком подходе каждое клиентское устройство должно быть включено в виртуальную частную сеть (virtual private network, VPN). Доступ к защищенной сети разрешается только через эту VPN. Следовательно, для доступа к ресурсам компании хакеру придется использовать соответствующим образом сконфигурированную VPN, что весьма непросто.

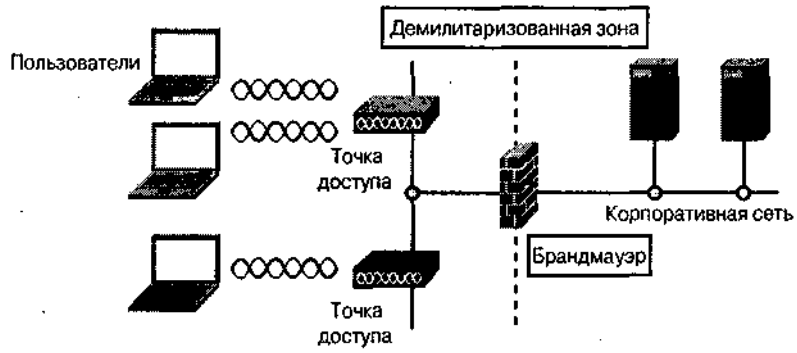

Рис. 8.8. Брандмауэр обеспечивает дополнительную защиту для беспроводных сетей

Проблема, связанная с использованием решения на основе VPN для всех пользователей, состоит в том, что такой сетью трудно управлять. Кроме того, иногда наблюдается снижение производительности. Поэтому многие рассматривают возможность использования VPN только для пользователей, перемещающихся в общедоступные зоны.

Использование эффективных систем шифрования

Опытные хакеры могут проникнуть в защищенную по протоколу WEP сеть, используя свободно распространяемое программное обеспечение. Однако WEP надежно защищает многие домашние сети и сети небольших фирм от любопытных. Для того чтобы взломать WEP-сеть, нужно знать, как пользоваться сложными средствами и захватывать распространяющиеся в сети пакеты. Большинство пользователей вряд ли захотят этим заниматься, если только ресурсы сети не окажутся для них очень привлекательными и они не запасутся бесконечным терпением. Использование стандарта 802.11 WEP для сетей с малым риском атаки со стороны злоумышленников — это тот минимум, которому должна удовлетворять политика безопасности сети.

Если аппаратное обеспечение беспроводной сети поддерживает какую-либо форму шифрования (например, WPA), позволяющую часто изменять ключи, следует ею воспользоваться. Это более защищенное решение, чем дают статические методы, такие как WEP. Если необходима предельно высокая степень безопасности, помогут такие стандарты шифрования, как AES.

Своевременное обновление встроенного программного обеспечения

Производители часто выпускают "заплаты" для встроенного программного обеспечения базовых станций и радиоплат интерфейса сети, устраняющие часть проблем, связанных с безопасностью. Обновление встроенного программного обеспечения базовых станций следует начинать почти сразу же после его установки. Возьмите за правило периодически проверять все устройства и устанавливать последние версии встроенного программного обеспечения, ликвидирующего все уже известные бреши в системе защиты. Именно поэтому следует удостовериться в том, что вы способны обновлять встроенное программное обеспечение базовой станции, которую собираетесь приобрести.

Физическая защита базовых станций

Некоторые базовые станции могут возвращаться в состояние, когда их параметры соответствуют заданным по умолчанию и не обеспечивают какой-либо защиты, в результате того, что кто-то нажмет кнопку <Reset>. Это делает такую базовую станцию уязвимой точкой входа. Поэтому следует обеспечить адекватную физическую защищенность аппаратному обеспечению базовых станций.

Например, не следует располагать базовую станцию на общедоступном столе в офисе. Наоборот, ее нужно установить под облицовкой потолка так, чтобы она по возможности была незаметной. Некоторые базовые станции не имеют кнопки <Reset>, но их можно перезапустить с помощью кабеля, подключенного к разъему RS-232, через соединение с консолью. Чтобы воспрепятствовать этому, ^обеспечьте недоступность физического порта консоли.

Также не следует оставлять базовые станции в пределах досягаемости хакеров, которые могут заменить легитимную защищенную базовую станцию на незащищенную, подставную, к которой может получить доступ любой пользователь. Поэтому неплохая идея — скрывать, насколько это возможно, базовые станции, чтобы хакер не смог так просто их найти. Только не забудьте где-то отметить места расположения беспроводного аппаратного обеспечения, иначе вам самим через некоторое время будет трудно найти его.

На периоды бездействия базовые станции следует делать недоступными. Если это возможно, отключайте базовые станции, которые временно не нужны пользователям. Это сузит "окно возможностей" для хакера. Можно вынимать вилку из розетки электропитания каждой такой станции, но есть возможность использования оборудования, электропитание которого осуществляется через сеть Ethernet; такие базовые станции можно включать и отключать дистанционно.

Использование сильных паролей для базовых станций

Не используйте на базовых станциях пароли, заданные по умолчанию. Пароли по умолчанию хорошо известны, поэтому кто-то сможет с легкостью изменить параметры базовой станции в свою пользу. Вместо них установите пароли, которые трудно отгадать. Неплохо использовать вперемешку символы верхнего и нижнего регистров, а также специальные символы. Не забывайте периодически изменять пароли. Также добейтесь того, чтобы пароли передавались по сети только в зашифрованном виде.

Запрет на передачу SSID в широковещательном режиме

По возможности избегайте применения пользовательских устройств, автоматически наблюдающих за SSID, используемым точкой доступа беспроводной локальной сети. Windows XP и другие средства наблюдения будут автоматически просматривать маячковые фреймы стандарта 802.11, чтобы получить SS1D. Если широковещательный режим передачи SSID отключен, базовая станция не включает SSID во фрейм маячкового сигнала, поэтому большинство средств пассивного наблюдения окажутся бесполезными. Кроме того, Windows XP и применяющие ее пользователи не будут знать о существовании беспроводной локальной сети.

Однако отключение механизма широковещательной передачи SSID не считается достаточно надежной мерой, поскольку кто-то может отследить фреймы привязки, посылаемые в соответствии со стандартом 802.11, и узнать SSID. Но отключение механизма широковещательной передачи SSID ограничит доступ.

Ограничение распространения радиоволн

За счет использования направленных антенн можно ограничить распространение радиоволн областью, к которой хакеры не будут иметь физического доступа. Например, сеть проектируется таким образом, что за счет выбора коэффициентов усиления антенн и их ориентации уменьшается "утечка" радиоволн за пределы помещения. Благодаря этому не только оптимизируется уровень сигнала в области действия сети, но и минимизируется возможность для постороннего наблюдателя прослушивать сигналы, передаваемые пользователем, или осуществить взаимодействие с корпоративной сетью через точку доступа.

