



# **Основы построения беспроводных локальных сетей стандарта 802.11**

Практическое руководство по изучению, разработке  
и использованию беспроводных ЛВС стандарта  
802.11

[www.wiley.com/publishing/uk](http://www.wiley.com/publishing/uk)  
[www.ciscopress.ru](http://www.ciscopress.ru)  
[ciscopress.com](http://ciscopress.com)

**Педжман Рошан  
Джонатан Лиэри**



# 802.11 WIRELESS LAN FUNDAMENTALS

Pejman Roshan  
Jonathan Leary

**Cisco Press**

800 East 96th Street  
Indianapolis, IN 46240 USA

# ОСНОВЫ ПОСТРОЕНИЯ БЕСПРОВОДНЫХ ЛОКАЛЬНЫХ СЕТЕЙ СТАНДАРТА 802.11

Педжман Рошан  
Джонатан Лизри



Москва • Санкт-Петербург • Киев  
2004

ББК 32.973.26-018.2 75

Р81

УДК 681.3.07

Издательский дом "Вильямс"

Зам. редакции С.И. Трунов

Перевод с английского и редакция В.С. Гусева

По общим вопросам обращайтесь в Издательский дом "Вильямс" по адресу:  
info@williamspublishing.com, <http://www.williamspublishing.com>

**Рошан, Паджмил, Лиэри, Джонатан.**

**Р81** Основы построения беспроводных локальных сетей стандарта 802.11. : Пер. с англ. — М. : Издательский дом "Вильямс", 2004. — 304 с. : ил. — Парал. тит. англ.  
ISBN 5-8459-0701-2 (рус.)

Книга посвящена беспроводным локальным сетям, соответствующим стандартам серии 802.11. Разрабатываемые согласно этому стандарту Wi-Fi-технологии сейчас бурно развиваются. Поскольку востребованы рынками и дают ощутимые преимущества пользователям. Несмотря на относительно небольшой объем, в книге рассмотрены практически все вопросы, которые могут возникнуть у администратора сети при выборе компонентов, разработке и развертывании беспроводной ЛВС. Книгу можно использовать и в качестве учебника по основам работы беспроводных ЛВС, и как практическое руководство по их разработке и использованию.

ББК 32.973.26-018.2 75

Все названия программных продуктов являются зарегистрированными торговыми марками соответствующих фирм.

Никакая часть настоящего издания ни в каких целях не может быть воспроизведена в какой бы то ни была форме и какими бы то ни было средствами, будь то электронные или механические, включая фотоконтроль, и запись на магнитный носитель, если не есть письменного разрешения издателя Cisco Press.

Authorized translation from the English language edition published by Cisco Press, Copyright © 2004.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Russian language edition published by Williams Publishing House according to the Agreement with R&J Enterprises International. Copyright © 2004.

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

ISBN 5-8459-0701-2 (рус.)  
ISBN 1-5870-3077-2 (англ.)

© Издательский дом "Вильямс", 2004  
© Cisco Press, 2004

# Оглавление

Глава 1. Технологии Ethernet	23
Глава 2. Беспроводные локальные сети стандарта 802.11	41
Глава 3. Технологии физического уровня стандарта 802.11	95
Глава 4. Безопасность беспроводных LAN	131
Глава 5. Мобильность	163
Глава 6. Качество обслуживания беспроводных LAN – стандарт 802.11e	187
Глава 7. Радиочастотный тракт	201
Глава 8. Развертывание беспроводных LAN	223
Глава 9. Будущее беспроводных LAN	243
Глава 10. Конструктивные особенности WLAN	255
Словарь терминов	271
Предметный указатель	282

# Содержание

<b>Об авторах</b>	<b>11</b>
О технических рецензентах	11
<b>Посвящения</b>	<b>12</b>
Благодарности	12
Пиктограммы, используемые в книге	14
Условные обозначения	15
Предисловие	15
<b>Введение</b>	<b>18</b>
<b>Глава 1. Технологии Ethernet</b>	<b>23</b>
Стандарт Ethernet 802.3	23
Ethernet 802.3 и модель OSI	24
Формат фрейма по стандарту 802.3	25
Адресация в Ethernet	26
Архитектура CSMA/CD	27
Диаметр сети Ethernet и ее интервал	27
Одноадресатные, многоадресатные и широковещательные фреймы	28
Общая среда	30
802.3a Fast Ethernet	32
Работа в полнодуплексном режиме	33
Gigabit Ethernet	34
Стандарт 802.3ab 1000BASE-T	35
Стандарт 802.3x 1000BASE-X	35
Интервал Gigabit Ethernet	36
Автоматическое согласование	37
Автоматическое согласование в Gigabit Ethernet	38
<b>Резюме</b>	<b>38</b>
<b>Глава 2. Беспроводные локальные сети стандарта 802.11</b>	<b>41</b>
Обзор топологий WLAN	41
Независимые базовые зоны обслуживания (IBSS)	42
Базовые зоны обслуживания (BSS)	43
Расширенные зоны обслуживания (ESS)	43
Механизм доступа к среде стандарта 802.11	44
Обзор CSMA/CA	44
Фрагментация фрейма по стандарту 802.11	53
PCF	53
Нестандартные устройства	56
Точки доступа-повторители	57
Универсальные клиенты и доступ рабочих групп	58

Беспроводные мосты	59
Операции, осуществляемые на уровне MAC стандарта 802.11	60
Возможность соединения станций	60
Работа в режиме энергосбережения	66
Форматы фреймов MAC стандарта 802.11	70
Резюме	93
<b>Глава 3. Технологии физического уровня стандарта 802.11</b>	<b>95</b>
Концепции беспроводных физических уровней	96
Составляющие физического уровня	98
Беспроводные локальные сети стандарта 802.11a	102
Локальные беспроводные локальные сети со скачкообразной перестройкой частоты (FHSS)	102
Беспроводные локальные сети, использующие широкополосную модуляцию DSSS с расширением спектра методом прямой последовательности	108
Беспроводные локальные сети стандарта 802.11b	112
Подуровень PLCP технологии HR-DSSS стандарта 802.11b	112
Модуляция CCK на подуровне PMD стандарта 802.11b	114
Технология дуплексного пакетного сверхтонкого кодирования (PBSS)	115
Беспроводные локальные сети стандарта 802.11a	116
Стандарт 802.11a	117
Подуровень PLCP технологии OFDM стандарта 802.11a	117
Основа технологии OFDM	118
Настройка OFDM	120
Подуровень PMD технологии OFDM стандарта 802.11a	121
Беспроводные локальные сети стандарта 802.11g	124
Подуровень PLCP стандарта 802.11g	125
ERP-OFDM	126
ERP-PBCC	126
Стандарт 802.11g: резюме	127
Оценка целостности канала (CCA)	127
Резюме	128
<b>Глава 4. Безопасность беспроводных LAN</b>	<b>131</b>
Безопасность беспроводных сетей	131
Обзор систем шифрования	132
Векторы инициализации	133
Режимы с обратной связью	134
Калибровка по стандарту 802.11	134
Механизмы аутентификации стандарта 802.11	137
Аутентификация с использованием MAC-адресов	139
Уязвимость системы защиты стандарта 802.11	140
Уязвимость открытой аутентификации	140
Уязвимость аутентификации с совместно используемым ключом	140
Уязвимость аутентификации с использованием MAC-адресов	142
Уязвимость WEP-шифрования	142
Проблемы управления статическими WEP-ключами	144

Защищенные LAN стандарта 802.11	145
Первая составляющая: базовая аутентификация	145
Вторая составляющая: алгоритм аутентификации	150
Третья составляющая: алгоритм защиты данных	152
Четвертая составляющая: целостность данных	155
Усовершенствованный механизм управления ключами	157
Шифрование по алгоритму AES	160
Резюме	161
<b>Глава 5. Мобильность</b>	<b>163</b>
Характеристики роуминга	163
Механизм роуминга стандарта 802.11	164
Функционирование и применение	164
Домен роуминга	165
Длительность роуминга	167
Роуминг уровня 2	167
Алгоритмы роуминга	167
В какую сторону перемещается пользователь	168
Процесс роуминга уровня 2	171
Роуминг уровня 3	174
Роуминг между доменами роуминга	174
Обзор мобильного протокола IP	176
Туннелирование	182
Резюме	183
<b>Глава 6. Качество обслуживания беспроводных LAN — стандарт 802.11e</b>	<b>187</b>
Задачи по достижению заданного QoS в сетях стандарта 802.11	187
Влияние на QoS полудуплексной среды	188
Перекрывание по совмещенному каналу	189
Влияние скрытого узла на качество связи	189
Обзор механизма QoS	190
HCF в режиме конкуренции — механизм доступа EDCF	190
HCF с работой в режиме поочередного доступа	194
Резюме. Проблемы, стоящие перед EDCF и HCF	198
<b>Глава 7. Радиочастотный тракт</b>	<b>201</b>
Основы радиотехники	201
Основы антенной техники	202
Свойства антенны	203
Типы антенн	207
Основные характеристики приемника	209
Минимальные характеристики радиостанции стандарта 802.11b	209
Минимальные характеристики радиостанции стандарта 802.11a	210
Характеристики системы	211
Индикатор качества беспроводной связи	215
Частоты диапазона ISM	216



Уровни мощности передатчика диапазона 2,4 ГГц ISM	216
Частоты диапазона U-NII, применяемого в WLAN	218
Повышенное радионепущение и спектральная маска диапазона U-NII	219
Ограничения на передаваемую мощность диапазона U-NII	220
Резюме	221
<b>Глава 8. Развертывание беспроводных LAN</b>	<b>223</b>
Развертывание WLAN и влияние приложений	223
Планирование развертывания WLAN	225
Беспроводные LAN с максимальной зоной обслуживания	225
Беспроводные LAN с максимальной пропускной способностью	227
Позднее развертывание точек доступа	228
Картирование места развертывания сети	229
Проблемы, возникающие при картировании места работ	230
Инструменты, используемые при картировании места работ	233
Проведение картирования места работ	234
Исследования более высоких уровней	236
Развертывание LAN стандарта 802.1X	236
Управление беспроводными LAN	239
Резюме	240
<b>Глава 9. Будущее беспроводных LAN</b>	<b>243</b>
Технология VLSi00th	243
Технология UWB	247
Технология FSO	250
WLAN со скоростью передачи 100 Мбит/с	252
Резюме	252
<b>Глава 10. Конструктивные особенности WLAN</b>	<b>255</b>
Сфера розничной торговли	255
Сфера здравоохранения	259
Филиалы, офисы и выездные работники	260
Развертывание сетей в филиалах	260
Выездные работники	262
Сфера образования	264
Доступ в общественных местах	266
Сфера общественной безопасности	267
Резюме	268
<b>Словарь терминов</b>	<b>271</b>
<b>Предметный указатель</b>	<b>282</b>



## Об авторах

**Реджман Рохан** (Reghan Roxhan) — менеджер линейки продуктов (product line manager) подразделения беспроводных сетей (Networking Business Unit) корпорации Cisco Systems. Он руководит продвижением программных продуктов для беспроводных LAN корпорации Cisco, в том числе предназначенных для обеспечения безопасности и управления сетью. Прежде чем перейти в подразделение беспроводных сетей, Реджман проработал шесть лет сетевым инженером, а также техническим руководителем группы сетевых информационных технологий (IT networking group) компании Cisco, где он помогал разрабатывать и развертывать сеть в кампусе корпорации Cisco (Сан-Хосе, Калифорния).

**Джонатан Деври** (Jonathan Deary) — менеджер линейки продуктов подразделения беспроводных сетей корпорации Cisco Systems. Джонатан занимается в основном использованием технологии WLAN вне помещений. Он отвечает за основные продукты и построение сетевых графиков для беспроводных мобильных соединений, а также обеспечивает помощь и руководство в части развертывания наружных сетей системными инженерами. Джон получил степень доктора технических наук (B.S. degree in electrical engineering) в Гарвардском университете и степень магистра электротехники (electrical engineering) в Стэнфордском университете. Он является автором нескольких технических статей по обработке сигналов в беспроводных системах и владельцем патента США на оценку канала для передачи сигналов при мультиплексировании с разделением по ортогональным частотам (OFDM).

## О технических рецензентах

**Брюс Александер** (Bruce Alexander) — технический управляющий по маркетингу (technical marketing manager) подразделения беспроводных сетей корпорации Cisco Systems. Брюс начал работать в Cisco после приобретения ею компании Algorit Wireless Communication, где Брюс был руководителем службы технической поддержки. Он проработал в области радиотехники более 25 лет и занимался технологией радиочастотных WLAN последние 16 лет. Он занимался как аппаратным, так и программным обеспечением в группе проектирования радиосистем в компании Telxon, работал старшим инструктором в центрах народного образования (National Education centers), является соучредителем компании Amentrol Amateur Radio Control. Брюс посещает университет в с. Акроне, где он специализируется по компьютерному программированию и управлению торгово-промышленной деятельностью.

**Дарил Кайзе** (Daryl Kaiser) перешел в группу по разработке беспроводных сетей компании Cisco Systems в 2001 году с целью улучшить характеристики WLAN (с учетом или окружающей радиосреды). Будучи активным участником процесса разработки стандартов IEEE серии 802.11, он помогал разрабатывать проект дополнения IEEE 802.11k на радиомикрометрии. Ранее он отвечал за управление и технические характеристики систем беспроводной обработки сигналов для базовых станций глобальной системы мобильной связи (GSM) — от гигагерц до микроволн. До этого коммерческой деятельности Дарил работал старшим инженером, компанией Silicon Valley, разрабатывая важные алгоритмы для детектирования сигналов и автоматического распознавания.

**Брюс Макмилл** (Bruce McMillin), сертифицированный специалист по объединенным сетям Cisco, сотрудничает с Cisco семь лет в качестве инженера-консультанта по сетям. Последние три года Брюс занимается WLAN и мобильной связью.

# Посвящения

## Педжман Рошан

Моей жене, Шелби, за самоотверженную поддержку всех моих начинаний. Я не знаю, чем я заслужил такого терпеливого, любящего и понимающего партнера. Теперь, когда книга написана, выходные дни снова твои!

Мои родители, Билл и Джен. Вы всегда верили в меня, гордились мной и, прямо или косвенно, оказывали поддержку, в которой я нуждался. И если вам нравится, что у вас такой сын, как я (ха-ха!), я еще более счастлив от того, что у меня такие родители.

## Джонатан Тинри

Мои родители, Норрис и Эдвард, которые передали мне желание достигать успеха и осуществлять мечты. Без вашей любви и поддержки эта книга никогда не была бы написана, как не было бы и других моих достижений.

# Благодарности

## Педжман Рошан

Я начал свою карьеру и должности администратора сети, управляя сетями всевозможных размеров, а также их разработкой. Когда в 2000 году WLAN стали основным направлением оснащения предприятий, я понял то, что всегда делал, когда приходило время изучать новые технологии: попытаться найти книгу издательства Cisco Press. Я ничего не нашел и вынужден был обратиться к чтению (ужас!) спецификации IEEE, чтобы разобраться в этих беспроводных технологиях. Это не было идеальным, которое я должен был пройти в одиночку. Многие люди из моего окружения полагали, что я смогу написать книгу по беспроводным LAN. Именно им я должен быть благодарен.

Мне повезло работать с Раулем Ромеро (Raul Romero), моим коронным другом. Рауль всегда играл положительную роль в моей жизни и карьере и возвращал меня к реальности, когда я собирался надеться слишком. Эта книга не появилась бы без его повседневных советов и если бы не была написана для него.

Мои руководители — Кристин Фэлсетти (Christine Falsetti), Эрик Блауфайрб (Eric Blaufairb) и Брюс Александер (Bruce Alexander), именно они дали мне возможность написать эту книгу. Кристин — отличный “сетевой рабочий” с миллионами контактов и идеями. Ее энтузиазм и поддержка на протяжении всей моей карьеры и команде беспроводных сетей Cisco были бесконечны.

Вы даже не представляете, как я благодарен Эрику Блауфайрбу, моему другу и сослуживцу. Именно Эрик убедил меня в том, что я должен начать работу над этой книгой.

Брюс Александер — технический редактор этой книги, мой руководитель и, что более важно, мой друг. Брюс — это тот человек, к которому шуг за ответами на вопросы, касающиеся взаимодействия или развертывания сети. Он — ходячая энциклопедия по радиотехнике, и его участие в создании этой книги большая честь для меня.

Брис Макмид (Bris McMurdo) — второй технический редактор этой книги. Брис — гуру по части WLAN, до уровня которого мне расти и расти. Я никогда не встречал кого-нибудь, кто был бы так предан работе. Его внимание к деталям и настойчивость на конечный результат — это то, что помогло Джону и мне в мучительном процессе написания технической книги.

Дарил Кайзе (Daryl Kaiser) — специалист по MAC и, к счастью для нас, технический редактор этой книги. Вы можете задать Дарилу любой вопрос относительно стандарта 302.11 — о качестве обслуживания (QoS), радиотракте или чьей-либо, — и он ответит просто и доходчиво. К тому же его помощь обходится очень дешево. Все, что я ему должен, — это оплатить lunch в Le Bonfanger (гарежа супа и кофе Classico — вот все, что он заказывает). Спасибо ему за то, что он стал техническим редактором, сослуживцем и большим моим другом.

Тим Олсон (Tim Olson) благодарно отказался от работы над этой книгой, как в качестве соавтора, так и в роли технического редактора. К счастью для меня, я мог задать ему тысячи копиров, и он всегда отвечал на них, даже на вопросы, касающиеся технологий. Большое спасибо Тиму за техническую помощь — как и подготовке этой книги, так и за игру в гольф. Теперь, когда работа над этой книгой закончена, мы можем пойти туда, где пиво льется рекой и играет маленький Golden Tee.

Я благодарен Бретту Бартоу и Крису Клейленду, редакторам этой книги и мастерам по части постановки задач. Почему эти два профессионала возлись с такими дилетантами, как я и Джон, я не знаю! Большое спасибо им за электронные письма, понимание, терпение и поощрение нашей работы.

Наконец (но не в последнюю очередь), я сердечно благодарю моего соавтора, Джона Лизри, который помог мне подняться после того, как я пал под тяжестью этой книги. Если бы он не был моим соавтором, я остался бы страным парнем с кипой недоброжелательных глав на руках, истощенным из-за потраченных на работу усилий, которому нечего было бы предъявлять издателям.

#### Джонатан Лизри

Прежде всего я хотел бы поблагодарить Педа за предоставление мне возможности "помочь ему выдаться". С момента, когда он упомянул о том, что пишет книгу для Cisco Press и нуждается в соавторе, я вложил в участие в этой работе.

Работа над этой книгой подтолкнула меня лучше разобраться в том, как пишутся книги. — вещь нужно было не только разобраться в особенностях того или иного технического решения, но и описать его, используя повседневный язык. Описание словами того, что может быть записано одним уравнением, представляло для меня наибольшую проблему при работе над этой книгой. Я искренне благодарен Брюсу Александру, Дарилу Кайзе и Брюсу Макмаду за выявление первых набросков и рисунков, которые не согласовывались с текстом.

Наконец, Педа и я многим обязаны Бретту Бартоу, Гранту Манрино и Кристоферу Клейленду за нашу более-менее постоянную и деловитую занятость на соблюдение сроков и руководство нами в процессе написания книги.

## Пиктограммы, используемые в книге



Маршрутизатор



Мост



Концентратор



DSU/CEU



Коммутатор  
Catalyst



Многоуровневый  
коммутатор



ATM-коммутатор



Клиент 100  
ISDN/Frame Relay



Коммуникационный  
сервер



Шпина



Сервер доступа



ПК



ПК с программной  
обеспеченностью



Рабочая  
станция Sun



Mac



Терминал



Сайловый  
сервер



Web-сервер



Станция  
OscoNites



Принтер



Портативный ПК



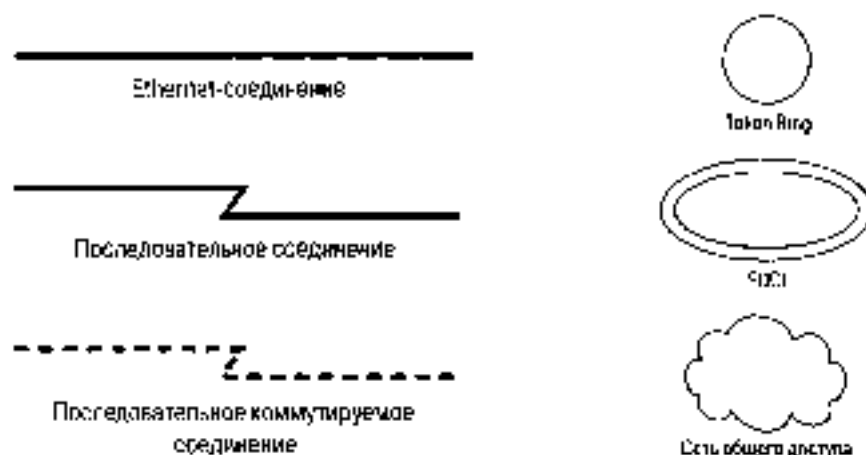
Майн-фрейм  
IBM



Высокоскоростная  
станция



Контрольный  
к56100a



## Условные обозначения

Обозначения, используемые в этой книге для представления синтаксиса команд, точно такие же, как используемые в книге *Ссылка IOS Command Reference*. В упомянутом справочнике по командам используются такие обозначения:

- Вертикальной чертой, |, отделяются альтернативные, взаимоисключающие элементы.
- Квадратные скобки, [ ], указывают на опциональные элементы.
- Фигурные скобки, { }, указывают на обязательный выбор одного из приведенных значений.
- Фигурные и квадратные скобки, [{}], указывают на обязательный выбор среди опциональных элементов.
- Полужирным шрифтом выделены команды и ключевые слова, которые вводятся символами. В примерах конфигурации и результатов (не существующих общепринятому синтаксису команд) полужирный шрифт указывает на команды, которые вручную вводятся пользователем (например, команда show).
- Курсивом обозначаются аргументы, вместо которых должны быть подставлены реальные значения.

## Предисловие

Технология Wi-Fi изменяет мир. Эти изменения касаются того, как мы работаем, играем и взаимодействуем друг с другом. Экономика Wi-Fi быстро изменяет мир за счет видеокадрированных беспроводных служб работы с информацией. Она позволяет пользователю всегда быть "подключенным", удешевляет время, поскольку он может быть продуктивным независимо от того, где находится. И действительно, в то время как я пишу эти строки, я нахожусь в аэропорту г. Токио и ожидаю рейс на Бейджинг, подключившись к локальной Wi-Fi-сети, я получаю электронную почту из США, от которых меня разделяют многие часы полета.

Скромно начав в 1997 году как стандарт на беспроводную передачу данных со скоростью 1 и 2 Мбит/с в стандартизируемом диапазоне 2,4 ГГц, этот стандарт поднял скорость передачи данных в 1999 году до 11 Мбит/с, а недавно и до 54 Мбит/с в частотных диапазонах 2,4 и 5 ГГц. Его популярность быстро растет, поскольку он дает возможность работникам оставаться подключенными к сети, даже когда они находятся вне стен офиса. Многие производители следуют этому общепринятому стандарту и сертификационным программам, нацеленным на обеспечение взаимодействия оборудования разных производителей (эти программы разрабатывает Wi-Fi Alliance). В результате характеристики оборудования улучшаются, а цена быстро падает. Wi-Fi скоро станет популярной и как технологией для потребительского рынка, уже сейчас она стала стандартной для многих моделей ноутбуков и портативных устройств. На сегодняшний день широко распространены сетевые карты для персональных компьютеров (ПК), позволяющие работать со скоростями от 1 до 54 Мбит/с в обоих частотных диапазонах (2,4 и 5 ГГц) при стоимости меньшей, чем большинство людей платит за мобильный телефон. Сравните эту скорость, мобильность и сумму до 700 долларов, которую вы могли бы выложить за модем со скоростью передачи 4600 Кбит/с примерно 10 лет назад, и вы поймете, что технология Wi-Fi развивается с ускорением, которым можно похвастаться лишь немногие технологические компании.

Стандарт 802.11, или Wi-Fi, переходит из изначально присущего ему разряда вертикальных приложений для сканеров, управлений запасами и средств связи для хостовых аппаратов к горизонтальным приложениям, используемым многими из нас дома и на работе. На сегодняшний день Wi-Fi в основном используется как высокоскоростное беспроводное расширение сетей Ethernet, позволяя нам взаимодействовать и без каких-либо усилий с нашей стороны с Internet и нашими фирменными приложениями, где бы мы ни находились – в офисе, аэропорту, доме, в нашем любимом кафе или в ближайшем парке.

Технология Wi-Fi будет продолжать свое внедрение в приложения, о которых ее создатели даже не мечтали. Сейчас разрабатываются новые расширения этого стандарта, которые повысят защищенность, обеспечат поддержку стандарта на качество услуг передачи данных (QoS), улучшат управляемость и повысят скорость передачи данных до уровня, превышающего 100 Мбит/с. Эти новые расширения не только улучшат характеристики Wi-Fi в существующих приложениях, но и позволят реализовать новые, такие как телефонные разговоры с качеством междугородных, использование технологий передачи речи через Wi-Fi для передачи видеосигналов от потребительских электронных устройств на информационное табло, висящее на стене в коридоре дома. Многие из этих приложений уже применяются, другие начнут использоваться, когда Wi-Fi станет частью нашей повседневной жизни. Поскольку интеграция между компьютерами и потребительской электроникой продолжается, возрастает желание соединить эти устройства, не прибегая для этого к каким-либо усилиям. Олажды, ярая в свой любимый магазин электронных товаров, вы купите чирный аудиовизуальный центр, который без проводов будет передавать через вашу домашнюю сеть видеосигналы на дисплей с плоским экраном, расположенный в другой части дома.

Новые расширения стандарта, мобильность клиентов и быстрая эволюция оборудования – все вместе это может привести к некоторым замечательным. Что означают буквы в разновидности стандарта 802.11 и каковы из этих разновидностей представляет для вас интерес? Сколько точек доступа нужно развернуть и где они



должны быть установлены? Что можно сказать о мобильности транспорта и как она повлияет на выполнение старых приложений? Следует ли учитывать какие-то особенности, связанные со спецификой вашего бизнеса? Мы пока еще находимся в начале развития технологии Wi-Fi, и многие интересные вещи еще ждут нас впереди. Эта книга поможет вам быстро разобраться в основах создания сетей и подготовиться к тому еще более интересному, что ждет нас в будущем.

Деннис Этон (Dennis Eaton),  
председатель Wi-Fi Alliance  
([www.wi-fi.org](http://www.wi-fi.org))

# Введение

Сколько раз вам, когда вы были дома, был нужен доступ к Internet, но вы хотели бы перейти работать в другую комнату или вообще выйти во двор и не могли взять с собой длинный кабель Ethernet? Сколько раз вы были в каком-нибудь людном месте, таком как аэропорт или гостиница, и обнаруживали, что вам нужно срочно послать письмо электронной почтой? Сколько часов вы провели в конференц-залах, ожидая начала очередного совещания, а в это время в вашем ящике накапливались электронные письма?

Если вы подобны тысячам других пользователей сетей корпораций, ведомств, университетов, связывающихся со своими фирмами через Internet, сотрудникам, совершающим деловые поездки, или являетесь просто домашним пользователем, ответ будет не один раз. Пользователи сетей получили то, что им нужно: беспроводные локальные сети (WLANs), основанные на стандарте 802.11, предлагают необходимое им решение. Сети, базирующиеся на стандарте 802.11, обеспечивают те мобильность и свободу частот, которые необходимы пользователям сетей.

Беспроводные LAN -- не новая концепция. Они существуют десятки лет. Стандарт 802.11 был ратифицирован в 1997 году, почему же реально WLAN начали развиваться только с этого времени? Все дело в полосе частот и стоимости. Первые беспроводные сети, такие как Aloha, ARDIS и Ricohnet, обеспечивали скорость передачи данных менее 1 Мбит/с. Стандарт 802.11 позволяет производителям обеспечивать взаимодействие со скоростями 2 Мбит/с. В результате ратификации в 1999 году стандарта 802.11b планка поднялась до 11 Мбит/с, эта скорость конкурентоспособна с Ethernet на 10 Мбит/с. Стандарты 802.11a и 802.11g регламентируют скорость передачи данных порядка 54 Мбит/с, что сравнимо с 1 гбит Ethernet при тех же затратах.

Как и первые разработчики WLAN, вертикальные (охватывающие все стадии производства) отрасли, такие как розничная торговля, здравоохранение и производство, оценили преимущества WLAN и беспроводных приложений. Многие из этих отраслей рассматривают WLAN как неотъемлемую часть своего бизнеса. В результате производители стремятся удовлетворить требования, предъявляемые к экономически эффективным, основанным на WLAN техническим решениям, необходимым потребителям такого рода. Благодаря высокому спросу производители могут увеличить объемы производства и снизить себестоимость, а значит, и цену своих изделий, поэтому аппаратное обеспечение WLAN становится доступным потребителям и предприятиям по умеренным ценам.

Хотя сети стандарта 802.11 имеют топологию LAN, они ставят новые проблемы перед сетевыми администраторами, которые привыкли к проводным и основанным на неопределенности проводных технологиям, таким как сети Ethernet стандарта 802.3. Такие проблемы, как картирование места размещения сети, безопасность, качество услуг связи и мобильность сетевых устройств требуют от сетевых администраторов решения неприемлемых для него задач.

Цель этой книги -- рассмотреть аспекты стандарта 802.11 с точки зрения специалиста по информационным технологиям и сетевых инженерии. Книга представляет собой справочное руководство по работе сетей стандарта 802.11 и только неспециалисты в них, а также является первым камнем, заложенным в брешь, образовавшуюся между проводными и беспроводными сетями.

## Структура книги

Начиная с главы 1, "Технологии Ethernet", мы рассматриваем разновидности сетей Ethernet — от Ethernet на 10 Мбит/с до Gigabit Ethernet. В этой главе Ethernet рассматривается как пример жизнеспособности WLAN, и ссылки на эту главу вы встретите неоднократно. Обзор простой и уже зрелой технологии Ethernet должен помочь вам лучше разобраться в проблемах, возникающих при развертывании и планировании WLAN стандарта 802.11.

В главе 2, "Беспроводные локальные сети стандарта 802.11", дан обзор этой технологии в системе координат Ethernet. В ней рассматриваются уровни управления доступом к передающей среде (Media Access Control, MAC) стандарта 802.11 и достаточно подробно — функции, которые им выполняет.

В главе 3, "Технологии физического уровня стандарта 802.11", речь пойдет о технологиях физического уровня (PHY), используемых при создании физических уровней стандартов 802.11a, 802.11b, 802.11g и 802.11n. Они рассматриваются в контексте характеристик основных узлов радиостанций. Кроме того, описывается специфический интерфейс между MAC и PHY, который позволяет легко вносить в стандарт изменения физического уровня.

Глава 4, "Безопасность беспроводных LAN", представляет собой введение в проблемы безопасности, включая вопросы аутентификации и шифрования. Эта информация является "прелюдией" к рассмотрению системы безопасности, как она определена в стандарте 802.11i 1997 года, и слабых мест в системе защиты. В этой главе описаны также детали проекта стандарта 802.11i на безопасность беспроводных сетей, кратко рассматривается защищенный доступ к Wi-Fi (WiFi Protected Access, WPA) и временные спецификации на системы защиты WLAN, обеспечивающие совместимость оборудования разных поставщиков.

В главе 5, "Мобильность", рассматриваются проблемы мобильности клиентских устройств стандарта 802.11. Особое внимание обращается на то, как беспроводные приложения оказывают влияние на развертывание точек доступа (access point, AP). Мобильность клиентов оказывает влияние на MAC-протокол стандарта 802.11, а также на IP-сети, так что кратко рассмотренный мобильный IP-протокол также включен в эту главу.

В главе 6, "Качество обслуживания беспроводных LAN — стандарт 802.11e", рассматриваются проблемы, возникающие при развертывании беспроводных приложений, требующих соединений с малой задержкой, например приложений, обеспечивающих передачу речи через IP (Voice over IP, VoIP). В этой главе дан обзор протокола 802.11 и кратко рассказывается об основных особенностях разрабатываемого стандарта 802.11e — стандарта на QoS беспроводных LAN.

В главе 7, "Радиочастотный тракт", рассматриваются основы технологии передачи сигналов через радиочип применительно к WLAN. Описаны антенны, приемники и характеристики радиосистем; рассказывается о различных лицензируемых радиодиапазонах, используемых в разных странах мира. Цель этой главы — познакомить вас с явлениями, которые вы можете увидеть характеристики физического уровня, обеспечиваемые радиостанциями различных производителей.

Глава 8, "Развертывание беспроводных LAN", посвящена различным аспектам развертывания беспроводной сети — от физического уровня до уровня приложений. После рассмотрения приложений, которые должны использоваться, описываются требования к более высоким уровням, сопровождаемые советами по размерности кли-

кретных сетей. Рассматриваются WLAN, ориентированные на достижение максимальной пропускной способности обслуживания, и WLAN, ориентированные на достижение максимальной производительности. В этой главе описано несколько различных подходов к процессу картирования места развертывания сетей, показано, что для успешной планировки необходим специальный инструментарий. Описаны аспекты развертывания, связанные с политикой обеспечения безопасности WLAN, и инструментарий, необходимый для упрощения задачи.

Глава 9, "Будущее беспроводных LAN", кратко знакомит читателя с тенденциями развития беспроводных технологий. В ней рассматриваются такие технологии, как Bluetooth, Ultra Wide Band, Free Space Optics и будущие наноскопические технологии стандарта 802.11.

В главе 10, "Конструктивные особенности WLAN", читатель узнает о нескольких областях применения WLAN и предъявляемых к ним требованиях. Эти области применения — ритейл, торговля, организации здравоохранения, филиалы предприятий и учебные заведения. Также рассматриваются вопросы использования клиентских устройств от различных производителей. Обращается внимание на специфические потенциальные "разрешающие камни", которые могут встретиться при развертывании WLAN на удаленных площадках. Приводятся примеры конструктивных сетей, обеспечивающих доступ в людных местах, а также описываются специфические требования предъявляемые к WLAN органами, обеспечивающими безопасность граждан.

Одно важное применение Индустрии WLAN развивается эксклюзивно. Каждый день производители предлагают нововведения, благодаря которым WLAN становится более защищенными, удобными в развертывании и управлении и, самое главное, более рентабельными. Эта книга не затумывалась как итоговое описание WLAN. Ее задача — предоставить основные сведения сетевому администратору, чтобы он знал, как следует планировать, развертывать WLAN и работать с ними. Мы выбрали темы и примеры из мира реальных проблем, с которыми сами столкнулись при разработке изделий в компании Cisco Systems и в которых узнали от многих компаний, которые осваивают возможность применения или уже активно развертывают WLAN.

## От издательства

Вы, читатель этой книги, и есть главный ее критик и комментатор. 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, нравятся или нет нам 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 книги 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 контакты:

E-mail: [info@williamspublishing.com](mailto:info@williamspublishing.com)

WWW: <http://www.williamspublishing.com>

Информация для писем из:

Россия: 115419, Москва, а/я 783

Украины: 03150, Киев, а/я 152

## В этой главе...

- Ethernet 10 Мбит/с
- Fast Ethernet 100 Мбит/с
- Gigabit Ethernet 1000 Мбит/с и варианты топологии

## Технологии Ethernet

---

Беспроводные локальные сети (WLAN) — это новейшая технология, пытающаяся привлечь сердца потребителей. Сети WLAN, иногда называемые “беспроводные Ethernet”, или Wi-Fi (for Wireless Fidelity — высокая точность воспроизведения с использованием беспроводной технологии), становятся популярными также потому, что они могут использоваться параллельно с проводными сетями Ethernet. Поэтому, прежде чем детально рассматривать беспроводную Ethernet, имеет смысл сделать обзор технологии проводной Ethernet. Чтобы понять, куда нужно идти, нужно знать, где вы в данный момент находитесь!

Вообще говоря, в иерархии сетей можно выделить три основных уровня.

**Уровень доступа (access layer)**, на котором обеспечивается соединение конечной станции с сетью.

**Уровень распределения (distribution layer)** — сегменты сетей определенного широковещательного домена уровня 2, ограниченного маршрутизаторами, или уровня 3, ограниченного коммутаторами. Службы сети, такие как списки контроля доступа, фильтрация маршрута (route filtering) и трансляция сетевых адресов, работают именно на уровне распределения.

**Базовый уровень (core layer)** предназначен для максимально быстрой пересылки фреймов между уровнями распределения. Не следует искать на этом уровне какие-либо службы, потому что для большинства сетевых сервисов необходимыми уже обработанные фреймы или пакеты, которые неупакованы и коллизируют на всем “протяжении” уровня. Базовый уровень может быть или уровнем 2 (несегментированный уровень), или уровнем 3.

Хотя технологии Ethernet применяются на любом из названных уровней, в этой главе мы рассмотрим в основном их работу на уровне доступа и особенно специфику функционирования семейства Ethernet 802.3.

### Стандарт Ethernet 802.3

Любой сетевой стандарт хорош в случае применения его к изолированной однородной среде. Как правило, в большинстве сетей используются различные топологии. Сети стандарта Ethernet 802.3 включаются с помощью мостов или маршрутизаторов в сети стандарта Token Ring 802.5, сети стандарта ANSI X3T5 FDDI включаются с помощью мостов или маршрутизаторов в сети Fast Ethernet 802.3 и т.д. Для того чтобы обрисовать перспективы использования WLAN, основанных на стандарте 802.11, в проводных сетях и взаимодействии с ними, в следующих разделах рассматриваются следующие темы

- Стандарт 802.3 и эталонная модель взаимодействия открытых систем (OSI).
- Формат фрейма стандарта 802.3.
- Адресация в Ethernet.
- Технологии множественного доступа с контролем несущей и обнаружением коллизии (CSMA/CD).
- Общая среда передачи.

## Ethernet 802.3 и модель OSI

Повторное рассмотрение модели OSI не входит в наши задачи, но для оценки перспектив технологии Ethernet нам следует рассмотреть уровни 2 модели OSI, т.е. канальный уровень передачи данных. Как видно на рис. 1.1, канальный уровень передачи данных имеет два подуровня.

**Канальный подуровень (data link sublayer)**, также известный как уровень MAC (Media Access Control — управление доступом к передающей среде). Характеристики этого подуровня определяются топологией. Например, сети стандарта Token Ring 802.3 используют MAC, отличный от уровня MAC, используемого в сетях стандарта Ethernet 802.3.