Использование персональных брандмауэров

Если хакер имеет возможность привязаться к базовой станции, он сможет получить доступ к файлам других пользователей через операционную систему Windows, которая привязана к какой-нибудь точке доступа, включенной в ту же беспроводную локальную сеть. Поэтому очень важно, чтобы все пользователи отменили возможность совместного использования файлов всех папок и применяли персональные брандмауэры. Это особенно важно для пользователей, работающих в общедоступных местах.

Отслеживание конфигураций базовых станций

Используйте средства оперативной поддержки для постоянного наблюдения за сетью и выявления базовых станций, не соответствующих принятым правилам конфигурации. Базовая станция, параметры которой не соответствуют определенным правилам безопасности, скорее всего или перезапущена, или является подставной.

Если обнаружена базовая станция с неправильными параметрами, следует как можно быстрее восстановить нужные. Обязательно шифруйте управляющий трафик, используя для этого *секретный* вариант простого протокола управления сетью (simple network management protocol, SNMP). Например, SNMP версии 1.0 пересылает все в открытом виде. Можно также использовать датчики охранной сигнализации, имеющиеся в некоторых средствах оперативной поддержки, для определения присутствия хакеров по незаконным MAC-адресам. Основная идея — поднять тревогу, если замечено что-то подозрительное.

Применение средств контроля

Добейтесь того, чтобы служащие и подразделения компании координировали действия по развертыванию беспроводных сетей с соответствующими группами специалистов в области информационных технологий. Например, запретите использование неавторизованных точек доступа. Разрешите использование изделий надежных поставщиков только после того, как убедитесь в обеспечении ими необходимой вам степени защиты.

Ведите список MAC-адресов авторизованных радиоплат интерфейса сети и базовых станций, он станет основой для выявления подставных базовых станций в процессе обследования сети. Кроме того, используйте средства управления, вынуждающие базовые станции следовать политике безопасности, принятой в компании.

Следуя этим рекомендациям, вы заложите основы формирования действенной политики безопасности. Решая, какие именно методы следует применить, учитывайте и актуальные потребности безопасности. Например, WEP вполне приемлем

для беспроводной локальной сети, развернутой дома или в небольшом офисе. Но в финансовом учреждении или в магазине розничных продаж, когда речь идет о передаче конфиденциальных данных, полезнее будет более сильный механизм — WPA или AES.

Резюме

Система защиты — это один из важнейших и сложных элементов беспроводных сетей. Способность хакеров отслеживать трафик, получать неавторизованный доступ к ресурсам и вызывать отказ в обслуживании беспроводной сетью ее пользователей — вот те проблемы, которые придется решать. Используя эффективные механизмы аутентификации и шифрования, можно существенно снизить опасность. Однако следует иметь в виду, что необходимый уровень безопасности зависит от предъявляемых к сети требований. Уровень защиты, приемлемый для домашней сети, совершенно не соответствует требованиям, предъявляемым к системе безопасности сети предприятия.

Вопросы для самопроверки

Ответы на эти вопросы вы можете найти в приложении А.

1. Каковы три основные угрозы безопасности беспроводной сети?
2. Каково основное средство противодействия мониторингу трафика?
3. Как можно воспрепятствовать хакерам в получении доступа к ресурсам компании через беспроводную сеть?
4. Какой метод поможет уменьшить урон от успешно проведенной DoS-атаки?
5. Почему WEP не пригоден для защиты секретной информации?
6. Чем TKIP отличается от WEP?
7. Верно ли, что WPA использует TKIP и является поднабором требований стандарта 802. Hi?
8. Почему использование фильтрации MAC-адресов неэффективно?
9. Что такое подставная точка доступа, и почему при ее использовании возникают проблемы?
10. Что следует установить на ноутбуке, который пользователь будет включать в общедоступную беспроводную локальную сеть, чтобы неавторизованные пользователи не могли получить доступ к его файлам?

Ответы на вопросы для самопроверки

Глава 1

1. В беспроводной сети связь осуществляется между компьютерными устройствами.
2. Беспроводная сеть обеспечивает передачу электронной почты, MSN, Web-страниц, баз данных, потокового видео и речи.
3. Беспроводные сети подразделяются на персональные, локальные, региональные и глобальные.
4. Максимальная протяженность беспроводной персональной сети 15 м (50 футов).
5. Да.
6. Общепринятый стандарт на беспроводные локальные сети называется ШЕЕ 802.11, или Wi-Fi.
7. Для беспроводных региональных сетей предложен новый стандарт IEEE 802.16.
8. Системы беспроводных глобальных сетей обычно устанавливаются вне помещений, внутри помещений интенсивность сигналов значительно снижается.
9. Общим при применении беспроводных сетей в домашних условиях и небольших офисах являются совместно используемые Internet-соединения, осуществляемые многими мобильными компьютерами.
10. Примерами использования беспроводных глобальных сетей могут служить доступ к Internet-приложениям при нахождении вне помещений, транзакции при сделках с недвижимостью, связь для сотрудников, находящихся в командировках, передача информации о состоянии торговых автоматов и данных утилит, считывающих показания счетчиков.

Глава 2

1. В миниатюрных беспроводных компьютерных устройствах эффективнее других функционируют платы интерфейсов беспроводной сети с форм-фактором , PC Card, Mini-PCI и CompactFlash.
2. Факторами, отрицательно влияющими на передачу коммуникационных сигналов через воздушную среду, могут быть дождь, снег, смог и туман.

3. Основное назначение базовой станции — это обеспечение передачи сигналов через среду, используемую беспроводной сетью.
4. К основным особенностям промежуточного программного обеспечения беспроводной сети относятся мягкий перезапуск, методы оптимизации, пакетирование данных, формирование и восстановление изображений на экранах и поддержка оконечных систем.
5. Беспроводная сеть работает на физическом и канальном уровнях эталонной модели OSI.
6. Пропускная способность определяется с учетом "накладных расходов" протоколов.
7. Нет, компьютерное устройство хранит данные в цифровой форме.
8. Прежде чем передавать сигналы через воздушную среду, плата интерфейса беспроводной сети должна преобразовывать их в аналоговую форму.
9. Общепринятым для беспроводных сетей является протокол CSMA.
10. Приемная плата интерфейса сети обеспечивает контроль ошибок и посылает запрос на повторную передачу фрейма, если обнаружена ошибка.

Глава 3

1. Нет.
2. Наибольшее влияние на распространение радиочастотных сигналов оказывает ливень.
3. Помехи обусловливают неправильное распознавание сигнала из-за того, что приемной антенны достигают одновременно два сигнала.
4. Часто в качестве источников радиочастотных помех выступают беспроводные мобильные телефоны, микроволновые печи и Bluetooth-устройства.
5. Действительно, приемнику трудно отличить один бит от другого при демодуляции сигналов, передаваемых с большой скоростью, поскольку обозначающие их символы слишком близко расположены по отношению друг к другу.
6. Под ИК-системами, использующими рассеянный свет, понимается система, излучающая свет во всех направлениях, который затем отражается от потолка и стен.
7. Направленные ИК-системы используются примерно на расстоянии 1,6км (1 миля).
8. В процессе модуляции информационный сигнал накладывается на несущую, частота которой наилучшим образом подходит для распространения через воздушную среду.
9. Для представления информации при квадратурной амплитудной модуляции изменяются амплитуда и фаза сигнала.
10. Для использования систем с расширением спектра лицензия пользователю не нужна.

Глава 4

1. Для радиоплат беспроводных персональных сетей наиболее употребительны форм-факторы PC Card и CF.
2. Любое приложение, которое удобно синхронизировать с ПК или ноутбуком через USB-порт; это может быть, например, PDA, беспроводная мышь или беспроводная цифровая камера.
3. Использование маршрутизатора в беспроводной персональной сети эффективно в тех случаях, когда беспроводная сеть имеет ограниченные размеры, т.е. развернута в доме или небольшом офисе.
4. Зона действия беспроводной персональной сети — около 9 м (30 футов), этого вполне достаточно для одной комнаты.
5. Bluetooth в качестве основы при разработке своего стандарта использовала группа 802.15.
6. Bluetooth-устройства работают в диапазоне 2,4 ГГц.
7. Обе эти системы работают в одном и том же частотном диапазоне 2,4 ГГц, в результате чего возникают помехи и ухудшаются характеристики сети.
8. Нет.
9. Максимальная скорость передачи для устройств IrDA 4 Мбит/с.
10. Технология IrDA обеспечивает помехоустойчивость беспроводных локальных сетей.

Глава 5

1. В домашних условиях и небольших офисах наиболее часто используется маршрутизатор беспроводной локальной сети.
2. Именно маршрутизатор беспроводной локальной сети направляет пакеты к месту назначения. Точка доступа не использует протоколы DHCP и NAT, маршрутизатор использует их.
3. В беспроводной локальной сети повторитель применяется в тех случаях, когда необходимо увеличить радиус действия точки доступа или маршрутизатора до области, куда не так просто протянуть провода.
4. Радиоштата беспроводной локальной сети прослушивает маячковые сигналы, периодически передаваемые каждой точкой доступа, и привязывается к той из них, маячковый сигнал которой имеет большую интенсивность.
5. Нет.
6. Устройства стандарта 802.11а работают в диапазоне 5 ГГц.
7. В беспроводных локальных сетях стандарта 802.11Ь доступны три неперекрывающихся канала.
8. Да, устройства стандарта 802.11g работают со скоростью до 54 Мбит/с и совместимы с сетями стандарта 802.11Ь.
9. Почти повсеместно доступны частоты 2,4 ГГц (стандарты 802.11Ь и 802.11g).
10. Изделия, прошедшие сертификацию Wi-Fi, совместимы с другими изделиями, имеющими сертификат Wi-Fi, независимо от их производителя.

Глава 6

1. Беспроводные региональные сети избавляют от необходимости прокладывать дорогие кабели или арендовать каналы связи.
2. Нет, самообучающиеся мосты не передают повторно все полученные пакеты.
3. Мост соединяет сети, а точка доступа позволяет соединяться пользователям.
4. Полосковая антенна и антенна Яги.
5. Остронаправленная антенна имеет намного более узкую диаграмму направленности, из-за чего радиус ее действия при той же излучаемой мощности увеличивается.
6. Зеркальная антенна.
7. Вертикальная поляризация.
8. Система типа "точка-несколько точек" может оказаться менее дорогостоящей; с •œ помощью проще осуществлять соединения для нескольких площадок.
9. Маршрутизаторы пакетной радиосвязи не нужно соединять между собой кабелями, чем и достигается относительно высокая живучесть системы, поскольку, если один из маршрутизаторов выйдет из строя, пакеты могут быть переданы через другой маршрутизатор.
10. При создании беспроводных региональных сетей используются стандарты 802.11, Wi-Fi и 802.16.

Глава 7

1. В беспроводных глобальных сетях используются ноутбуки, PDA и мобильные телефоны.
2. Развертывание беспроводной глобальной сети требует больших капитальных вложений, которые нужно окупить.
3. Потому что существует много беспроводных глобальных сетей различных типов, несовместимых между собой.
4. Спутниковая система способна обеспечивать связь на огромных пространствах. Например, сигнал со спутника может быть принят примерно на трети поверхности земного шара.
5. С такой скоростью передают данные сотовые системы третьего поколения (3G).
6. Наиболее распространенными являются сотовые системы.
7. Более высокие скорости передачи данных обеспечивает UMTS.
8. Основная проблема метеорной связи состоит в низкой скорости передачи данных.
9. Нет.
10. Отсутствие взаимных помех при использовании технологии МДКР обеспечивается за счет то, что каждый пользователь при передаче применяет отличный от других код.

Глава 8

1. Мониторинг трафика, неавторизованный доступ и атаки типа "отказ в обслуживании" (DoS).
2. Использование шифрования.
3. Путем внедрения эффективной системы аутентификации.
4. Наличие альтернативного плана поддержания жизнедеятельности компании способами, не требующими использования беспроводной сети.
5. Хакеры могут взломать алгоритм шифрования WEP, используя свободно распространяемое программное обеспечение.
6. TKIP позволяет использовать механизм распределения динамических ключей, благодаря чему ключи периодически обновляются. В случае WEP применяются статические ключи, которые не обновляются.
7. Действительно, WPA использует TKIP и является поднабором требований стандарта 802.111.
8. Использование фильтрации MAC-адресов неэффективно, поскольку ею трудно управлять, но ее легко "обмануть".
9. Подставная точка доступа имеет параметры, не обеспечивающие безопасность, чем могут воспользоваться хакеры или служащие. Подставная точка доступа позволяет хакерам проникнуть в сеть через ее открытый порт.
10. Персональный брандмауэр.

Глоссарий

1G cellular — сотовые системы телефонной связи первого поколения, в которых используются аналоговые сигналы; не способны эффективно передавать компьютерные данные.

2G cellular — сотовые системы телефонной связи второго поколения, обеспечивающие передачу цифровых сигналов и поддерживающие скорость передачи данных около 20 кбит/с.

3G cellular — сотовая система связи третьего поколения; модифицированная версия сотовой системы связи 2G для передачи данных с большей скоростью.

802.11 — стандарт IEEE, определяющий характеристики и особенности работы локальной сети со средним радиусом действия, использующей для передачи информации радиоволны. Регламентирует использование метода CSMA как основного для совместного использования среды передачи (радиоэфира).