**Подуровень управления логическим соединением (logical link control, LLC)**. Общий уровень для всех сетей, основанных на стандарте 802. Предоставляет простой протокол передачи фреймов, который обеспечивает передачу фреймов без установления соединения. Механизм уведомления отправителя о том, что фрейм доставлен или не доставлен, отсутствует.



Рис. 1.1. Эталонная модель OSI

Далее мы рассмотрим подуровень MAC. Он является специфическим для сетей стандарта 802.3. Таким образом, в следующих разделах будут представлены сведения, которые необходимы для чтения всех глав, в которых упоминается подуровень MAC беспроводных сетей.



## Формат фрейма по стандарту 802.3

Структура фрейма, соответствующего стандарту 802.3, представлена на рис. 1.2.

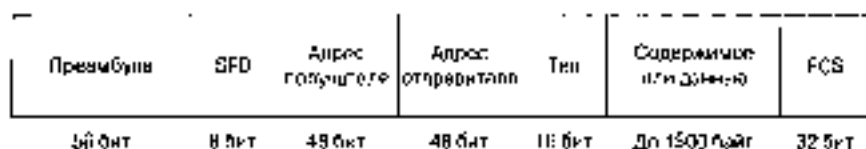


Рис. 1.2. Структура фрейма Ethernet

Фрейм Ethernet состоит из следующих полей (см. рис. 1.2).

**Преамбула.** Представляет собой набор из семи шестерки (октет содержит 8 битов), т.е. всего 56 бит, попеременно принимающих значения 0 и 1. Каждая октет представляет собой следующую битовую комбинацию: 10101010. Преамбула указывает станции-получателю, что передается фрейм. Следует отметить, что в более поздней Ethernet-технологии, рассчитанной на скорость 10 Мбит/с, тоже используются преамбула, хотя нужды в них уже нет.

**Флаг начала фрейма (start of frame delimiter, SFD).** Представляет собой 8-битовое поле, содержащее битовую комбинацию, аналогичную таковой октетом заголовка, но эти последние разряды имеют значение 1 (10101111). Эта комбинация указывает станции-получателю, что вслед за данным полем будет передана содержательная часть фрейма.

**MAC-адрес получателя.** Поле адреса приемника имеет 48 разрядное значение, указывающее адрес станции-приемника, для которой предназначен фрейм.

**Адрес отправителя.** Поле адреса отправителя представляет собой 48-разрядное значение, указывающее адрес станции-отправителя.

**TLV-кодирование (кодирование тип/длина/значение, type/length/value, TLV).** Поле TLV использует 16 разрядов, для того чтобы указать, какой тип протокола более высокого уровня инкапсулирован в поле данных или в поле содержимого пакета. Это поле также называют полем типа фрейма Ethernet: его значение указывает на *режим работы Ethernet (Ethernet type)*. В табл. 1.1 представлены некоторые наиболее часто используемые значения режима работы Ethernet.

Таблица 1.1. Некоторые наиболее часто используемые значения режима работы Ethernet

Значения режима Ethernet	Что оно означает
0800	Internet Protocol (IP)
0806	Протокол разрешения адресов (ARP)
0BAD	Banyan Systems
6304	Протокол сетевого виртуального терминала разработанный Digital Equipment Corporation (LAT)
8037	Internetwork Packet Exchange (IPX) (междетевой пакетный обмен; протокол, используемый в сетях Novell NetWare)
809B	EtherTalk (AppleTalk через Ethernet)
80D5	Сервисы системной сетевой архитектуры IBM (SNA) через Ethernet
80F3	Протокол преобразования адресов AppleTalk (AARP)
8600	IP версии 6

**Содержимое или данные.** Поле содержимого или данных содержит пакеты протокола более высокого уровня и должно иметь ширину не менее 46 бит и не более 1500 бит. Минимальное значение размера данных или содержимого обусловлено необходимостью предоставления места присоединения к каждому стартику. Эту проблему мы рассмотрим далее, в разделе "Диаметр сети Ethernet и ее интервал". Если размер данных или содержимого менее 46 бит, передающая станция дополняет содержимое, чтобы размер поля составил как минимум 46 бит.

**Контрольная избыточность фрейма (FCS).** Поле FCS содержит значение циклического избыточного кода (CRC), вычисленное на основе битовой комбинации фрейма. Когда принимающая станция получает фрейм, она вычисляет его значение CRC и сравнивает с тем, которое содержится в поле FCS. Если эти значения совпадают, считается, что фрейм не содержит ошибок (рис. 1.3).

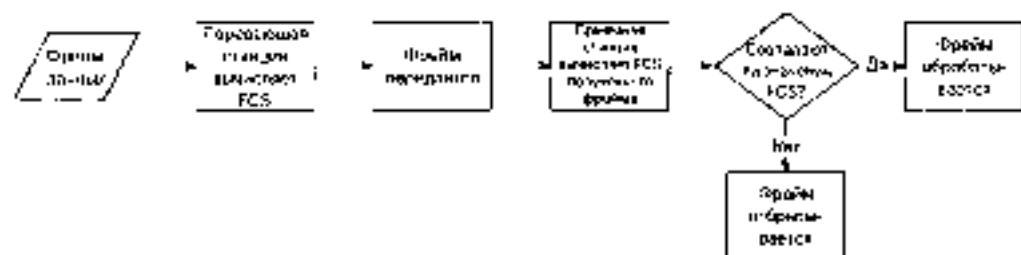


Рис. 1.3. Вычисление значения FCS

## Адресация в Ethernet

Адреса Ethernet представляют собой 48-разрядные значения, которые однозначно идентифицируют Ethernet-станции локальной сети. Ethernet-адреса относятся к категории адресов в рамках глобальной системы идентификации (журнируемой IEEE), которая — производными оборудования. Организация IEEE назначает каждому поставщику 24-разрядный уникальный организационный идентификатор (OUI). Этот идентификатор включается в Ethernet-адрес в качестве первых 24-х разрядов. Благодаря этому гарантируется уникальность Ethernet-адреса. Каждая станция может быть включена в любую сеть мэра и быть одновременно идентифицирована. Поскольку при такой системе адресация используется физический интерфейс, ее также называют *MAC-адресами*. В большинстве случаев MAC-адреса представляются в шестнадцатеричной форме, причем каждый байт отделяется дефисом или подчеркивом, либо каждые два байта отделяются точкой. Например, Ethernet-адрес маршрутизатора Cisco может быть таким:

00-03-6b-4e-e9-20

Это же значение можно представить как

00-03-6b:4e-e9-20 или 00036b4ee920

Организация IEEE назначила для Cisco первые 24 бита, 00-03-6b. Оставшиеся 24 бита, 4e-e9-20, назначаются устройству компанией Cisco. Уникальный организационный идентификатор 00-03-6b позволяет данному производителю назначать адреса в диапазоне 00-03-6b-00-00-00-00-03-ff-ff-ff. Это предоставляет в распоряжение производителя  $10^{24}$ , или 16 777 216, возможных адресов.

## Архитектура CSMA/CD

Стандарт, регламентирующий работу Ethernet, основан на архитектуре CSMA/CD. Это — полудуплексная архитектура, что означает возможность передавать информацию в тот или иной момент времени только для одной станции. Архитектуру CSMA/CD можно сравнить с общением людей, участвующих в селекторном совещании.

- Ни один из участников не знает, когда состоится выступление другого человека.
- Участник, который хочет сделать сообщение, должен ждать у телефона, пока телефонная линия не освободится, только тогда он сможет говорить.
- Когда телефонная линия освобождается, одновременно могут начать говорить два или несколько участников.
- Если двое участников заговорят одновременно, слушателю трудно их понять, поэтому они должны замолчать и подождать, пока линия освободится, прежде чем вновь начать говорить.

Очень похожим образом функционирует Ethernet. Отвечаящая за контроль несущей часть CSMA/CD опирается на возможность станции определить, используется ли среда Ethernet в данный момент. На самом деле наличие сигнала несущей нет, потому что в действительности станции выявляют отсутствие сигнала; это означает в том, что среда передачи свободна. Часть CSMA/CD, относящаяся к множественному доступу, опирается на возможность среды быть доступной одновременно для многих пользователей. Подобно участникам селекторного совещания, все станции имеют одинаковые возможности доступа к среде, но им приходится ждать, пока среда передачи не освободится. Поскольку число станций, использующих Ethernet, возрастает, повышается и вероятность возникновения коллизии фреймов. Коллизия возникает, когда две станции пытаются одновременно передать информацию через одну и ту же среду. Данные, переданные как одной, так и другой станцией, не являются целыми, поэтому станции должны повторно передать информацию. Наконец, обнаружение коллизии означает возможность станций выявлять возникновение коллизий. Технология Ethernet предлагает эффективный механизм повторной передачи для станций, переданные фреймы которых подверглись коллизии.

## Диаметр сети Ethernet и ее интервал

*Диаметр сети* определяется расстоянием между Ethernet-станциями, расположенными на максимально удаленных (противоположных) сторонах ширковещательного домена. Устройства могут быть соединены с использованием кабелей, повторителей, коммутаторов или мостов. Правила, установленные для сетей Ethernet стандарта IEEE.3, требуют, чтобы коллизия была обнаружена в течение времени, которое необходимо для передачи наименьшего по длительности фрейма, допустимого в сети Ethernet. Размер наименьшего допустимого фрейма составляет 64 байт, или 512 бит. С учетом скорости передачи электрического сигнала по проводам и скорости передачи данных (10 Мбит/с) получаем, что максимально допустимая длина провода в сетях Ethernet составит 2000 м. Время, необходимое фрейму Ethernet для преодоления диаметра сети, называется *интервалом Ethernet* (slot time Ethernet).

---

### На заметку

Под ширковещательным доменом понимаются устройства, подключенные к сети, которые могут обмениваться друг с другом фреймами ширковещания.

---

Рассмотрим рис. 1.4, на котором представлены две станции, расположенные на противоположных сторонах широкополосной шины.

- Станция А передает фрейм размером менее 512 бит.
- В тот же самый момент времени начнется передача фрейма станция В.
- Станция А передает последний бит фрейма.
- Станция А не обнаруживает коллизии при передаче и выгружает фрейм из буфера передачи.
- Станция А предполагает, что станция назначения переданного фрейма приняла его.
- Фрейм станции А вступает в коллизию с фреймом станции В.
- Станция А уже выгрузила фрейм из буфера передачи и поэтому не может передать его повторно.

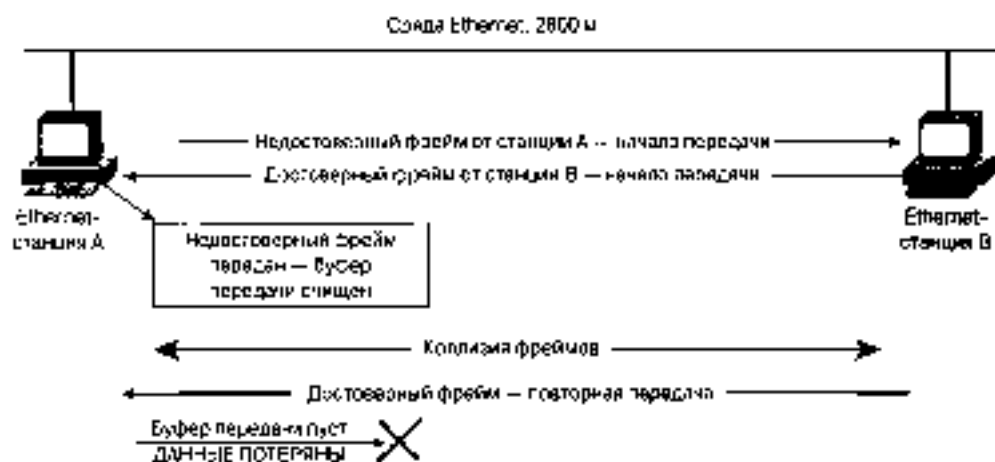


Рис. 1.4 Коллизия в широкополосной шине

Этот сценарий справедлив и для случая, когда прозаженность передающей среды превышает 2800 м.

## Одноадресатные, многоадресатные и широковещательные фреймы

Станция может адресовать передаваемые фреймы тремя способами.

- **Широковещательная адресация.** Станция направляет фрейм всем станциям широковещательного домена.
- **Групповая или многоадресная рассылка.** Станция адресует свои фреймы части (подмножеству) станций широковещательного домена, входящих в предварительно определенную группу.
- **Одноадресатная рассылка.** Станция адресует свои фреймы определенной станции.

Эти типы адресации схематично представлены на рис. 1.5. В сетях Ethernet используются все три метода адресации. Ни один из них не является универсальным, каждый имеет преимущества и недостатки.

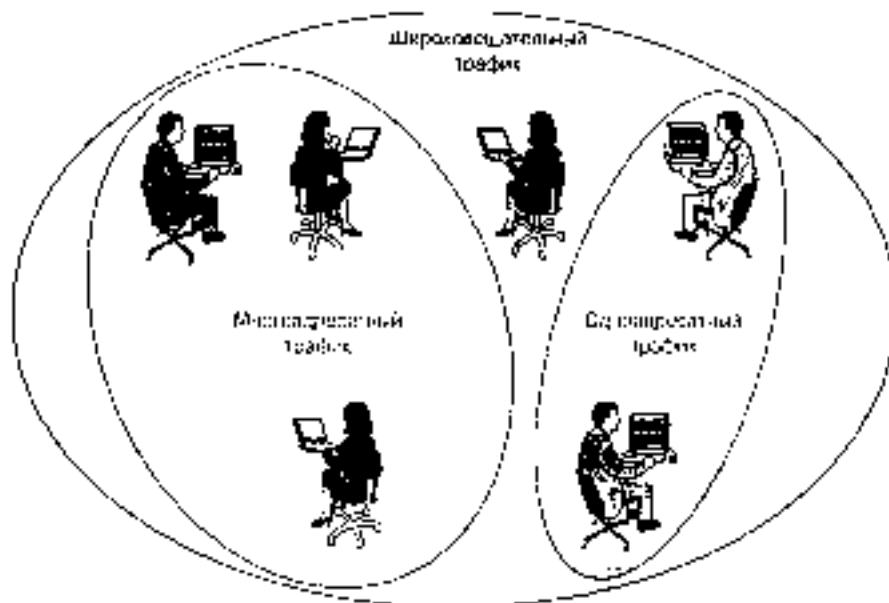


Рис. 1.5. Типы адресации

Широковещательный адрес Ethernet содержит особый 48-разрядный адрес приемника. Это называется "адрес для единицы", потому что все эти биты имеют значение 1 (или  $11$  в шестнадцатеричном виде). Широковещательный адрес может иметь вид  $FF-FF-FF-FF-FF-FF$  или  $(1111-1111-1111)$ . Станция, намеревающаяся передать фрейм всем станциям, посылает фрейм, в котором в качестве адреса приемника указывается широкоэшелетный адрес.

Широковещательные фреймы принимаются и обрабатываются всеми станциями домена. Каждая станция действует в соответствии с алгоритмом, представленным на рис. 1.6; фрейм шлюза содержит ли фрейм данные, предназначенные именно для нее. Станция, получающая "чужие" широкоэшелетные фреймы, использует свой центральный процессор (ЦП) для их обработки, и во время как это должны были бы использовать для своих нужд другие ресурсы станции. Процесс обработки таких фреймов может показаться простым делом, однако, как известно, широкоэшелетная лампа может вызвать перегрузку в сети и подключенных к ней станций.

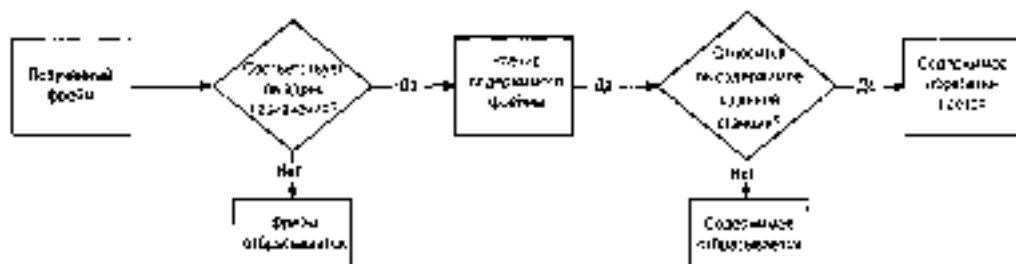


Рис. 1.6. Станция определяет, должен ли она обрабатывать фрейм

Мультиадресные фреймы похожи на широкоэшелетные в том смысле, что они позволяют отправителю направлять их сразу группе получателей, а не одному. Благо-

дари этому процессу в определенных ситуациях снижается нагрузка на сеть за счет того, что станциям не приходится передавать некоторые фреймы несколько раз, чтобы их могли получить все станции, для которых предназначены фреймы. На многоадресные фреймы должна быть "проведена подписка"; это означает, что станция-приемник должна извещать желателее получить их. Если станция-приемник не подписана на многоадресные фреймы, предназначенные определенной группе станций, она отвергает эти фреймы.

В каждом примере рассмотрим процесс передачи для станций потокового видеосигнала. Обычно при этом скорость передачи высокая, и если источник передает видеоинтервал всем станциям широковещательного домена, станция, которая не использует активно видеопоток, тратит большое число тактов ЦП на обработку и отбрасывание содержимого фреймов. Обширивший механизм работы с содержимым потокового видео — *многоадресное IP-вещание*. Фреймы многоадресного IP-вещания передаются по предназначенным специально для этого IP-адресам, содержащим MAC OUI 01-00-5e. Например, расширенный протокол маршрутизации между шлюзами (EIGRP), или протокол маршрутизации IP включает данные об обновлении маршрутов многоадресной группе IP 224.0.0.10. Эта группа соответствует Ethernet-адресу 01-00-5e-00-00-0d. Все устройства, которые заинтересованы в получении данных об обновлении маршрутов EIGRP, получают фреймы с этим адресом получателя. Устройства, не подписанные на получение данных об обновлении маршрутов EIGRP, отвергают такой фрейм.

Вдобавок говоря, многоадресные и широковещательные фреймы могут снизить нагрузку на сеть, позволив станциям получать один фрейм вместо станциям-приемникам одновременно. Но если передающая станция направляет фреймы небольшому числу приемных или даже одной станции, широковещательный и многоадресный трафик могут вызвать ненужную загрузку станций, которым эти фреймы не предназначены.

Одноадресная рассылка представляет собой простейший и прямой способ передачи данных станциям-получателям. Передающая станция направляет фрейм с адресом назначения, соответствующим Ethernet-адресу конкретной станции. Только эта приемная станция получает и обрабатывает фрейм и его содержимое.

Ethernet предлагает еще три метода адресации, благодаря чему приложения могут использовать наиболее приемлемый для них метод и тем самым снизить нагрузку на сеть.

## Общая среда

Ethernet имеет ряд разновидностей, среди которых можно назвать 10BASE2, 10BASE5, 10BASE-T и 10BASE-FL. Каждый из вариантов Ethernet имеет преимущества и недостатки по сравнению с другими типами. Кроме того, некоторые похожие типы сред не упоминали нами из-за малости внебюджетной базы и отсутствия признания со стороны потребителей.

10BASE-T — наиболее часто используемая Ethernet-среда, представляющая собой витую пару. Она позволяет создавать сети с помощью кабелей на витых неэкранированных витых пар (категории 3), предназначенных для передачи речевого сигнала с использованием только двух пар проводков. Хотя разновидность 10BASE-T требует применения кабелей только категории 3, многие используют в таких сетях кабели категории 5 в расчете на дальнейшую модернизацию сетей до уровня 10BASE-TX или 100BASE-T. Кроме того, кабели категории 5 имеют более высокие характеристики, что позволяет повысить качество сигнала. Термин 10BASE-T подразумевает способность

среды передавать сигналы со скоростью 10 Мбит/с с использованием основной пары проводки кабеля на основе витых пар. Разновидность 10BASE-T позволяет передавать сигнал на расстояние, примерно равное 100 м, хотя сама по себе технология Ethernet работоспособна при расстояниях между станциями до 2000 м. Разница в возможностях обусловлена затуханием сигнала в кабелях, созданных на основе неэкранированных витых пар.

Станции при использовании 10BASE-T подключаются к объединяющему их устройству (таким как маршрутизатор, концентратор или коммутатор) в соответствии с топологической схемой "звезда", реализуемой на физическом уровне. Хотя физически сеть имеет топологию "звезда", логически она функционирует как шина (рис. 1.7). Преимуществом топологии "звезда" (на физическом уровне) состоит в том, что выход из строя кабеля, соединяющего с сетью одну из станций, не мешает другим станциям работать в сети.

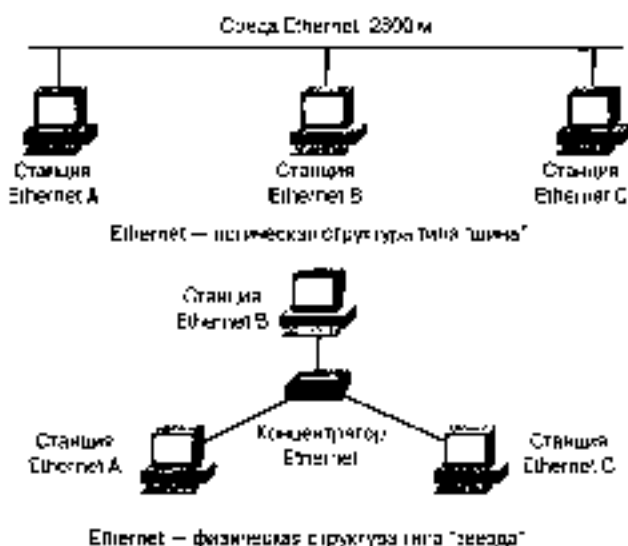


Рис. 1.7 Топология 10BASE-T

Прежде чем топология 10BASE-T завоевала популярность, в мире небольших сетей Ethernet тон задавала топология 10BASE2. Под этой аббревиатурой понимается передача сигнала со скоростью 10 Мбит/с на расстояние до 200 м по коаксиальному кабелю типа RG-58 (рис. 1.9). Хотя цифра "2" в обозначении указывает на 200 м, максимально допустимая длина кабеля для сетей 10BASE2 составляет 185 м. Очевидно, организация IEEE оптимистично округлила цифры в пользу стирну. Технология 10BASE2 была популярной потому, что кабель стоил относительно недорого и сеть можно было быстро развернуть. Сигналы в сетях 10BASE2 передаются по кабелю RG-58 или RG-59, и вся сеть физически соединена в одну непрерывную линию. Станции подключены непосредственно к среде передачи с помощью T-образных соединителей. Повреждение кабеля на любом участке приводит к выходу из строя всей сети.

Другим примером обильной среды передачи может служить разновидность 10BASE5, при использовании которой сигналы передаются по более толстому коаксиальному кабелю (его диаметр примерно соответствует диаметру штыкового шланга). Этот кабель стоит намного дороже и применяется редко. Кроме того, при использовании 10BASE5

станции должны быть оснащены медными трансиверами, которые подключаются к среде передачи через адаптеры. Как и в случае с 10BASE2, повреждение кабеля на любом участке приводит к выводу из строя всей сети.

10BASE-FL — наиболее часто используемый вариант Ethernet с передачей сигналов по волоконно-оптическому кабелю. Допустимая длина кабеля составляет 2 км, поэтому нередко 10BASE-FL используется для соединения удаленных сетей Ethernet. 10BASE-FL использует два оптических волокна, одно для передачи, другое для приема.

## 802.3u Fast Ethernet

По мере того как Ethernet становился все более востребованным стандартом передачи данных в сетях, пользователи начинали требовать расширения полосы пропускания. Чтобы ускорить процесс, в 1995 году IEEE анонсировал стандарт 802.3u, направленный на продвижение Ethernet со скоростью 100 Мбит/с. Хотя существовало несколько решений для передачи данных со скоростью 100 Мбит/с, наибольшее распространение получили два из них, 100BASE-TX и 100BASE-FX (оба называются стандартом 100BASE-X). Технология 100BASE-X основывается на разработанном не организацией IEEE стандарте FDDI (ANSI X3T9.5). FDDI стал стандартом де-факто еще до появления Fast Ethernet и имел ряд преимуществ перед обычным Ethernet.

Технология 100BASE-TX ориентирована на спецификацию 100BASE-X и кабелей категории 5 на основе витой пары. 100BASE-TX во многом аналогична технологии 10BASE-T, но, в отличие от нее, рассчитана на использование кабеля категории 5. Технология 100BASE-TX рассчитана на передачу и приемное высокочастотных сигналов и требует кабелей более высокого качества, нежели кабель категории 3, используемый в сетях 10BASE-T. Ограничения по расстоянию при использовании технологии 100BASE-TX точно такие же (100 м), как и в 10BASE-T. Это означает, что в обоих случаях может использоваться одна и та же кабельная инфраструктура (если она выполнена на основе кабелей категории 5 или более высокого качества).

Диаметр сети и интервал Ethernet для Fast Ethernet отличаются от таковых для Ethernet 10 Мбит/с. Интервал Ethernet ограничивает максимальный диаметр сети условием, что диаметр не должен превышать расстояние, которое преодолит 512-битовый фрейм, прежде чем передающая станция закончит его передачу. Системы Fast Ethernet поддерживают 512-битовый размер фрейма в обеспечение обратной совместимости с предыдущим поколением систем Ethernet.

Для сетей Ethernet максимальный диаметр составляет 200 м. В случае 100BASE-TX операция передачи заканчивается в 10 раз быстрее, чем требуется для ее проведения станциями Ethernet. Соответственно, для того чтобы передающая станция успела обнаружить коллизии в ходе передачи 512-битового фрейма, он не должен пройти более чем одну десятую пути, характерного для Ethernet. Этот предел снижает диаметр сети приблизительно до 200 м. Такое сокращение допустимого расстояния не создает какую-либо проблему, поскольку в большинстве систем Fast Ethernet используется технология 100BASE-TX, для которой максимальное расстояние составляет лишь 100 м.

Технология 100BASE-FX является разновидностью технологии 100BASE-TX, в которой среда передачи является многомодовое оптическое волокно. Сетевая карта генерирует электрические сигналы в виде импульсов, которые передаются по волокну сетевой карте приемной станции. Эта сетевая карта осуществляет обратное преобразование сетевых импульсов в электрические сигналы, которые и обрабатывает станция-приемник.



Технология 100BASE-FX использует такой же механизм кодирования, как и 100BASE-TX, но на этом сходство между ними и заканчивается. Поскольку 100BASE-FX использует в качестве носителя данных свет, ее сигналы не подвержены влиянию электромагнитных помех. Благодаря этому можно использовать более совершенные схемы передачи сигналов. Диаметр сети для технологии 100BASE-FX составляет примерно 400 м при работе в полдуплексном режиме. В сетях на основе 100BASE-FX можно использовать также полнодуплексный режим (о нем мы будем говорить ниже). При работе в полнодуплексном режиме не возникает проблема коллизий, поэтому максимальное расстояние может значительно превышать 400 м. И действительно, при использовании в качестве среды передачи оптоволоконного кабеля с оптическим диаметром сердцевины/оболочки 62,5/125 мкм 100BASE-FX способна работать в полнодуплексном режиме при расстояниях между станциями до 2 км. По мере необходимости дальнейшего увеличения расстояния можно использовать оптоволоконные кабели с оптическими диаметрами сердцевин/оболочек в этом случае максимально допустимое расстояние превышает 40 км. Стоимость оптоволоконного кабеля и предназначенных для работы с ним приемопередатчиков на порядок превышает стоимость кабелей для многопользователя, но технические проблемы существуют, и по необходимости его можно использовать.

## Работа в полнодуплексном режиме

CSMA/CD — это методология, на которой основаны полудуплексный Ethernet и Fast Ethernet. Как уже говорилось ранее, технология CSMA/CD напоминает селективное совещание, проводимое с помощью телефонной связи. Каждый участник должен ждать, пока среда передачи освободится, и только после этого он может говорить. В 1995 году IEEE утвердил стандарт 802.3х, в котором описывается новая методология передачи сигналов в сетях Ethernet, известная как работа в *полнодуплексном* режиме. Такой режим работы позволяет передавать и принимать сигналы одновременно, благодаря чему более полно используются возможности среды передачи (рис. 1.8). Однако требования, предъявляемые к станциям, работающим в полнодуплексном режиме, существенно меняются.



Рис. 1.8. Работа в полнодуплексном режиме

Полнодуплексный режим применим только к устройствам, соединенным по схеме "точка-точка". В домен коллизий может входить только одно другое устройство. Станции, подключенные к концентраторам (хабам), повторителям и т.п., не могут функционировать в полнодуплексном режиме. Станции, непосредственно соединенные одна с другой (connected back-to-back) или подключенные на уровне 2, способны работать в полнодуплексном режиме.

Способность передавать и одновременно принимать сигналы позволяет станциям полнее использовать возможности среды передачи. Доступная станциям ширина полосы пропускания теоретически удваивается, поскольку станция имеет полный доступ к среде как при передаче, так и при приеме сигнала. В случае использования техни-

логии 100BASE-TX это дает каждой станции возможность обмениваться информацией с максимальной скоростью до 200 Мбит/с. Для конечной станции, например ПК, это означает, что несколько станций могут передавать и принимать информацию одновременно. Серверы и устройства инфраструктуры сети, такие как повторители и коммутаторы, могут получить такие преимущества от работы в полнодуплексном режиме только в целостных конечных станциях. Эти устройства группируют сеансы связи и соединения от периферии сети к ее центру и обратно. Они передают и получают трафик как приема, так и передачи, потому что вся сеть способна получить максимальную пользу от расширения полосы пропускания, обеспечиваемого полнодуплексным режимом работы.

Полнодуплексный режим работы позволяет технологии Ethernet избежать ограничений на расстановку передатчиков, характерных для полудуплексного режима. Ирония судьбы заключается в том, что преимущества от увеличения расстояния можно реализовать только с помощью волоконно-оптического интерфейса (используемого в технологии 100BASE-FX), поскольку ограничения, накладываемые на максимальное расстояние при использовании кабелей на основе витых пар, обусловлены физическими свойствами среды передачи, а не диаметром сети, который ограничен интервалом Ethernet или Fast Ethernet.

---

### На заметку

Полнодуплексные устройства не могут работать совместно с полудуплексными. Главная проблема сетей с разнородной средой передачи состоит в возникновении «ошибок дуплексного несоответствия» (duplex mismatch errors). Эти ошибки появляются при соединении полудуплексной и полнодуплексной станций. В результате возникает множество ошибок при передаче пакетов, таких как незадавленная коллизия и утерянные пакеты. Полнодуплексные устройства начинают передавать данные, как только могут сделать это, не контролируя наличие несущей в среде передачи. Если полудуплексное устройство передает в это время информацию, возникает коллизия, которую полнодуплексное устройство не обнаруживает. Поэтому так важно спланировать режимы работы входящих в сеть устройств.

---

## Gigabit Ethernet

В результате перехода от Ethernet к Fast Ethernet пользователи получили в десять раз более широкую полосу передачи сигналов Gigabit Ethernet, с его скоростью 1000 Мбит/с, предлагает в смысле привлекательной стоимости тот же резкий переход для производителей, но разница в 900 Мбит/с расширяет возможности гораздо больше, чем разница 90 Мбит/с. Столь существенное расширение полосы пропускания создает серьезные проблемы для разработчиков, которые должны решить возникающие при таком переходе проблемы, связанные с диаметром сети и разводкой кабелей. Gigabit Ethernet имеет две основные разновидности.

- **1000BASE-T.** Как и технологии 100BASE-T и 100BASE-TX, может использовать кабели с неэкранированными витыми парами длиной не более 100 м.
- **1000BASE-X** имеет три варианта.
  - **1000BASE-SX.** Волоконно-оптический среды передачи на основе стандартных многомодовых волокон, предназначенная для использования на коротких расстояниях (до 300 м).

- **1000BASE-LX.** Волоконно-оптическая среда передачи на основе одномодовых волокон, предназначенная для использования на расстояниях до 10 км, в некоторых случаях допускает использование многомодовых волокон.
- **1000BASE-CX.** Экранированная медная среда, используемая в случаях небольших расстояний между устройствами. 1000BASE-CX применяется при расстояниях не более 25 м.

## Стандарт 802.3ab 1000BASE-T

Развитие стандарта 1000BASE-T явилось следствием усилий по внедрению стандарта Fast Ethernet. Поиск идеального решения для Fast Ethernet на основе медной среды передачи привел к появлению 100BASE-TX. Хотя теперь уже не все об этом говорят, изначально было два других стандарта: 100BASE-T4 и 100BASE-T2. Стандарт 100BASE-T4 не завоевал популярности, потому что требовал использования всех 4-х пар кабелей категории 3 или 5. Однако некоторые сети имели разилку, выполненную на основе кабелей категории 3 или 5 только с двумя витыми парами (что вполне соответствует требованиям стандарта 10BASE-T). Недостатком стандарта 100BASE-T4 было также то, что он не поддерживал работу в полнодуплексном режиме.

Стандарт 100BASE-T2 был более удобным, поскольку предусматривал передачу данных со скоростью 100 Мбит/с по кабелям категории 3 с использованием только двух витых пар. Проблема состояла в том, что ни один производитель не поддерживал этот стандарт. Однако когда пришло время предложить гигабитовое решение для стандарта Ethernet, разработчики одновременно все лучшее из всех стандартов на 100 Мбит/с и объединили их в спецификацию на технологию 1000BASE-T.

## Стандарт 802.3z 1000BASE-X

Стандарт 802.3z был утвержден в 1999 году и включает в число стандартов 802.3 Спецификация 1000BASE-X предусматривает использование среды в виде оптических волокон. Лежащая в основе этого стандарта технология сама по себе не нова, поскольку основана на стандарте ANSI Fibre Channel (ANSI X3T11). Технология 1000BASE-X допускает использование трех различных сред передачи, откуда три разновидности: 1000BASE-SX, 1000BASE-LX и 1000BASE-CX. Наиболее часто используется самая дешевая технология 1000BASE-SX на основе стандартного многомодового волокна. За дешевизну приходится платить максимальные расстояния для 1000BASE-SX составляет 220 м (сравните: полнодуплексная технология 100BASE-FX допускает передачу на расстояние 2 км). Технология 1000BASE-LX обычно используется с одномодовыми волокнами, здесь допустимое расстояние составляет 5 км.

Технология 1000BASE-CX использует наиболее своеобразную среду из трех. Это основано на применении меди решения, в котором используются кабели, выполненные на основе предварительно закрученных (prestranded) экранированных витых пар. Соединитель — не просто RJ-45, обычно используются в 10/100/1000BASE-T. Вместо него используется или 10B-9, или HSSDS, завершающий эти две пары проводов. Технология 1000BASE-CX пригодна для расстояний до 25 м, что ограничивает ее применение небольшими площадками. 1000BASE-CX трудно отнести к популярным, потому что 1000BASE-T выполняет те же функции за меньшую цену и передает сигналы на вчетверо большее расстояние, причем использует для этого стандартную разводку на основе кабелей категории 5 с четырьмя витыми парами.

## Интервал Gigabit Ethernet

С диаметром сети в Gigabit Ethernet возникают проблемы. При работе в полудуплексном режиме действует правило Ethernet относительно 512-битового фрейма — фрейма минимально допустимого размера, установленного для того, чтобы все станции могли его "услышать" и послать сообщение об обнаружении коллизии всем станциям, прежде чем передающая станция выгрузит фрейм. Если следовать этой методологии, описанной в нами в предыдущих разделах, то максимальная длина кабелей в системах 1000BASE-T и 1000BASE-X была бы примерно величиной 20 м, потому что эта среда способна передавать фреймы в 10 раз быстрее, чем ее предшественница (грубо говоря, 200 м, характерные для среды 1000BASE-TX, деленные на 10, дают 20 м).

Кабелей длиной 20 м явно недостаточно в большинстве ситуаций, поэтому, чтобы преодолеть названный предел, IEEE потребовал для Gigabit Ethernet увеличения минимального размера фрейма в 8 раз — до 4096 бит (512 байт). Вместо того чтобы "наблизать" полезную часть фрейма бесполезной информацией, этот стандарт вводит новую характеристику, получившую название *расширение несущей* (carrier extension).

Предпожим, например, что Gigabit Ethernet-станция обнаруживает, что среда передачи свободна и пытается передать 512-битовый фрейм. Сетевая плата добавляет к концу фрейма расширение, состоящее из 3584 бит. Другим стандартам Gigabit Ethernet известно, что эти биты не несут какой-либо информации, однако считаются частью фрейма (рис. 1.9). Когда станция-приемник получает такой фрейм, она отбрасывает расширение несущей. Благодаря этому процессу небольшие фреймы можно передавать, не беспокоясь об угрозе возникновения запоздалой коллизии.

Метод расширения несущей решает проблему диаметра сети, однако он порождает другую. Для каждого переданного фрейма размером 512 бит передается также в 7 раз более многочисленные биты расширения несущей. Это — явное расточительство по отношению к пользе пропускания. Для снижения "накладных расходов" стандарт предписывает в качестве дополнительного использовать *лакейный режим* (burst mode), позволяющий решить проблему диаметра сети в неэффективного использования пользы пропускания.

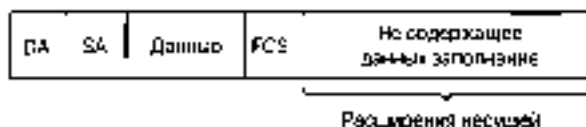


Рис. 1.9. Расширение несущей в Gigabit Ethernet

Пакетный метод позволяет объединять небольшие фреймы: в промежутках между ними передаются биты расширения несущей. Другие станции ожидают очереди на передачу, "слыша" на межфреймовые пробелы (interframe gaps), при этом они обнаруживают несущую и воздерживаются от передачи. Стандарт позволяет передавать до 64 Кбит в пакетном режиме, прежде чем будет послан стандартный межфреймовый пробел.

При использовании этого механизма вначале передается маленький фрейм размером 4096 бит (включая биты расширения несущей). Это делается во избежание возникновения коллизий с фреймами, переданными другими станциями. После успешного приема первого фрейма последующие межфреймовые пробелы заполняются битами расширения несущей, чтобы другие станции не могли занять среду передачи (рис. 1.10). Последующие фреймы передаются без битов расширения несущей. Стан-

ция может пакетировать до 64 Кбит дополнительных фреймов, прежде чем должна освободить среду передачи (рис. 1.11). Этот механизм, хотя и не обеспечивает оптимальной, все же позволяет полностью использовать возможности среды, чем это происходит при использовании только расширения несущей.

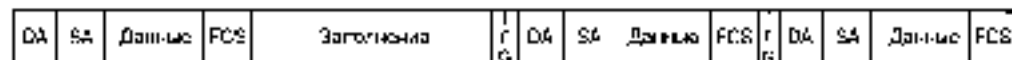


Рис. 1.10. Метод пакетирования в среде Gigabit Ethernet

### На заметку

Расширение несущей и метод пакетирования необходимо применять только при работе в полудуплексном режиме. При работе в полнодуплексном режиме станциям не приходится конкурировать за контроль над средой передачи, поэтому не приходится беспокоиться об интервале Ethernet и о связанном с ним минимальном размере фрейма.

## Автоматическое согласование

Поскольку при использовании Ethernet возможны этногенезисные комбинации скоростей передачи и дуплексных режимов, для повышения совместимости используемых устройств был предложен механизм *автоматического согласования*. Вообще говоря, механизм согласования скоростей и дуплексных режимов был разработан для среды передачи "витая пара", поскольку устройства, ориентированные на использование многоканной оптики, не поддерживают автоматическое согласование; это относится ко всем типам мультимедийно-оптической среды передачи.

Процесс автосогласования начинается, когда устройство определяет активность канала на своем интерфейсе.

- Устройство посылает быстрый канальный импульс (fast link pulse, FLP), оповещая о желательных для себя скорости и режиме передачи. В табл. 1.2 представлены иерархия предпочтительных режимов передачи.
- Если удаленная станция поддерживает автоматическое согласование, она посылает в ответ быстрый канальный импульс, указывая свои предпочтения.
- Обе станции автоматически выбирают наиболее выгодный режим передачи и ее скорость из числа поддерживаемых обеими станциями.

Таблица 1.2. Иерархия режимов автосогласования

Приоритет	Режим работы
1	100BASE-TX, полнодуплексный режим
2	100BASE-T4
3	100BASE-TX
4	10BASE-T, полнодуплексный режим
5	10BASE-T

Если одна станция поддерживает автоматическое согласование, а другая нет, в результате автоматического согласования все равно выбирается среда, устраивающая обе стороны. Допустим, станция старого образца 10BASE-T может быть подключена

к коммутатору, поддерживающему автоматическое согласование. Коммутатор посылает станции 10BASE-T быстрые каналные импульсы, предлагая работу в полнодуплексном режиме со скоростью 100 Мбит/с. Станция 10BASE-T “не понимает”, что посылает полнодуплексный импульс, и игнорирует сигналы автоадаптации. Иначе говоря, станция 10BASE-T не способна послать быстрые каналные импульсы, поскольку не поддерживает технологию автоадаптации. Порт коммутатора “понимает”, что это быстрый каналный импульс преобразованный и что, следовательно, он имеет дело со станцией типа 10BASE-T. В данном случае, поскольку станция 10BASE-T не поддерживает автоматическое согласование, коммутатор интерпретируется к “принимателю общему знаменателю”, которым и является станция 10BASE-T.

Хорошо, но что будет, если используется станция 100BASE-TX, работающая в полнодуплексном режиме и не поддерживающая автоматическое согласование? Неужели она начнет туго работать в режиме станции 10BASE-T? Ответ отрицателен. Быстрые каналные импульсы основаны на канальных импульсах сети (network link pulse, NLP), описанных в стандарте Ethernet. Канальные импульсы сети — это периодические послепериодические импульсы, огибающей рода “пульс” Ethernet. Быстрые каналные импульсы выполняют аналогичные функции в сетях 100BASE-X, только передаются они в 10 раз чаще. Поэтому, хотя станция 100BASE-TX и не поддерживает автоматическое согласование, она посылает быстрые каналные импульсы, указывающие коммутатору, что данная станция способна работать на скорости 100 Мбит/с. Именно благодаря этой информации устройствам, поддерживающим автоадаптацию, удается определить, с какой станцией они имеют дело, 100BASE-TX или 10BASE-T.

## Автоматическое согласование в Gigabit Ethernet

В сетях Gigabit Ethernet автоматическое согласование осуществляется иначе, чем в сетях Ethernet и Fast Ethernet. Используемая в качестве передающей среды медь, технология 1000BASE-T применяет, как и следовало ожидать, тот же механизм, что и другие технологии. Но 1000BASE-X использует иной механизм. Автоматическое согласование зависит от используемой среды передачи, в результате только устройства 1000BASE-X могут автоматически согласовывать работу друг с другом. Поскольку скорость доступа предопределена (т.е. согласование скоростей передачи не производится), единственной возможностью — дуплексный режим. В отличие от Ethernet и Fast Ethernet, быстрые каналные импульсы не используются для автоматического согласования и играют незначительную роль по сравнению с управляющими сигналами, что характерно для всех технологий 1000BASE-X, независимо от типа используемой среды.

## Резюме

Ethernet эволюционирует, стараясь удовлетворить новым требованиям, предъявляемым к ней пользователями и администраторами сетей. Она продолжает эволюционировать и после появления Gigabit Ethernet — на горизонте уже маячит Ethernet 10 Гбит/с. В табл. 1.3 приведены основные параметры (топология и среда передачи) семейства Ethernet. Каждая топология находит свое место при развертывании сетей, удовлетворяя таким параметрам, как стоимость, требуемая скорость передачи данных, протяженность и уже имеющаяся кабельная проводка. Для протокола Ethernet характерна обратная совместимость, благодаря чему новые топологии появляются, совершенствуются и получают статус стандартных.

Таблица 1.3. Ethernet-технологии

Топология	Скорость передачи данных (Мбит/с)	Среда передачи	Максимальная протяженность среды (М)
10BASE5	10	Толстый коаксиальный кабель	485
10BASE2	10	Тонкий коаксиальный кабель RG-58	185
10BASE-T	10	Две неэкранированные витые пары кабелей категории 3/5	100
10BASE-FL	10	Двухжильный многомодовый волоконно-оптический кабель	2000
100BASE-TX	100	Две неэкранированные витые пары кабелей категории 5	100
100BASE-FX	100	Двухжильный многомодовый волоконно-оптический кабель	2000
1000BASE-T	1000	Четыре неэкранированные витые пары кабелей категории 5	100
1000BASE-CX	1000	Экранированные витые пары	25
1000BASE-SX	1000	Двухжильный многомодовый волоконно-оптический кабель	
1000BASE-LX	1000	Двухжильный одномодовый волоконно-оптический кабель	10 000

В этой главе...

- Обзор топологий бесконечных локальных сетей
- Механизм доступа к среде по стандарту 802.11
- Операции на уровне MAC по стандарту 802.11
- Форматы фреймов по стандарту 802.11



## Беспроводные локальные сети стандарта 802.11

Беспроводные локальные сети стандарта 802.11 получили все большее распространение в основном благодаря тому, что они просты в развертывании и удобны в эксплуатации. С точки зрения пользователя их функции и характеристики почти такие же, как и у разделенных (shared) локальных сетей Ethernet. Но архитектуру 802.11 можно назвать какой угодно, только не простой. Проблемы, которые приходится решать в неконтролируемой среде, сложнее, чем в контролируемой проводной среде Ethernet.

Подуровень MAC стандарта 802.11 должен управлять механизмом, обеспечивающим беспрепятственный доступ к среде передачи. Станции стандарта 802.11 не обладают способностью обнаруживать коллизии, как это делают Ethernet-станции, осуществляющие множественный доступ к среде с контролем несущей и обнаружением коллизии. Реализация этого для доступа к среде необходима более сложный и масштабируемый подуровень MAC при минимальных дополнительных издержках.

В данной главе рассматриваются основные механизмы доступа к среде стандарта 802.11.

### Обзор топологий WLAN

Сети стандарта 802.11 можно конструировать по-разному. Разработчик может выбрать любую из следующих топологий.

- Независимые базовые зоны обслуживания (independent basic service sets, IBSSs).
- Базовые зоны обслуживания (basic service sets, BSSs)
- Расширенные зоны обслуживания (extended service sets, ESSs)

Зона обслуживания (service set) в данном случае — это логически сгруппированные устройства. Технология WLAN обеспечивает доступ к сети путем передачи широкополосных сигналов через эфир на несущей в диапазоне радиочастот. Принимающая станция может принимать сигналы в данной зоне работы нескольких передаточных станций. Передаточная станция вначале передает идентификатор зоны обслуживания (service set identifier, SSID). Станция-приемник использует SSID для фильтрации поступающих сигналов и выделения того, который ей нужен.

## Независимые базовые зоны обслуживания (IBSS)

IBSS представляет собой группу работающих в соответствии со стандартом 802.11 станций, связывающихся непосредственно одна с другой. IBSS также известен специализацией, или сетью (ad-hoc), сетью, потому что она по сути представляет собой простую одноранговую WLAN. На рис. 2.1 показано, как две станции, оборудованные беспроводными сетевыми интерфейсными картами (network interface card, NIC) стандарта 802.11, могут формировать IBSS и напрямую связаться одна с другой.

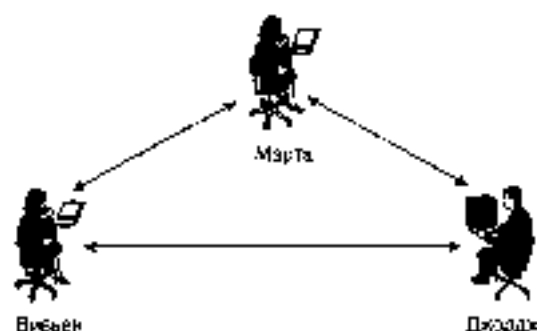


Рис. 2.1. Независимая (ad-hoc) сеть (IBSS)

Специальная сеть, или независимая базовая зона обслуживания (IBSS), идентифицирует, когда отдельные устройства-клиенты формируют самоподдерживающуюся сеть без использования отдельной точки доступа. При создании таких сетей не разрабатывают какие-либо карты места их развертывания и предварительные планы, поэтому они обычно невелики и имеют ограниченную протяженность, достаточную для передачи совместно используемых данных при возникновении такой необходимости. В отличие от варианта использования расширенной зоны обслуживания (ESS), клиенты непосредственно устанавливали соединения друг с другом, в результате чего создается только одна базовая зона обслуживания (BSS), но без интерфейса для подключения к проводной локальной сети (т.е. отсутствует какая-либо распределительная система, которая необходима для глобальной IBSS и организации таким образом ESS). Не существует каких-либо отраслевых стандартов ограничений на количество устройств, которые могут входить в одну независимую базовую зону обслуживания. Но, поскольку каждое устройство является клиентом, зачастую определенное число членов IBSS не может связываться (или с другим вследствие проблемы скрытого узла (hidden node issue)). Несмотря на это, в IBSS не существует какого-либо механизма для реализации функции ретрансляции.

Поскольку в IBSS отсутствует точка доступа, распределение времени (timing) осуществляется децентрализованно. Клиент, участвующий в передаче в IBSS, запрашивает специальный (его еще называют маячковый) интервал (beacon interval) для создания набора моментов времени передачи маячкового сигнала (set of target beacon transmission time, TBTT). Когда завершается TBTT, каждый клиент IBSS выполняет следующее:

- Приостанавливает все несработавшие таймеры задержки (backoff timer) на предыдущего TBTT.
- Определяет новую случайную задержку.
- Если маячковый сигнал поступает до окончания случайной задержки, возобновляет работу приостановленных таймеров задержки. Если никакой маячко-

ции сигнал не поступает до окончания случайной задержки, посылает маячковый сигнал и возобновляет работу приостановленных таймеров задержки.

Вы можете, что распределение времени для передачи маячковых сигналов осуществляется в специализированных сетях не только доступ и не каким-то одним из клиентов. Поскольку такой схеме связи присуща проблема скрытого узла, вполне возможно, что в течение сигнального интервала будет передано множество маячковых сигналов от разных клиентов и другие клиенты получат множество маячковых сигналов. Однако стандарт вполне допускает такую ситуацию и никаких проблем не возникает, поскольку клиенты ожидают приема только первого маячкового сигнала, относящегося к их собственному таймеру случайной задержки.

В маячковые сигналы встроена функция синхронизации таймера (*timer synchronization function, TSF*). Каждый клиент сравнивает TSF в маячковом сигнале со своим собственным таймером и, если полученное значение больше, считает, что часы передающей станции идут быстрее и подстраивает свой собственный таймер в соответствии с полученным значением. Это имеет долговременный эффект синхронизации работы всей беспроводной сети по клиенту с самым быстрым таймером. В больших распределенных беспроводных сетях, когда многие клиенты не могут связываться напрямую, может потребоваться некоторое время для достижения синхронизации всех клиентов.

## Базовые зоны обслуживания (BSS)

BSS — это группы работающих по стандарту 802.11 станций, связывающихся одна с другой. Технология BSS предполагает наличие особой станции, которая называется *точкой доступа (access point)*. Точка доступа — это центральный пункт связи для всех станций BSS. Клиентские станции не связываются непосредственно одна с другой. Вместо этого они связываются с точкой доступа, а уже она параллельно формирует станции-адресату. Точка доступа может иметь порт восходящего канала (*uplink port*), через который BSS подключается к проводной сети (например, входящий канал Ethernet). Поэтому BSS иногда называют инфраструктурой BSS. На рис. 2.2 представлена типичная инфраструктура BSS.

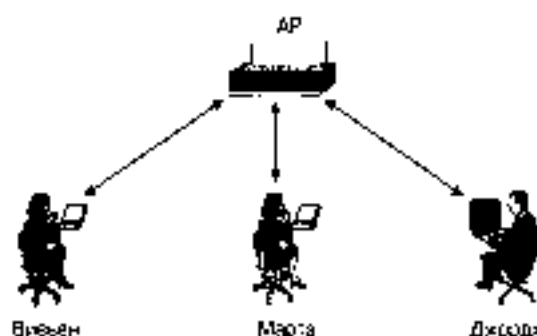


Рис. 2.2 Инфраструктура беспроводной локальной сети BSS

## Расширенные зоны обслуживания (ESS)

Несколько инфраструктур BSS могут быть соединены через их интерфейсы восходящего канала. Там, где действует стандарт 802.11, интерфейс восходящего канала соединяет BBS с распределительной системой (*distribution system, DS*). Несколько BBS,

соединенных между собой через распределительную систему, образуют расширенную зону обслуживания (ESS). Возходящий канал к распределительной системе не обязательно должен использовать проводное соединение. На рис. 2.3 представлен пример практического воплощения ESS. Спецификация стандарта 802.11 оставляет возможность реализации этого канала в виде беспроводного. Но чаще возходящие каналы к распределительной системе представляют собой кабели проводной Ethernet.

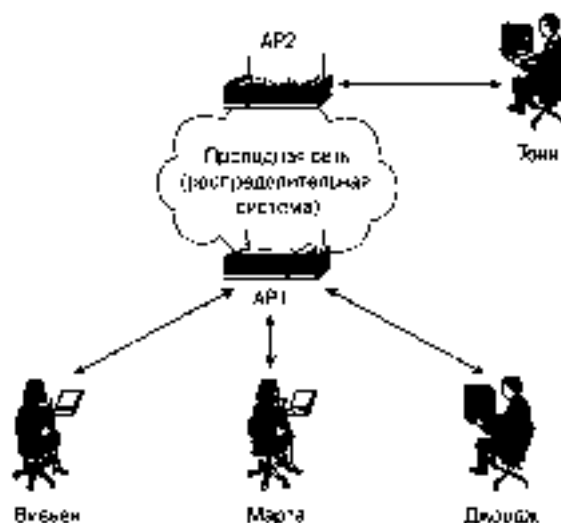


Рис. 2.3. Расширенная зона обслуживания ESS беспроводной локальной сети

## Механизм доступа к среде стандарта 802.11

В главе 1, "Технология Ethernet", описан механизм доступа к среде CSMA/CD, применимый в сетях Ethernet, функционирующих в соответствии со стандартом 802.3. Основываясь на стандарте 802.11 беспроводные сети используют похожий механизм, который называется "многократный доступ с контролем несущей и предотвращением коллизий" (carrier sense multiple access with collision avoidance, CSMA/CA). CSMA/CA представляет собой механизм "прослушивание перед передачей" (listen before talk, LBT). Передающая станция проверяет, присутствует ли в среде сигнал несущей и, прежде чем начать передачу, ожидает ее освобождения.

Проводная Ethernet способна обнаруживать коллизии в среде передачи. Две станции, передающие данные одновременно, усиливают уровень сигнала и при этом, в это служит сигналом передающей станции, что возникла коллизия. Беспроводные станции стандарта 802.11 не обладают такой возможностью. Механизм доступа стандарта 802.11 должен предпринять все усилия для того, чтобы коллизии не возникали в принципе.

## Обзор CSMA/CA

В главе 1, "Технология Ethernet", технология CSMA/CD сравнивается с селективным совещанием. Каждый участник, желающий что-то сказать, должен подождать, пока не перестанет говорить другой. Если линия свободна, участник должен побы-

таться говорить. Если два участника начинают говорить одновременно, оба должны замолчать и повторить попытку.

При использовании CSMA/CA порядки более строгие. Если обратиться к той же аналогии селективного совещания, в сценарий его проведения нужно внести некоторые изменения:

- Прежде чем участник начнет говорить, он должен сообщить, насколько длительной будет его речь. Это сообщение дает потенциальным высказывающимся представление о том, как долго им придется ждать возможности говорить.
- Участники не могут говорить до тех пор, пока не истечет время, зарезервированное предыдущим участником для своей речи.
- Участники не знают, услышан ли их голос, когда они говорят, до тех пор, пока они не получат подтверждение по окончании речи.
- Если два участника начали говорить одновременно, они не знают о том, что пытаются перекричать друг друга. Говорящие определяют, что они говорят одновременно, по тому факту, что не получают подтверждения того, что их речь услышана.
- Участники выжидают некоторое неопределенное (случайное) время и снова пытаются говорить, если не получат подтверждения того, что были услышаны.

Как видите, технология CSMA/CA применяет более строгие правила, чем CSMA/CD. Они помогают избежать коллизий. Предотвращение коллизий является критическим моментом для беспроводных сетей, поскольку последние не имеют явного механизма для их обнаружения. При использовании технологии CSMA/CA коллизия обнаруживается только при неопределенности передающей станции ожидаемого подтверждения.

Реализация технологии CSMA/CA стандартом 802.11 осуществляется при помощи распределенной функции координации (distributed coordination function, DCF). Прежде чем описывать работу CSMA/CA, имеет смысл вначале отметить важные для CSMA/CA 802.11 компоненты:

- Контроль несущей.
- Распределенная функция координации.
- Фреймы подтверждения.
- Резервирование среды с помощью механизма "готовность к передаче/готовность к приему" (RTS/CTS).

Кроме того, два других механизма характерны для доступа к среде по стандарту 802.802.11, но не связаны непосредственно с технологией CSMA/CA.

- Фрагментация фреймов.
- Точечная функция координации (point coordination function, PCF).

## Контроль несущей

Станция, которая собирается осуществить передачу в проводной среде, должна вначале проверить, используется ли несущая. Если это так, станция должна отложить передачу до момента освобождения среды. Станция определяет состояние среды с помощью двух методов:

- Проверка физического уровня PHY (уровня 1) на предмет наличия несущей.
- Использование виртуальной функции контроля несущей, вектор распределения сети (network allocation vector, NAV).

Станция может проверить физический уровень и убедиться в том, что несущая свободна. Но в некоторых случаях среда может быть все еще занята другой станцией через вектор распределения сети. Это таймер, значение которого обновляется данными фреймов, передаваемых через среду. Например, предположим, что в инфраструктуре BSS Марта посылает фрейм Джорджу (рис. 2.4). Поскольку беспроводная среда — это совместно используемая среда с широковещанием, Вивьен также получает этот фрейм. Фреймы стандарта 802.11 содержат поле продолжительности (Duration field). Значение продолжительности достаточно велико для того, чтобы осуществлять передачу фрейма и получить подтверждение от приемки. Вивьен обновляет свой вектор распределения сети значением поля продолжительности и не пытается начать передачу, пока вектор распределения сети не уменьшится до нуля.

Обратите внимание на то, что эта станция обновляет значение вектора распределения сети только тогда, когда полученное значение поля продолжительности превышает таковое, хранящееся в ее векторе распределения сети. Так, в рассматриваемом случае, если значение вектора распределения сети станции Вивьен составляет 10 мс, она не станет обновлять свой вектор распределения сети, если получит фрейм со значением поля продолжительности 5 мс. Она обновит свой вектор распределения сети, если получит фрейм со значением поля продолжительности 20 мс.

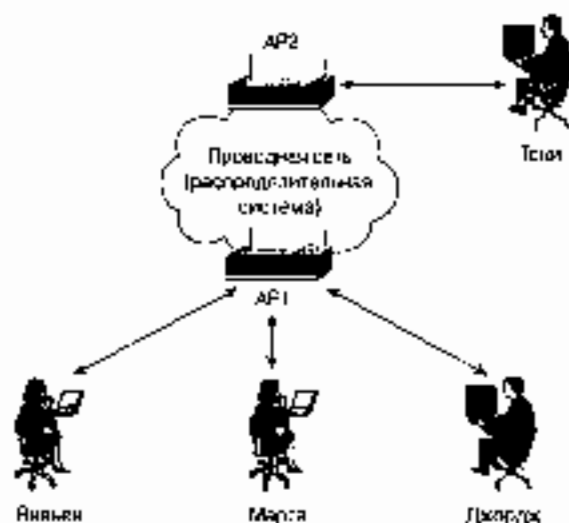


Рис. 2.4. Процесс обновления вектора распределения сети

## Распределенная функция координации (DCF)

Утвержденный IEEE миллиметровая архитектура для сетей стандарта 802.11 — это распределенная функция координации (DCF), механизм доступа к среде, основанный на методе CSMA/CA. Прежде чем приступить к описанию работы DCF, мы введем некоторые понятия. На рис. 2.5 представлена временная диаграмма для сценария, показанного на рис. 2.4.

При работе с использованием DCF станция, намеренная передать фрейм, должна выждать определенное время после того, как среда понадобится. Этот интервал времени называется *межфреймовый зазор DCF* (DCF interframe space, DIFS). По истечении интервала времени DIFS станция может принять участие в состязании за право доступа к среде.

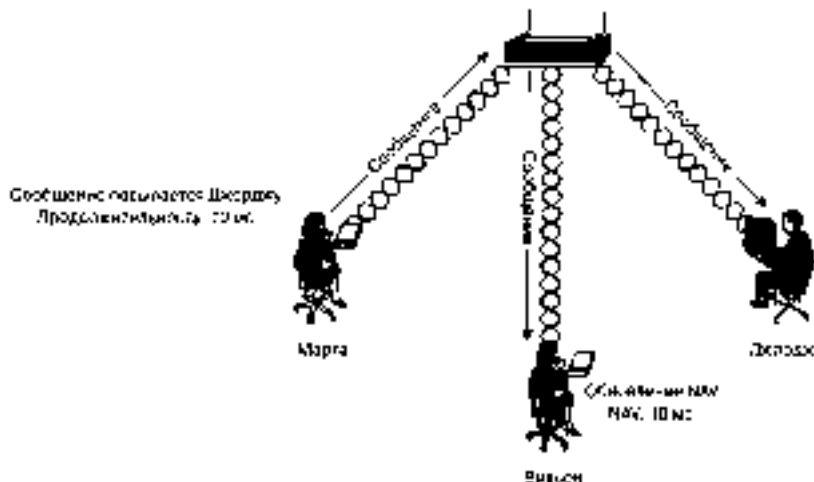


Рис. 2.4. Временная диаграмма доступа к среде с использованием распределенной координирующей функции (DCF)

В случае, проиллюстрированном на рис. 2.5, Вивен и Джордж должны воздержаться от передачи фреймов до тех пор, пока с аналогичной задачей не справится Марта. Обе станции должны использовать одно и то же значение вектора распределения сети (NAV) и обе должны "физически почувствовать", когда среда освобождается. Существует большая вероятность того, что обе станции одновременно попытаются начать передачу только после освобождения среды, что приведет к возникновению коллизии. Чтобы избежать этой ситуации, DCF использует таймер случайной задержки (random backoff timer).

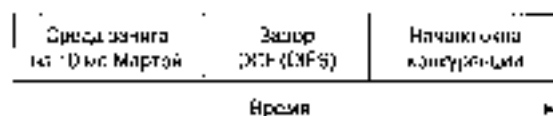


Рис. 2.5. Временная диаграмма доступа к среде с использованием DCF

При использовании случайного алгоритма задержки случайным образом выбирается значение в диапазоне от 0 до значения, соответствующего ширине окна конкуренции (конкуренционный window, CW). По умолчанию значение CW устанавливается производителем и хранится в памяти сетевой карты станции. Диапазон значений случайной задержки начинается с 0 и заканчивается максимальным значением, т.е. лежит в пределах от  $CW_{min}$  до  $CW_{max}$ . Предположим, что в рассматриваемом нами случае значение  $CW_{min}$  равно 7, а значение  $CW_{max}$  — 255. На рис. 2.6. показаны значения  $CW_{min}$  и  $CW_{max}$  для случайной задержки, заданной в двоичном виде.

Станция случайным образом выбирает значение между 0 и текущим значением CW. Случайное значение представляет собой количество канальных интервалов по стандарту 802.11, в течение которых станция, уже после освобождения среды и в окне конкуренции, должна воздерживаться от передачи. Канальный интервал (slot time) — это значение времени, определяемое параметрами физического уровня, основанными на характеристиках радиочастотного канала BSS.

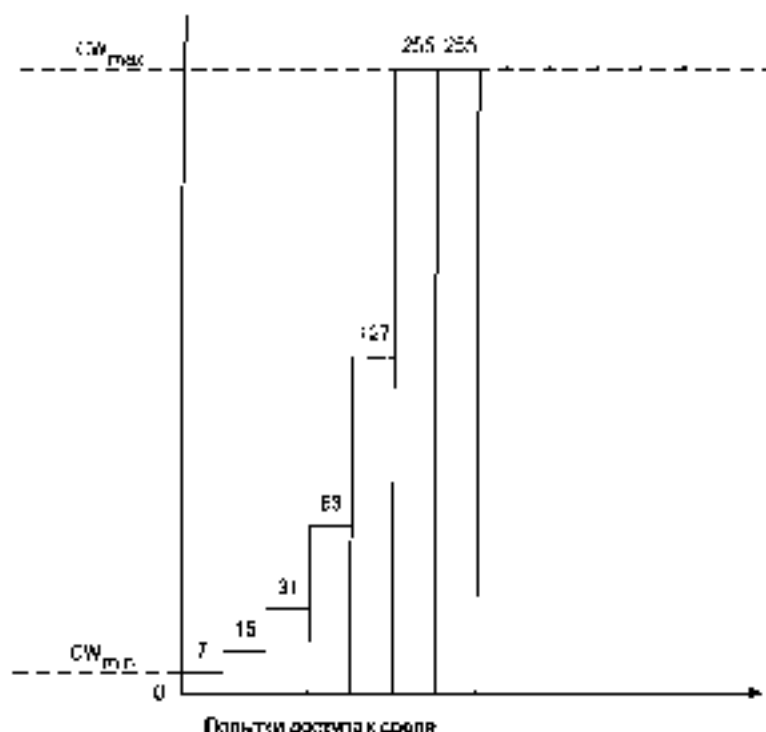


Рис. 2.6. Случайная задержка при доступе к среде с использованием DCF

Возвратимся к каждому примеру. Вивьен пытается начать передачу. Значение ее таймера NAV уменьшено до 0, а PSY показывает, что среда свободна. Вивьен выбирает случайное время задержки в диапазоне от 0 до CW (в данном случае значение CW равно 7) и подерживается от передачи в течение выбранного количества канальных интервалов. Этот процесс проиллюстрирован на рис. 2.7, где случайное значение задержки составляет 4 канальных интервала.

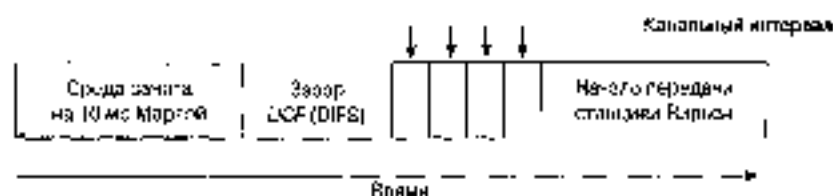


Рис. 2.7. Передача фрейма по истечении времени случайной задержки

По прошествии четырех канальных интервалов Вивьен может начать передачу. Но что произойдет, если станция Джорджи имеет случайное время задержки, равное двум канальным интервалам? Вивьен получает новое значение поля продолжительности из фрейма станции Джорджи, когда она начинает передачу, и обновляет свой NAV, привязывая ему новое значение. Станция Вивьен должна подождать, пока ее NAV уменьшится до 0 и ее PSY сообщит, что среда вновь свободна, прежде чем она возобновит свою случайную задержку. (В данном примере станция Вивьен должна подождать дополнительно два канальных интервала, прежде чем сделать попытку начать передачу.)



В предположении, что станция Вивьен может отправить передачу на все четыре канальных интервала, она передает фрейм. Но как станция Вивьен узнает, что этот фрейм получен станцией называемая? Спецификация 802.11 требует, чтобы принимающая станция передала станции отправившей фрейм подтверждение. Этот фрейм подтверждения позволяет станции-отправителю непосредственно определить, произошла ли в среде передачи коллизия. Если передающая станция не получает фрейм подтверждения, она считает, что в среде передачи произошла коллизия. Передающая станция обновляет значение своего счетчика числа попыток, удаляет экран окна конкуренции и начинает процесс доступа к среде сначала. На рис. 2.8 представлены все действия, которые должна выполнить станция, использующая DCF, для того чтобы передать фрейм.

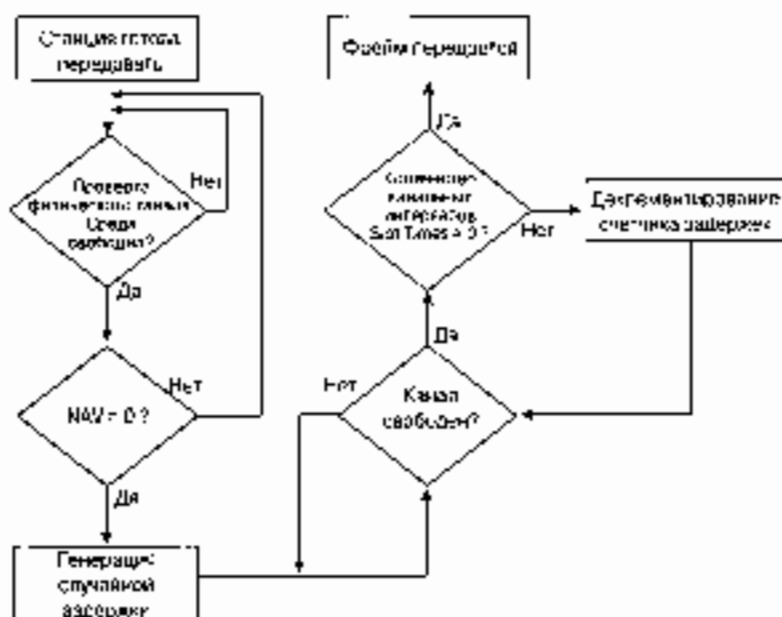


Рис. 2.8. Процесс доступа к среде с использованием DCF

## Фрейм подтверждения

Станция, получившая фрейм, подтверждает факт его безошибочного приема путем отправки передающей станции фрейма подтверждения. Убав, что принимающая станция должна получить доступ к среде и передать фрейм подтверждения, вы могли бы предположить, что передача фрейма подтверждения может задержаться вследствие конкуренции станций за среду. Однако передача фрейма подтверждением — это особый случай. Фреймам подтверждения разрешается не принимать участия в процессе случайной задержки, долго ждать возможности передать подтверждение после вступления фрейма не придется. Короткий промежуток времени, который принимающая станция проводит в ожидании такой возможности, называется *короткий межфреймовый интервал* (short interframe space, SIFS). Интервал SIFS короче, чем интервал DIFS, на два канальных интервала. Это гарантирует принимающей станции максимальный шанс получения доступа к среде для передачи по сравнению с другими станциями.

Возвращаясь к случаю передачи информации от Вивьен Джорджу отметим, что станция первой отправила попытку передачи на четыре канальных интервала. Среда

стала доступной, поэтому она передает свой фрейм Джорджу (рис. 2.9). Точка доступа получает фрейм и ожидает в течение времени, равного интервалу SIFS, прежде чем передавать фрейм подтверждению.

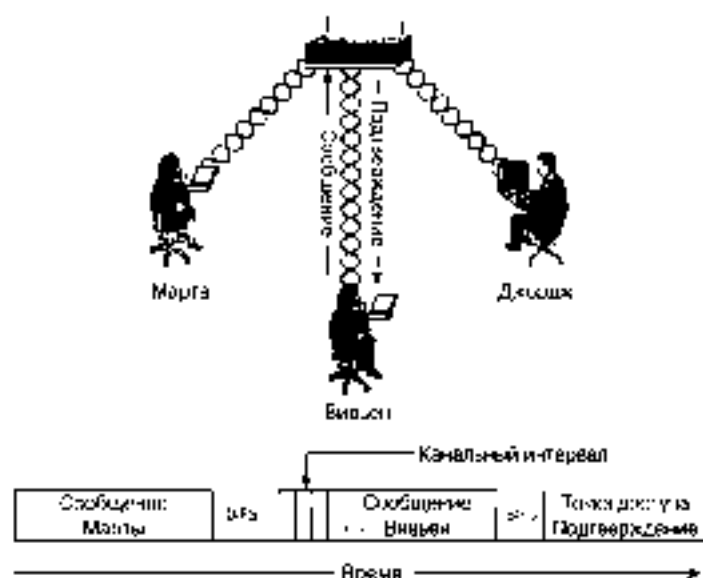


Рис. 2.9. Передача фрейма и подтверждение

Предположим, что станция Вивьен не получила фрейм подтверждения. Тогда она увеличивает ширину окна конкуренции CW до 15 и повторяет процесс задержки. При каждой неуспешной попытке доступа к среде станция, работающая по стандарту 802.11, увеличивает значение счетчика числа попыток. Ширина окна конкуренции каждый раз удваивается, пока не достигнет значения  $CW_{max}$ . Уровень MAC может предпринимать попытки передачи фрейма, но когда значение счетчика числа попыток достигает установленного администратором сети порога, станция Вивьен пытается зарезервировать среду.

## Проблема скрытого узла и RTS/CTS

Вивьен может оказаться не в состоянии доложить до среды из-за другой станции, находящейся в пределах досягаемости точки доступа, но вне пределов досягаемости станции Вивьен. Эта ситуация представлена на рис. 2.10. Станции Вивьен и Джорджа находятся в зоне действия друг друга и точки доступа. При этом ни одна из них не находится в зоне действия станции Тони. Однако Тони находится в зоне действия точки доступа и тоже пытается осуществлять передачу через среду. Эта ситуация известна как *проблема скрытого узла*, поскольку станции Тони невидны для станций Вивьен и Джорджа.

Вивьен пытается зарезервировать среду с помощью специального управляющего фрейма, который называется фрейм RTS (фрейм готовности к передаче). Фрейм RTS посылается точке доступа, и все, находящиеся в зоне действия станции Вивьен, ожидают в течение времени, указанного в поле продолжительности обмена фреймами со станцией Вивьен. Обмен фреймами включает тот фрейм, который станция Вивьен намеревается передать, а также ожидаемый ею фрейм подтверждения.

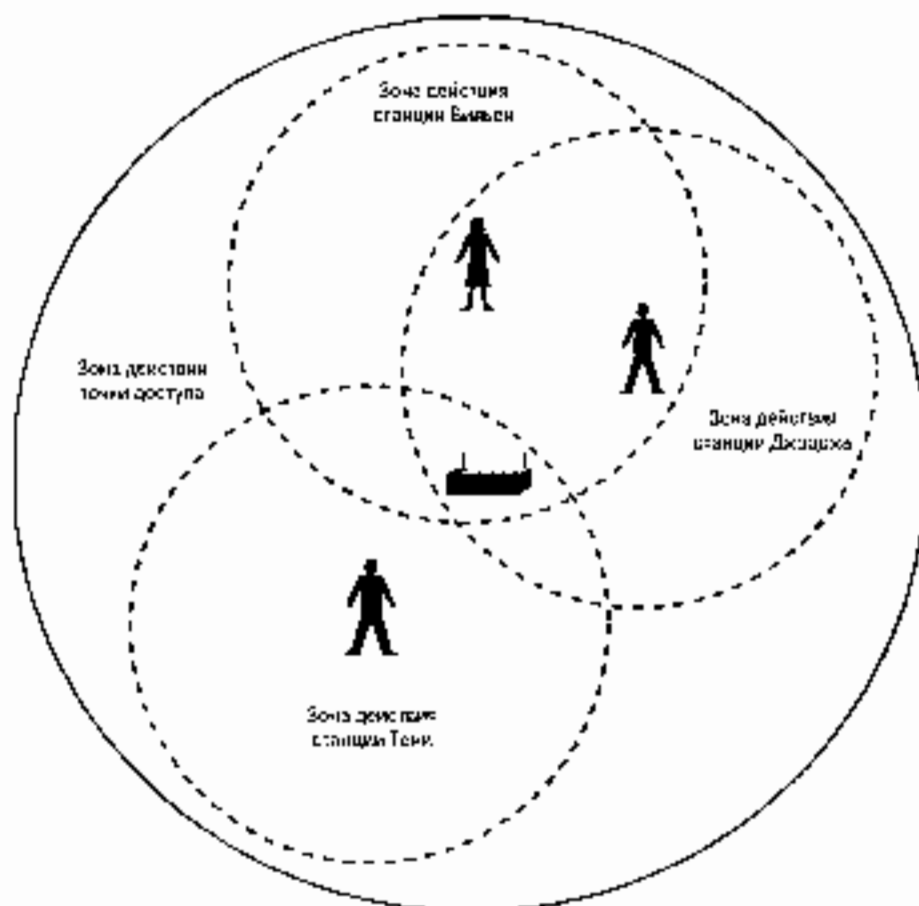


Рис. 2.10. Проблема скрытого узла

Точка доступа получает фрейм RTS от станции Вивьен и отвечает управляющим фреймом CTS (фреймом готовности к приему). Последний содержит поле Приблизительная длительность, значение которого достаточно для того, чтобы станция Вивьен могла завершить обмен фреймами. Все станции, находящиеся в зоне действия точки доступа, в том числе станции Тони и Джорджа, получают фрейм CTS и обновляют значения своих NAV (векторов распределения сети), как показано на рис. 2.11.