802.15 — стандарт IEEE, определяющий характеристики и особенности работы беспроводных персональных сетей, основанный на спецификации Bluetooth.

802.16 — стандарт IEEE, определяющий характеристики и особенности работы беспроводных региональных сетей.

802.3 — стандарт IEEE, определяющий характеристики и особенности работы проводных локальных сетей. Регламентирует применение метода CSMA, который аналогичен применяемому в беспроводных локальных сетях стандарта 802.11.

Access **point** (точка доступа) — тип базовой станции, которую беспроводная локальная сеть использует для обеспечения взаимодействия беспроводных пользователей с проводной сетью и осуществления роуминга в пределах здания.

Ad hoc mode (режим неплановой сети) — конфигурация беспроводной сети, при которой пользователи могут непосредственно устанавливать соединения между своими устройствами, обходясь без услуг базовой станции. В этом режиме могут работать беспроводные персональные и локальные сети.

Analog signal (аналоговый сигнал) — сигнал, амплитуда которого меняется со временем. Примером аналогового сигнала могут служить радиоволны.

Antenna (антенна) — физическое устройство, преобразующее электрические сигналы в радио- или световые волны, и наоборот — для передачи их через воздушную среду. Может быть всенаправленной, передавая радиоволны во всех направлениях, или направленной, когда интенсивность радиоволн, передаваемых в одном направлении, больше, чем в других.

Association (привязка) — процесс, в результате которого станция стандарта 802.11 становится частью беспроводной локальной сети, после чего пользователь получает доступ к различным службам сети.

Authentication (аутентификация) — процесс подтверждения идентичности пользователя или базовой станции. Обычно для проведения аутентификации применяют имена пользователей и пароли, но существуют и другие, более сложные механизмы аутентификации. Например, по цифровым мандатам без участия пользователя.

Base station (базовая станция) — аппаратура, обеспечивающая взаимодействие беспроводных компьютерных устройств между собой и с проводной сетью. В беспроводной локальной сети используются базовые станции следующих типов: точка доступа и беспроводной маршрутизатор.

Bluetooth — спецификация, опубликованная Специальной группой по интересам Bluetooth. Определяет характеристики и особенности работы маломощной радиосети с небольшим радиусом действия. На сегодняшний день многие устройства поддерживают технологию Bluetooth, а Рабочая группа 802.15 разрабатывает соответствующие стандарты.

Bridge (мост) — устройство, соединяющее две сети на уровне 2. Мост направляет пакеты в другую сеть, руководствуясь MAC-адресом, содержащимся в заголовке пакета. Мосты играют ключевую роль при развертывании беспроводных региональных сетей.

Carrier sense access (доступ с контролем несущей) — процесс совместного использования общей среды передачи, при котором перед передачей данных определяется, свободна ли среда. Является частью протокола CSMA.

Carrier signal (несущая) — первичный радиосигнал, посредством которого данные передаются через радиоэфир. Для представления информации за счет модуляции различных типов изменяется частота, фаза или амплитуда сигнала.

CDMA (code division multiple access) — множественный доступ с кодовым разделением каналов (МДКР). Процесс, при котором каждый пользователь модулирует свои сигналы отличным от других кодом во избежание возникновения взаимных помех.

CDPD (cellular digital packet data) — цифровая пакетная передача данных по сети сотовой связи, позволяющая передавать данные через аналоговую сотовую систему телефонной связи со скоростью 19,2 кбит/с. По мере внедрения новейших систем 3G технология CDPD выходит из употребления.

CF (CompactFlash) — плата интерфейса сети для PDA, фотокамер и других компьютерных устройств. Можно без труда приобрести CF для Bluetooth и в качестве платы интерфейса сети стандарта 802.11.

Client device (клиентское устройство) — аппаратное обеспечение, имеющее пользовательский интерфейс, позволяющий применять приложения беспроводной сети. Клиентское устройство — это другое название компьютерного устройства.

Computer device (компьютерное устройство) — любая конечная точка беспроводной сети, например ноутбук, PDA или робот. Компьютерные устройства часто называют клиентскими устройствами.

CSMA (carrier sense multiple access) — множественный доступ с контролем несущей (МДКН). Процесс, позволяющий многим станциям стандарта 802.11 совместно использовать среду передачи (радиоэфир). Станции только тогда пытаются осуществить передачу, когда этого не делает ни одна другая станция сети. В противном случае происходит коллизия и станции приходится повторно передавать данные.

Data (данные) — информация, например в виде электронных файлов, которая хранится и передается через беспроводную сеть. Зачастую данные передают, разделив их на несколько пакетов, каждый из которых передается по сети отдельно.

Data rate (скорость передачи данных) — количество битов в секунду при передаче данных. Например, беспроводные локальные сети стандарта 802.lib передают данные со скоростью до 11 Мбит/с.

DCF (distributed coordination function) — распределенная функция координации. Часть стандарта 802.11, определяющая, как станции должны конкурировать за право доступа к среде передачи. Для регулирования трафика сети DCF использует технологию CSMA.

DHCP (dynamic host configuration protocol) — протокол динамического конфигурирования узла, автоматически назначающий сетевому устройству уникальный IP-адрес из определенного диапазона. Во многих домашних и общедоступных беспроводных локальных сетях используется DHCP, облегчающий для пользователей получение доступа к Internet. DHCP автоматически назначает правильные адреса этим пользователям.

Digital certificate (цифровой мандат) — электронное сообщение, содержащее мандат определенного пользователя. Используется как средство аутентификации пользователей или их компьютерных устройств.

Digital signal (цифровой сигнал) — сигнал, амплитуда которого ступенчато изменяется с течением времени и представляющий данные в компьютерном устройстве. Перед передачей через воздушную среду должен быть преобразован в аналоговую форму — этот процесс называется модуляция.

DSSS (direct sequence spread spectrum) — высокоскоростная передача с расширением спектра методом прямой последовательности. Тип расширения спектра, при котором расширяющий код увеличивает скорость передачи потока данных, чтобы сигнал занял большую часть частотного диапазона. Беспроводные локальные сети стандарта 802.11Ь используют технологию расширения спектра методом прямой последовательности.

Directional antenna (направленная антенна) — тип антенны, которая фокусирует радиоволны, из-за чего они распространяются в одном направлении дальше, чем в других. Такие антенны обычно применяются в системах беспроводных региональных и глобальных сетей. За счет направленности антенны увеличивается радиус действия в одном направлении и уменьшается в других.

Distribution system (распределительная система) — проводная система, обеспечивающая физическое соединение точек доступа в беспроводной локальной сети. Наиболее часто используемой распределительной системой в беспроводных локальных сетях является Ethernet.

Encryption (шифрование) — перестановка битов данных в соответствии с ключом перед передачей данных через сеть. WEP и WPA — примеры систем шифрования, применяемых в беспроводных локальных сетях.