Изначальный фрейм RTS, передаваемый Вивьен, должен пройти через процедуру ДСР, как любой другой фрейм. Но, аналогично фрейму подтверждения, соответствующий CTS-фрейм, передаваемый точкой доступа, пропускает процедуру случайной задержки и, перед тем как быть переданным, должен выждать только время, равное интервалу SIFS. На рис. 2.12 детально показана процедура передачи станцией Вивьен фрейма RTS. Станция Джорджа и Тони обновляют значения своих NAV одновременно, но фрейм подтверждения, который точка доступа передает станции Вивьен, не обязан подчиняться правилам ДСР. После получения фрейма станция Джорджа немедленно отправляет обратно фрейм подтверждения. Хотя значение NAV станции Джорджа не равно 0, она все же рассылает фрейм подтверждения точке доступа спустя время, заданное интервалом SIFS.

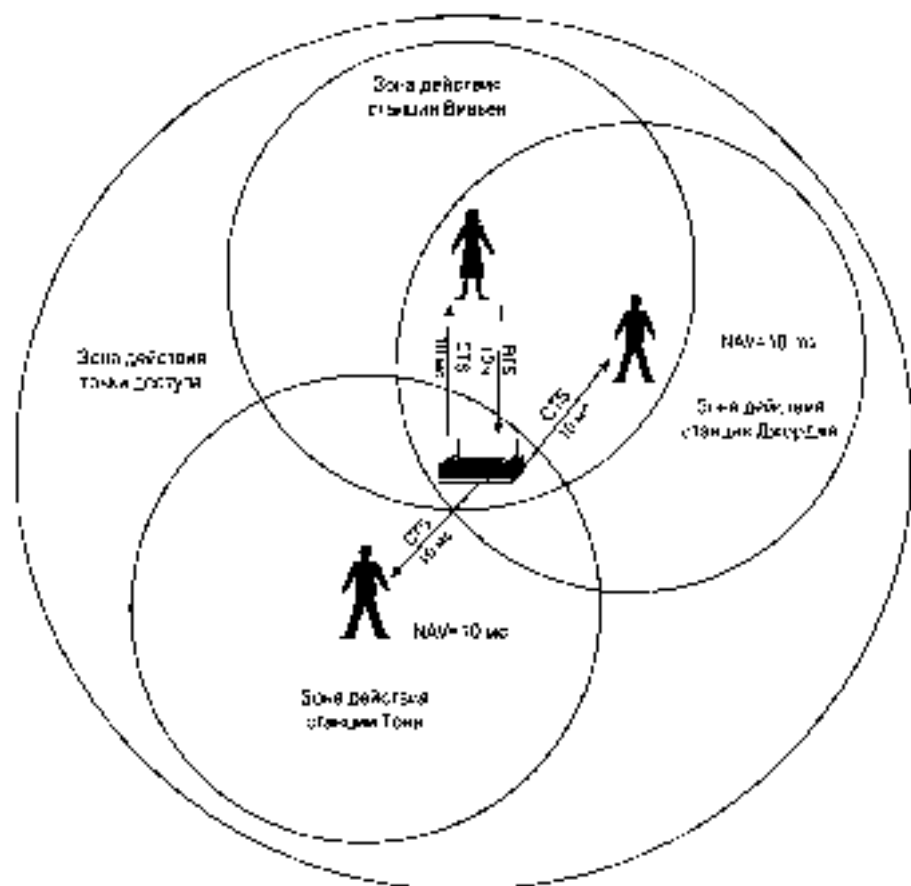


Рис. 2.11. Резервирование среды с помощью фреймов RTS/CTS

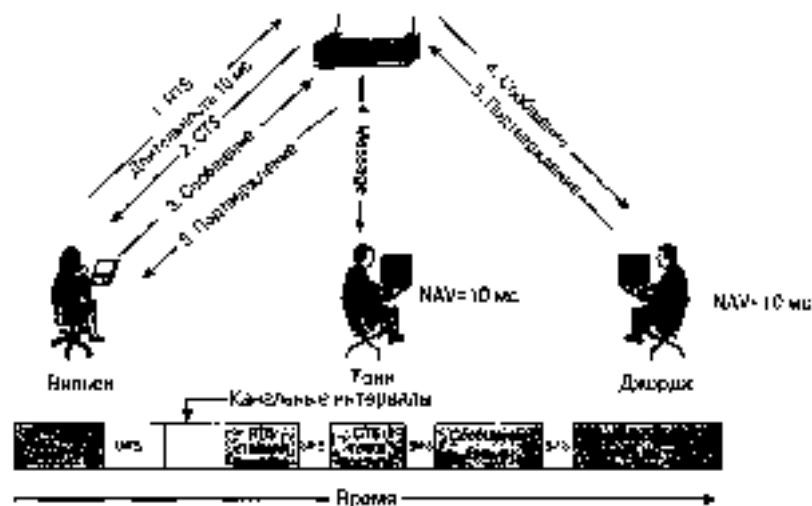


Рис. 2.12. Пример обмена фреймами RTS/CTS

## Фрагментация фрейма по стандарту 802.11

*Фрагментация фрейма* — это выполняется на уровне MAC функции. Назначение функций — повысить надежность передачи фреймов через беспроводную среду. Под фрагментацией понимается разбиение фрейма на меньшие фрагменты и передача каждого из них отдельно (рис. 2.13). Предполагается, что вероятность успешной передачи меньшего фрагмента через зашумленную беспроводную среду выше. Получение каждого фрагмента фрейма подтверждается отдельно, следовательно, если какой-нибудь фрагмент фрейма будет поврежден с ошибкой или вступит в коллизия, только его придется переслать повторно, а не весь фрейм. Это увеличивает пропускную способность среды.

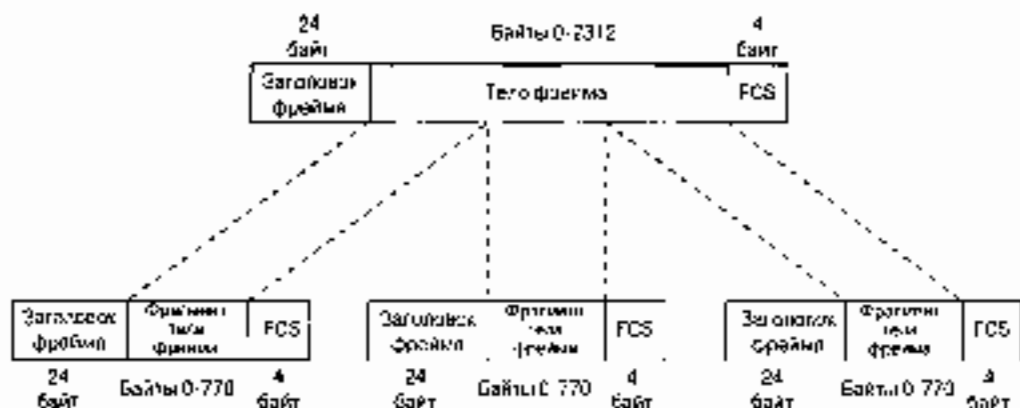


Рис. 2.13. Фрагментация фрейма

Размер фрагмента может задавать администратор сети (рис. 2.14). Фрагментацией подвергаются только одноадресные фреймы. Широковещательные, или многоадресные, фреймы передаются целиком. Кроме того, фрагменты фрейма передаются пакетом, с использованием только одной итерации механизма доступа к среде DCF.

Хотя за счет фрагментации можно повысить надежность передачи фреймов в беспроводных локальных сетях, она приводит к увеличению "накладных расходов" MAC-протокола стандарта 802.11. Каждый фрагмент фрейма включает информацию содержимую в заголовке 802.11 MAC, а также требует передачи соответствующего фрейма подтверждения. Это увеличивает число служебных сигналов MAC-протокола и снижает реальную производительность беспроводной станции. Фрагментация — это баланс между надежностью и непроизводительной загрузкой среды.

## PCF

Точечная функция координации (point coordination function, PCF) — это опциональный, необязательный механизм доступа к среде, который используется дополнительно к механизму DCF. Механизм PCF обеспечивает не подтвержденную конкуренцию за среду передачу фреймов к точке доступа и от нее. Большинство производителей не обеспечивают поддержку механизма PCF в своих устройствах, потому что он увеличивает нагрузку (количество передаваемых служебных, т.е. немультимедийных, сигналов) на протокол HSS. В результате его распространяемость невелика. Предполагается, что с повышением качества и класса представляемых услуг передачи дан-

ных (Quality of Service, QoS) в будущей спецификации стандарта 802.11 будет использоваться какой-нибудь другой механизм.

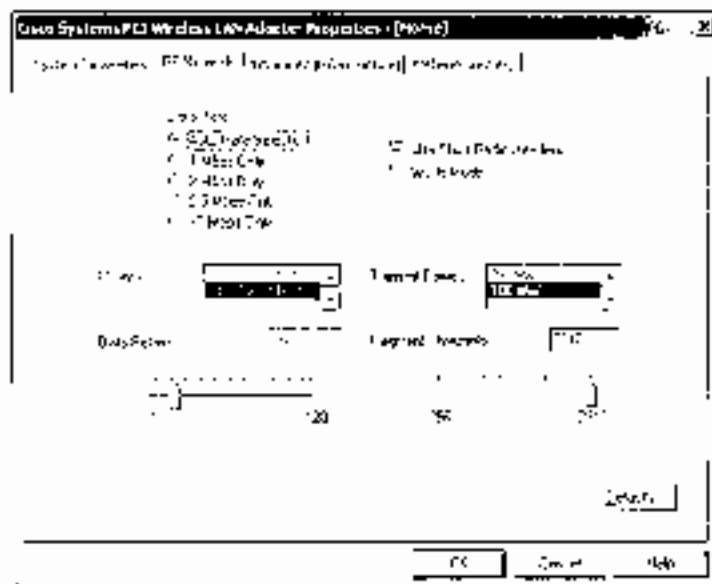


Рис. 2.14. Задание параметров дефрагментации утилитой *Wireless Network Setup Wizard*

В данном разделе рассказывается о работе механизма PCF, а именно о работе точки координации (point coordinator, PC) и реализующих механизм PCF станциях (в спецификации 802.11 они называются станциями CF-Pollable — станциями, обслуживаемые точкой координации).

## Период, свободный от конкуренции

*Период, свободный от конкуренции* (contention free period, CFP), — это временное окно, период, в течение которого осуществляется работа механизма PCF. Период CFP начинается с набора интервалов, следующих за сигнальным (маячковым) фреймом (beacon frame), содержащим информационный элемент с картой маршрутов трафика (delivery traffic indication map, DTIM) (он описывается ниже в данной главе). Частота следования периодов CFP определяется администратором сети. После начала периода CFP точка доступа начинает играть роль точки координации (за это означает, что работа PCF возможна только в инфраструктурах BSS). Каждый клиент 802.11 устанавливает значение NAV данным CFPMaxDuration (максимальное значение продолжительности для механизма CFP). Это значение включается в информационный элемент, содержащий набор параметров функции координации (описанный ниже в данной главе). Величина CFPMaxDuration определяет значение времени, максимального для продолжительности CFP. Точка координации может закончить работу в соответствии с механизмом CFP раньше, чем истечет время, заданное значением CFPMaxDuration. Точка доступа передает сигнальные фреймы через регулярные промежутки времени, а сигнальные фреймы, передаваемые в течение CFP, содержат поле CFPDurationRemaining (оставшаяся продолжительность CFP), посредством которого NAV станции обновляется значением, соответствующим

шим оставшейся продолжительности CFP. На рис. 2.15 представлена временная диаграмма CFP в период конкуренции (contention period, CP).

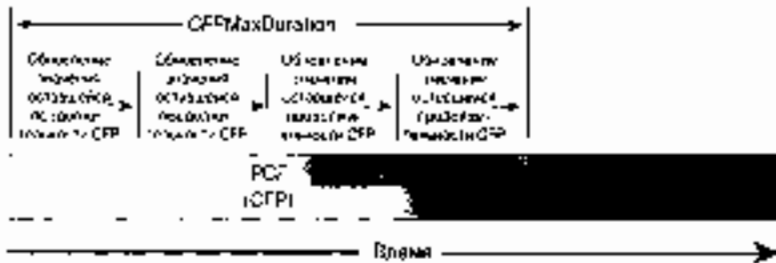


Рис. 2.15. Временная диаграмма CFP и CP

В отличие от работы в соответствии с DCF, при работе под управлением механизма PCF станции не имеют свободного доступа к среде и не могут свободно передавать данные. Станции могут передавать данные (по одному фрейму за один раз) только тогда, когда точка координации производит их запрос. Точка координации может досылать фреймы станциям, опрашивать их на предмет передачи фреймов, подтверждать прием фреймов в соответствии с требованиями MAC-уровня или закончить CFP.

## Работа точки координации

Когда начинается CFP (напомним, эта аббревиатура означает "период свободный от конкуренции"), точка координации должна включать доступ к среде таким же образом, как это делает станция DCF. Но, в отличие от станции DCF, точка координации пытается получить доступ к среде через интервал времени, называемый *приоритетным межфреймовым интервалом* (priority interframe space, PIFS). Интервал PIFS на один канальный интервал больше, чем интервал SIFS, и на один канальный интервал короче, чем интервал DIFS, что позволяет PCF-станциям получить доступ к среде раньше DCF-станций. Вдобавок они могут использовать управляющие фреймы, такие как фреймы подтверждения, для обеспечения наибольшей вероятности получения доступа к среде. На рис. 2.16 показаны отношения между SIFS, PIFS, DIFS и канальным интервалом.

После ожидания в продолжение интервала PIFS точка координации посылает сигнальный фрейм, содержащий информационный элемент с параметром функции координации (CF). Точка координации ожидает в продолжение одного интервала SIFS следующей за сигнальным фреймом передачи и затем досылает CF-опрашиваемой станции один из следующих фреймов:

- Фрейм данных
- Фрейм опроса (CF-Poll)
- Комбинация фреймов данных и опроса (Data+CF-Poll).
- Фрейм конца периода CFP (CF-End).

Если точка координации не имеет фреймов, которые нужно передать, и ей не нужно опрашивать CF-Poll станции, CFP считается равным нулю и немедленно следует сигнальный фрейм, точка координации посылает фрейм конца периода CFP, завершающий период CFP.

□ ← каналный интервал

SIFS

SIFS - □ = PIFS

SIFS + □ + □ = DIFS

Рис. 2.16. Отношения между SIFS, PIFS и каналным интервалом

## Пример работы PCF

Приблизкая рассматривание нашего примера, предположим, что Вивьен, Марта и Джордж связываются через точку доступа API (рис. 2.17).

Точка доступа API передает сигнальный фрейм, указывающий на начало периода CFP. Продолжительность периода CFP задана равной 20 с. Станции Вивьен, Марты и Джорджа объявляют значение своего NAV с тем, чтобы он соответствовал 20 секундам CFP. После ожидания, равного интервалу SIFS, API передает фрейм, находящийся в ее буфере и предназначенный для станции Вивьен, а также приглашает станции Вивьен на предмет того, имеет ли она фреймы, предназначенные для пересылки с использованием комбинации приемов данных и опроса (Data+CF-Poll). Станция Вивьен получает фрейм (Data+CF-Poll) и передает один фрейм данных и же содержащий полезной информации фрейм подтверждения (Data+CF-ACK) после ожидания в течение интервала SIFS. Обратите внимание на то, что станция Вивьен игнорирует значение своего NAV при передаче фреймов и ответ на получение фрейма CF-Poll.

Точка доступа API продолжает свою работу, посылая опросный лист Марте. API использует другую комбинацию фреймов, для того чтобы послать фрейм данных станции Марте, фрейм подтверждения станции Вивьен и опросить станцию Марты на предмет передачи фреймов (Data+CF-ACK+CF-Poll). Заметьте, что этот фрейм, предназначенный для станции Марты, содержит также последний фрейм подтверждения станции Вивьен. Используемая в стандарте 802.11 процедура множественного доступа вполне позволяет поступать таким образом. Марта ждет в течение интервала SIFS и посылает фрейм Data+CF-ACK.

Наконец, API переходит к работе со станцией Джорджа. В ее буфере нет данных, предназначенных для этой станции, поэтому она посылает ей фрейм опроса CF-Poll, чтобы узнать, намеревается ли станция Джорджа передать какие-то фреймы. Поскольку буфер станции Джорджа пуст, она посылает фрейм с нулевыми данными (null data frame). Хотя CFP еще не достиг своей максимальной продолжительности, API посылает фрейм CF-End (конец периода CF) для завершения периода, свободен от конкуренции, и переходит к периоду конкуренции (CFP) и нормальному доступу к среде в режиме DCF. Вивьен, Марта и Джордж получают фрейм CF-End и восстанавливают исходные значения своих NAV.

## Нестандартные устройства

В предыдущем разделе говорилось о том, как основанные на стандарте 802.11 устройства получают доступ к беспроводной среде. В данном разделе речь пойдет об уст-



устройств, не соответствующих стандарту 802.11. Они используют технологию 802.11 способами, которые приводят к нарушению стандарта или его расширению, но могут оказаться полезными для вашей сети. К специфическим устройствам, которые рассматриваются ниже, относятся следующие.

- Точки доступа-повторители (перезет апс)
- Универсальные клиенты (мосты рабочих групп).
- Беспроводные мосты.

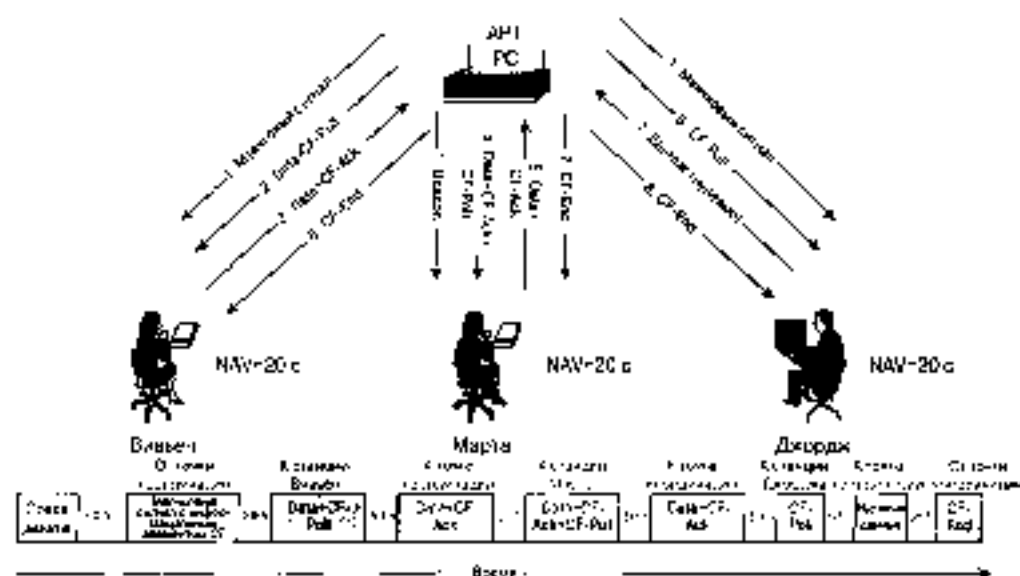


Рис. 2.17. Операции доступа к среде РСР

Хотя каждое из этих устройств может оказаться полезным при развертывании сети, следует помнить, что в настоящее время они не описаны в стандарте 802.11 и нет гарантии их совместимости с взаимодействиями, поскольку различные производители могут ориентироваться на различные способы их применения. Чтобы гарантировать надежность сети, если уж вы решили их использовать, следует позаботиться о том, чтобы они взаимодействовали с устройствами выбранного вами производителя или устройствами, для которых производитель гарантирует совместимость.

## Точки доступа-повторители

Может случиться так, что окажется неудобно или нецелесообразно соединить точку доступа с проводной инфраструктурой, или какое-либо препятствие затруднит осуществление связи точки доступа к проводной сети с местом расположения беспроводных станций-клиентов напрямую. В такой ситуации можно использовать точку доступа-повторитель. Описанная возможность представлена на рис. 2.18, где станция Элефит не находится в зоне видимости точки доступа 2 (AP2), но видима для точки доступа 3 (AP3), которая не соединена с проводной сетью, но может "видеть" AP2.

Почти аналогично проводному повторителю его беспроводной собрат просто ретранслирует все пакеты, поступающие на его беспроводной интерфейс. Эти ретрансляции осу-

предоставляет через тот же канал, через который пакеты были получены. Точка доступа-повторитель расширяет BSS, а также домен коллизии. Хотя она может оказаться эффективным средством, применять ее следует осторожно, поскольку широковещательных сообщений может привести к сокращению пропускной способности канала связи, потому что начальная точка доступа также «слышит» ретранслированный сигнал. Эта проблема может еще более обостриться при использовании соточки точек доступа-повторителей. Кроме того, точка доступа-повторитель может ограничить нас в использовании клиентов с расширениями, которые позволяют им поддерживать привязку к станциям и их использование через точки доступа-повторители. Несмотря на названные ограничения, весьма вероятно, что мы найдем применение точкам доступа-повторителям в нашей сети.

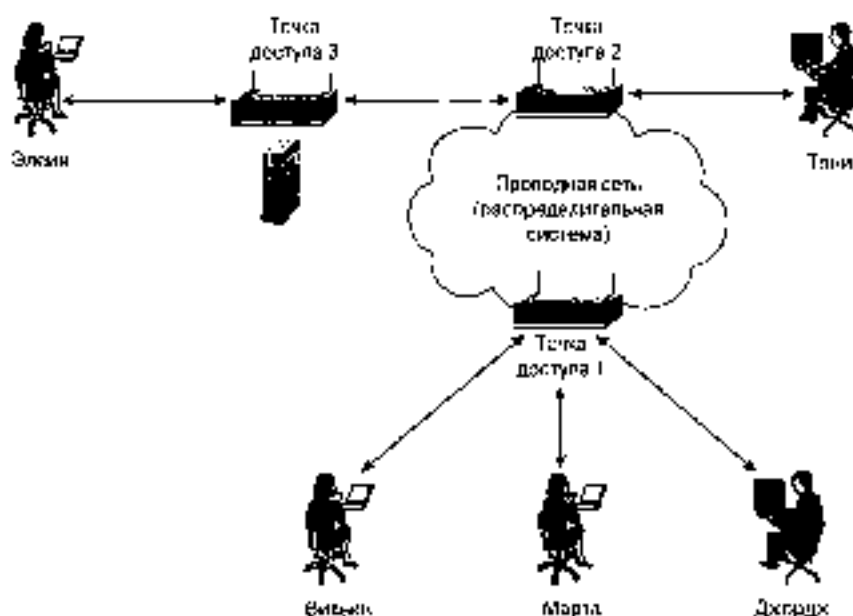


Рис. 2.18. Применение точки доступа-повторителя

## Универсальные клиенты и мосты рабочих групп

При переходе от проводной архитектуры к беспроводной вы можете обнаружить, что имеющиеся у вас сетевые устройства поддерживают проводную Ethernet или последовательный интерфейс, но не имеют интерфейсных разъемов для беспроводных NIC. Если эти устройства необходимы в вашей беспроводной сети, можно использовать универсальный клиент или мост рабочей группы (рис. 2.19).

Примерами устройств, относящихся к этой категории, могут служить каскадные терминалы магазинов, принтеры, устаревшие ПК, коинтегральные устройства и небольшие мобильные сети. Универсальный клиент или мост рабочей группы инкапсулирует получаемые им пакеты проводной сети в пакеты беспроводной и таким образом предоставляет для точки доступа интерфейс стандарта 802.11. Термин *универсальный клиент* наиболее часто используется, когда речь идет о подключении одного проводного устройства, термин *мост рабочей группы* используется, если подключается небольшая сеть, состоящая из нескольких устройств. Не существует какого-либо стан-

диртного подхода к инкапсуляции или пересылке этих полученных через проводной интерфейс данных, поэтому вместо него нужно проверить, сертифицирован ли универсальный клиент или мост рабочей группы для работы с вашей точкой доступа.

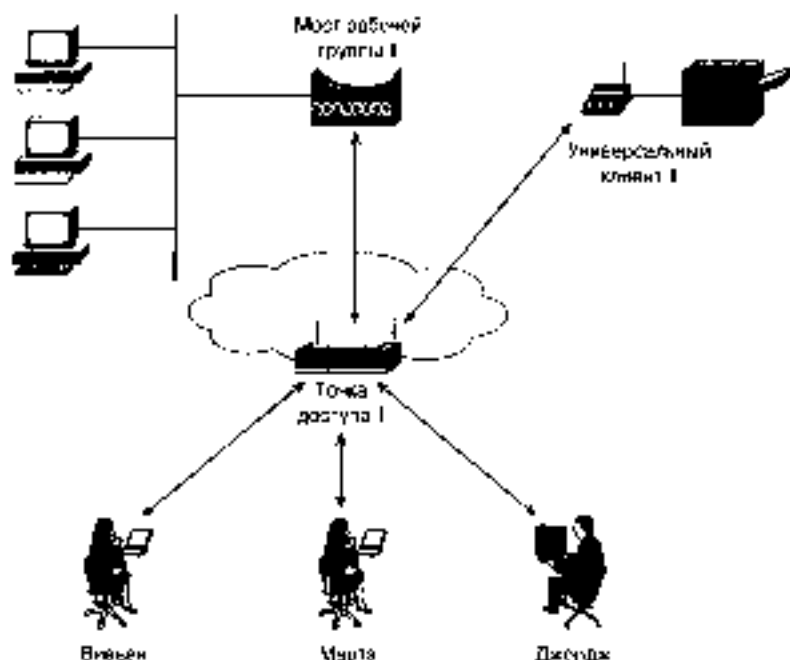


Рис. 2.19. Применение универсального клиента и моста рабочей группы

## Беспроводные мосты

Если расширить концепцию моста рабочей группы до точки, в которой вы соединяете две или несколько проводных сетей, мы приходим к концепции беспроводных мостов. Аналогично проводным мостам, беспроводные соединяют между собой сети. Вы можете создавать их без проводов, потому что соединяемые сети изначально мобильны. Сети, которые должны быть соединены, могут быть размещены на одной территории (co-located), в этом случае применение беспроводных мостов дает способ соединения таких сетей. Основное отличие между мостами и мостами рабочей группы состоит в том, что последние обеспечивают беспроводной доступ только к небольшой рабочей группе типа офиса, в то время как первые во названных способны соединять большие сети, размещенные на расстояния, намного большие, чем характерные для беспроводных локальных сетей. На самом деле многие поставщики предлагают продукты, работоспособные на расстояниях, значительно превышающих оговоренные в стандарте 802.11. На рис. 2.20 приведен пример использования беспроводных мостов.

Как видно на рисунке, один из мостов играет роль точки доступа к беспроводной локальной сети, другие выступают в роли клиентов. Хотя в случае применения беспроводных мостов используется в основном технология 802.11, отдельные производители предлагают собственные патентованные методы инкапсуляции трафика проводной сети и для расширения в перспективе диапазона за ого-

воренный стандарты на подуровни MAC и PHY. Поэтому вам вновь придется проверить сертификацию или иных беспроводной мост на предмет совместности.

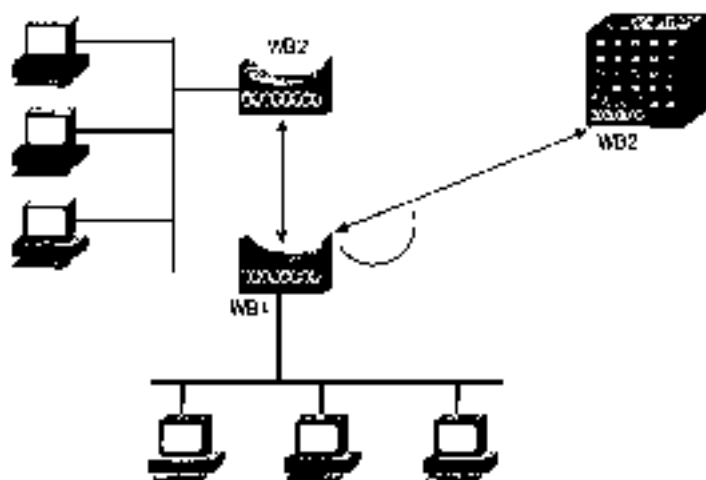


Рис. 2.20. Пример использования беспроводных мостов (WB)

## Операции, осуществляемые на уровне MAC стандарта 802.11

В предыдущем разделе мы рассказывали о том, каким образом станция получает доступ и конкурирует за обладание беспроводной средой. В данном разделе рассматриваются следующие вопросы.

- **Возможность соединения станций.** Подробное описание того, как станции стандарта 802.11 выбирают точки доступа и связываются с ними.
- **Работа в режиме экономии энергопотребления.** Подробное описание распределения фреймов для энергосберегающих станций.
- **Форматы фреймов стандарта 802.11.** Подробное описание форматов фреймов, описанных в предыдущих разделах.

### Возможность соединения станций

Ранее в этой главе мы описывали, как Джордж, Марта, Вивьен и Тони совместно используют среду своего BSS. В этом разделе мы сделаем шаг назад и подробно опишем, как беспроводные станции стандарта 802.11 соединяются в BSS. Трехсторонний обмен происходит между беспроводной станцией и точкой доступа.

- Процесс зондирования.
- Процесс аутентификации.
- Процесс приема (ассоциирования).

## Процесс зондирования

На рис. 2.21 показано, что станция Вилкен находится в пределах досягаемости трех точек доступа. Две из них принадлежат зоне обслуживания отдела маркетинга, третья — зоне обслуживания отдела продаж. Станция Вилкен сконфигурирована таким образом, что она относится к зоне обслуживания отдела маркетинга.

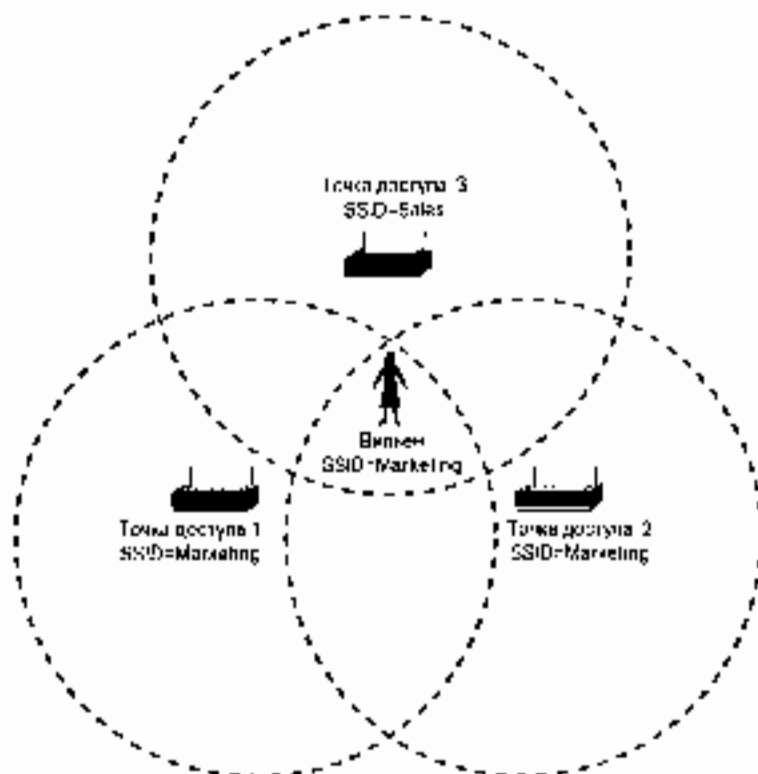


Рис. 2.21. Станция Вилкен и ближайшие точки доступа

Эта станция-клиент посылает зондирующий фрейм запроса (probe request frame) стандарта 802.11. Обычно станция стандарта 802.11 посылает зондирующий фрейм запроса по каждому доступному ей каналу (для Северной Америки это каналы с первого по одиннадцатый). Этот процесс не описан в спецификации стандарта 802.11. Зондирующий фрейм запроса содержит информацию о беспроводной станции стандарта 802.11 — какую скорость передачи данных поддерживает станция и к какой зоне обслуживания она принадлежит. На рис. 2.22 представлена расшифровка протокола зондирующего фрейма запроса. Ключевые поля зондирующего запроса следующие.

- **Элемент SSID.** Данный элемент содержит SSID, посредством которого сконфигурирована станция.
- **Элемент поддерживаемых скоростей.** Данный элемент указывает все скорости передачи данных, поддерживаемые клиентом.

Клиентские станции посылают зондирующие фреймы запроса вслепую, как будто они ничего не знают о точках доступа, которые зондируют. А так как, то многие ли-

просы посылаются с наименьшей возможной скоростью передачи данных, составляющей 1 Мбит/с (см. рис. 2.22).

000	Signal level	0	000
001	Tagged	1	
010	Copy mode	1	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
011			
012	Frame Control Field FC	48	
013		05	0000000000000000
014		08	0000000000000000
015		03	0000000000000000
016		00	0000000000000000
017		00	0000000000000000
018		00	0000000000000000
019		00	0000000000000000
020		00	0000000000000000
021		00	0000000000000000
022		00	0000000000000000
023		00	0000000000000000
024		00	0000000000000000
025		00	0000000000000000
026		00	0000000000000000
027		00	0000000000000000
028		00	0000000000000000
029		00	0000000000000000
030		00	0000000000000000
031		00	0000000000000000
032		00	0000000000000000
033		00	0000000000000000
034		00	0000000000000000
035		00	0000000000000000
036		00	0000000000000000
037		00	0000000000000000
038		00	0000000000000000
039		00	0000000000000000
040		00	0000000000000000
041		00	0000000000000000
042		00	0000000000000000
043		00	0000000000000000
044		00	0000000000000000
045		00	0000000000000000
046		00	0000000000000000
047		00	0000000000000000
048		00	0000000000000000
049		00	0000000000000000
050		00	0000000000000000
051		00	0000000000000000
052		00	0000000000000000
053		00	0000000000000000
054		00	0000000000000000
055		00	0000000000000000
056		00	0000000000000000
057		00	0000000000000000
058		00	0000000000000000
059		00	0000000000000000
060		00	0000000000000000
061		00	0000000000000000
062		00	0000000000000000
063		00	0000000000000000
064		00	0000000000000000
065		00	0000000000000000
066		00	0000000000000000
067		00	0000000000000000
068		00	0000000000000000
069		00	0000000000000000
070		00	0000000000000000
071		00	0000000000000000
072		00	0000000000000000
073		00	0000000000000000
074		00	0000000000000000
075		00	0000000000000000
076		00	0000000000000000
077		00	0000000000000000
078		00	0000000000000000
079		00	0000000000000000
080		00	0000000000000000
081		00	0000000000000000
082		00	0000000000000000
083		00	0000000000000000
084		00	0000000000000000
085		00	0000000000000000
086		00	0000000000000000
087		00	0000000000000000
088		00	0000000000000000
089		00	0000000000000000
090		00	0000000000000000
091		00	0000000000000000
092		00	0000000000000000
093		00	0000000000000000
094		00	0000000000000000
095		00	0000000000000000
096		00	0000000000000000
097		00	0000000000000000
098		00	0000000000000000
099		00	0000000000000000
100		00	0000000000000000

Рис. 2.22. Расшифровка протокола инициирующего фрейма запроса

Когда точка доступа получает инициирующий фрейм запроса, по отношению к которому была успешно выполнена процедура проверки контрольной последовательности фрейма (frame check sequence, FCS), она посылает ответ на инициирующий фрейм запроса (probe response frame): для однообразия мы будем называть его инициирующим фреймом ответа. На рис. 2.23 представлена расшифровка протокола инициирующего фрейма ответа.

Ключевые поля инициирующего фрейма ответа следующие.

**Поле временной метки (timestamp field).** Значение TSFTIMER фрейма отправителя.

**Поле сигнала интервала (beacon interval field).** Число тактов (time units, TUs) между маячковыми сигналами. Длительность такта составляет 1024 мкс.

**Поле информационной способности (capability information field).** Указывает на возможности MAC и PHY уровня. Это поле подробно описывается ниже, в разделе "Форматы фреймов MAC стандарта 802.11".

**Элемент SSID SSID,** с которым сконфигурирована точка доступа.

**Элемент поддерживаемых скоростей передачи.** Все скорости передачи данных, поддерживаемые точкой доступа.

**Элемент набора параметров PHY (PHY parameter set element)** Может указывать или на технологию расширения спектра путем скачкообразного переключения частоты (frequency hopping), или на технологию широкополосной модуляции с прямым расширением спектра (direct sequence). Этот элемент обеспечивает предоставление специфической информации уровня PHY для клиентской станции. Оба элемента подробно описываются ниже, в разделе "Форматы фреймов MAC стандарта 802.11".

970	Phase Control Field 4	= 50
971	CC	= 300 Predefined Version
972	AD	= 300 Management Flags
973	0000	= 300 Phase Predefined Distribution
974	Phase Control Field 4	= 20
975	0	= 400 To Distribution Predefined
976	0	= 400 To Distribution Predefined
977	0	= 400 To Distribution Predefined
978	0	= 400 To Distribution Predefined
979	0	= 400 To Distribution Predefined
980	0	= 400 To Distribution Predefined
981	0	= 400 To Distribution Predefined
982	0	= 400 To Distribution Predefined
983	0	= 400 To Distribution Predefined
984	0	= 400 To Distribution Predefined
985	0	= 400 To Distribution Predefined
986	0	= 400 To Distribution Predefined
987	0	= 400 To Distribution Predefined
988	0	= 400 To Distribution Predefined
989	0	= 400 To Distribution Predefined
990	0	= 400 To Distribution Predefined
991	0	= 400 To Distribution Predefined
992	0	= 400 To Distribution Predefined
993	0	= 400 To Distribution Predefined
994	0	= 400 To Distribution Predefined
995	0	= 400 To Distribution Predefined
996	0	= 400 To Distribution Predefined
997	0	= 400 To Distribution Predefined
998	0	= 400 To Distribution Predefined
999	0	= 400 To Distribution Predefined

Рис. 2.11. Зондирующий фрейм ответа

Клиентская станция получает зондирующий фрейм ответа, она может определить уровень сигнала полученного фрейма. Эта станция сравнивает зондирующие фреймы ответа и определяет, к какой точке доступа они относятся. Механизм, благодаря которому клиентская станция выбирает точку доступа для привязки к ней, не описан в стандарте 802.11, так что он реализуется поставщиком самостоятельно. В общем случае критерии выбора точки доступа может включать согласование SSID, уровня сигнала и собственные критерии поставщика.