Ethernet — под этим названием стали широко известными проводные локальные сети стандарта 802.3. Ethernet — широко распространенный тип сети, которую компании используют для соединения ПК и серверов, обеспечивает распределительную систему для большинства беспроводных локальных сетей.

FDMA (frequency division multiple access) — множественный доступ с частотным разделением. Процесс, в ходе которого относительно широкий частотный диапазон

делится на узкие поддиапазоны. Каждый пользователь передает речь и данные в выделенном для него поддиапазоне.

FHSS (frequency hopping spread spectrum) — расширение спектра путем скачкообразного переключения частоты. Тип расширения спектра, отличающийся тем, что приемопередатчик переходит с одной частоты на другую в соответствии с определенной схемой переключений, для того чтобы сигнал занимал большую часть частотного диапазона. Технология переключения частоты используется в старых беспроводных локальных сетях стандарта 802.11.

Firewall (брандмауэр) — устройство, не позволяющее пользователям, установившим соединение с определенной частью сети, получать доступ к ее важным ресурсам. Учитывая уязвимость точек доступа беспроводных локальных сетей, их часто размещают за брандмауэрами.

Frequency (частота) — количество раз в секунду повторения сигналом самого себя. Измеряется в герцах (Гц), соответствующее значение равно количеству циклов изменения сигнала в каждую секунду. Например, частоты сигналов, используемых в беспроводных локальных сетях, лежат в диапазоне 2,4-5 ГГц.

FSK (frequency shift-keying)— частотная манипуляция (ЧМн). Процесс модуляции, при которой слегка изменяется частота несущего сигнала, за счет чего осуществляется представление информации способом, подходящим для ее передачи через воздушную среду.

GPS (global positioning system)— глобальная система навигации и определения положения, позволяющая пользователям иметь клиентские GPS-устройства, с помощью которых они могут легко определить свое географическое местоположение. GPS — основа навигационной системы, а также служб, основанных на определении местоположения через беспроводные сети.

Hacker (хакер) — человек, имеющий желание и возможности похитить информацию, находящуюся в сети. Хакеры часто пытаются проникнуть в корпоративные системы шутки ради, пользуясь уязвимостью беспроводных сетей.

Hotspot ("горячая точка") — место, где развернута общедоступная беспроводная локальная сеть. "Горячие точки" располагаются в зонах, где концентрируются люди с компьютерными устройствами, таких как аэропорты, гостиницы, дворцы съездов и кафе.

Interference (помехи) — нежелательные сигналы, нарушающие работу беспроводных сетей и снижающие их производительность.

Interoperability (возможность взаимодействия) — условия, при которых компьютерное устройство способно эффективно взаимодействовать с беспроводной сетью.

IP (Internet protocol) — протокол Internet, осуществляющий маршрутизацию пакетов между компьютерными устройствами, подключенными к сети. Протокол IP помещает перед каждым пакетом поле заголовка, содержащее IP-адреса отправителя и получателя каждого пакета.

IP address (IP-адрес) — численный адрес, соответствующий соединению сетевого устройства с сетью. Например, каждая плата интерфейса беспроводной сети должна иметь IP-адрес. Каждая плата интерфейса сети должна иметь связанный с нею IP-адрес, если пользователь хочет применять TCP/IP-приложения, обеспечивающие,

например, получение и отправку электронной почты, просмотр Web-страниц или взаимодействие с корпоративным сервером приложений.

IPSec (IP security) — протокол, поддерживающий защищенный обмен пакетами на сетевом уровне. Часто используется в VPN и шифрует пакеты данных во всей сети; часто это называют "сквозное шифрование" (end-to-end encryption).

IrDA (Infrared data association) — Ассоциация по средствам передачи данных в инфракрасном диапазоне. Разработанный ею стандарт IrDA регламентирует правила последовательной передачи данных на короткие расстояния с низкой стоимостью и малым энергопотреблением, при этом обеспечивается возможность взаимодействия сетей. IrDA применяется во многих ноутбуках и PDA.

LDAP (lightweight directory access protocol) — упрощенный протокол доступа к каталогам, позволяющий получать доступ к сетевым каталогам.

Location-based services (сервисы, основанные на определении местонахождения) — способность отслеживать местонахождение пользователей и доставлять им информацию, имеющую отношение к конкретной зоне, где они в данный момент находятся.

Medium access control (MAC) layer (нижний подуровень канального уровня, или уровень управления доступом к среде передачи, MAC-уровень) — часть структуры сети, управляющая ею и поддерживающая связь через совместно используемую среду. MAC-уровень— это "мозговой центр" платы интерфейса сети или базовой станции, именно здесь обеспечивается выполнение правил, обязательных для всех устройств сети.

Medium (среда) — пространство, в котором распространяются коммуникационные сигналы, например радиоволны. В случае беспроводных сетей такой средой является воздух.

Medium access (доступ к среде) — процесс, в ходе которого несколько компьютерных устройств используют общую среду. Наиболее распространенным методом осуществления доступа к среде в беспроводных сетях является множественный доступ с контролем несущей (CSMA).

Modulation (модуляция) — в процессе модуляции создаются радио- или световые сигналы на основе данных, предназначенных для передачи через сеть, таким образом, что становится возможной их передача через воздушную среду. Примеры типов модуляции— ЧМн (FSK), ФМн (PSK) и квадратурная амплитудная модуляция (QAM).

NAT (Network Address Translation) — трансляция сетевых адресов. Протокол, преобразующий официальный IP-адрес в частные адреса, которые могут быть использованы во внутренней сети. Например, провайдер, предлагающий беспроводной доступ в Internet, может предоставить клиенту только один официальный IP-адрес. Однако протоколы NAT и DHCP позволят клиенту иметь много ПК и ноутбуков, совместно использующих единственный официальный IP-адрес.

NIC (Network Interface Card) — плата интерфейса сети, обеспечивающая взаимодействие компьютерного устройства с сетью. Ее иногда называют радиоплатой или клиентской платой.

Noise floor (минимальный уровень шума) — амплитуда электромагнитных сигналов в определенной зоне, когда беспроводная сеть не функционирует.

OFDM (orthogonal frequency division multiplexing) — мультиплексирование с разделением по ортогональным частотам. Процесс, в ходе которого сигнал перед передачей его через воздушную среду распределяется по многим поднесущим. Используется с целью повышения характеристик беспроводных локальных сетей стандартов 802. Паи 802.1 lg и в некоторых патентованных беспроводных региональных сетях.

Optical fiber (оптическое волокно) — длинная тонкая стеклянная нить с покрытием, способная передавать световые сигналы. Волоконно-оптические кабели имеют защитную оболочку, из-за чего их иногда бывает трудно отличить от кабелей с медными жилами.

PC Card (PC-карта) — устройство размером с кредитную карту, обеспечивающее наращивание памяти или содержащее модем, или обеспечивающее соединение с внешними устройствами, такими как ноутбук и PDA. Во многих PC-картах применяются технологии Bluetooth и 802.11.

PDA (personal digital assistant) — компактное устройство, используемое для хранения контактной информации, ведения деловых дневников и т.п. Некоторые PDA способны выполнять функции клиентов электронной почты и Web-браузеров.

Point-to-multipoint system (система типа "точка-несколько точек") — система, позволяющая одному пользователю напрямую связываться с несколькими другими.

Point-to-point system (система типа "точка-точка") — система, в которой связь между двумя пользователями осуществляется напрямую.

PSK (phase shift keying) — фазовая манипуляция (ФМн). Процесс модуляции, при котором для представления информации используются небольшие изменения фазы несущей, в результате чего возможна передача данных через радиоэфир.

Public wireless LAN (общедоступная беспроводная локальная сеть) — тип беспроводной локальной сети, которую часто называют "горячая точка". Ее услугами может воспользоваться любой владелец сконфигурированного соответствующим образом компьютерного устройства.

QAM (quadrature amplitude modulation) — квадратурная амплитудная модуляция. Процесс модуляции, при котором для представления информации используются небольшие изменения фазы и амплитуды несущей, в результате чего передача данных возможна через радиоэфир.

Radio NIC (радиоплата интерфейса сети) — тип платы интерфейса сети, обеспечивающей передачу и прием радиосигналов.

RADIUS (Remote Authentication Dial-In User Service) — служба дистанционной аутентификации пользователей по коммутируемым линиям. Система аутентификации и учета, которую многие поставщики услуг широкополосного доступа к Internet используют для управления доступом к Internet и выписки счетов за пользование беспроводной сетью.

Repeater (повторитель) — устройство, принимающее и ретранслирующее сигналы с единственной целью — увеличить дальность их распространения.

RF signal (радиосигнал) — сигнал, частота которого соответствует диапазону радиоволн, используется для передачи информации через воздушную среду.

Rogue access point (подставная точка доступа) — неавторизованная точка доступа, имеющая параметры конфигурации, позволяющие кому угодно получить доступ к сетевым ресурсам.

Router (маршрутизатор) — тип базовой станции, применяющей специальные сетевые протоколы, такие как DHCP и NAT, позволяющие пользователям выполнять TCP/1P-приложения.

Satellite (спутник) — ретранслятор сигнала, размещенный на орбите. Спутники обеспечивают работу беспроводных глобальных сетей, используя для этого радиосигналы.

Snooper (снупер) — некто, по воле случая (а иногда и неслучайно) нарушивший работу беспроводной сети.

Spread spectrum (расширение спектра) — расширение спектра несущего сигнала на большую, чем необходимо для его передачи, часть частотного диапазона. Основные способы расширения спектра — метод прямой последовательности и переключение частоты.

TCP (transmission control protocol) — протокол управления передачей, устанавливающий и поддерживающий соединения между компьютерными устройствами, подключенными к сети. Используется вместе с протоколом IP, поэтому общепринятая аббревиатура для них — TCP/IP.

TDMA (time division multiple access) — множественный доступ с временным разделением каналов (МДВР). Процесс, позволяющий только одному пользователю осуществлять передачу в данный промежуток времени. Каждый пользователь занимает всю полосу канала в течение выделенного для него временного интервала.

Terminal emulation (эмуляция терминала) — механизм, позволяющий пользователям через сеть взаимодействовать с приложениями, выполняемыми на центральном компьютере. Примерами эмуляторов терминала являются устройства типов VT-220, 3270 и 5250.

Transceiver (приемопередатчик) — устройство, которое как передает, так и получает информацию; размещается в радиоплате интерфейса сети.

VPN (virtual private network) — виртуальная частная сеть, использующая специальное программное обеспечение на клиентском устройстве, которое управляет доступом к отдаленным приложениям и обеспечивает безопасность соединения за счет сквозного шифрования.

WEP (Wired Equivalent Privacy) — защищенность, эквивалентная таковой проводных сетей. Часть стандарта 802.11, определяющая порядок шифрования данных, передаваемых между устройствами беспроводной локальной сети.

Wi-Fi — логотип, который разрешается размещать на компонентах беспроводных локальных сетей, удовлетворяющих стандартам, определенным Альянсом Wi-Fi. Стандарты Wi-Fi базируются на стандарте 802.11.

Wi-Fi Protected Access (WPA) — защищенный доступ к Wi-Fi. Протокол безопасности, определенный Альянсом Wi-Fi, позволяющий компьютерным устройствам

периодически получать новые ключи шифрования. В WPA версии 1 применяются временный протокол целостности ключа (temporal key integrity protocol, TKIP) и WEP; в WPA версии 2 используется весь стандарт 802.11i, включающий AES.

Wireless LAN (беспроводная локальная сеть) — сеть, удовлетворяющая потребность в соединениях в зонах, размеры которых соответствуют зданию или кампусу. Популярными стандартами, которым соответствуют многие беспроводные локальные сети, являются стандарты 802.11 и Wi-Fi.

Wireless MAN (беспроводная региональная сеть) — сеть, удовлетворяющая потребность в соединениях в зонах, размеры которых соответствуют городу. Беспроводные региональные сети соответствуют стандарту 802.16 и патентованным стандартам.

Wireless PAN (беспроводная персональная сеть) — сеть, удовлетворяющая потребность в соединениях в зонах, размеры которых соответствуют небольшой комнате или пространству в непосредственной близости от человека. Популярными технологиями, применяемыми при развертывании беспроводных персональных сетей, являются Bluetooth и стандарт 802.15.

Wireless WAN (беспроводная глобальная сеть) — сеть, удовлетворяющая потребность в соединениях в больших географических зонах, сравнимых по размерам со страной или континентом. Для передачи радиосигналов в беспроводных глобальных сетях применяются спутники.

WISP (wireless Internet service provider) — поставщик услуг по беспроводному доступу в Internet. Компания, которая предлагает службы беспроводного подключения к Internet для квартир и офисов. Компании такого рода часто обеспечивают беспроводной доступ в "горячих точках" общедоступных беспроводных локальных сетей.