Ввиду отсутствия подобного образа предположим, что критериями являются согласование SSID, поддерживаемые скорости передачи данных и уровень сигнала (рис. 2.24).

В табл. 2.1 системы введены данные из зондирующих фреймов ответа, полученных станцией Вивьер.

Таблица 2.1. Информация из зондирующих фреймов ответа

Название точки доступа	Поддерживаемые скорости передачи	ID набора сервисов	Уровень сигнала (%)
AP1	Все	Маркетинг	50
AP2	Все	Маркетинг	100
AP3	Все	Продажи	20



Рис. 2.24. Процесс ассоциации

Станция Вивьен намеревается привязаться к точке доступа 2 (AP2). AP2 имеет подходящий SSID, поддерживает высокую скорость передачи данных и имеет уровень сигнала 100%. Точка AP1 — близкий конкурент, но уровень ее сигнала на 50% меньше. Теперь, когда станция Вивьен определила, с какой точкой доступа ей лучше ассоциироваться, она может приступить к следующей фазе установления возможности следования станции — процессу аутентификации.

## Процесс аутентификации

Процесс аутентификации по стандарту 802.11 может выполняться в двух режимах: аутентификация с открытым ключом (open authentication) и аутентификация с закрытым ключом (shared-key authentication). Оба эти режима подробно рассматриваются в главе 4, "Безопасность беспроводных локальных сетей стандарта 802.11". Аутентификация в соответствии с этим стандартом ориентирована в основном на аутентификацию устройства (а не пользователя), и ее процесс состоит в определении, принадлежит ли данное устройство локальной сети. В данном разделе мы коснемся лишь вопроса об аутентификации и ответа на запрос относительно аутентификации (рис. 2.25).

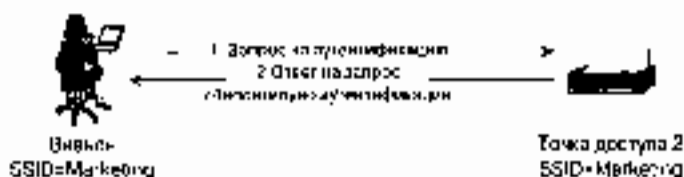


Рис. 2.25. Процесс аутентификации



## Процесс привязки

Процесс привязки по стандарту 802.11 позволяет точке доступа выделить для беспроводной станции логический порт или драйвер с её идентификатором ассоциации (association identifier, AID). Процесс привязки начинается беспроводной станцией с фрейма запроса на ассоциацию, содержащим информацию о возможностях клиента и кодируется ответом от точки доступа на ассоциацию, посылаемого точкой доступа. Ответ на ассоциацию может быть положительным или отрицательным и содержит код, указывающий на причину отказа. На рис. 2.26 представлена расшифровка протокола фрейма запроса на ассоциацию, а на рис. 2.27 — расшифровка протокола фрейма ответа на ассоциацию.

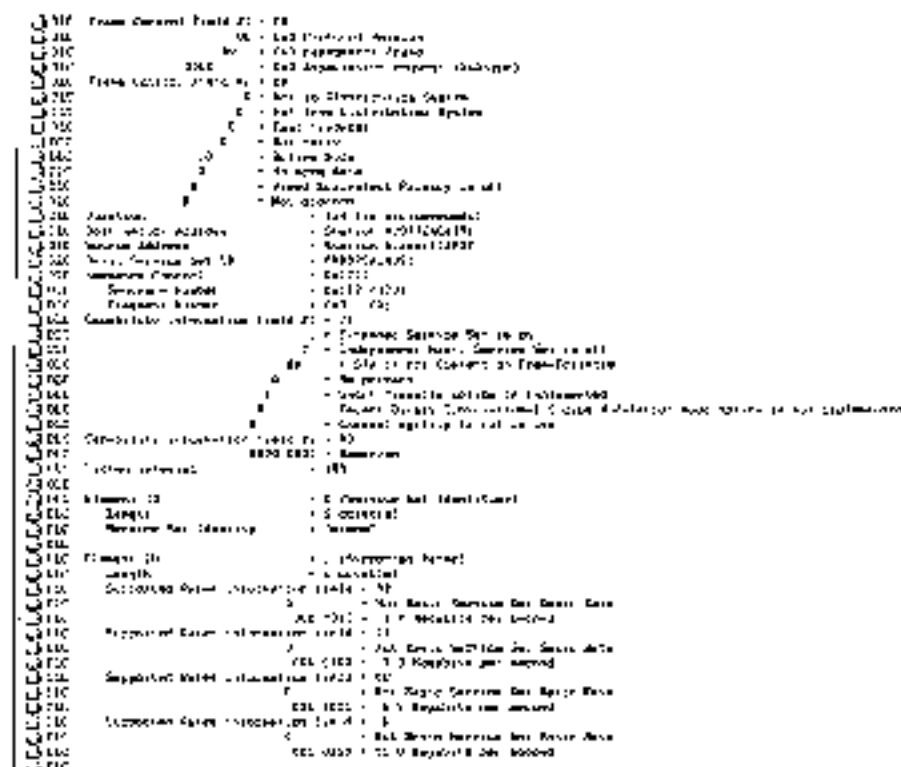


Рис. 2.26. Фрейм запроса на ассоциацию

Ключевые поля фрейма запроса на создание следующие:

- **Интервал прослушивания (listen interval)** Значение интервала прослушивания устанавливается в режиме экономии энергии/отрицательная и сообщается клиентской станцией точке доступа. Оно информирует точку доступа о том, как часто эта станция “пробуждается” (выходит из режима экономии/энергосбережения), чтобы получить фреймы, буферизированные в точке доступа. Более подробно об этом рассказывается ниже.
- **Элемент SSID** Определяет SSID клиентской станции для точки доступа. В нормальном режиме работы точка доступа не принимает запросы на ассоциацию от станции с SSID, отличающимся от тех, которые санифицированы в точке доступа.

21	Type Frame Field 21	00
22		00 - No Protocol Version
23		01 - 802.11 Management Frame
24		02 - 802.11 Authentication response (Ack/Resp)
25	Frame Control Field 25	00
26		00 - Not to be interpreted (Control)
27		01 - Not from Authentication System
28		02 - Not to be interpreted
29		03 - Not to be interpreted
30		04 - Not to be interpreted
31		05 - Not to be interpreted
32		06 - Not to be interpreted
33		07 - Not to be interpreted
34		08 - Not to be interpreted
35		09 - Not to be interpreted
36		0A - Not to be interpreted
37		0B - Not to be interpreted
38		0C - Not to be interpreted
39		0D - Not to be interpreted
40		0E - Not to be interpreted
41		0F - Not to be interpreted
42		10 - Not to be interpreted
43		11 - Not to be interpreted
44		12 - Not to be interpreted
45		13 - Not to be interpreted
46		14 - Not to be interpreted
47		15 - Not to be interpreted
48		16 - Not to be interpreted
49		17 - Not to be interpreted
50		18 - Not to be interpreted
51		19 - Not to be interpreted
52		1A - Not to be interpreted
53		1B - Not to be interpreted
54		1C - Not to be interpreted
55		1D - Not to be interpreted
56		1E - Not to be interpreted
57		1F - Not to be interpreted
58		20 - Not to be interpreted
59		21 - Not to be interpreted
60		22 - Not to be interpreted
61		23 - Not to be interpreted
62		24 - Not to be interpreted
63		25 - Not to be interpreted
64		26 - Not to be interpreted
65		27 - Not to be interpreted
66		28 - Not to be interpreted
67		29 - Not to be interpreted
68		2A - Not to be interpreted
69		2B - Not to be interpreted
70		2C - Not to be interpreted
71		2D - Not to be interpreted
72		2E - Not to be interpreted
73		2F - Not to be interpreted
74		30 - Not to be interpreted
75		31 - Not to be interpreted
76		32 - Not to be interpreted
77		33 - Not to be interpreted
78		34 - Not to be interpreted
79		35 - Not to be interpreted
80		36 - Not to be interpreted
81		37 - Not to be interpreted
82		38 - Not to be interpreted
83		39 - Not to be interpreted
84		3A - Not to be interpreted
85		3B - Not to be interpreted
86		3C - Not to be interpreted
87		3D - Not to be interpreted
88		3E - Not to be interpreted
89		3F - Not to be interpreted
90		40 - Not to be interpreted
91		41 - Not to be interpreted
92		42 - Not to be interpreted
93		43 - Not to be interpreted
94		44 - Not to be interpreted
95		45 - Not to be interpreted
96		46 - Not to be interpreted
97		47 - Not to be interpreted
98		48 - Not to be interpreted
99		49 - Not to be interpreted
100		4A - Not to be interpreted
101		4B - Not to be interpreted
102		4C - Not to be interpreted
103		4D - Not to be interpreted
104		4E - Not to be interpreted
105		4F - Not to be interpreted
106		50 - Not to be interpreted
107		51 - Not to be interpreted
108		52 - Not to be interpreted
109		53 - Not to be interpreted
110		54 - Not to be interpreted
111		55 - Not to be interpreted
112		56 - Not to be interpreted
113		57 - Not to be interpreted
114		58 - Not to be interpreted
115		59 - Not to be interpreted
116		5A - Not to be interpreted
117		5B - Not to be interpreted
118		5C - Not to be interpreted
119		5D - Not to be interpreted
120		5E - Not to be interpreted
121		5F - Not to be interpreted
122		60 - Not to be interpreted
123		61 - Not to be interpreted
124		62 - Not to be interpreted
125		63 - Not to be interpreted
126		64 - Not to be interpreted
127		65 - Not to be interpreted
128		66 - Not to be interpreted
129		67 - Not to be interpreted
130		68 - Not to be interpreted
131		69 - Not to be interpreted
132		6A - Not to be interpreted
133		6B - Not to be interpreted
134		6C - Not to be interpreted
135		6D - Not to be interpreted
136		6E - Not to be interpreted
137		6F - Not to be interpreted
138		70 - Not to be interpreted
139		71 - Not to be interpreted
140		72 - Not to be interpreted
141		73 - Not to be interpreted
142		74 - Not to be interpreted
143		75 - Not to be interpreted
144		76 - Not to be interpreted
145		77 - Not to be interpreted
146		78 - Not to be interpreted
147		79 - Not to be interpreted
148		7A - Not to be interpreted
149		7B - Not to be interpreted
150		7C - Not to be interpreted
151		7D - Not to be interpreted
152		7E - Not to be interpreted
153		7F - Not to be interpreted
154		80 - Not to be interpreted
155		81 - Not to be interpreted
156		82 - Not to be interpreted
157		83 - Not to be interpreted
158		84 - Not to be interpreted
159		85 - Not to be interpreted
160		86 - Not to be interpreted
161		87 - Not to be interpreted
162		88 - Not to be interpreted
163		89 - Not to be interpreted
164		8A - Not to be interpreted
165		8B - Not to be interpreted
166		8C - Not to be interpreted
167		8D - Not to be interpreted
168		8E - Not to be interpreted
169		8F - Not to be interpreted
170		90 - Not to be interpreted
171		91 - Not to be interpreted
172		92 - Not to be interpreted
173		93 - Not to be interpreted
174		94 - Not to be interpreted
175		95 - Not to be interpreted
176		96 - Not to be interpreted
177		97 - Not to be interpreted
178		98 - Not to be interpreted
179		99 - Not to be interpreted
180		9A - Not to be interpreted
181		9B - Not to be interpreted
182		9C - Not to be interpreted
183		9D - Not to be interpreted
184		9E - Not to be interpreted
185		9F - Not to be interpreted
186		A0 - Not to be interpreted
187		A1 - Not to be interpreted
188		A2 - Not to be interpreted
189		A3 - Not to be interpreted
190		A4 - Not to be interpreted
191		A5 - Not to be interpreted
192		A6 - Not to be interpreted
193		A7 - Not to be interpreted
194		A8 - Not to be interpreted
195		A9 - Not to be interpreted
196		AA - Not to be interpreted
197		AB - Not to be interpreted
198		AC - Not to be interpreted
199		AD - Not to be interpreted
200		AE - Not to be interpreted
201		AF - Not to be interpreted
202		B0 - Not to be interpreted
203		B1 - Not to be interpreted
204		B2 - Not to be interpreted
205		B3 - Not to be interpreted
206		B4 - Not to be interpreted
207		B5 - Not to be interpreted
208		B6 - Not to be interpreted
209		B7 - Not to be interpreted
210		B8 - Not to be interpreted
211		B9 - Not to be interpreted
212		BA - Not to be interpreted
213		BB - Not to be interpreted
214		BC - Not to be interpreted
215		BD - Not to be interpreted
216		BE - Not to be interpreted
217		BF - Not to be interpreted
218		C0 - Not to be interpreted
219		C1 - Not to be interpreted
220		C2 - Not to be interpreted
221		C3 - Not to be interpreted
222		C4 - Not to be interpreted
223		C5 - Not to be interpreted
224		C6 - Not to be interpreted
225		C7 - Not to be interpreted
226		C8 - Not to be interpreted
227		C9 - Not to be interpreted
228		CA - Not to be interpreted
229		CB - Not to be interpreted
230		CC - Not to be interpreted
231		CD - Not to be interpreted
232		CE - Not to be interpreted
233		CF - Not to be interpreted
234		D0 - Not to be interpreted
235		D1 - Not to be interpreted
236		D2 - Not to be interpreted
237		D3 - Not to be interpreted
238		D4 - Not to be interpreted
239		D5 - Not to be interpreted
240		D6 - Not to be interpreted
241		D7 - Not to be interpreted
242		D8 - Not to be interpreted
243		D9 - Not to be interpreted
244		DA - Not to be interpreted
245		DB - Not to be interpreted
246		DC - Not to be interpreted
247		DD - Not to be interpreted
248		DE - Not to be interpreted
249		DF - Not to be interpreted
250		E0 - Not to be interpreted
251		E1 - Not to be interpreted
252		E2 - Not to be interpreted
253		E3 - Not to be interpreted
254		E4 - Not to be interpreted
255		E5 - Not to be interpreted
256		E6 - Not to be interpreted
257		E7 - Not to be interpreted
258		E8 - Not to be interpreted
259		E9 - Not to be interpreted
260		EA - Not to be interpreted
261		EB - Not to be interpreted
262		EC - Not to be interpreted
263		ED - Not to be interpreted
264		EE - Not to be interpreted
265		EF - Not to be interpreted
266		F0 - Not to be interpreted
267		F1 - Not to be interpreted
268		F2 - Not to be interpreted
269		F3 - Not to be interpreted
270		F4 - Not to be interpreted
271		F5 - Not to be interpreted
272		F6 - Not to be interpreted
273		F7 - Not to be interpreted
274		F8 - Not to be interpreted
275		F9 - Not to be interpreted
276		FA - Not to be interpreted
277		FB - Not to be interpreted
278		FC - Not to be interpreted
279		FD - Not to be interpreted
280		FE - Not to be interpreted
281		FF - Not to be interpreted

Рис. 2.27. Фрейм ответа на ассоциирование

- Элемент поддерживаемых скоростей передачи. Указывает точке доступа, какие скорости передачи поддерживает клиентская станция.

Ключевые поля фрейма пинга на ассоциирование следующие:

- Код состояния (status code). Этот элемент указывает код состояния, определенным из фрейма ответа на ассоциирование. Все коды состояния описываются ниже, в разделе "Форматы фреймов MAC стандарта 802.11".
- Идентификатор ассоциации (AID). Можно считать AID похожим на физический порт хаба или коммутатора Ethernet. Клиентская станция должна иметь это значение, когда она работает в режиме энергосбережения. Точка доступа посылает оповещения в сигнальных фреймах, указывающие, какие AID имеют буферизованные фреймы. Более подробно об этом рассказывается ниже, в разделе "Работа в режиме энергосбережения".
- Элемент поддерживаемых скоростей передачи. Указывает, какие скорости передачи поддерживает точка доступа.

## Работа в режиме энергосбережения

Чтобы продлить срок службы батарей портативных клиентов беспроводных локальных сетей, стандарт 802.11 предусматривает их работу в режиме сниженного энергопотребления, или режиме энергосбережения (power save operations). Работа в режиме сниженного энергопотребления осуществляется в двух вариантах.

- Работа с одноадресными фреймами.
- Работа с широковещательными/многоадресными фреймами.

Предполагается, что клиентская база работает в режиме энергосбережения, просто клиентская станция переходит в режим энергосбережения, когда отключает свою радиостанцию. Точка доступа буферизирует фреймы, предназначенные для определенной станции, находящейся в режиме энергосбережения. Через определенный интервал времени клиент "просыпается" (активизируется) и принимает сигнал от точки доступа, локализации, имеются ли в буфере фреймы для данной клиентской станции.

При работе с одноадресными фреймами интервал прослушивания или активизации определяется клиентом. И наоборот, при работе в режиме энергосбережения с широковещательными/многоадресными фреймами интервал прослушивания определяется точкой доступа и объявляется в ее сигналах фрейма.

Клиент активизируется и принимает сигналы фреймы точки доступа, чтобы определить, буферизированы ли для него фреймы. Если это не так, клиент возвращается к работе в режиме энергосбережения и пребывает в нем до истечения очередного периода "снайки".

## Работа с одноадресными фреймами в режиме энергосбережения

Когда клиент связывается с точкой доступа, он указывает значение интервала прослушивания по фрейму запроса на ассоциацию. Интервал прослушивания — это число сигнальных фреймов, которые клиент отсчитывает, прежде чем перейти в активный режим. Например, интервал прослушивания 200 означает, что клиент активизируется через каждые 200 сигнальных фреймов.

Сигнальный фрейм включает информационный элемент, называемый *карта индикации трафика* (traffic indication map, TIM). Этот элемент содержит перечень адресов AID, которые несут трафик, буферизированный точкой доступа. Может быть до 2048 уникальных AID, так что размер одного элемента TIM может достигать 251 бита. Чтобы минимизировать нагрузку на сеть, TIM использует сокращенный метод перечисления AID. На рис. 2-29 представлена расшифровка протокола сигнального фрейма с элементом TIM, указывающим на наличие буферизированного трафика для клиента.

Обратите внимание на то, что поле в расшифровке протокола не указан в явном виде AID клиентской станции. Чтобы определить AID клиентской станции (или станции), необходимо обладать следующей информацией.

- Значение в поле длины (the value of length field).
- Значение в поле смещения битовой карты (the value of bitmap offset field).
- Значение в поле частичный пертурбированный битовой карты (the value of partial virtual bitmap field).

```
01C Element ID      01C      01C      01C      01C      01C      01C      01C      01C      01C
000 Length          000      000      000      000      000      000      000      000      000
01C Delivery Traffic Indication Message Count = 6
000 Delivery Traffic Indication Message Period = 10
01C Bitmap control field = 00
000 Traffic Indication bit
01C Offset = 1
000 Partial Virtual Bitmap = 000
```

Рис. 2.29. Расшифровка протокола элемента TIM

Стандарт 802.11 регламентирует применение виртуальной битовой карты индикации трафика (traffic indication virtual bitmap) как средства указания на ID, идентификаторы ассоциации (AID) каких станций имеют буферизированные фреймы. Виртуальная битовая карта привязана к AID 1 и идентифицирует AID 2007. AID 0 зарезервирован для многоадресной/одноадресной передачи. Табл. 2.2 дает представление о том, на что может быть похожа виртуальная битовая карта индикации трафика. Каждая станция с фреймами, буферизированными в точке доступа, имеет значение флага, равное 1 для AID данной станции. Станции, для которых не имеется буферизированных фреймов, имеют значение флага 0.

Таблица 2.2. Пример виртуальной битовой карты индикации трафика

AID	:	2	3	...	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	...	2007	
Флаг	:	0	0	0	...	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	...	0

Затененные значения включены в частичную виртуальную битовую карту

Частичная виртуальная битовая карта исключает все несуществующие нулевые значения флага путем их суммирования. Все клиентские станции, для которых имеется буферизированные фреймы (т. е. следовательно, установлены значения флага, равные 1, в виртуальной битовой карте индикации трафика), включаются в частичную виртуальную битовую карту. Все AID со значением флага, равным 0, предшествующие частичной виртуальной битовой карте, суммируются с произвольной величиной, обозначенной в нижеследующих примерах буквой X. Все AID со значением флага, равным 0, следующие за частичной виртуальной битовой картой, суммируются с произвольной величиной, обозначенной в нижеследующих примерах буквой Y. Если мы обратимся к табл. 2.2, то для нее AID с 1-го по 15-й суммируются с величиной X, а AID с 32-го по 2007-й суммируются с величиной Y.

Чтобы вычислить X и Y, вначале нужно вывести значения N1 и N2. Формулы, по которым можно вычислить X, Y, N1 и N2, приведены ниже.

$N1 = (\text{сумма значений битовой карты}) * 2$

$N2 = (\text{длина} - 4) + N1$

$X = (N1 * 8) - 1$

$Y = (N2 - 1) * 8$

В примере ретрансляции, приведенном на рис. 2.28,  $N1 = 11 * 21 = 231$  и  $N2 = (5 - 4) + 231 = 236$ . Значение X составляет  $(231 * 8) - 1$ , или 1847, а Y — это  $(236 - 1) * 8$ , или 1888. Величина X указывает, что все AID с 1-го по 15-й имеют значение флага, равное 0, а величина Y свидетельствует о том, что все AID с 32-го по 2007-й имеют значение флага, тоже равное 0.

Проочтенными остаются AID с 16-го по 31-й, и именно здесь вступает в игру частичная виртуальная битовая карта. В данном примере значение частичной виртуальной битовой карты составляет 2 байта, 0x0020. Первый байт, 0x00, или 00000000 в двоичной записи, показывает, что все следующие 8 флагов станций, следующих за X (AID с 16-го по 23-й), равны 0. Второй байт — это 0x20, или 00100000 в двоичной записи. Итак, в рассматриваемом примере AID с 24-го по 28-й имеют значение флага, равное 0, а AID 29 — значение флага, равное 1. Поскольку AID 29 — это единственный AID со значением флага, равным 1, для станции с AID 29 имеется трафик, буферизированный в точке доступа.

Если клиент понимает, что для него буферизированы фреймы, он присылает служебный (management) фрейм уровня MAC стандарта 802.11, размещенный *фрейм отриса режима энергосбережения* (power save poll, PS-Poll). На рис. 2.29 представлена расшифровка протокола PS-Poll, посланного клиентской станцией в ответ на сигнальный фрейм. Обратите внимание, что поле AID имеет значение, равное 29, именно это было определено для AID на основе анализа частичной виртуальной битовой карты в элементе TIM.

Точка доступа отвечает на фрейм PS-Poll одним из буферизированных фреймов клиента и указывает на то, имеются ли для него другие буферизированные фреймы. Этот клиент должен послать фрейм PS-Poll точке доступа, чтобы получить каждый из буферизированных фреймов, имеющихся для него в точке доступа. На рис. 2.29 представлена расшифровка протокола передачи фрейма PS-Poll. Обратите внимание на то, что поле AID указывает на AID 29, как и было нами вычислено в предыдущем примере.

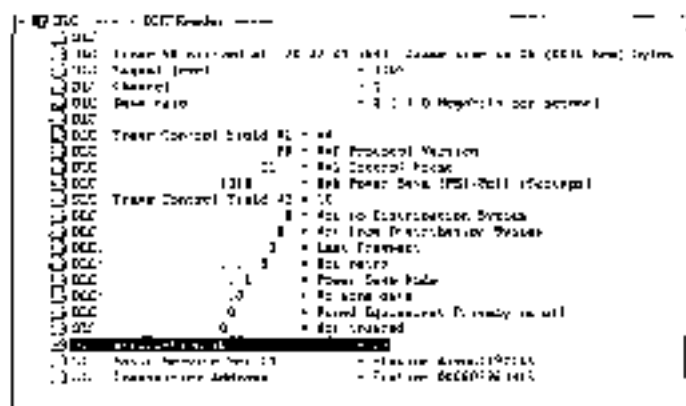


Рис. 2.24. Расшифровка протокола передачи фрейма PS-Poll

## Широковещание в режиме энергосбережения

Широковещание в режиме энергосбережения осуществляется в основном так же, как и одноканальная передача в режиме с энергосбережением. Отличия таковы:

- Администратор определяет интервал, по истечении которого клиент должен активизироваться и получить буферизированный трафик широковещания или многоадресной рассылки.
- Особый информационный элемент TIM, называемый DTIM, указывает, имеется ли в точке доступа буферизированный трафик широковещания или многоадресной рассылки.
- Фреймы широковещания или многоадресной рассылки буферизируются для всех станций (включая неэнергосберегающие, ассоциированных в BSS, если одна или больше станций ассоциированы с точкой доступа).

Информационный элемент TIM имеет два поля, указывающие, буферизирован ли трафик широковещания/многоадресной рассылки и как скоро он будет распространен в пределах BSS.

- Поле подсчета DTIM (DTIM count field) Указывает, сколько сигнальных фреймов должно быть передано, прежде чем будут распространены буферизированные фреймы. Значение 0 говорит о том, что этот информационный элемент

DTIM является элементом DTIM, и если имеются буферизированные фреймы, они должны быть переданы немедленно вслед за сигнальным фреймом.

- Поле периода DTIM (DTIM period field). Указывает количество сигнальных фреймов, передаваемых между DTIM. Например, значение 10 указывает, что каждый десятый сигнальный фрейм будет содержать DTIM.

На рис. 2.39 представлена расшифровка протокола сигнального фрейма, содержащего DTIM. На рис. 2.41 обратите внимание на то, что все фреймы, следующие за сигнальным, являются многоадресными.

DIC:	Element ID	= 5 (Traffic Indicator Map)
DIC:	Length	= 4 octets
DIC:	Priority Traffic Indication Response Count	= 0
DIC:	Delivery Traffic Indication Message Period	= 10
DCC:	...Bitmap control bitmap	= 01
DCC:	...Traffic Indicator bit	= 1
DCC:	DCC C03	= 0 Bitmap offset
DCC:	Partial Bitmap Bitmap	= 10

Рис. 2.39 Расшифровка протокола элемента DTIM

[0]	13 2 0 0 11	000 0 0 101	0000 0000 0001
[1]	13 2 0 0 11	0000 0000 0000	0000 0000 0000
[2]	13 2 0 0 11	1000 0 0 101	0000 0000 0000

Рис. 2.41 Многоадресные фреймы, следующие за сигнальным, содержащим элемент DTIM

## Форматы фреймов MAC стандарта 802.11

На уровне MAC стандарта 802.11 используются фреймы трех категорий.

- Управляющие фреймы (control frames). Способствуют передаче фреймов данных при нормальном обмене информацией станциями стандарта 802.11.
- Служебные фреймы (management frames). Обеспечивают соединения беспроводных локальных сетей, аутентификацию и указывают состояние.
- Фреймы данных (data frames). Переносят данные станции от передатчика к приемнику.

Все фреймы стандарта 802.11 ложатся на основной фрейм этого стандарта. Названные три типа фреймов расширяют и используют специфические участки основного фрейма MAC для своих целей. На рис. 2.32 представлены основной фрейм MAC и его поля.

Формат фрейма	Продолжительность	Адрес 1	Адрес 2	Адрес 3	Управление фреймом	Адрес 4	Точка доступа	FCF
2 байт	2 байт	1 байт	1 байт	1 байт	2 байт	1 байт	0-2 байта	1 байт

Рис. 2.32 Основной фрейм MAC по стандарту 802.11

- Поле контроля фрейма (frame control). Размер этого поля равен 2 байтам; оно состоит из шестнадцати подполей. На рис. 2.33 показаны подполя поля контроля фрейма, а на рис. 2.34 дана расшифровка протокола ведущей контрольной фрейма.

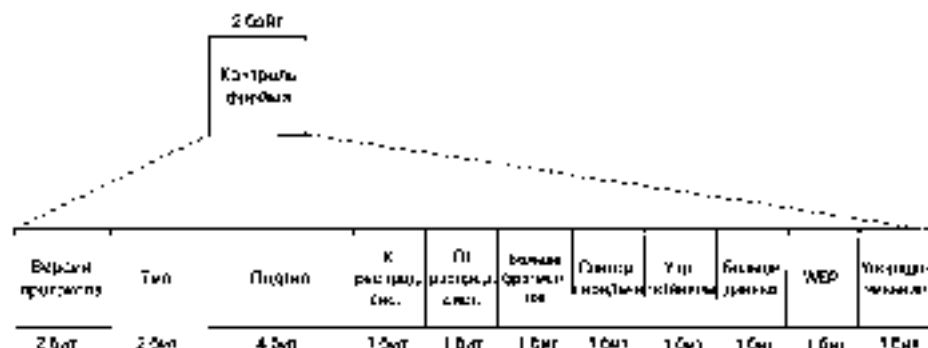


Рис. 2.33. Структура поля контроля фрейма

000	Frame Control Field #1	00	
000		10	000 Protocol Version
000		10	000 Management Frame
000	1011	.	000 Authentication (Subtype)
010	Frame Control Field #2	00	
000		0	Not to Distribution System
000		1	Not from Distribution System
000		0	Not to DS
000		1	Not from DS
000		0	Active data
000		1	Not active data
010		0	Wired Equivalent Privacy on
010		1	Not ordered

Рис. 2.34. Расшифровка протокола подтипов поля контроля фрейма

Ниже перечислены значения полей поля контроля фрейма.

- **Версия протокола (protocol version).** Указывает версию протокола 802.11 MAC. На сегодняшний день существует только одна версия, поэтому для этого поля справедливо только значение 0. Все остальные значения зарезервированы.
- **Тип (type).** Указывает тип фрейма MAC: управляющий, служебный или фрейм данных. Четвертое значение зарезервировано.
- **Подтип (subtype).** Указывает подтип фрейма. Возможные значения этого поля представлены в табл. 2.3.

Таблица 2.3. Типы и подтипы фрейма

Значение типа (бит 3, бит 2)	Описание типа	Значение подтипа (бит 7, бит 6, бит 5, бит 4)	Описание подтипа
00	Управляющий	0000	Запрос на соединение
00	Служебный	0001	Ответ на запрос на соединение
00	Служебный	0010	Запрос на повторное соединение
00	Служебный	0011	Ответ на запрос на повторное соединение
01	Служебный	0100	Запланированный запрос

Значение типа (бит 3, бит 2)	Описание типа	Значение подтипа (бит 7, бит 6, бит 5, бит 4)	Описание подтипа
00	Служебный	0000	Ответ на зондирующий запрос
00	Служебный	0110–0111	Зарезервированы
00	Служебный	1000	Сигнал
00	Служебный	1001	Событие карты индикации трафика (aggregation traffic indication frame, ATIM)
00	Служебный	1010	Различение
00	Служебный	1011	Аутентификация
00	Служебный	1100	Деаутентификация
00	Служебный	1101–1111	Зарезервированы
01	Управляющий	0000–1001	Зарезервированы
01	Управляющий	1010	PS-Poll
01	Управляющий	1011	RTS
01	Управляющий	1100	CTS
01	Управляющий	1101	Подтверждение (ACK)
01	Управляющий	1110	CF-end
01	Управляющий	1111	CF-End+CF-Ack
10	Данные	0000	Данные
10	Данные	0001	Данные+CF-Ack
10	Данные	0010	Данные+CF-Poll
10	Данные	0011	Данные+CF-Ack+CF-Poll
10	Данные	0100	Нулевая функция (длины отсутствуют)
10	Данные	0101	CF-Ack (данные отсутствуют)
10	Данные	0110	CF-Poll (данные отсутствуют)
10	Данные	0111	CF-Ack+CF-Poll (данные отсутствуют)
10	Данные	1000–1111	Зарезервированы
11	Зарезервированы	0000–1111	Зарезервированы

- **К распределительной системе (to DS)**. Указывает, предназначен ли фрейм для распределительной системы.
- **От распределительной системы (from DS)**. Указывает, получен ли фрейм из распределительной системы.
- **Больше фрагментов (more fragments)**. Указывает, является ли данный фрейм только служебным или только фреймом данных, либо следует ожидать других фрагментов.
- **Повторная передача (retry)**. Указывает, передается ли данный фрейм повторно. Позволяет приемнику отвергать дублирующие фреймы.



- **Управление питанием (power management)**. Указывает на режим энергопотребления станции. Значение 1 говорит о том, что станция работает в режиме экономии энергопотребления, а значение 0 — что она находится в активном режиме. Фреймы точки доступа всегда имеют данное значение, равное 0.
- **Большие данные (more data)**. Если бит этого поля установлен, принимающая станция оповещается о том, что имеются предпочтительные для нее данные, буферизированные в точке доступа.
- **Защищенность, эквивалентная тиковым проводным сетям (wired equivalent privacy, WEP)**. Указывает, используется ли шифрование WEP для защиты поля фрейма.
- **Параметр упорядочивания (order)**. Значение этого поля равно 1, если фрейм данных использует StrictlyOrdered service class, в противном случае оно равно 0.
- **Продолжительность/ID (Duration/ID)**. Это поле используется спонтанно, в зависимости от того, получает ли доступ к среде станция, работающая в энергосберегающем режиме, находится ли среда в режиме PCF периода, свободного от конкуренции (CFP), и получает ли доступ к среде станция DCF. В табл. 2.4 представлены значения битов для различных станций.

Таблица 2.4. Значения поля продолжительности

Бит 15	Бит 14	Биты 13–0	Когда используется
0	0–32 767		Продолжительность обмена фреймами (в мкс) для станций DCF
1	0	0	Значения, используемые во время обмена фреймами в период CFP
1	0	1–1683	Зарезервированы
1	1	0	Зарезервированы
1	1	1–2007	AID для использования по фреймам PS-Poll
1	1	2008–16 383	Зарезервированы

- **Адреса 1, 2, 3 и 4**. Эти поля помещаются в зависимости от типа и режима фрейма.
- **Управление очередностью (sequence control)**. В этом поле содержится порядковый номер и номер фрагмента фрейма.
- **FCS**. Это контрольная сумма фрейма. В данном поле содержится 32-разрядное значение циклического избыточного контроля (cyclic redundancy check, CRC), вычисленное для всех полей заголовка и тела фрейма MAC.

На рис. 2.35 представлена расшифровка протокола оставшихся полей основного фрейма MAC.

0000	Sequence Control	• Seq. Control (sequence control)
0000	Seq. Control Address	• Station Address 33159C
0000	Seq. Control Address	• Station Address 56C292
0000	Seq. Control Seq. ID	• Seq. ID 31E8EC
0000	Seq. Control Control	• Seq. ID 0
0000	Seq. Control Number	• Seq. ID (114)
0000	Seq. Control Number	• Seq. ID (1)

Рис. 2.35. Расшифровка протокола оставшихся полей основного фрейма MAC

## Управляющие фреймы стандарта 802.11

В спецификации стандарта 802.11 оговорены шесть уникальных управляющих фреймов:

- Очередь режима сниженного энергопотребления (PS-Poll).
- RTS.
- CTS.
- ACK.
- Конец периода, свободного от конкуренции (Contention-free End, CF-End).
- CF-End – конец периода, свободного от конкуренции, и подтверждение приема последнего фрейма (contention-free acknowledgment, CF-End-CF-ACK).

На первых четырех фреймах стоит остановиться подробнее. Фреймы CF-End и CF-End-CF-ACK используются с PCF и поэтому применяются не часто.

### Фрейм PS-Poll

Фрейм PS-Poll указывает точке доступа на то, что беспроводная станция, работающая в режиме энергосбережения, требует, чтобы ей были доставлены буферизированные фреймы. Фрейм PS-Poll имеет следующие отличия от основного фрейма MAC:

- AID: AID беспроводного клиента с двумя битами самых старших разрядов, указывающими значение 1.
- Идентификатор BSS (BSSID): MAC-адрес точки доступа к инфраструктуре сети.
- Адрес передатчика (transmission address, TA), MAC-адрес беспроводной энерго-сберегающей станции.

На рис. 2.36 показан формат фрейма PS-Poll, а на рис. 2.37 приведена расшифровка протокола фрейма PS-Poll.

Контроль фрейма	AID	BSSID	Адрес передатчика	FCS
2 байт	2 байт	6 байт	6 байт	4 байт

Рис. 2.36 Формат фрейма PS-Poll

```

0000 0000: ... IEEE Standard ...
0001 0000:
0002 0000: Фрейм PS-Poll (тип: 0x00, 0x00, 0x00, 0x00, 0x00, 0x00)
0003 0000: Signal Rate: 20.000 MHz
0004 0000: Channel: 11
0005 0000: Data rate: 2.000 Mbps (802.11g)
0006 0000:
0007 0000: Фрейм Control Frame (тип: 0x00, 0x00, 0x00, 0x00, 0x00, 0x00)
0008 0000:   00: - Set Acknowledgment Sequence
0009 0000:   01: - Set Control Frame
0010 0000:   02: - Set Frame Type (PS-Poll) (отключено)
0011 0000: Фрейм Control Frame (тип: 0x00, 0x00, 0x00, 0x00, 0x00, 0x00)
0012 0000:   00: - Max. Rx Power/Receive Sensitivity
0013 0000:   01: - Max. Tx Power/Transmit Power
0014 0000:   02: - Cap. Extension
0015 0000:   03: - Max. Power
0016 0000:   04: - Power Save Mode
0017 0000:   05: - Power Mgmt.
0018 0000:   06: - Clear Extension/Extend/Energy Detect
0019 0000:   07: - Poll Interval
0020 0000:
0021 0000:
0022 0000:
0023 0000:
0024 0000:
0025 0000:
0026 0000:
0027 0000:
0028 0000:
0029 0000:
0030 0000:
0031 0000:
0032 0000:
0033 0000:
0034 0000:
0035 0000:
0036 0000:
0037 0000:
0038 0000:
0039 0000:
0040 0000:
0041 0000:
0042 0000:
0043 0000:
0044 0000:
0045 0000:
0046 0000:
0047 0000:
0048 0000:
0049 0000:
0050 0000:
0051 0000:
0052 0000:
0053 0000:
0054 0000:
0055 0000:
0056 0000:
0057 0000:
0058 0000:
0059 0000:
0060 0000:
0061 0000:
0062 0000:
0063 0000:
0064 0000:
0065 0000:
0066 0000:
0067 0000:
0068 0000:
0069 0000:
0070 0000:
0071 0000:
0072 0000:
0073 0000:
0074 0000:
0075 0000:
0076 0000:
0077 0000:
0078 0000:
0079 0000:
0080 0000:
0081 0000:
0082 0000:
0083 0000:
0084 0000:
0085 0000:
0086 0000:
0087 0000:
0088 0000:
0089 0000:
0090 0000:
0091 0000:
0092 0000:
0093 0000:
0094 0000:
0095 0000:
0096 0000:
0097 0000:
0098 0000:
0099 0000:
0100 0000:
0101 0000:
0102 0000:
0103 0000:
0104 0000:
0105 0000:
0106 0000:
0107 0000:
0108 0000:
0109 0000:
0110 0000:
0111 0000:
0112 0000:
0113 0000:
0114 0000:
0115 0000:
0116 0000:
0117 0000:
0118 0000:
0119 0000:
0120 0000:
0121 0000:
0122 0000:
0123 0000:
0124 0000:
0125 0000:
0126 0000:
0127 0000:
0128 0000:
0129 0000:
0130 0000:
0131 0000:
0132 0000:
0133 0000:
0134 0000:
0135 0000:
0136 0000:
0137 0000:
0138 0000:
0139 0000:
0140 0000:
0141 0000:
0142 0000:
0143 0000:
0144 0000:
0145 0000:
0146 0000:
0147 0000:
0148 0000:
0149 0000:
0150 0000:
0151 0000:
0152 0000:
0153 0000:
0154 0000:
0155 0000:
0156 0000:
0157 0000:
0158 0000:
0159 0000:
0160 0000:
0161 0000:
0162 0000:
0163 0000:
0164 0000:
0165 0000:
0166 0000:
0167 0000:
0168 0000:
0169 0000:
0170 0000:
0171 0000:
0172 0000:
0173 0000:
0174 0000:
0175 0000:
0176 0000:
0177 0000:
0178 0000:
0179 0000:
0180 0000:
0181 0000:
0182 0000:
0183 0000:
0184 0000:
0185 0000:
0186 0000:
0187 0000:
0188 0000:
0189 0000:
0190 0000:
0191 0000:
0192 0000:
0193 0000:
0194 0000:
0195 0000:
0196 0000:
0197 0000:
0198 0000:
0199 0000:

```

Рис. 2.37 Расшифровка протокола фрейма PS-Poll

## Фрейм RTS

Фрейм RTS — это запрос на резервирование среды: он является частью механизма доступа стандарта 802.11.

- **Продолжительность (duration).** Время, необходимое для того, чтобы станции могли обмениваться фреймами. Оно включает время передачи фрейма RTS, время приема фрейма CTS (включая интервал SIFS), время передачи фрейма данных (включая интервал SIFS) и время приема фрейма ACK (включая интервал SIFS). Измеряется в микросекундах (мкс).
- **Адрес приемника (receiver address, RA).** MAC-адрес предполагаемого получателя фрейма.
- **Адрес передатчика (transmitter address, TA).** MAC-адрес передатчика станции-отправителя фрейма.

На рис. 2.38 показан формат фрейма RTS, а на рис. 2.39 представлена расшифровка протокола фрейма RTS.

Контроль фрейма	Продолжительность	RA	Адрес передатчика	FCS
2 байт	2 байт	6 байт	6 байт	4 байт

Рис. 2.38. Формат фрейма RTS

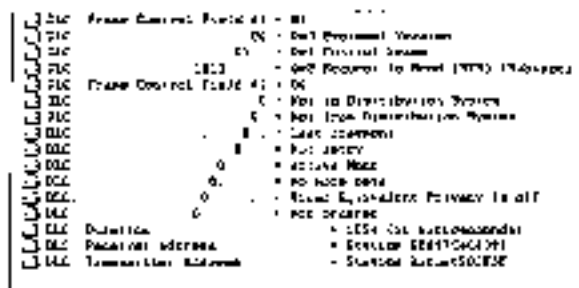


Рис. 2.39. Расшифровка протокола фрейма RTS

## Фрейм CTS

Фрейм CTS — это ответ на фрейм RTS. Это указание приемной станции, что среда была резервирована на указанный период.

- **Продолжительность (duration).** Величина, полученная из поля Duration предыдущего фрейма RTS, уменьшенная на время, необходимое для передачи фрейма CTS, и интервал SIFS.
- **Адрес приемника (receiver address, RA).** MAC-адрес предполагаемого получателя фрейма.

На рис. 2.40 показан формат фрейма RTS, а на рис. 2.41 представлена расшифровка протокола фрейма RTS.



## Фреймы CF-End и CF-End+CF-ACK

Фреймы CF-End и CF-End+CF-ACK предназначены для работы в режиме PCF. Они указывают на окончание периода, свободного от конкуренции, а фрейм CF-End+CF-ACK также включает подтверждение получения точкой координации последнего фрейма. На рис. 2.44 показан формат фреймов CF-End и CF-End+CF-ACK, а ниже описаны их ключевые поля.

Контроль фрейма	Продолжительность	Адрес приемника	BSSID	FCF
2 байт	2 байт	6 байт	6 байт	4 байт

Рис. 2.44. Формат фреймов CF-End и CF-End+CF-ACK

- **Продолжительность (duration).** Установлена равной 0.
- **Адрес приемника (receiver address, RA).** MAC-адрес предполагаемого получателя фрейма. В случае фреймов CF-End это произвольный MAC-адрес, потому что каждая станция зоны обслуживания должна получить это уведомление.
- **BSSID.** MAC-адрес точки доступа.

## Поля и элементы служебного фрейма по стандарту 802.11

Служебные фреймы по стандарту 802.11 имеют поля, выделяющиеся по сравнению ранее с некоторыми фреймами MAC, и используют структуры данных, которые называются *информационные элементы (information elements)* и *фиксированные поля (fixed fields)*.

На рис. 2.45 показан формат информационного элемента. Цель введения IE и фиксированных полей — предоставить гибкие возможности определения для существующих фреймов и обеспечить масштабируемый метод расширения функциональных возможностей служебных фреймов MAC. Служебные фреймы стандарта 802.11 сконструированы с использованием соответствующих полей формата основного фрейма MAC с добавлением подходящих информационных элементов и фиксированных полей (рис. 2.46).

Контроль фрейма	Цели	Информация
1 байт	1 байт	

Рис. 2.45. Формат информационного элемента

Контроль фрейма	Продолжительность	Адрес приемника	Адрес источника	BSSID	Контроль поля	Информационный элемент	Информационный элемент
-----------------	-------------------	-----------------	-----------------	-------	---------------	------------------------	------------------------

Рис. 2.46. Структура служебного фрейма, включающего информационные элементы и фиксированные поля

В табл. 2.5 приведены информационные элементы, определенные в стандарте 802.11



IE	Решение IE	- 1 (состояние IE)
IE	Length	- 4 (длина IE)
IE	Controlled Rate Information Field	- 02
IE		- Set: Set 0, Set 1, Set 2, Set 3, Set 4, Set 5
IE		- 0 (Reserved, not assigned)
IE	Supported Rates Information Field	- 04
IE		- Set: Set 0, Set 1, Set 2, Set 3, Set 4, Set 5
IE		- 0 (Reserved, not assigned)
IE	Controlled Rate Information Field	- 08
IE		- Set: Set 0, Set 1, Set 2, Set 3, Set 4, Set 5
IE		- 0 (Reserved, not assigned)
IE	Controlled Rate Information Field	- 10
IE		- Set: Set 0, Set 1, Set 2, Set 3, Set 4, Set 5
IE		- 0 (Reserved, not assigned)

Рис. 2.50. Расшифровка протокола IE поддерживаемых скоростей передачи

## IE набора параметров скачкообразного переключения частоты

На рис. 2.51 показан формат информационного элемента параметров скачкообразного переключения частоты, а ниже описаны его ключевые поля.

- **Время пребывания (dwell time).** Время сохранения частотой определенного значения, измеряется в тактах (TU).
- **Набор схем скачков (hup set).** Набор схем скачкообразного переключения частоты.
- **Схема скачков (hop pattern).** Индивидуальная схема скачкообразного переключения частоты.
- **Индекс канала (hop index).** Индекс текущего канала из схемы скачкообразного переключения частоты.

## Информационный элемент набора параметров распределительной системы

На рис. 2.52 представлен формат информационного элемента набора параметров распределительной системы. Поле текущего канала указывает канал, используемый беспроводной станцией, применяющей технологию широкополосной модуляции с прямым расширением спектра (direct-sequence).

Элемент ID	Длина	Текущий канал
1 байт	1 байт	1 байт

Рис. 2.52. Формат информационного элемента набора параметров распределительной системы

## Информационный элемент набора параметров CF

На рис. 2.53 представлен формат информационного элемента набора параметров CF, а ниже описаны его ключевые поля.

- **Счетчик CFP (CFP count).** Подсчет DTIM (включая текущий фрейм), оставшихся до начала следующего CFP.
- **Период CFP (CFP period).** Число интервалов DTIM между периодами, свободными от конкуренции (CFP).
- **CFP MaxDuration.** Максимальная продолжительность CFP, измеренная в тактах (TU).

- **CFR Delayed Remaining** Продолжительность (измеряется в TUs), оставшаяся до конца текущего CFR.

Элемент	Длина	Счетчик CFR	Период CFR	Макс. пропуск. CFR (в пакетах)	Состояние пропуск. CFR (в пакетах)
1 байт	1 байт	1 байт	1 байт	2 байт	2 байт

Рис. 2.53. Формат информационного элемента набора параметров CF

## Информационный элемент TTM

На рис. 2.54 показан формат фрейма информационного элемента TTM, а на рис. 2.55 представлена расшифровка протокола информационного элемента TTM. Ниже описаны ключевые поля фрейма информационного элемента TTM.

- **Счетчик DTIM (DTIM count)**. Поле указывает, сколько пакетов с таймингом фреймов (включая текущий фрейм), прежде чем придет следующий DTIM. Значение 0 свидетельствует о том, что текущий фрейм есть DTIM.
- **Период DTIM (DTIM period)**. Количество интервалов DTIM между фреймами DTIM. Значение 1 указывает на то, что все TTM являются DTIM. Значение 0 зарезервировано.
- **Контроль битовой карты (bitmap control)**. Разряд 0 этого поля содержит бит индикатора трафика, связанный с AID 0. Этот бит имеет значение 1 для элементов TTM со значением 0 в поле счетчика DTIM, когда в точке доступа буферизированы один или несколько фреймов, маркированных либо многоадресными фреймами. Оставшиеся 7 бит этого поля формируют смещение битовой карты (bitmap offset).
- **Частичная виртуальная битовая карта (partial virtual bitmap)**. Позиционная индикация состояния буфера фреймов точки доступа. Индикация для AID 0 указывает, что буферизированы фреймы широковещательные или многоадресные фреймы.

Элемент	Длина	Счетчик	Период	Контроль битовой карты	Частичная виртуальная бит.карта
1 байт	1 байт	1 байт	1 байт	1 байт	1 251 байт

Рис. 2.54. Формат фрейма информационного элемента TTM

```

DLC: Element: DTIM
DLC:          Length: 5 (Traffic Indication Map)
DLC:          Length: 5 (offsets)
DLC:          Delivery Traffic Indication Message Count: 5
DLC:          Delivery Traffic Indication Message Period: 10
DLC:          Bitmap control field: 03
DLC:          Traffic Indication Bit
DLC:          CCSD bit: 1 (bitmap offset)
DLC:          Partial Virtual Bitmap: 002

```

Рис. 2.55. Расшифровка протокола информационного элемента TTM

## Информационный элемент набора параметров IBSS

На рис. 2.56 представлен формат информационного элемента набора параметров IBSS. Поле окна ATIM указывает ширину окна ATIM в пакетах (TU).



Элемент ID	Длина	Описание
1 байт	1 байт	2 байт

Рис. 2.56 Формат аутентификации для ланной сети стандарта IEEE 802.11

## Информационный элемент изменяющегося текста

На рис. 2.57 представлен формат информационного элемента изменяющегося текста.

Элемент ID	Длина	Изменяющийся текст
1 байт	1 байт	1-255 байт

Рис. 2.57 Формат аутентификации для элемента изменяющегося текста

Поле изменяющегося текста указывает изменяющийся текст для использования во фреймах аутентификации.

## Элементы фиксированных полей стандарта 802.11

В дополнение к информационным элементам в спецификации стандарта 802.11 определены также десять элементов фиксированных полей для использования в служебных фреймах (табл. 2.6).

Таблица 2.6. Фиксированные поля стандарта 802.11

Элемент типа "фиксированное поле"	Размер (бит)
Номер алгоритма аутентификации	16
Порядковый номер транзакции аутентификации	16
Сигнальный интервал	16
Информационная способность	16
Текущий адрес точки доступа	48
Интервал приема	16
Код причины	16
AID	16
Код состояния	16
Метка времени (timestamp)	64

### Поле номера алгоритма аутентификации

Значение 0 для этого поля указывает на аутентификацию с открытым ключом (open authentication). Значение 1 указывает на аутентификацию с общим секретным ключом (shared-key authentication). Все остальные значения зарезервированы.

### Поле порядкового номера транзакции аутентификации

В этом поле указывается текущий этап многоэтапного процесса аутентификации.

## Поле сигнального интервала

В этом поле указывается число тактов между передачами сигнального фрейма.

## Поле информационной способности

Поле информационной способности включает подполя, каждое из которых для служебных фреймов, для которых определены правила передачи. На рис. 2.58 представлен формат поля информационной способности, а ниже описаны ключевые подполя.

- **ESS**. Точка доступа устанавливает значение этого подполя равным 1, а подполя IBSS — равным 0 для сигнальных фреймов и фреймов ответа на зондирование.
- **IBSS**. Станция из IBSS устанавливает значение этого подполя равным 1 и подполя ESS — равным 0 для сигнальных фреймов и фреймов ответа на зондирование.
- **Подлежит опросу CF (CF-Prtable)**. Это подполе использует точки доступа и беспроводные станции.
- **Ответ на запрос CF-Poll (CF-Poll request)**. Это подполе используют точки доступа и беспроводные станции. В табл. 2.7 и 2.8 описаны возможные значения этих подполей.
- **Конфиденциальность (privacy)**. Значение этого подполя устанавливается равным 1, если для фреймов данных требуется применить WEP-кодирование. Подполе включается в сигнальный фрейм, во фреймы ответов на зондирование, ассоциацию и релассоциацию. Если применять WEP-кодирование не нужно, значение данных подполя устанавливается равным 0.

ESS	IBSS	Отражается во CF	Запрос по информации во CF	Конфиденциальность	Сорезервировано
1 бит	1 бит	1 бит	1 бит	1 бит	11 бит

Рис. 2.58. Формат поля информационной способности

Таблица 2.7. Поле ответа на CF-опрос во фреймах, источником которых является клиентская станция

Подлежит опросу CF	Ответ на запрос CF-Poll	Значение
0	0	Станция не подлежит опросу CF
1	0	Станция подлежит опросу CF и требует, чтобы ее включили в список опроса
0	1	Станция подлежит опросу CF, но не требует, чтобы ее включили в список опроса
1	1	Станция подлежит опросу CF и требует, чтобы ее не включали в список опроса

## Поле текущего адреса точки доступа

Это поле указывает MAC-адрес точки доступа, с которой в текущий момент ассоциирована беспроводная станция.

**Таблица 2.8. Поле ответа на CF-опрос во фреймах, источником которых является точка доступа**

Подверженность опросу CF	Отвечает на запрос CF-Poll	Значение
0	0	Точка доступа не поддерживает FCF и не является точкой координации (PC)
1	0	PC поддерживает только распределение фреймов
0	1	PC поддерживает распределение фреймов и проводит опрос
1	1	Зарезервировано

### Поле интервала прослушивания

Это поле указывает число сигнальных интервалов, через которое энергосберегающая станция активируется для того, чтобы принять сигналы от фрейма.

### Поле кода причины

В этом поле указывается причина для передачи по собственной инициативе фрейма деаутентификации или диссоциации. В табл. 2.9 перечислены коды причин и их значения.

**Таблица 2.9. Коды причин стандарта 802.11**

Код причины	Значение
0	Зарезервирован
1	Причина, не включенная в спецификацию
2	Предшествующая аутентификация уже недействительна
3	Деаутентификация из-за того, что передающая станция покидает (или уже покинула) BSS либо ESS
4	Диссоциирована вследствие неактивности
5	Диссоциирована из-за того, что точка доступа не способна удержать все ассоциированные станции
6	Получен фрейм класса 2 от неаутентифицированной станции
7	Получен фрейм класса 3 от неаутентифицированной станции
8	Диссоциирована из-за того, что передающая станция покидает (или уже покинула) BSS
9	Станция, требующая реассоциации, не аутентифицирована отсоединившей станцией
10-65 535	Зарезервированы

### Поле AID

Данное поле указывает значение, назначенное точкой доступа для представления ID ассоциированного ID для беспроводной станции. Это значение представляет собой логический порт для беспроводной станции.

### Поле кода состояния

Этот поле в служебных фреймах ответа содержит значение, указывающее на успешность или неуспешность регистрации на служебный фрейм запроса. В табл. 2.16 перечислены все коды состояния стандарта 802.11 и их значения.

Таблица 2.10. Коды состояния

Код состояния	Значение
0	Успешно
1	Неудача, не указанная в спецификации
2-9	Зарезервированы
10	Но в состоянии поддерживать все запрошенные в возможности, указанные в поле информационной способности
11	Резассоциация отклонена из-за невозможности подтверждения того, что ассоциация существует
12	Ассоциация отклонена по причине, не оговоренной в данном стандарте
13	Отвечающая станция не поддерживает специальный алгоритм аутентификации
14	Получен аутентификационный фрейм с номером последовательности транзакций аутентификации, не соответствующий ожидаемой последовательности
15	Аутентификация отвергнута из-за невозможности ответить на вызов (challenge failure)
16	Аутентификация отвергнута из-за тайм-аута в ожидании следующего фрейма последовательности
17	Аутентификация отвергнута из-за того, что точка доступа неспособна управлять дополнительными ассоциированными станциями
18	Аутентификация отвергнута из-за того, что запрашивающая станция не поддерживает все скорости передачи данных, указанные в параметре BSSBasicRateSet
19-63 535	Зарезервированы

## Поле метки времени (Timestamp)

Это поле указывает значение TSFTIME.R отправителя фрейма.

## Службные фреймы стандарта 802.11

К числу службных фреймов стандарта 802.11 относятся следующие.

- Сигнальный фрейм.
- Фрейм запроса на зондирование.
- Фрейм ответа на зондирование.
- Фрейм аутентификации.
- Фрейм деаутентификации.
- Фрейм запроса на ассоциирование.
- Фрейм ответа на ассоциирование.
- Фрейм запроса на резассоциирование.
- Фрейм ответа на резассоциирование.
- Фрейм диссоциирования.
- Фрейм индикация объема трафика (announcement traffic indication frame, ATIM).

В следующих разделах каждый из службных фреймов описан более подробно.

## Сигнальный фрейм

Сигнальный (маркерный) фрейм – это служебный фрейм, который точка доступа (или контроллер сигнала в IBSS) передает с частотой, определяемой сигнальным интервалом. Сигнальный фрейм (это в данный книге часто называемый просто “марк” (в сленге)) обеспечивает временную синхронизацию между точкой доступа и беспроводной станцией, а также синхронизацию специфичных для физического канала параметров. Кроме того, энергоэффективности станции способствуют тот, что точка доступа имеет для них буферы инициальных фреймов. В дополнение к определенным в стандарте 802.11 полям и информационным элементам в сигнальных фреймах могут быть также включены специфичные для конкретной реализации информацииные элементы.

На рис. 2.59 показан формат сигнального фрейма, а на рис. 2.60 представлена расшифровка протокола сигнального фрейма.

Сигн. элемент	Положение (байты)	Сигн. элемент	Положение (байты)	Сигн. элемент	Положение (байты)	Сигн. элемент	Положение (байты)	Сигн. элемент	Положение (байты)	Сигн. элемент	Положение (байты)	Сигн. элемент	Положение (байты)
Сигн. элемент	0-1	Сигн. элемент	2-3	Сигн. элемент	4-5	Сигн. элемент	6-7	Сигн. элемент	8-9	Сигн. элемент	10-11	Сигн. элемент	12-13

Рис. 2.59. Формат сигнального фрейма

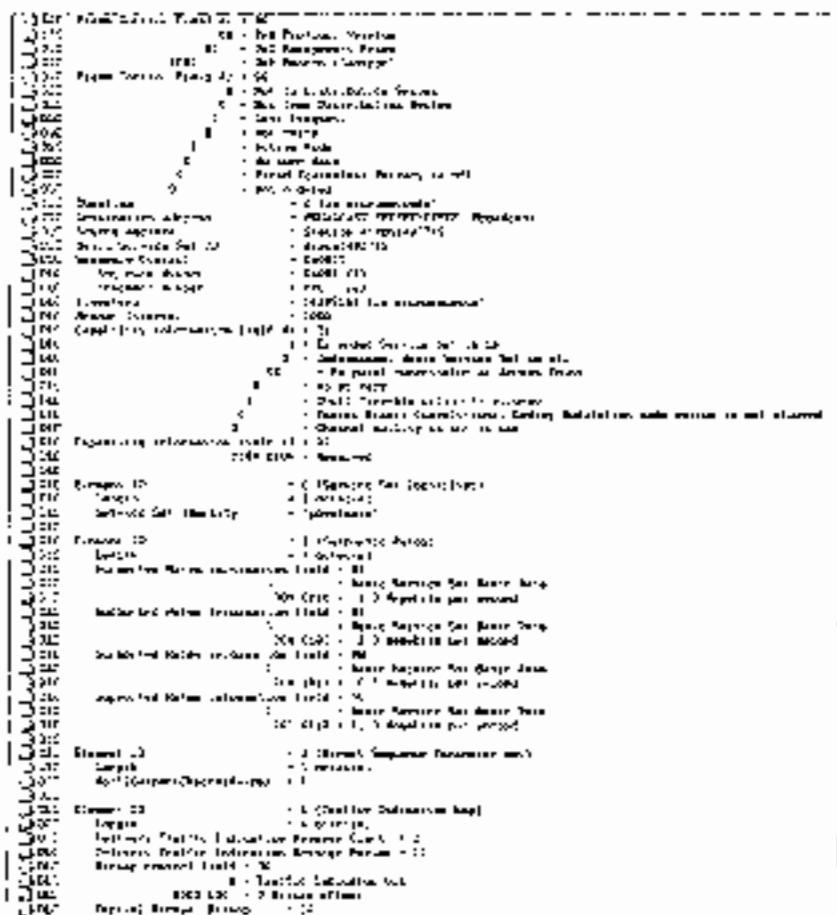


Рис. 2.60. Расшифровка протокола сигнального фрейма

## Фрейм запроса на зондирование

На рис. 2.61 показан формат фрейма запроса на зондирование, а на рис. 2.62 представлена расшифровка протокола фрейма запроса на зондирование.

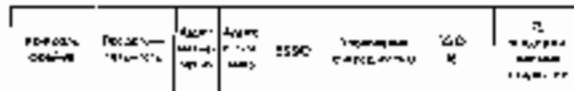


Рис. 2.61. Формат фрейма запроса на зондирование

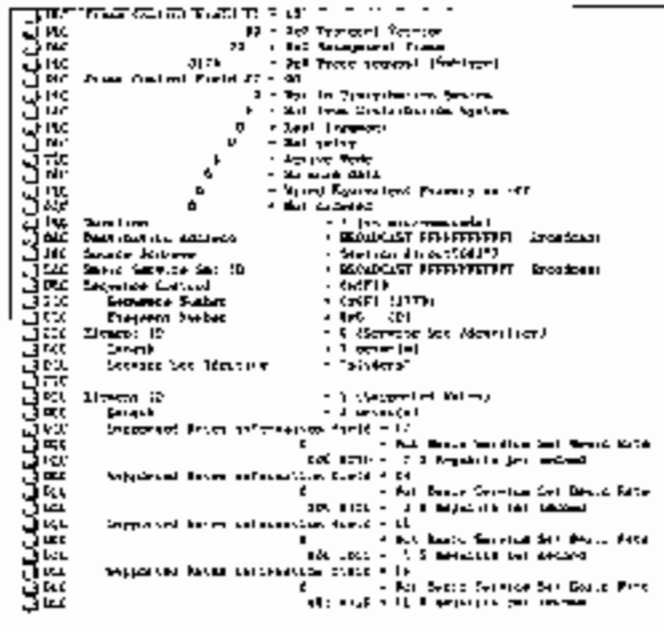


Рис. 2.62. Расшифровка протокола фрейма запроса на зондирование

## Фрейм ответа на зондирование

На рис. 2.63 показан формат фрейма ответа на зондирование, а на рис. 2.64 представлена расшифровка протокола фрейма ответа на зондирование.

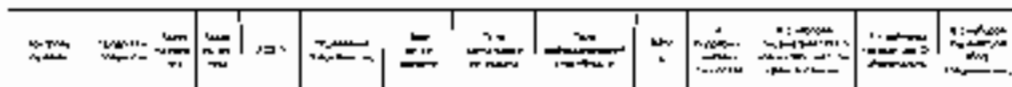


Рис. 2.63. Формат фрейма ответа на зондирование

## Фрейм аутентификации

На рис. 2.65 показан формат фрейма аутентификации, а на рис. 2.66 представлена расшифровка протокола фрейма аутентификации.



## Фрейм деаутентификации

На рис. 2.67 показан формат фрейма деаутентификации, а на рис. 2.68 представлена расшифровка протокола фрейма деаутентификации

Кодовое поле	Протокол	Адрес назначения	Адрес источника	Порт	Идентификатор фрейма	Тип сообщения
--------------	----------	------------------	-----------------	------	----------------------	---------------

Рис. 2.67. Формат фрейма деаутентификации

```

0000  Frame Control Field #1 = 03
0001  03 = 348 Protocol Version
0002  00 = 348 Authentication Frame
0003  1100 = 348 Authentication -Sublayer
0004  Frame Control Field #2 = 35
0005  0 = Not In Distribution System
0006  0 = Not In Distribution System
0007  0 = Data Integrity
0008  0 = Not set
0009  0 = Action Mode
000A  0 = No more data
000B  0 = Frame Delimitation Strategy is off
000C  0 = Not defined
000D  Duration = 212 110 000000000000
000E  Destination Address = Station 000453073F
000F  Source Address = Station 000070AC079
0010  Basic Service Set ID = 00070AC079
0011  Sublayer Control = 0x25 00
0012  Authentication Reason = 0x20 1000
0013  Reason code = 0x 12
0014  Reason code = 1 (Unauthorized access)
    
```

Рис. 2.68. Расшифровка протокола фрейма деаутентификации

## Фрейм запроса на ассоциирование

На рис. 2.69 показан формат фрейма запроса на ассоциирование, а на рис. 2.70 представлена расшифровка протокола фрейма запроса на ассоциирование.

Кодовое поле	Протокол	Адрес назначения	Адрес источника	ESSEL	Идентификатор фрейма	Тип сообщения	Идентификатор ассоциации	SSD	Состояние ассоциации
--------------	----------	------------------	-----------------	-------	----------------------	---------------	--------------------------	-----	----------------------

Рис. 2.69. Формат фрейма запроса на ассоциирование

```

0000  Frame Control Field #1 = 03
0001  03 = 348 Protocol Version
0002  00 = 348 Authentication Frame
0003  1100 = 348 Authentication -Sublayer
0004  Frame Control Field #2 = 35
0005  0 = Not In Distribution System
0006  0 = Not In Distribution System
0007  0 = Data Integrity
0008  0 = Not set
0009  0 = Action Mode
000A  0 = No more data
000B  0 = Frame Delimitation Strategy is off
000C  0 = Not defined
000D  Duration = 212 110 000000000000
000E  Destination Address = Station 000453073F
000F  Source Address = Station 000070AC079
0010  Basic Service Set ID = 00070AC079
0011  Sublayer Control = 0x25 00
0012  Authentication Reason = 0x20 1000
0013  Reason code = 0x 12
0014  Reason code = 1 (Unauthorized access)
    
```

Рис. 2.70. Расшифровка протокола фрейма запроса на ассоциирование





доступа может запросить старую точку доступа, имеет ли она буферизированные для этой станции фреймы с полезным содержанием клиента; подобная возможность может быть реализована производителем, но она не описана в стандарте 802.11.

```

0300 From Control Field 2, = 20
0301 From Control Field 2, = 20
0302 From Control Field 2, = 20
0303 From Control Field 2, = 20
0304 From Control Field 2, = 20
0305 From Control Field 2, = 20
0306 From Control Field 2, = 20
0307 From Control Field 2, = 20
0308 From Control Field 2, = 20
0309 From Control Field 2, = 20
0310 From Control Field 2, = 20
0311 From Control Field 2, = 20
0312 From Control Field 2, = 20
0313 From Control Field 2, = 20
0314 From Control Field 2, = 20
0315 From Control Field 2, = 20
0316 From Control Field 2, = 20
0317 From Control Field 2, = 20
0318 From Control Field 2, = 20
0319 From Control Field 2, = 20
0320 From Control Field 2, = 20
0321 From Control Field 2, = 20
0322 From Control Field 2, = 20
0323 From Control Field 2, = 20
0324 From Control Field 2, = 20
0325 From Control Field 2, = 20
0326 From Control Field 2, = 20
0327 From Control Field 2, = 20
0328 From Control Field 2, = 20
0329 From Control Field 2, = 20
0330 From Control Field 2, = 20
0331 From Control Field 2, = 20
0332 From Control Field 2, = 20
0333 From Control Field 2, = 20
0334 From Control Field 2, = 20
0335 From Control Field 2, = 20
0336 From Control Field 2, = 20
0337 From Control Field 2, = 20
0338 From Control Field 2, = 20
0339 From Control Field 2, = 20
0340 From Control Field 2, = 20
0341 From Control Field 2, = 20
0342 From Control Field 2, = 20
0343 From Control Field 2, = 20
0344 From Control Field 2, = 20
0345 From Control Field 2, = 20
0346 From Control Field 2, = 20
0347 From Control Field 2, = 20
0348 From Control Field 2, = 20
0349 From Control Field 2, = 20
0350 From Control Field 2, = 20
0351 From Control Field 2, = 20
0352 From Control Field 2, = 20
0353 From Control Field 2, = 20
0354 From Control Field 2, = 20
0355 From Control Field 2, = 20
0356 From Control Field 2, = 20
0357 From Control Field 2, = 20
0358 From Control Field 2, = 20
0359 From Control Field 2, = 20
0360 From Control Field 2, = 20
0361 From Control Field 2, = 20
0362 From Control Field 2, = 20
0363 From Control Field 2, = 20
0364 From Control Field 2, = 20
0365 From Control Field 2, = 20
0366 From Control Field 2, = 20
0367 From Control Field 2, = 20
0368 From Control Field 2, = 20
0369 From Control Field 2, = 20
0370 From Control Field 2, = 20
0371 From Control Field 2, = 20
0372 From Control Field 2, = 20
0373 From Control Field 2, = 20
0374 From Control Field 2, = 20
0375 From Control Field 2, = 20
0376 From Control Field 2, = 20
0377 From Control Field 2, = 20
0378 From Control Field 2, = 20
0379 From Control Field 2, = 20
0380 From Control Field 2, = 20
0381 From Control Field 2, = 20
0382 From Control Field 2, = 20
0383 From Control Field 2, = 20
0384 From Control Field 2, = 20
0385 From Control Field 2, = 20
0386 From Control Field 2, = 20
0387 From Control Field 2, = 20
0388 From Control Field 2, = 20
0389 From Control Field 2, = 20
0390 From Control Field 2, = 20
0391 From Control Field 2, = 20
0392 From Control Field 2, = 20
0393 From Control Field 2, = 20
0394 From Control Field 2, = 20
0395 From Control Field 2, = 20
0396 From Control Field 2, = 20
0397 From Control Field 2, = 20
0398 From Control Field 2, = 20
0399 From Control Field 2, = 20

```

Рис. 2.74. Расшифровка протокола фрейма запроса на реассоциирование

### Фрейм ответа на реассоциирование

На рис. 2.75 показан формат фрейма ответа на реассоциирование, а на рис. 2.76 представлены расшифровка протокола фрейма ответа на реассоциирование

Фрейм ответа на реассоциирование идентичен фрейму ответа на ассоциирование.

Поле	Позиция	Размер	Тип	Содержимое	Значение	Имя	Содержимое
Frame Control	0-3	4	2	0000	0000	0000	0000
Duration	4-7	4	2	0000	0000	0000	0000
Address 1	8-11	4	2	0000	0000	0000	0000
Address 2	12-15	4	2	0000	0000	0000	0000
Address 3	16-19	4	2	0000	0000	0000	0000
Address 4	20-23	4	2	0000	0000	0000	0000
Address 5	24-27	4	2	0000	0000	0000	0000
Sequence Control	28-31	4	2	0000	0000	0000	0000
Variable Length Information	32-255	224	1	0000	0000	0000	0000

Рис. 2.75. Формат фрейма ответа на реассоциирование

### Фрейм диссоциирования

На рис. 2.77 показан формат фрейма диссоциирования, а на рис. 2.78 представлена расшифровка протокола фрейма диссоциирования.

### Фрейм АТІМ

Фрейм АТІМ не имеет фиксированных полей или информационных элементов.

006	Frame Control Field (FC) = 02
007	00 = 02 Protocol Version
008	02 = 02 Broadcast Frame
009	00 = 02 Broadcast (0000000000000000)
010	00 = 02 Broadcast (0000000000000000)
011	00 = 02 Broadcast (0000000000000000)
012	00 = 02 Broadcast (0000000000000000)
013	00 = 02 Broadcast (0000000000000000)
014	00 = 02 Broadcast (0000000000000000)
015	00 = 02 Broadcast (0000000000000000)
016	00 = 02 Broadcast (0000000000000000)
017	00 = 02 Broadcast (0000000000000000)
018	00 = 02 Broadcast (0000000000000000)
019	00 = 02 Broadcast (0000000000000000)
020	00 = 02 Broadcast (0000000000000000)
021	00 = 02 Broadcast (0000000000000000)
022	00 = 02 Broadcast (0000000000000000)
023	00 = 02 Broadcast (0000000000000000)
024	00 = 02 Broadcast (0000000000000000)
025	00 = 02 Broadcast (0000000000000000)
026	00 = 02 Broadcast (0000000000000000)
027	00 = 02 Broadcast (0000000000000000)
028	00 = 02 Broadcast (0000000000000000)
029	00 = 02 Broadcast (0000000000000000)
030	00 = 02 Broadcast (0000000000000000)
031	00 = 02 Broadcast (0000000000000000)
032	00 = 02 Broadcast (0000000000000000)
033	00 = 02 Broadcast (0000000000000000)
034	00 = 02 Broadcast (0000000000000000)
035	00 = 02 Broadcast (0000000000000000)
036	00 = 02 Broadcast (0000000000000000)
037	00 = 02 Broadcast (0000000000000000)
038	00 = 02 Broadcast (0000000000000000)
039	00 = 02 Broadcast (0000000000000000)
040	00 = 02 Broadcast (0000000000000000)
041	00 = 02 Broadcast (0000000000000000)
042	00 = 02 Broadcast (0000000000000000)
043	00 = 02 Broadcast (0000000000000000)
044	00 = 02 Broadcast (0000000000000000)
045	00 = 02 Broadcast (0000000000000000)
046	00 = 02 Broadcast (0000000000000000)
047	00 = 02 Broadcast (0000000000000000)
048	00 = 02 Broadcast (0000000000000000)
049	00 = 02 Broadcast (0000000000000000)
050	00 = 02 Broadcast (0000000000000000)
051	00 = 02 Broadcast (0000000000000000)
052	00 = 02 Broadcast (0000000000000000)
053	00 = 02 Broadcast (0000000000000000)
054	00 = 02 Broadcast (0000000000000000)
055	00 = 02 Broadcast (0000000000000000)
056	00 = 02 Broadcast (0000000000000000)
057	00 = 02 Broadcast (0000000000000000)
058	00 = 02 Broadcast (0000000000000000)
059	00 = 02 Broadcast (0000000000000000)
060	00 = 02 Broadcast (0000000000000000)
061	00 = 02 Broadcast (0000000000000000)
062	00 = 02 Broadcast (0000000000000000)
063	00 = 02 Broadcast (0000000000000000)
064	00 = 02 Broadcast (0000000000000000)
065	00 = 02 Broadcast (0000000000000000)
066	00 = 02 Broadcast (0000000000000000)
067	00 = 02 Broadcast (0000000000000000)
068	00 = 02 Broadcast (0000000000000000)
069	00 = 02 Broadcast (0000000000000000)
070	00 = 02 Broadcast (0000000000000000)
071	00 = 02 Broadcast (0000000000000000)
072	00 = 02 Broadcast (0000000000000000)
073	00 = 02 Broadcast (0000000000000000)
074	00 = 02 Broadcast (0000000000000000)
075	00 = 02 Broadcast (0000000000000000)
076	00 = 02 Broadcast (0000000000000000)
077	00 = 02 Broadcast (0000000000000000)
078	00 = 02 Broadcast (0000000000000000)
079	00 = 02 Broadcast (0000000000000000)
080	00 = 02 Broadcast (0000000000000000)
081	00 = 02 Broadcast (0000000000000000)
082	00 = 02 Broadcast (0000000000000000)
083	00 = 02 Broadcast (0000000000000000)
084	00 = 02 Broadcast (0000000000000000)
085	00 = 02 Broadcast (0000000000000000)
086	00 = 02 Broadcast (0000000000000000)
087	00 = 02 Broadcast (0000000000000000)
088	00 = 02 Broadcast (0000000000000000)
089	00 = 02 Broadcast (0000000000000000)
090	00 = 02 Broadcast (0000000000000000)
091	00 = 02 Broadcast (0000000000000000)
092	00 = 02 Broadcast (0000000000000000)
093	00 = 02 Broadcast (0000000000000000)
094	00 = 02 Broadcast (0000000000000000)
095	00 = 02 Broadcast (0000000000000000)
096	00 = 02 Broadcast (0000000000000000)
097	00 = 02 Broadcast (0000000000000000)
098	00 = 02 Broadcast (0000000000000000)
099	00 = 02 Broadcast (0000000000000000)
100	00 = 02 Broadcast (0000000000000000)

Рис. 2.76 Расшифровка протокола фрейма пакета на диссоциацию

Control	Frame	Sequence	Length	Control	Frame	Sequence	Length	Control	Frame	Sequence	Length
00	00	00	00	00	00	00	00	00	00	00	00

Рис. 2.77 Формат фрейма диссоциации

### Фреймы данных стандарта 802.11

В стандарте 802.802.11 описаны восемь уникальных фреймов данных:

- Данные.
- Нулевые данные.
- Данные+CF-Ack.
- Данные+CF-Poll.
- Данные-CF-Ack+CF-Poll.
- CF-Ack
- CF-Poll
- CF-Ack+CF-Poll

### Фрейм данных

На рис. 2.79 показан формат фрейма данных, а на рис. 2.80 представлена расшифровка протокола фрейма данных.