Предметный указатель

100BASE-T, 51
100BASE-T4, 51
100BASE-TX, 51
10BASE-T, 51
1G cellular, 138

Access point, 43
ACK, 109
Acknowledgement, 109
Ad hoc mode, 107
Ad hoc wireless LAN, 106
Address resolution protocol, 151
ADSL, 81
Advanced encryption standard, 159
AES, 119; 159
Analog signal, 59
ARP, 151
  защищенный, 153
ARQ, 62
ASCII, 60
Association, 111
Automatic repetition query, 62

B

Back-offtimer, 108
Basic bridge, 125
Beacon, 109
Beacon interval, 110
Bluetooth, 20
BRAN, 119
Bridge, 123
Brute-force attack, 153

C

CDMA, 145
CDPD, 25
Cellular Digital Packet Data, 25
CF.41
Challenge text, 110
Clear to send, 111
Code division multiple access, 145
CompactFlash, 41
CRC, 157
CSMA/CA, 108
Cyclical redundancy check, 157

D

Data encryption standard, 159
DBPSK, 114; 115
DCF, 107
Demilitarized zone, 167
Denial ofservice, 153
DES, 159
DPS, 121
DHCP, 99
Digital certificate, 46
Digital signal, 57
Direct database connectivity, 47
Distributed coordination function, 107
Distribution system, 98
DMZ, 167
DoS, 153
DQPSK, 115
DSSS, 113
Duration field, 108
Dynamic frequency selection, 121
Dynamic host configuration protocol, 99

E

EAP, 162
EDGE, 139
EIA, 50
ETSI, 119
Extensible authentication protocol, 162

F

FCC, 72
FDMA, 144
FEC, 62
Federal Communication Commission, 72
FHSS, 112
Forward error correction, 62
Frequency division multiple access, 144
Frequency-shift keying, 77
FSK, 77

G

Go-back-n, 64
GPRS, 139

H

HiperLAN/2, 119
Hotspot, 104
HR-DSSS, 112

I

IBSS, ПО
ICV, 157
Independent basic service set, 110
Industry-Standard Architecture, 40
Infrared data association, 94
Infrastructure mode, 103
Initialization vector, 157
Integrity check value, 157
Interference, 72
Interoperability, 97
IP address, 99
IPSec, 46
IP-адрес, 99
IrDA, 94
ISA, 40
ISM, 80
ISO, 55
IV, 157

L

LDAP, 46
Location-based service, 32

M

MAC, 107
MAC-фильтрация, 161
Man-in-the-middle attacks, 151
Media Access Control, 107
Medium, 37
Medium access, 60
Mini-PCI, 41
Mobile broadband wireless access, 131

N

NAT, 99
NAV, 108
Network address translation, 99
Network allocation vektor, 108
Network interface card, 39
Noise floor, 62

O

OFDM, 80; 113; 115; 119
Orthogonal frequency division multiplexing, 113;119
OSI, 55

P

Patch antenna, 126
PC Card, 41
PCI, 40
PCMCIA, 41
Peripheral Component Interconnect, 40
Phase-shift keying, 78
Plaintext, 155
PoE, 51
Point coordination function, 107
Point-to-point system, 127
Power-ower-Ethernet, 51
Pre-shared key mode, 119
Probe frame, 110
Probe responce, 110
PSF, 107
PSK, 78
Public wireless LAN, 104

R

RADIUS, 46
Repeater, 100
Request to send, 111
Rogue access point, 150
RTS/CTS, 111

S

SARP, 153
SDMA, 146
Secure ARP, 153
Service set identifier, 98
Session persistence, 48
Short massage service, 140
Simple network management protocol, 170
SMS, 140
SNMP, 170
Snooper, 150
Space division multiple access, 146
Spread spectrum, 79
SSID, 98; 109
Status code, 110
Subnet, 46
Supplicant, 163

T

TDM, 119
TDMA, 120; 145
Temporal key integrity protocol, 119; 158
Therminal emulation, 47
TIA, 50
Time division multiple access, 120; 145
Time slot, 120
Time-division multiplexing, 119
TKIP, 119; 158
TPC, 120
Transceiver, 20
Transmit power control, 120

U

Ultrawideband, 81
UMTS, 139
USB-адаптер, 86
UWB, 81

V

Virtual private network, 160
VPN, 160

W

WECA, 117
WEP, 111; 155; 156
WEP2, 158
WEP-ключ, 110
Wi-Fi, 22; 117
Wi-Fi Alliance, 117
Wi-Fi Protected Access, 118; 159
Wired equivalent privacy, 155
Wireless dongle, 86
Wireless ethernet compatibility alliance, 117
Wireless Fidelity, 22
Wireless Internet service provider, 43
Wireless markup language, 141
Wireless middleware, 48
WISP, 43; 130
WML, 141
WPA, 118; 159

А

Автоматический запрос на повторение, 62
Адаптер сетевой, 39
Альянс Wi-Fi, 117
Аналоговый сигнал, 59
Антенна
  всенаправленная, 125
  направленная, 125
  остронаправленная, 126
  полунаправленная, 126
  поляризация,127
Архитектура сети, 54
Ассоциация
  IrDA, 94
  WECA, 117
Атака
  типа отказ в обслуживании, 153
  типа человек посредине, J51
Аутентификация, 46; 110; 160
  взаимная, 151
  открытая, ПО
  с совместно используемым ключом, 110
АЦП, 60

Б

Базовая станция, 43

В

Вектор
  инициализации, 157
  распределения сети, 108
Виртуальная частная сеть, 160
Волокно оптическое, 51

Г

Горячая точка, 104

Д

Динамический выбор частоты, 121
Доступ
  асинхронный, 120
  к среде, 60
  многостанционный с кодовым разделением каналов, 145
  множественный с временным разделением каналов, 145
  множественный с пространственным разделением, 146
  мобильный широкополосной беспроводной,131
  неавторизованный, 150
  с частотным уплотнением, 144

Ж

Живучая связь, 48

З

Затухание, 76
Защищенность, эквивалентная таковой проводных сетей, 155
Зона обслуживания независимая базовая, 110

И

Идентификатор
  зоны обслуживания, 109
  набора служб, 98
Инженерная поддержка, 54
Интервал маячковый, 110
Инфраструктура беспроводной сети, 43

К

Квадратурная амплитудная модуляция, 79
Клиент, 38
Клиентское устройство, 46
Компьютерное устройство, 17; 38
Конечный пользователь, 38
Контроллер доступа, 44
Контроль ошибок, 62
Контрольный признак целостности, 157
Конфигурирование точки доступа, 98
Коэффициент усиления антенны, 126

Л

Логотип Wi-Fi, 118

М

Манипуляция
фазовая, 78
фазовая двоичная относительная, 115
фазовая относительная квадратурная, 115
частотная, 77
Маршрутизатор, 87
Механизм
WPA,118
контроля мощности передачи, 120
Многолучевое распространение, 73
Множественный доступ с временным разделением каналов, 120 ,
Модуляция, 77
квадратурная амплитудная, 79
сверхширокополосная, 81
Мониторинг сети, 53
Мост, 123
базовый, 125
рабочей группы, 125
Мультиплексирование с разделением по ортогональным частотам, 80; 113
Мягкий перезапуск, 49

О

Оптическое волокно, 51
Ответ на зондирующий фрейм, 110
Отказ в обслуживании, 153
Отчетность, 53