002	Frame Control Field #1 = 00	
003	00	CS Protocol Version
004	18	CS Data Frame
005	0000	CS Data Directory
006	Frame Control Field #2 = 00	
007	00	To Distribution System
008	00	Seq from Distribution System
009	00	Seq to transmit
010	00	Seq sent
011	00	Seq from Peer
012	00	Seq from Data
013	00	Seq to transmit (Priority is off)
014	00	Seq received
015	Description	• 000 (in microseconds)
016	Destination Address	• Station Address 2327F
017	Source Address	• Station 00020034531
018	Length of Frame Set ID	• 0010001001
019	Sequence Control	• 80200
020	Sequence Number	• 80200 (40)
021	Fragment Number	• 800 (0)
022	Access code	• (Reserved) (not present)
023		

Рис. 2.78. Расшифровка протокола фрейма беспроводной

Символ фрейма	Продолжительность	Адрес отправителя	SSSID	Адрес получателя	Уровень доступа к сети	Идентификатор	CS
2000h	2600h	6600h	0500h	E600h	2600h	00120001	4000h

Рис. 2.79. Формат фрейма данных

002	Frame Control Field #1 = 00	
003	00	CS Protocol Version
004	18	CS Data Frame
005	0000	CS Data Directory
006	Frame Control Field #2 = 00	
007	00	To Distribution System
008	00	Seq from Distribution System
009	00	Seq to transmit
010	00	Seq sent
011	00	Seq from Peer
012	00	Seq from Data
013	00	Seq to transmit (Priority is off)
014	00	Seq received
015	Description	• 000 (in microseconds)
016	Destination Seq ID	• Station Address 23266
017	Source Address	• Station 00020034531
018	Destination Seq Address	• Station Seq 80000
019	Sequence Control	• 80200
020	Sequence Number	• 80200 (40)
021	Fragment Number	• 800 (0)
022		
023	• CS Data Frame ID	
024	• Channel Seq-8000 (CS)	
025	• 00000000000000000000000000000000	
026	• 0000	
027	Frame address: 13 bytes	

Рис. 2.80. Расшифровка протокола фрейма данных

### Фреймы Данные+CF-Ask, Данные+CF-Poll и Данные+CF-Ask+CF-Poll

Эти фреймы данных имеют такое же поле фрейма, как и стандартный фрейм данных. Значения параметров отличаются в обеспечении реализации функциональных возможностей CF-Ask и (или) CF-Poll, необходимых при работе в режиме PCF.

### Нулевые данные

На рис. 2.81 показан формат фрейма нулевых данных, а на рис. 2.80 представлена расшифровка протокола фрейма нулевых данных.

Фрейм нулевых данных равен так потому, что он не имеет "новой полезной нагрузки". Его задача — указать на изменение бита режима энергоэкономии в контрольном поле фрейма.

Контроль фрейма	№. данных фрейма/симв.	Адрес адреса/симв.	ИДПО	Коды адресации	Срок жизни фрейма/симв.	FCF
7 байт	1 байт	6 байт	2 байт	6 байт	3 байт	1 байт

Рис. 2.31 Формат фрейма пустых данных

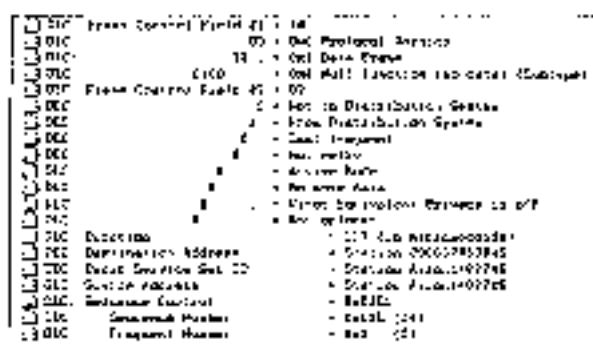


Рис. 2.32 Реализованная структура фрейма пустых данных

## Фреймы CF-Ack, CF-Poll и CF-Ack + CF-Poll

Эти фреймы имеют такое же тело, как и стандартный фрейм пустых данных. Значение поля типа различно в зависимости от реализации функциональных возможностей CF-Ack и/или CF-Poll, необходимых при работе в режиме PCF.

## Резюме

Как следует из данной главы, уровень MAC стандарта 802.11 более сложен, чем уровень MAC стандарта 802.3. Безусловно, среди областей ниже проблемы по части доступа к ней, в результате вам необходимо более надежно работать на уровне MAC. Прочитав эту главу, вы должны иметь четкое представление об основных операциях, выполняемых на уровне MAC. После изучения материала последующих глав вы получите представление о более сложных проблемах, решаемых на уровне MAC стандарта 802.11, таких как безопасность уровня MAC, качество и класс предоставляемых услуг передачи данных или распределение приоритетов доступа к каналу, мобильность. Эти темы подробно рассматриваются в последующих главах и дополняют информацию, содержащуюся в данной главе.



## Технологии физического уровня стандарта 802.11

Благодаря утверждению в 1999 году стандартов 802.11a и 802.11b технология беспроводных локальных сетей (WLAN) перешла из числа решений для сканеров штрих-кодов в универсальное решение для доступа к мобильным, беспроводным, взаимодействующим между собой сетям. На сегодняшний день многие поставщики предлагают станции-клиенты стандартов 802.11a и 802.11b и точки доступа с характеристиками, сравнимыми с таковыми проводной Ethernet. Отсутствие необходимости подключения к проводной сети обеспечивает пользователям свободу передвижения, характерную для мобильных устройств. Хотя изначально был выбран стандарт IEEE, использование частот, на правах лицензирования которыми не нужно получать стоящую денег и требующую времени на оформление лицензию, также способствовало быстрому и широкому распространению данной технологии.

Набор стандартов 802.11 на самом деле определяет целый ряд технологий реализации физического уровня (PHY), которые могут быть использованы на уровне стандарта 802.11 MAC. В этой главе рассматривается каждая из уровней PHY, перечисленных ниже.

- Уровень PHY стандарта 802.11 со скачкообразной перестройкой частоты (frequency hopping) в диапазоне 2,4 ГГц
- Уровень PHY стандарта 802.11 с расширением спектра методом прямой последовательности (direct sequence) в диапазоне 2,4 ГГц
- Уровень PHY стандарта 802.11b с расширением спектра методом прямой последовательности в диапазоне 2,4 ГГц
- Уровень PHY стандарта 802.11a с разделением на ортогональных частотах (orthogonal frequency division multiplexing, OFDM) в диапазоне 5 ГГц
- Расширенный физический уровень (extended rate physical (ERP) layer) стандарта 802.11d в диапазоне 2,4 ГГц

Ethernet стандарта 802.3 эволюционировал долгие годы, прежде чем в него вошел Fast Ethernet стандарта 802.3z и Gigabit Ethernet стандартов 802.3z/802.3ab. Аналогичным образом эволюционировал беспроводной Ethernet стандарта 802.11, и теперь в него входит стандарт 802.11n на высокоскоростную передачу с расширением спектра методом прямой последовательности (high-rate direct sequence spread spectrum, HR-DSSS), стандарт 802.11g OFDM и недавнее дополнение, стандарт 802.11i (ERP). Главным отличительным признаком названных стандартов как раз и является физический уровень.

# Концепции беспроводных физических уровней

Основное назначение физических уровней стандарта 802.11 — обеспечить механизмы беспроводной передачи для подуровня MAC, а также поддерживать выполнение вторичных функций, таких как оценка состояния беспроводной среды и сообщение о нем подуровню MAC. Поскольку эти механизмы передачи независимы от подуровня MAC, стандарт 802.11 усовершенствовал как подуровень MAC, так и подуровень PHY, а также поддерживаемый последним интерфейс. Именно независимость между MAC и подуровнем PHY и позволяет использовать дополнительные высокоскоростные физические уровни, описанные в стандартах 802.11b, 802.11a и 802.11g.

Каждый из физических уровней стандарта 802.11 имеет два подуровня.

- Physical Layer Convergence Procedure (PLCP). Процедура определения состояния физического уровня.
- Physical Medium Dependent (PMD). Подуровень физического уровня, зависящий от среды передачи.

На рис. 3.1 показано, как эти подуровни соотносятся между собой и с вышестоящими уровнями.

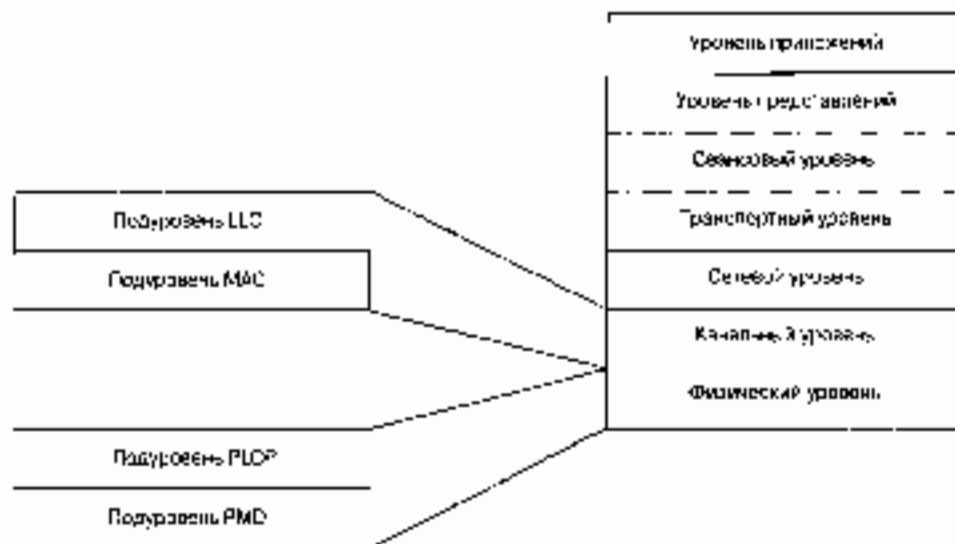


Рис. 3.1 Подуровни уровня PHY модели взаимодействия открытых систем (Open System Interconnection, OSI)

Подуровень PLCP по существу является уровнем обеспечения взаимодействия (handshaking layer), на котором осуществляется перемещение элементов данных протокола MAC (MAC protocol data units, MPDU) между MAC-станциями с использованием подуровня PMD, на котором реализуется тот или иной метод передачи в прямо или через беспроводную среду. До известной степени можно считать, что PMD выполняет функцию службы беспроводной передачи; взаимодействие этих служб осуществляется посредством PLCP. Подуровни PLCP и PMD описаны для разных вариантов стандарта 802.11.



Все подуровни PLCP, независимо от типа уровня PHY стандарта 802.11, используют базисные элементы данных, или примитивы данных (data primitives), обеспечивающие интерфейс для передачи октетов данных между уровнями MAC и PMD. Кроме того, они предоставляют примитивы, которые позволяют подуровню MAC сообщать уровню PHY, когда начинается передача, а уровню PHY информировать подуровень MAC об окончании передачи. На приемной стороне примитивы PLCP, передаваемые уровнем PHY на подуровень MAC, указывают, когда он начинает прием информации от другой станции и когда эта передача завершается. В обеспечение поддержки функции оценки занятости канала (clear channel assessment (CCA) function) все PLCP обеспечивают для подуровня MAC механизм, посредством которого он может возвратиться в исходное состояние CCA-модулю (CCA engine), а для уровня PHY – возможность сообщать о текущем состоянии беспроводной среды.

Вообще говоря, подуровни PLCP работают в соответствии с диаграммой состояний, показанной на рис. 3.2. Их основное рабочее состояние связано с выполнением процедуры обнаружения несущей/оценки занятости канала (sense/clear channel assessment, CS/CCA). Эта процедура обнаруживает начало передачи сигнала от другой станции и выключает, освобождая канал для передачи. Получив запрос на начало передачи (Tx Start), она переходит в состояние "передача" (transmit) путем переключения PMD из режима "прием" в режим "передача" и посылает элемент данных протокола PLCP (PLCP data unit, PPDU). Затем генерируется сигнал "конец передачи" (Tx End) и процедура возвращается в состояние CS/CCA. Подуровень PLCP активизирует состояние "прием" (receive), когда процедура CS/CCA обнаруживает начальную часть PLCP и убеждается в правильности заголовка PLCP. Если подуровень PLCP обнаруживает ошибку, он сообщает об этом подуровню MAC и выполняет процедуру CS/CCA. Различные механизмы CCA рассматриваются далее в этой главе.

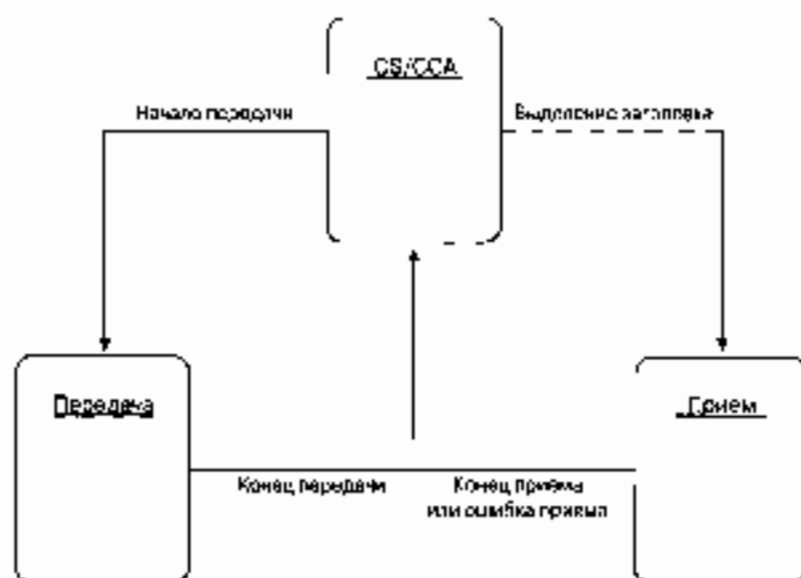


Рис. 3.2 Диаграмма состояний PLCP

## Составляющие физического уровня

Чтобы разобраться в различных подуровнях РМД, которые обеспечивает каждый уровень РНУ стандарта 802.11, нужно вначале рассмотреть следующие основные концепции и «триггерные блоки» РНУ:

- Скремблирование (scrambling)
- Кодирование (coding)
- Чередуание (interleaving)
- Преобразование символов и модуляция (symbol mapping and modulation).

### Скремблирование

Одна из особенностей, лежащих в основе современных передатчиков, благодаря которой данные можно передавать с высокой скоростью, — это предположение о том, что данные, которые предлагаются для передачи, поступают, с точки зрения передатчика, случайным образом. Без этого предположения многие преимущества, получаемые за счет применения остальных составляющих физического уровня, остались бы реализованными. Однако вполне вероятно и часто происходит на практике, что принимаемые данные не вполне случайны и на самом деле могут содержать повторяющиеся наборы и длинные последовательности нулей и единиц. Скремблирование (перестановка элементов) — это метод, посредством которого принимаемые данные делаются более похожими на случайные: достигается это путем перестановки битов последовательности таким образом, чтобы превратить ее из структурированной в похожую на случайную. Эту процедуру иногда называют *шумлением* (whitening) потока данных. Дескремблер (descrambler) приемника затем выполняет обратное преобразование этой случайной последовательности с целью выявления исходной структурированной последовательности. Большинство из способов скремблирования относится к числу синхронизирующихся: это означает, что дескремблер способен самостоятельно синхронизироваться со скремблером.

### Кодирование

Скремблирование — важный инструмент, позволяющий инженерам разрабатывать системы связи с высокой эффективностью использования спектра (spectral efficiency). *Кодирование* — это механизм, позволяющий осуществлять высокоскоростную передачу данных по шумленным каналам. Все каналы передачи подвержены помехам, из-за чего возникают ошибки в виде искаженных или модифицированных битов. Кодирование позволяет максимизировать объем данных, которые можно передать через шумленную среду передачи. Это можно сделать путем замены последовательностей битов более длинными последовательностями, которые позволят распознать и исправить искаженные биты. Например, если вы хотите передать другу по телефону последовательность 01101 (рис. 3.3), можно вместо этого, по предварительной договоренности с другом, повторить каждый бит трижды и передать последовательность 000111111000111. Если даже наш друг получит некоторые биты с ошибками например, примет последовательность 10011111000101, он все равно сможет восстановить исходную последовательность по схеме «большинство голосов». Хотя подобный кодер слишком груст и неэффективен, благодаря ему нам удалось изложить концепцию, лежащую в основе кодирования.



Рис. 3.3. Простой пример кодирования

Наиболее часто в современных системах связи применяется тип кодирования, реализуемый сверточным кодирующим устройством (convolutional coder), потому что такое кодирование может быть довольно просто реализовано аппаратно с использованием линии задержки (delay) и сумматора. В отличие от рассмотренного выше кода, который относится к блочным кодам без памяти, сверточный код относится к кодам с конечной памятью (finite memory code), это означает, что выходная последовательность кодера является функцией не только текущего входного сигнала, но также нескольких из числа последних предыдущих битов. Длина кодовой памяти (constraint length of a code) показывает, как много выходных элементов выводится из системы в пересчете на один входной бит. Коды часто характеризуются их эффективной скоростью (или коэффициентом кодирования  $1/2$ ). Этот коэффициент указывает, что на каждый входной бит приходится два выходных. При сравнении кодов обобщают внимание на то, что, хотя коды с более высокой эффективностью кодирования позволяют передавать данные с более высокой скоростью, они соответственно более чувствительны к шуму.

## Чередование

Одно из основных предположений, на которых основан механизм кодирования, состоит в том, что ошибки, возникающие при передаче информации, являются независимыми событиями. Это предположение справедливо для рассмотренного ранее случая передачи последовательности битов по телефону, когда были искажены биты 1 и 9. Однако зачастую вы можете обнаружить, что ошибки в передаче двоичных разрядов не независимы и происходят сериями. Например, предположим, что в следующем примере во время передачи первой части нашей фразы с другим код его окном приехал самовозвал, оказывая воздействие на его слух наряду с вашими сигналами. Последовательность, которую принял ваш друг, может в результате оказаться такой 011001111001111 (рис. 3.4). Он ошибочно может заключить, что исходной последовательностью была 10101.

По этим причинам стали использовать *чередование* для разброса битов блочных кодов, которые могли бы возникнуть, таким образом делая ошибки более похожими на независимые. Чередование может быть выполнено на аппаратном или программном уровне; независимо от этого, основываясь на идее — разбросать соседние биты путем размещения между ними битов несоседних. Возвращаясь к нашему примеру, предположим, что вместо простого зачитывания 16-разрядной последовательности своему другу вы могли бы вводить по пять бит в строки матрицы и затем считывать их уже как столбцы по три

бита в каждом (рис. 3.5). Ваш друг должен был затем записать их в матрицу столбцами по три бита, прочитать их затем в виде строк по 5 бит в каждой и применить кодирующее правило для получения исходной последовательности.



Рис. 3.4. Кодирующее правило скремблирует биты



Рис. 3.5. Кодирующее правило скремблирует биты

## Преобразование символов и модуляция

Процесс модуляции может быть осуществлен потоком битов по отношению к носителю в радиочастотной области. Если носитель является прямой синусоидальной волной, прекодированная может быть ее амплитуда, частота или фаза. На рис. 3.6 представлены примеры применения каждого из трех методов.

### На заметку

Идея модуляции битами данных амплитуды или частоты носителя имеет параллель в мире радиовещания в диапазонах AM и FM. Вместо того чтобы модулировать синусоиду битами данных, можно наложить сигналы музыки или речи на амплитуду или частоту синусоиды, осуществив тем самым амплитудную (AM) или частотную (FM) модуляцию. Концепция та же самая, единственное отличие состоит в формате передаваемой информации.

Иногда вместо одной синусоиды используют две, сдвинутые по фазе на 90 градусов. Эти две синусоиды называются *синфазная* (in-phase) и *квadrатурная* (quadrature) компоненты.

Хотя можно непосредственно модулировать один из параметров носителя, амплитуду, частоту или фазу, передать больше битов информации в той же полосе частот позволяет

способ, при использовании которого в символы преобразуются группы битов. *Преобразование символов (symbol mapping)* — это процесс, в ходе которого биты группируются и преобразуются в синфазные или квадратурные компоненты. Это часто представляется в декартовой системе координат таким образом: синфазные компоненты откладываются по оси  $x$ , квадратурные — по оси  $y$ , в результате получается *символьное пространство (constellation)*. Иногда это также представляют в виде комплексной плоскости с мнимой единицей,  $j$ , которая равносильно квадратурному из единицы, на квадратурной оси, или оси ординат, и действительной компонентой, откладываемой по синфазной оси, или оси  $x$ .

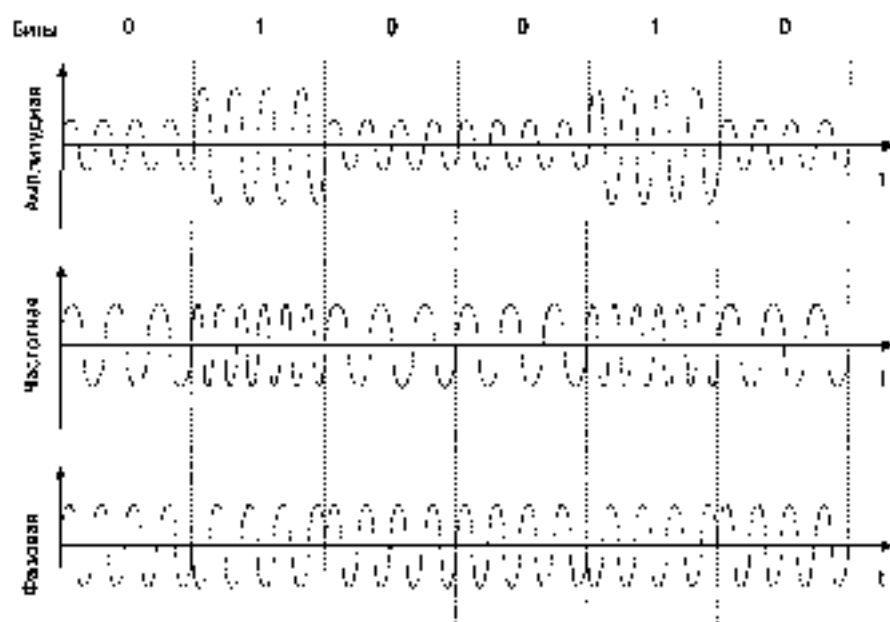


Рис. 3.6. Примеры модуляции

Если информация поступает со скоростью 11 Мбит/с, но для преобразования одного символа необходимы два бита, результирующая скорость передачи символов, или скорость двоичной передачи в бодах, составляет 5,5 Мбод<sup>1</sup>. Для выходной последовательности, полученной в результате чередования (см. рис. 3.5), можно использовать фазовую манипуляцию с квадратурными (фазовыми) сигналами (quadrature phase-shift keying, QPSK), преобразующую в символы сразу два бита. Карта преобразования символов представлена на рис. 3.7, где показаны входные биты и формы выходных сигналов. Синфазные сигналы обозначены возле каждой точки создателя сплошной линией, квадратурные — пунктирной. Этот процесс приводит к вынесению в комплексной временной области модулирующего сигнала, который затем сдвигается в частотную область с целью получения реального сигнала в заданной полосе пропускания.

<sup>1</sup> В ординате — 5,5 Мбит/с — Прим. ред.

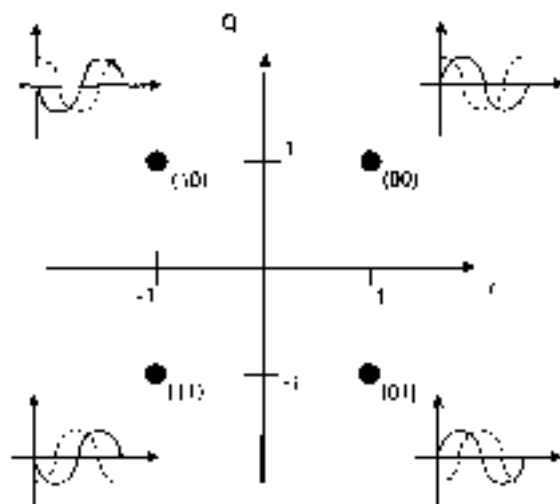


Рис. 3.7. Символы QPSK и соответствующие сигналы и коэффициенты модуля

## Беспроводные локальные сети стандарта 802.11

Исходный стандарт 802.11 определяет два метода передачи на физическом уровне.

- Технология расширения спектра путем скачкообразной перестройки частоты (FHSS) в диапазоне 2,4 ГГц.
- Технология широкополосной модуляции с расширением спектра методом прямой последовательности (DSSS) в диапазоне 2,4 ГГц.

Как уже говорилось, обе эти технологии работают в диапазоне 2,4 ГГц, в котором Федеральная комиссия связи США (FCC) выделена полоса шириной 82 МГц: для промышленного, научного и медицинского применения (ISM). Эта и другие полосы частот рассматриваются в главе 8, "Развертывание беспроводных LAN". Каждый физический уровень имеет свои собственные подуровни PLCP и PMD, о которых мы будем говорить в следующих разделах.

### Локальные беспроводные локальные сети со скачкообразной перестройкой частоты (FHSS)

Беспроводные локальные сети FHSS поддерживают скорости передачи 1 и 2 Мбит/с. Как следует из названия, устройства FHSS осуществляют скачкообразную перестройку частоты по определенной схеме, как показано на рис. 3.8. Устройства FHSS имеют предназначенную для их работы полосу частот от 2,402 до 2,480 ГГц на 79 неперекрывающихся каналов (это справедливо для Северной Америки и большей части Европы). Ширина каждого из 79 каналов составляет 1 МГц, поэтому беспроводные локальные сети FHSS используют относительно высокую скорость передачи символов, 1 МГц, и намного меньшую скорость перестройки с канала на канал.

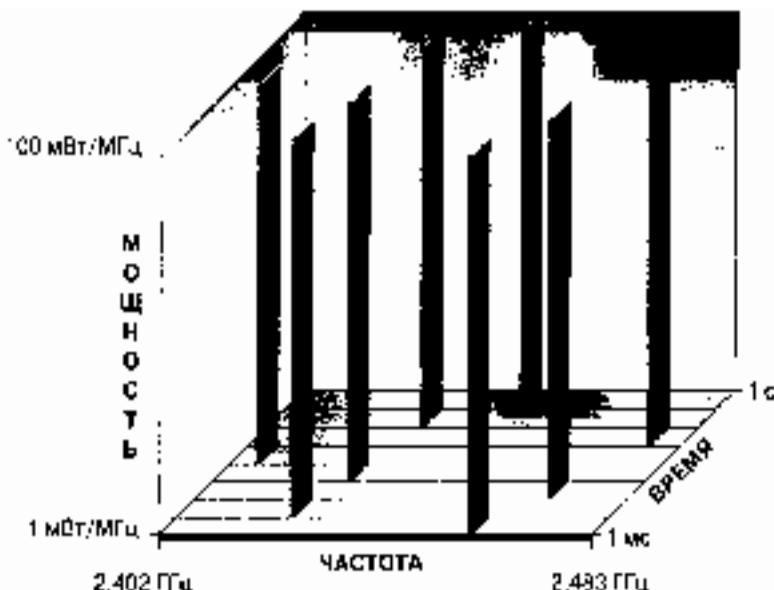


Рис. 3.8. Пример скачкообразной перестройки частоты

Последовательность перестройки частоты должна иметь следующие параметры: частота переключения не менее 2,5 раз в секунду как минимум между 6-ю (6 МГц) каналами. Чтобы минимизировать число коллизии между перекрывающимися зонами покрытия, возможные последовательности переключений должны быть разбиты на три набора последовательностей, длина которых для Северной Америки и большей части Европы составляет 26. В табл. 3.1–3.4 представлены схемы скачкообразной перестройки частоты, обеспечивающие минимальное перекрестие для различных стран, включая Японию, Испанию и Францию.

Таблица 3.1. Схема FHSS для Северной Америки и Европы

Набор	Схема скачкообразной перестройки частоты
1	{0,3,6,9,12,15,18,21,24,27,30,33,36,39,42,45,48,51,54,57,60,63,66,69,72,75}
2	{1,4,7,10,13,16,19,22,25,28,31,34,37,40,43,46,49,52,55,58,61,64,67,70,73,76}
3	{2,5,8,11,14,17,20,23,26,29,32,35,38,41,44,47,50,53,56,59,62,65,68,71,72,77}

Таблица 3.2. Схема FHSS для Японии

Набор	Схема скачкообразной перестройки частоты
1	{6,9,12,15}
2	{7,10,13,16}
3	{8,11,14,17}

Таблица 3.2. Схема FHSS для Испании

Набор	Схема скачкообразной перестройки частоты
1	{0, 3, 6, 9, 12, 15, 18, 21, 24}
2	{1, 4, 7, 10, 13, 16, 19, 22, 25}
3	{2, 5, 8, 11, 14, 17, 20, 23, 26}

Таблица 3.2. Схема FHSS для Франции

Набор	Схема скачкообразной перестройки частоты
1	{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30}
2	{1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31}
3	{2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32}

Но если, схема скачкообразной перестройки частоты обеспечивает исторически переход с одного возможного канала на другой таким образом, что после каждого скачка покрывается полоса частот, равная как минимум 6 МГц, благодаря чему в микросетевых сетях минимизируется возможность возникновения коллизий. Уменьшенная длина набора для таких стран, как Япония, Испания и Франция, обусловлена меньшей полосой частот, выделенной ими для промышленности, науки и медицинского применения в диапазоне 2,4 ГГц.

## FHSS на подуровне PLCP

После того как уровень MAC пропускает MAC-фрейм, который в локальных беспроводных сетях FHSS называется также *содержимый элемент данных PLCP*, или *PSDU* (сокращение от PLCP service data unit), подуровень PLCP добавляет два поля в начало фрейма, чтобы сформировать таким образом фрейм PPDU (дуплексим, PPDU — это элемент данных протокола PLCP). На рис. 3.9 представлен формат фрейма FHSS подуровня PLCP.

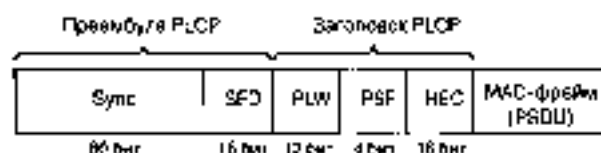


Рис. 3.9. Формат фрейма FHSS подуровня PLCP

Фрейм PLCP состоит из двух подполей.

- Подполе Sync размером 80 бит. Строка, состоящая из чередующихся 0 и 1, начинается с 0. Приемная станция использует это поле, чтобы принять решение о выборе антенны при наличии такой возможности, откорректировать уход частоты (frequency offset) и синхронизировать распределение пакетов (packet timing).
- Подполе флага начала фрейма (start of frame delimiter, SFD) размером 16 бит. Состоит из специфической строки (0000 1100 1011 1101, крайний слева бит первый) в обеспечении синхронизации фреймов (frame timing) для приемной станции.



Заголовок фрейма PLCP состоит из трех подполей.

- Слово длины служебного элемента данных PLCP (PSDU), PSDU length word (PLW) размером 12 бит. Указывает размер фрейма MAC (PSDU) в октетах.
- Сигнальное поле PLCP (signaling field PLCP, PSF) размером 4 бита. Указывает скорость передачи данных конкретного фрейма. Расшифровка значений скорости передачи представлена в табл. 3.5.

Таблица 3.5. Расшифровка значений PSF

b1	b2	b3	Скорость передачи данных (Мбит/с)
0	0	0	1,0
0	0	1	1,5
0	1	0	2,0
0	1	1	2,5
1	0	0	3,0
1	0	1	3,5
1	1	0	4,0
1	1	1	4,5

Служебный элемент данных PLCP (PSDU) проходит через операции скремблирования с целью отбеливания (рандомизации) последовательности входных битов (см. выше раздел "Систематизирующие физические уровни"). Получившийся в результате PSDU представлен на рис. 3.10. Заполняющие символы (stuff symbols) вставляются между всеми 32-разрядными блоками. Эти заполняющие символы устраняют любые систематические отклонения (bias) в данных, например, когда единиц больше, чем нулей, или наоборот, которые могли бы привести к нежелательным эффектам при дальнейшей обработке.

32-разрядный блок символов



Рис. 3.10. Скремблированный бит подуровня PSDU в технологии FHSS

## FHSS PMD-GFSK модуляция

Подуровень PLCP преобразует фрейм в поток битов и передает его на подуровень PMD. Подуровень PMD технологии FHSS модулирует поток данных с использованием модуляции, основанной на гауссовом переключении частот (Gaussian frequency shift keying, GFSK).

Чтобы понять, как осуществляется модуляция GFSK, мы должны сначала понять, как осуществляется частотная манипуляция (frequency-shift keying, FSK). В отличие от модуляции QPSK, описанной ранее, FSK осуществляется путем представления каждого символа сигналом отличной от других частоты. Например,

если мы хотим передать двоичное значение 0, мы передаем синусоидальный сигнал с частотой  $f_1$ , а чтобы передать 1, передаем сигнал с частотой  $f_2$ . Вы договориваетесь о периоде передачи одного символа с вашим другом на другом конце линии связи, и это обуславливает длительность передачи синусоидального сигнала одной частоты. Зачастую, вместо того чтобы указывать значения двух частот в абсолютных величинах, их указывают относительно несущей частоты  $f_c$ . На рис. 3.11 представлены частотная область сигналов с манитулой, представленной в виде высоты векторов  $f = f_c - f_d$  и  $f_2 = f_c + f_d$ .

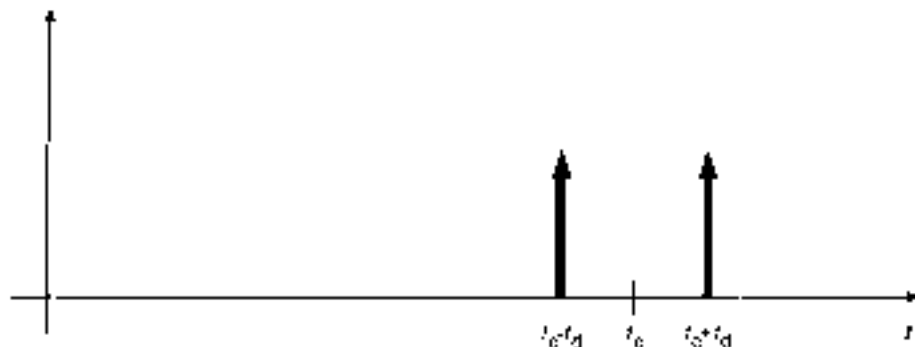


Рис. 3.11. Пример отображения сигнала в частотной области при модуляции FSK

Одним из преимуществ частотной манипуляции является легкость реализации соответствующих передатчика и приемника. FSK функционирует по тем же принципам, что и ГМ-радиоприемник в вашем автомобиле. Как вы увидите в главе 8, при использовании FSK значительно упрощается радиочастотный тракт, поскольку модуль сигнала остается постоянным: это означает, что никакая информация не передается амплитудой сигнала. Это позволяет передавать большую среднюю мощность при одинаковой пиковой. Однако частотная манипуляция имеет также несколько серьезных недостатков, не последним из которых является неэффективное использование полосы пропускания. Частотная манипуляция не позволяет передать так же много информации на "килогерцах спектра", как при использовании других методов. Кроме того, процесс модулирования не является линейным, и это приводит к возникновению проблем при корректировке сигналов, необходимой для компенсации ухудшения параметров канала или при расчете характеристик.

Вы можете понять, в чем состоит одна из серьезных задач, которую должен решить модулятор FSK, если рассмотрите процесс передачи 0, следующего сразу же после 1. При этом требуется, чтобы частота сигнала мгновенно изменилась со значения  $f_c - f_d$  на значение  $f_c + f_d$ . Это приводит к прерывному изменению выходного сигнала, во время которого выделяется много энергии на частотах, выходящих за рамки частотного диапазона. На рис. 3.12 показан пример такого изменения полосы частот, в предположении, что компонента несущей удалена.

Чтобы справиться с этой проблемой, приходится фильтровать сигнал, поступающий на частотный модулятор, это вызывает переход от частоты  $f_c - f_d$  на частоту  $f_c + f_d$ . В случае использования модуляции GFSK используется гауссов фильтр, наименование  $f_d$  происходит от термина "девиация частоты". Стандарт 802.11 указывает, что она должна составлять не менее 110 кГц. При ра-

Биты на скорости 2 Мбит/с кодируются модуляцией 4GFSK, в этом случае два бита модулируют сигнал одновременно с использованием двух девиации частоты. В табл. 3.6 представлена информация, которая поможет вам понять, как это делается;  $f_1$ , примерно в 5 раз больше, чем  $f_0$ .