П

Пакет ошибок, 62
Пакетирование данных, 49
Перезапуск мягкий, 49
Плата интерфейса сети, 39
Повторитель, 100
Подтверждение, 109
Поле
кода состояния, ПО
продолжительности, 108; 111
Политика безопасности, 164
Поляризация антенны, 127
Пользователь конечный, 38
Помехи, 72; 76
внешние, 73
внутренние, 72
Потери в свободном пространстве, 70
Привязка,111
Приемопередатчик, 20
беспроводной,69
Промежуточное программное обеспечение, 48
Пропускная способность, 58
Проситель, 163
Протокол
CSMA, 50
GPRS, 139
SARP, 153
TKIP, 158
аутентификации расширяемый, 162
динамического конфигурирования узла, 99
преобразования адресов, 151
трансляции сетевых адресов, 99
управления доступом к передающей среде, 107
управления сетью простой, 170
целостности ключа временный, 119; 158
Прямое исправление ошибок, 62
Прямое соединение с базой данных, 47

Р

Радиосигнал, 70
параметры, 70
Распределительная система, 43; 49
Распространение сигналов многолучевое, 73
Расширение спектра, 79
методом прямой последовательности, 79
методом скачкообразного переключения частоты, 79
Режим
RTS/CTS, 111
WEP, 111
инфраструктуры, 103
неплановой сети, 107
предварительного совместно используемого ключа, 119
спящий, 112
энергосбережения, 111
Роуминг через подсети, 46

С

Связь
полнодуплексная, 64
полудуплексная, 64
симплексная, 64
Сертификация Wi-Fi,. 118
Сетевой адаптер, 39
Сеть
глобальная беспроводная, 24
локальная беспроводная, 21
неплановая, 106
одноранговая, 106
персональная беспроводная, 19
пиринговая, 106
региональная беспроводная, 22
случайная, 106
специальная, 106

Сигнал
аналоговый, 59
искажение, 72
маячковый, 109
световой, 74
цифровой, 57
Синхронзация, 87
Система
2.5G, 139
мобильной связи универсальная, 139
открытой аутентификации, 161
пакетной радиосвязи, 128
распределительная, 43; 49
сотовая, 137
сотовая второго поколения, 139
сотовая первого поколения, 138
сотовая третьего поколения, 139
точка-несколько точек, 128
точка-точка, 127
управления сетью, 52
Сканирование, 109
активное, 110
пассивное, 109
Скорость передачи данных, 58
Служба
коротких сообщений, 140
определения местонахождения, 32
Снупер, 150
Сопровождение, 54
Способность
к взаимодействию, 97
пропускная, 58
Справочный стол, 52
Спуфинг, 152
Среда передачи, 37
Стандарт
100BASE-T, 51
10BASE-T, 51
802.11, 107; 112
802. Па, 113
802. lib, 114
802. llg, 115
802.111, 119
802.15, 20; 89
802.16, 23; 130
802.16a, 130
802.1x, 162
802.3, 50
HiperLAN/2, 119
Wi-Fi, 22
на защищенный доступ к Wi-Fi, 159
шифрования данных, 159
шифрования улучшенный, 159
шифрования усовершенствованный, 119
Станция базовая, 43
Стол справочный, 52
Структура сети, 54

Т

Таймер отката, 108
Точка доступа, 43
подставная, 150
тонкая, 45
умная, 44

У

Управление конфигурацией, 53
Управляющая система, 52
Уровень
PMD, 115
модели OSI, 55
шума, 62
Устройство
клиентское, 46
компьютерное, 17; 38

Ф

Фазовая манипуляция, 78
Форм-фактор, 40
Фрагментация, 112
Фрейм
CTS, 111
RTS, 111
запроса на аутентификацию, 110
зондирующий, ПО
ответа на запрос об аутентификации, 110
Функция координации
распределенная, 107
точечная, 107

Ц

ЦАП.60
Цифровой сигнал, 57

Ч

Частотная манипуляция, 77

Ш

Шифрование, 46; 155

Э

Эмулятор терминала, 47
Эффект поляризации, 127

Я

Язык гипертекстовой разметки для беспроводной связи, 141

Научно-популярное издание

Джим Гейер

Беспроводные сети

Первый шаг

Литературный редактор *Г.И. Якименко*
Верстка *О.В. Мишутина*
Художественный редактор *В.Г. Павлютин*
Корректоры *А.В. Луценко, О.В. Мишутина, Т.А. Корзун*

Издательский дом "Вильяме"
101509, г. Москва, ул. Лесная, д. 43, стр. 1

Подписано в печать с готовых диапозитивов 18.06.05.
Формат 70 x Ю0'/$_{16}$. Гарнитура Times. Печать офсетная.
Усл. печ. л. 15,48. Уч.-изд. л. 12,0.
Тираж *3* 000 экз. Заказ № 191.

ОАО «Санкт-Петербургская типография № 6».
191144, Санкт-Петербург, ул. Моисеенко, 10.
Телефон отдела маркетинга 271-35-42.

Cisco Systems

Беспроводные сети

Первый шаг

Ваш первый шаг в мир беспроводных сетей

- Узнайте, как в беспроводных сетях осуществляются передача и прием информации
- Откройте для себя основные концепции, лежащие в основе использования радиочастотных и световых сигналов
- Ознакомьтесь с основными терминами, относящимися к беспроводным сетям
- Примените на практике методы защиты беспроводных сетей

Джим Гейер — основатель и главный консультант компании Wireless-Nets, Ltd. (www.wireless-nets.com), консалтинговой фирмы, которая помогает компаниям разрабатывать и применять беспроводные локальные сети.
Джим — опытный автор, известный обозреватель, опубликовавший немало статей, посвященных беспроводным сетям

Добро пожаловать в мир беспроводных сетей!

Беспроводные технологии позволяют преобразить используемые в настоящее время коммуникационные системы, служащие для передачи речи и данных. Вам предстоит открыть уже существующий новый невидимый мир, наполненный сотовыми телефонами и беспроводными ноутбуками, домашними беспроводными сетями и беспроводными решениями, предназначенными для использования вне помещений.

Не требуется опыта работы с беспроводными сетями!

В книге рассматриваются основы беспроводных сетей, материал излагается простым языком, понятным любому читателю. Здесь дан обзор основных концепций, лежащих в основе беспроводных коммуникаций. Независимо от того, ищете вы пособие, которое поможет вам освоить новую сферу деятельности, оцениваете возможность применения беспроводной сети в своей фирме, планируете установить беспроводную сеть у себя дома или заинтересованы в освоении терминологии новой технологии — эта книга для вас!

Категория: Локальные сети
Предмет рассмотрения: Беспроводные сети

ISBN 5-8459-0852-3

05122

9 785845 908520

Вильямс

www.williamspublishing.com
www.ciscopress.ru
ciscopress.com