Рис. 3.12. Период частоты при FSK

Таблица 3.6. Карта преобразования символа в частоту при модуляции 4GFSK

Символ	Частота
10	$f_1 + f_0$
11	$f_1 + f_H$
01	$f_1 - f_H$
00	$f_1 - f_0$

Эта технология FHSS широко применялась в таких приложениях, как складское хранение и приблизительно на начальном периоде развития локальных беспроводных сетей, она имела ряд недостатков. Первый и основной заключается в том, что эта технология не обеспечивала ни качество высокоскоростной передачи данных, которое было характерно для проводных локальных сетей и которое предполагали новые стандарты сетей беспроводных. Вторым и менее очевидный возник в том, что, хотя для использования в последовательности перестройки частот были доступны 79 каналов и три стандартные схемы перестройки частоты, в чем мы говорили в начале данного раздела, сигнал мог «скачать» до всего диапазона ISM, независимо от того, имеются ли поблизости другие устройства (например, медицинские приборы), работающие в этом диапазоне. В главе X, «Галверизация беспроводных LAN» и в главе 9, «Будущее беспроводных локальных сетей», будет рассказано о том, что не существует никаких стандартизированных методов, которые позволяли бы исключить из этого диапазона те частоты, на которых помехи особенно ощутимы. Если помехи присутствуют на половине частот диапазона и вы работаете на скорости 1 Мбит/с, половину времени передачи информации будет осуществляться по каналам, которые зашумлены настолько, что фактически информация принята не будет. А это означает, что реальная скорость передачи составит только 500 Кбит/с.

Еще более интересно то, что не предусмотрено никакого механизма для координации или синхронизации последовательностей переключения частоты для соседствующих точек доступа. Их последовательности переключения могут перекрываться, создавая взаимные помехи. Если вы не предъявляете высоких требований к помехоустойчивости и не планируете увеличивать количество точек доступа, то можете развернуть небольшую сеть на основе FHSS.

## Беспроводные локальные сети, использующие широкополосную модуляцию DSSS с расширением спектра методом прямой последовательности

В спецификации стандарта 802.11 оговорено использование и других физического уровня — на основе технологии широкополосной модуляции с расширенным спектром методом прямой последовательности (DSSS). Как было указано в стандарте 802.11 разработки 1997 года, технология DSSS поддерживает скорости передачи 1 и 2 Мбит/с. В 1997 году рабочая группа ратифицировала стандарт 802.11b, позволяющий поддерживать скорости передачи 5,5 и 11 Мбит/с. Физический уровень DSSS стандарта 802.11b совместим с существующими WLAN стандарта 802.11. Подуровень PLCP технология DSSS стандарта 802.11b такой же, как и для стандарта 802.11, лишь с дополнительными специализированными короткими преамбулой и заголовком.

Беспроводные локальные сети DSSS используют каналы шириной 22 МГц, благодаря чему аналогичные WLAN могут работать в одной и той же зоне покрытия. В Северной Америке и большей части Европы каналы шириной 22 МГц позволяют создать в диапазоне 2,4–2,483 ГГц три неперекрывающихся канала передачи. Эти каналы показаны на рис. 3.13, а подробнее рассматриваться они будут в главе 8, “Развертывание беспроводных LAN”.

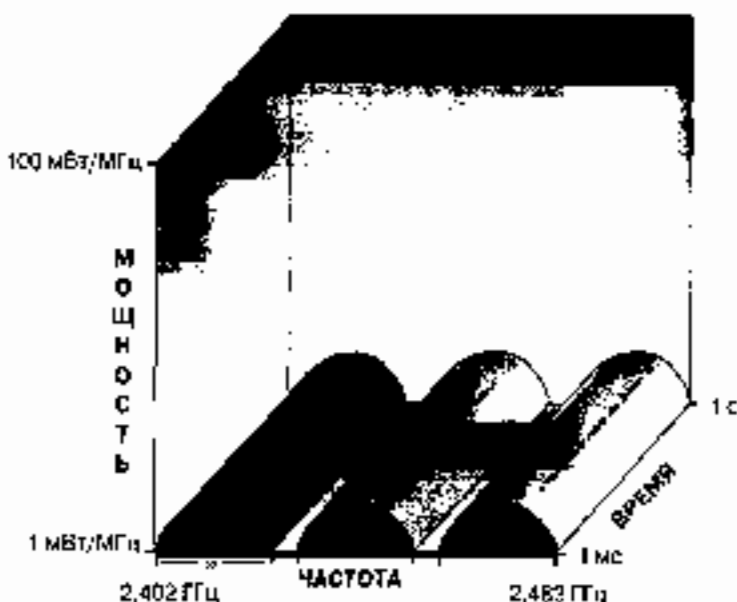


Рис. 3.13. Каналы, используемые в технологии DSSS

### Технология DSSS стандарта 802.11

Аналогично подуровню PLCP, используемому в технологии FHSS, подуровень PLCP технологии DSSS стандарта 802.11 добавляет два поля во фрейм MAC, чтобы сформировать PPDU: преамбулу PLCP и заголовок PLCP. Формат фрейма представлен на рис. 3.14.

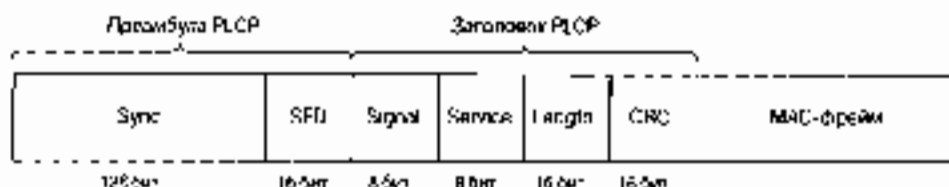


Рис. 3.14. Формат фрейма DSSS PPDU стандарта 802.11

Предузна PLCP состоит из двух подполей.

- Подполе Sync шириной 128 бит, представляющее собой строку, состоящую из единиц. Задача этого подполя — обеспечить синхронизацию для приемной станции.
- Подполе SFD шириной 16 бит, в нем содержится специфичная строка 0xF3A0, его задача — обеспечить тайминг (timing) для приемной станции.

Заголовок PLCP состоит из четырех подполей

- Подполе Signal шириной 8 бит, указывающее тип модуляции и скорость передачи для данного фрейма. В табл. 3.7 указаны соответствия между значением этого поля к скорости передачи.
- Подполе Service шириной 8 бит, зарезервировано. Это означает, что на время разработки спецификации стандарта оно осталось неопределенным; предполагается, что оно пригодится в будущих модификациях стандарта.
- Подполе Length шириной 16 бит, указывающее количество микросекунд (длительности  $16 \cdot 2^m - 1$ ), необходимое для передачи части MAC фрейма.
- Подполе CRC шириной 16 бит, обеспечивающее результирующее значение того же утвержденного ITU-T Международным телекоммуникационным союзом CRC 16, используемого в технологии FHSS, который применяется по отношению к подполям заголовка PLCP.

Таблица 3.7. Значения поля Signal и соответствующая им скорость передачи

Signal	Скорость передачи
0x0A	1 Мбит/с
0x14	2 Мбит/с

Подуровень PLCP преобразует фрейм в поток битов и передает данные на подуровень PMD. Весь PPDU проходит через процесс скремблирования с целью рандомизации данных.

Скремблированная предузна PLCP всегда передается со скоростью 1 Мбит/с, в то время как скремблированный фрейм MPDU передается со скоростью, указанной в подполе Signal. Подуровень PMD модулирует отбеленный поток битов, используя следующие методы модуляции.

- Двоичная относительная фазовая манипуляция (differential binary phase shift keying, DBPSK) для скорости передачи 1 Мбит/с
- Квадратурная фазовая манипуляция (quadrature phase shift key, QPSK) для скорости передачи 2 Мбит/с.

В следующем разделе описывается процесс модуляции DSSS на подуровне PMD

## Основы DSSS

Технология расширения спектра используют метод модуляции, при котором для передачи информации используется сигнал, спектр которого намного шире того, который необходим для передачи информации, и передается она с намного меньшей скоростью. Каждый бит заменяется или расширяется кодом, расширяющим полосу частот. Во многом благодаря кодированию (несколько информации заменяется намного большим числом информационных битов) эта технология позволяет передавать информацию при малом соотношении сигнал/шум, обусловленном или помехами, или недостаточной мощностью передатчика. При использовании DSSS переданный сигнал, по сути, увеличивается за счет применения расширяющей последовательности, совместной используемой передатчиком и приемником.

Беспроводные локальные сети типа DSSS особым образом кодируют данные, получая поток данных со скоростью 1 Мбит/с с канального уровня и преобразуя его в 11-битовый поток элементарных сигналов, или чипов (chips). Расширяющая спектр последовательность (she еще называют расширяющей (chipping) последовательностью или последовательностью Баркера), которая преобразует биты данных в элементарные сигналы, имеет длину 11 бит. В случае работы на скорости 1 и 2 Мбит/с один бит данных "расширяется" до 11 (двоичная 1 расширяется до значения 1111111111, а двоичный 0 — до значения 0000000000) "Расширяются" биты данных затем кодируются по схеме "ИЛИ" либо "исключающее ИЛИ" одновременно с расширяющей последовательностью, полученное в результате чипы преобразуются в символы и модулируются. Этот процесс представлен схематически на рис. 3.15 и 3.16.

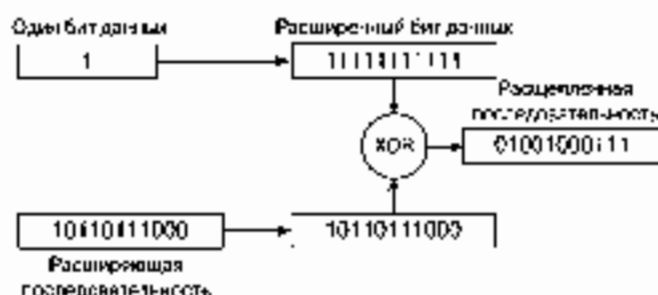


Рис. 3.15. Расширение битов данных с использованием значения 1

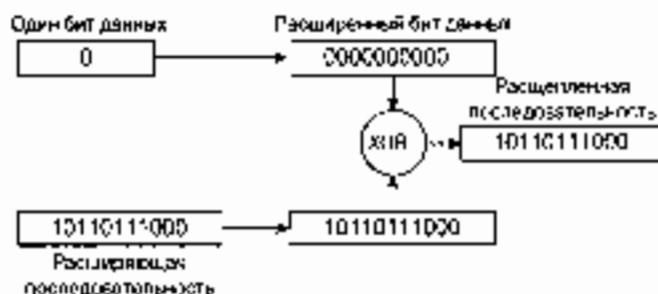


Рис. 3.16. Расширение битов данных с использованием значения 0

Вы можете удивиться: что хорошего для WLAN дает увеличение скорости передачи с 1 до 11 Мбит/с? 11-битовая последовательность представляет один бит данных. Предположим, например, что расширенная последовательность передается через

беспроводную среду. В ходе передачи и нескольких частотных каналах на сигнал не накладывался шум. Поскольку передатчик расширил спектр передаваемого сигнала до 22 МГц, только несколько чипов последовательности окажутся подверженными их влиянию. Приемник сможет восстановить исходную последовательность по шумным чипам. В качестве альтернативного данному процессу можно рассматривать таковой долучения необработанных данных; в этом случае часть данных из-за помех будет потеряна, и потребуется дублирующая их передача. При расширении спектра методом прямой последовательности все частоты канала используются для повышения пропускной способности канала и снижения задержек.

## Двоичная относительная фазовая манипуляция (DBPSK)

Вам следовало бы вспомнить описание отображения символов при использовании QPSK или представление модуляции в комплексной плоскости, рассмотренное нами ранее в разделе "Составляющие физического уровня". При модуляции BPSK используется аналогичный метод, но, поскольку каждый символ отображается только с помощью комплексной, или точки сигналами ошибки BPSK располагаются на действительной (Re) оси (рис. 3.17).

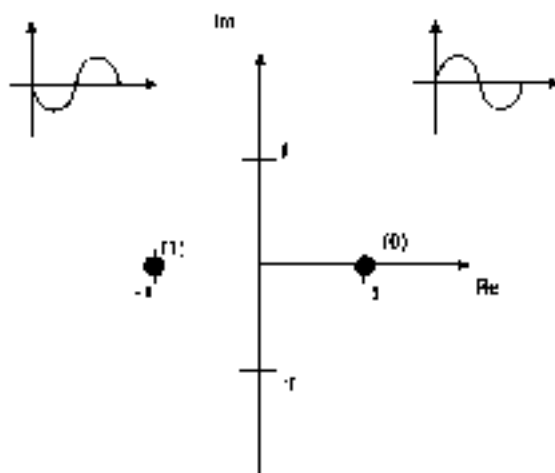


Рис. 3.17 Сигналы в плоскости BPSK

Глобальным приемнику не приходится удалять фазовую составляющую, возникающую при уходе частоты, используется относительное (инициально называют дифференциальное) кодирование, что приводит к методу DBPSK. Относительное кодирование осуществляется следующим образом. Каждый чип преобразуется в один символ. При поступлении 0 преобразователь символов (symbol mapper) передает тот же символ, который передавался в предыдущий период передачи символов. При поступлении 1 преобразователь символов изменит фазу на 180 градусов, или на  $\pi$  радиан. При модуляции BPSK модуль сигнала также остается неизменным, что упростит конструкцию радиотракта.

## Квадратурная относительная фазовая модуляция (DQPSK)

Для достижения скорости передачи 2 Мбит/с в сочетании QPSK отображаются два чипа на символ, как показано на рис. 3.6. При этом снова используется относительное

нее кодирование; символы этих двух чисел преобразуются в поворот фазы с целью реализации модуляции DQPSK (табл. 3.8).

**Таблица 3.8. Преобразование символов при модуляции DQPSK**

Входной чип	Изменение фазы (в градусах)
00	0
01	90
11	180
10	270 (-90)

Передача как с использованием BPSK, так и DQPSK приводит к необходимости переносить символы с частотой 11 МГц, но, поскольку при DQPSK каждый символ содержит два чипа, результирующая скорость передачи чипов составляет 22 МГц, что соответствует скорости передачи 2 Мбит/с.

Технология DSSS пользуется большим успехом на рынке благодаря ее устойчивости к внешним воздействиям, особенно при наличии помех. Однако ей свойственны те же недостатки, что и технологии FHSS. — относительно низкая скорость передачи данных. Этим и было обусловлено появление стандартов, обеспечивающих более высокую скорость передачи, — 802.11a и 802.11b.

## Беспроводные локальные сети стандарта 802.11b

Стандарт 802.11b, появившийся в 1999 году, регламентировал правила использования высокоскоростной технологии DSSS (HR-DSSS), обеспечивающей скорость передачи в локальных беспроводных сетях ISM-диапазона 2,4 ГГц вплоть до 5,5 и 11 Мбит/с. При этом используется кодирование с использованием комплементарных кодов (complementary code keying, CCK) или технология двойного неперекрывающегося сверточного кодирования (packet binary convolutional coding, PBCC). В технологии HR-DSSS используется та же схема организации каналов, что и в технологии DSSS. — малая частота шириной 22 МГц, 11 каналов, 3 неперекрывающихся, ISM-диапазон 2,4 ГГц. В данном разделе представлена информация, которая поможет вам понять, как достигаются эти повышенные скорости передачи.

### Подуровень PLCP технологии HR-DSSS стандарта 802.11b

Подуровень PLCP технологии HR-DSSS использует фреймы PPDU двух типов: длинный и короткий. Преамбула и заголовок длинного фрейма подуровня PLCP технологии HR-DSSS всегда передаются со скоростью 1 Мбит/с — в обеспечение обратной совместимости с технологией DSSS. И действительно, длинный фрейм подуровня PLCP технологии HR-DSSS почти такой же, как фрейм подуровня PLCP в технологии DSSS, но с небольшими расширениями, призванными обеспечить повышенные скорости передачи данных. Эти расширения таковы.



- В подполе **Signal** могут быть указаны дополнительные скорости передачи данных (табл. 3.9).
- Подполе **Service** определяет ранее зарезервированные биты (табл. 3.10).
- Подполе **Length** по-прежнему указывает количество микросекунд, необходимых для передачи PSDU.

### На заметку

При скоростях передачи данных, превышающих 8 Мбит/с, появляется неопределенность в числе октетов, поскольку значения в подполе **Length** округляются до ближайшего целого. Например, если необходимо передать 517 октетов, для этого понадобится время длительностью 376 мкс (округленное сверху произведение  $517/11$ ). Но для передачи 518 октетов также необходимо 376 мкс, поэтому в последнем случае вы вынуждены производить округление на величину, превышающую один октет. Вы можете установить флаг, сообщающий об этом приемнику, поместив в подполе **Service** «бит расширения длины» (**Length Extension bit**) со значением, равным 1. Благодаря ему приемник будет знать, что нужно вычесть 1 из числа октетов  $F_n$ , которые он ожидает. Обратите внимание: если вы используете PBCC, этот протокол имеет дополнительный октет, так что вы можете добавить значение бита выбора модуляции к числу октетов, прежде чем умножить на 11 для получения значения времени в микросекундах.

Таблица 3.9. Значения дополнительного подполя **Signal**

Signal	Скорость передачи данных
0x37	5,5 Мбит/с
0x3E	11 Мбит/с

Таблица 3.10. Определения битов подполя **Service**

Бит	Наименование	Что означает
B2	Генераторы синхронизированы (locked clocks)	0 = не синхронизированы (not locked), 1 = задающие генераторы частоты и символов синхронизированы (Tx frequency and symbol clocks are locked)
B3	Выбор модуляции (modulation selection)	0 = OQK, 1 = PBCC
B7	Увеличение длины (length extension)	Используется подполем длины

Короткий фрейм PLCP PDU обеспечивает средство для минимизации числа служебных сигналов, все еще позволяющих, однако, передатчику и приемнику связываться друг с другом надлежащим образом. Короткий фрейм, используемый в технологии HR-DSSS стандарта 802.11b, показан на рис. 3.18. Он использует те же преамбулу, заголовок и формат PSDU, но заголовок PLCP передается на скорости 2 Мбит/с, в то время как PSDU передается со скоростью 2, 5,5 или 11 Мбит/с. Кроме того, его подполя модифицированы следующим образом.

- Ширина поля **Sync** сокращена со 128 до 56 бит, оно представляет собой строку, состоящую из одних нулей.
- Поле **SFD** имеет ширину 16 бит и выполняет ту же функцию указания на начало фрейма, но также указывает на использование длинных или коротких заго-

двоичные. В случае коротких данных (менее 16 бит) передается в порядке, обратном по отношению к длинным заголовкам, поэтому они используют значение 0x05CE вместо 0x92Ad.

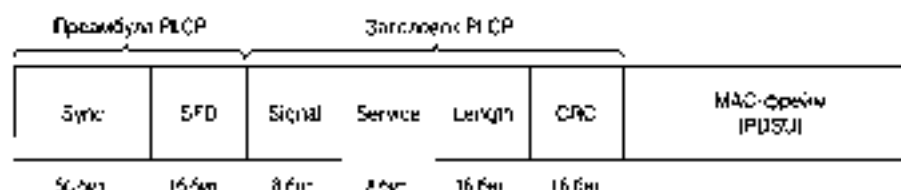


Рис. 3.18. Короткий PPDU формата HR-DSSS

Так же как и уровень PHY стандарта 802.11, PLCP преобразует весь PPDU посредством той же операции скремблирования, которая применяется в стандарте 802.11, на подуровне PMD. На этом подуровне различные подполя передаются с подводящей скоростью и с использованием соответствующего метода модуляции: CCK или PBSS.

## Модуляция CCK на подуровне PMD стандарта 802.11b

Хотя механизм расширения спектра, используемый для получения скорости 5,5 и 11 Мбит/с с применением CCK, относится к методам, которые применяются для скорости 1 и 2 Мбит/с, он по-прежнему уникален. В обоих случаях применяется метод расширения, но при использовании модуляции CCK расширенный код представляет собой код из 8 комплексных чипов (complex chip), в то время как при работе со скоростями 1 и 2 Мбит/с применяется 11-разрядный код. 8-чиповый код определяется или 4, или 8 битами — в зависимости от скорости передачи данных. Скорость передачи чипов составляет 11 Мчип/с, т.е. при 4 комплексных чипах на символ и 4 или 8 битов на символ можно достигнуть скорости передачи данных 5,5 и 11 Мбит/с.

Для того чтобы передать данные со скоростью 5,5 Мбит/с, нужно структурировать скремблированный поток битов в символы по 4 бита (b0, b1, b2 и b3). Последние два бита (b2 и b3) используются для определения 8 последовательностей комплексных чипов, как показано в табл. 3.11, где {c1, c2, c3, c4, c5, c6, c7, c8} представляющей чипов последовательности. В табл. 3.11  $j$  представляет минное число, корень квадратный из  $-1$ , и откладывается по мнимой, или квадратурной оси комплексной плоскости.

Таблица 3.11. Последовательность чипов CCK

(b2, b3)	c1	c2	c3	c4	c5	c6	c7	c8
00	1	1	1	-1	j	1	-1	1
01	-j	-1	-j	1	j	1	-j	1
10	-j	1	-j	-1	-j	1	1	1
11	j	-1	j	1	-j	1	1	1

Теперь, имея последовательность чипов, определенную битами (b2, b3), можно использовать первые два бита (b0, b1) для определения поворота фазы, осуществляемого при модуляции по методу DQPSK, который будет применен к последовательности

(табл. 3.12). Вы должны также пронумеровать каждый 4-битовый символ PSDU, начиная с 0, чтобы можно было определить, преобразуете вы четный либо нечетный символ в соответствии с этой таблицей. Следует помнить, что речь идет об использовании DQPSK, а не QPSK, и поэтому представленные в таблице изменения фазы отсчитываются по отношению к предыдущему символу или, в случае первого символа PSDU, по отношению к последнему символу предыдущего DQPSK символа, передаваемого со скоростью 2 Мбит/с.

Таблица 3.12. Поворот фазы при модуляции CCK

(b0, b1)	Изменение фазы четных символов	Изменение фазы нечетных символов
00	0 (0 градусов)	$\pi$ (180 градусов)
01	$\pi/2$ (90 градусов)	$-\pi/2$ (-90 градусов)
11	$\pi$ (180 градусов)	0 (0 градусов)
10	$-\pi/2$ (-90 градусов)	$\pi/2$ (90 градусов)

Это вращение фазы применяется по отношению к 8 комплексным числам символа, затем осуществляется модуляция на подходящей несущей частоте.

Чтобы передавать данные со скоростью 11 Мбит/с, скремблированная последовательность битов PSDU разбивается на группы по 8 символов. Последние 6 битов выбирают одну из четырех возможностей, соответствующую из 8 комплексных чисел, из числа 64 возможных последовательностей, почти так же, как использовались биты (b2, b3) для выбора одной из четырех возможных последовательностей. Биты (b0, b1) используются таким же образом, как при модуляции CCK на скорости 5,5 Мбит/с для вращения фазы последовательности и дальнейшей модуляции на подходящей несущей частоте.

## Технология двоичного пакетного сверточного кодирования (PBSS)

Как уже говорилось, стандарт HR-DSSS определяет также индивидуальный механизм модуляции для передачи данных со скоростью 5,5 и 11 Мбит/с. Эта технология отличается как от CCK, так и от DSSS стандарта 802.11. Вначале скремблированные биты PSDU передаются по линейный сверточный кодер, работающий с эфирной степенью кодирования 1/2, о чем впервые было упомянуто в разделе "Составляющие физического уровня". Особый полусверточный кодер (partial-rate half-rate encoder) имеет шесть линий задержки (delay), или запоминающих ячеек, и выдает 2 бита на каждой входной. Поскольку стандарт 802.11 рассчитан на использование фреймов и сверточные кодеры имеют память, все элементы задержки обнуляются с началом фрейма, и в его конце добавляется один октет нулей, чтобы обеспечить одинаковую помехоустойчивость для всех битов. Этот избыточный октет объясняет, почему вычисленные данные, рассмотренные в разделе "Подуровень PLCP технологии HR-DSSS стандарта 802.11b", слегка отличаются для CCK и PLCC. Затем закодированный поток битов преобразуется через преобразователь символов (symbol mapper) BPSK, чтобы достичь скорости передачи данных 5,5 Мбит/с, или через преобразователь символов QPSK, чтобы реализовать передачу со скоростью 11 Мбит/с. (Здесь не применяется относительное кодирование.) Особое преобразование символов, используемое в данном случае, зависит от двоичного значения, и, следовательно, от 256-битовой посто-

случайной последовательности. Как преобразуются два символа QPSK, показано на рис. 3.19, а как преобразуются два символа BPSK — на рис. 3.20. Для PSDU размером более 256 бит псевдослучайная последовательность просто повторяется.

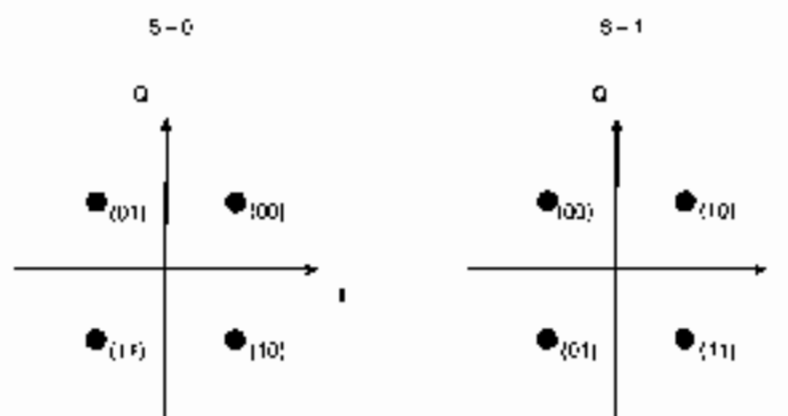


Рис. 3.19. Преобразование символов PBCC QPSK

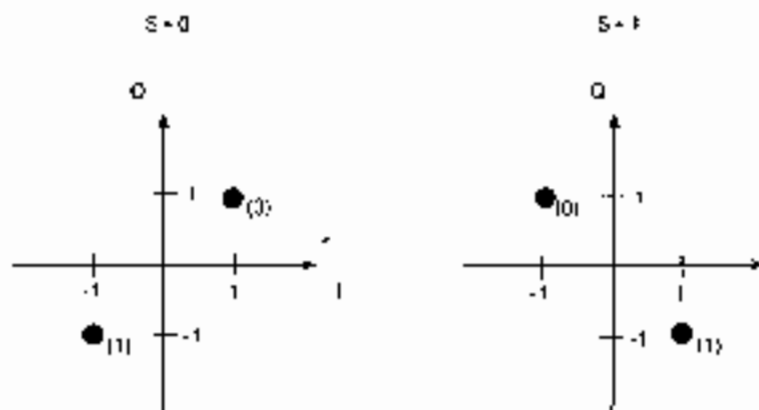


Рис. 3.20. Преобразование символов PBCC BPSK

## Беспроводные локальные сети стандарта 802.11a

В то же самое время, когда в проекте стандарта 802.11b в 1999 году был описан физически канал с технологией HR-DSSS, в проекте стандарта 802.11a были предложены использовать физический канал, в котором используется технология мультиплексирования с разделением по ортогональным частотам (orthogonal frequency division multiplexing, OFDM) в диапазоне 5 ГГц. Они увеличили скорость передачи до 24 Мбит/с и опционально — до 54 Мбит/с в безлицензионных диапазонах национальных информационных инфраструктур США U-NII (unlicensed national information infrastructure) 5,15–5,25 ГГц, 5,25–5,35 ГГц и 5,725–5,875 ГГц. Стандарт 802.11a регламентирует использование каналов шириной 20 МГц и определяет по четыре канала для каждого из трех диапазонов (о них подробно

рассказываться в главе 8, «Расширяющие Беспроводных LAN»). В данном разделе описывается технология OFDM.

## Стандарт 802.11j

Проект поправок 802.11j к стандарту для локальных/городских сетей (MAN) регламентирует работу в соответствии с правилами стандарта 802.11a в диапазоне 4,9 ГГц, выделенном в Японии и США для общественного применения с соблюдением правил безопасности, а также диапазона 5,03–5,091 в Японии. В схеме нумерации каналов (channel numbering scheme) этим каналам присвоены номера с 240 до 253, ширина каждого составляет 5 МГц.

## Подуровень PLCP технологии OFDM стандарта 802.11a

На подуровне PLCP физического уровня стандарта 802.11a применяется собственный уникальный формат фрейма PPDU (напомним, PPDU — это элемент данных протокола PLCP). Он представлен на рис. 3.21.

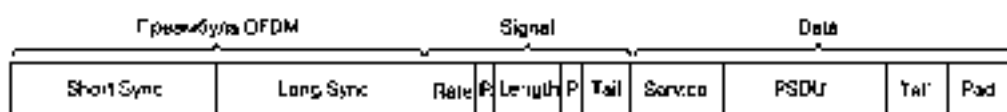


Рис. 3.21. Формат фрейма PPDU стандарта 802.11a

Фрейм PPDU состоит из трех основных частей: преамбулы OFDM, поля Signal и Data. Преамбула OFDM состоит из короткой настроечной последовательности (training sequence), Short Sync, и длинной настроечной последовательности символов, Long Sync. Первая используется приемником для автоматической регулировки усиления (AGC), тайминга (timing) и грубой оценки ухода частоты. Вторая — для оценки параметров канала, тайминга и точной оценки ухода частоты. Механизм, посредством которого все это выполняется, рассматривается ниже.

Поле Signal состоит из пяти подполей.

- Четырехразрядное подполе Rate, указывающее скорость передачи части Data фрейма. В табл. 3.13 представлены соотношения между значениями этих битов (R1–R4) и скоростью передачи части Data фрейма.
- Бит R зарезервирован для будущих применений.
- Подполе Length содержит беззнаковое 12-разрядное целое число, указывающее число октетов в PSDU.
- Бит P является битом проверки на четность для 17 битов подполей Rate, R и Length.
- Подполе Tail содержит 6 нескремблированных битов со значением 0.

Поле Data состоит из следующих подполей.

- Подполе Service, семь битов которого имеют значение, равное 0, за ними следуют 7 зарезервированных битов, значения которых пока также равны 0. Это подполе позволяет приемнику синхронизировать свой дескремблер (дешифратор последовательностей).

- Подполе PSDU, содержащее полезные данные, подлежащие передаче.
- Подполе Tail, заменяющее 6 заключительных скремблированных нулей нескремблированными нулями для ретрансляции (повторной установки в кадре (как состоянии) сверхканала кодера с конечной памятью).
- Подполе Rate позволяет добавить биты для получения необходимого числа кодирующих битов на символ OFDM. В разделе “Основы технологии OFDM” об этом рассказывается более подробно.

Таблица 3.13. Биты подполя Rate и соответствующие скорости передачи

A1-A4	Скорость передач (Мбит/с)
1101	6
1111	9
0101	12
0111	18
1001	24
1011	36
0001	48
0011	54

## Основы технологии OFDM

Чтобы разобраться во всех “как” и “почему” подуровня PMD технологии OFDM стандарта 802.11a, вначале нужно рассмотреть основы технологии OFDM, которая значительно отличается от методов модуляции, которые мы обсуждали ранее. OFDM является частью семейства схем многоканальной модуляции, которое было разработано для передачи данных в условиях сильной межсимвольной интерференции (inter-symbol interference, ISI). Рассмотрим процесс передачи сигнала по технологии QPSK (помним, QPSK — это физическая модуляция с квадратурными (фазовыми) сигналами). Он уже обсуждался нами ранее, в разделе “Составляющие физического уровня”. После этого предположим, что последовательно передаются два символа. В процессе “путешествия” этих двух символов от передатчика к приемнику через среду передачи они искажаются, а некоторые части сигнала могут быть задержаны. Если эти задержки существенны<sup>2</sup>, первый символ (как правило, его “хвост”) может наложиться на второй (т.е. на начало второго символа). Такое явление и приводит к возникновению межсимвольных помех, или межсимвольной интерференции. Время задержки между приемом первой “копии” сигнала и последней его “копии” называется разбросом задержек (delay spread) канала. Его можно также рассматривать как длительность времени, на которое первый символ расширяется за секунду. Обычно разработчики борются с межсимвольной интерференцией одним из следующих двух способов: применяя символы, которые достаточно длинны для того, чтобы быть правильно декодированными в условиях межсимвольной интерференции, или путем выравнивания (equalizing) для устранения искажений, вызванных межсимвольной интерференцией. При использовании пер-

<sup>2</sup> Существенные задержки могут быть вызваны множественным распространением сигнала. — *Прим. ред.*

ного метода скорость передачи символов ограничивается значением, несколько меньшим полосы пропускания канала, которая обратно пропорциональна разбросу задержек. При увеличении полосы пропускания канала можно увеличивать скорость передачи символов, тем самым добиваясь повышенной скорости передачи данных. Второй метод, часто используемый совместно с первым, требует использования более сложных и дорогостоящих устройств с применением схем выравнивания параметров каналов (channel equalization schemes), для максимального использования полосы пропускания канала. Схемы многоканальной модуляции (multichannel modulation schemes) могут реализовываться по-разному. Разработчик схемы многоканальной модуляции разбивает весь канал на небольшие, независимые, параллельные или ортогональные каналы передачи данных, в которых узкополосные сигналы, с низкой скоростью передачи символов, модулируют, обычно в частотной области, отдельные поднесущие. Аналогично тому как обычно ставится модуляция сигнала при скачкообразной перестройке частоты (FHSS), весь канал передачи разбивается на  $N$  независимых подканалов. При задании полосы пропускания канала чем больше выбранное число  $N$ , тем более длительный период передачи символа и уже ширина подканала; при стремлении числа подканалов к бесконечности межсимвольная интерференция приближается к нулевой.

Полным инструментарием для создания символов этих независимых подканалов является быстрое преобразование Фурье (БПФ), которое является эффективным методом применения дискретного преобразования Фурье (ДПФ) и позволяет преобразовывать сигналы из временной области в частотную и обратно. В частотной области генерируются  $N$   $M$ -QAM символы (от англ. quadrature amplitude modulation — квадратурная амплитудная модуляция), которые затем преобразуются во временную область посредством обратного БПФ. Следует также сказать о том, что при выборе размера входных данных БПФ (size of FFT) равным степени числа 2 позволяет упростить реализующие данные операции устройства и повысить их эффективность. По этим причинам в системах OFDM число  $N$  всегда выбирают равным степени 2.

Не идя дальше в добри математики, поскольку это не соответствует цели написания нашей книги, скажем, что обработка сигнала значительно упрощается, если проводится в частотной области с использованием БПФ. Однако, для того чтобы такая обработка стала возможной на временной стороне, принятый сигнал должен быть подвергнут циклической свертке (circular convolution) ввода с каналом (of the input with the channel)<sup>1</sup>. Это противоположно только свертке. Свертка — это математическая операция, применяемая для описания прохождения сигнала через канал и вычисления получаемого выходного сигнала. Чтобы быть уверенным в качестве принятого сигнала, вы должны взять временное представление сигнала OFDM и создать циклическим префиксом (cyclic prefix) окончания  $\mu$  символа в его начале. Этот процесс проиллюстрирован на рис. 3.22, где  $\mu$  — длина циклического префикса и  $N$  — используемый размер входных данных БПФ.

Длина циклического префикса должна превышать разброс задержек канала и обеспечить того, чтобы каждый полученный OFDM-символ являлся циклической сверткой импульсной характеристики канала с переданным символом. Другой способ обеспечить это — вставлять между символами охранные интервалы (guard time), которые будут гарантировать, что каждый остаточный сигнал (residual signal) предыдущего OFDM-символа затрет, прежде чем начнется обработка текущего символа. Эти ин-

<sup>1</sup> Важно, имеется в виду свертка двоякого сигнала с импульсной характеристикой канала — *Princ. ред.*

передатчик предпочтительно обрабатывать символы, и если идентифицировать данный процесс в частотной области. Это означает последовательную обработку подканалов.

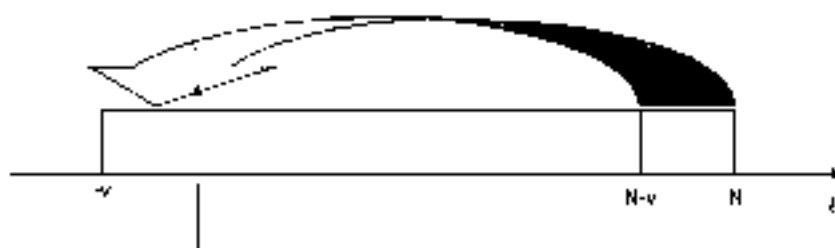


Рис. 3.22. Формирование циклического префикса в технологии OFDM.

Для того чтобы приемник мог определить импульсную характеристику канала (to estimate the channel), часто или вставляют известные настроенные символы на некоторых из  $N$  поднесущих частот, или передают предельный OFDM-символ, который приемник может использовать для определения импульсной характеристики канала. Зачастую также подканалы, расположенные на краях общей полосы пропускания, настраивают нулями, потому что фильтры передатчика и приемника очень удобно настраивать тогда, когда никакая информация не передается через них вообще.

В отличие от многих других методов многоканальной модуляции, OFDM использует одинаковое количество битов во всех подканалах. В беспроводных приложениях, таких как асимметричная цифровая абонентская линия (asymmetric digital subscriber line, ADSL), где параметры канала не изменяются со временем, передатчик использует знание о канале и передает больше битов, или информации, по тем абонентским линиям, которые меньше искажены шумом или имеют меньшее затухание.

## Настройка OFDM

Как уже упоминалось ранее, поле Sync состоит из длинных и коротких символов (рис. 3.23). Существует 18 коротких настроенных символов, и каждый из них представляет собой короткий OFDM-символ, который выполняет 12 из 52 используемых подканалов специальным QPSK-символом, умноженным на 4. Это приводит к увеличению во временной области периодичности последовательности, которую можно использовать для обнаружения начала фрейма, выполнения автоматической регулировки усиления, выбора подходящего значения, если имеется такая возможность, грубой оценки ухода частоты и синхронизации тайминга.



Рис. 3.23. Поле Sync

Для длинных настроенных символа идентичны и модулируют несущую частоту специальной последовательностью. Длинная настроенная последовательность позволяет выполнять оценку параметров канала и точно оценить уход частоты. Поскольку оба длинных настроенных символа предназначены для совместного использования, для них необходим только один охранной интервал, обозначенный на рис. 3.23 буквой G.



## Подуровень PMD технологии OFDM стандарта 802.11a

На рис. 3.24 представлена обобщенная схема передатчика OFDM, используемого на подуровне PMD технологии OFDM стандарта 802.11a. Как и на других физических каналах, биты данных пропускаются через скремблер и затем сверточный кодер, в результате чего получаются канальные биты<sup>4</sup>. Скорости их передачи определяется используемой скоростью передачи данных. Затем канальные биты разбиваются на группы, по размерам равные числу канальных битов, используемых для одного символа. Разбитые на группы канальные биты преобразуются в 48 симплинов с количеством бит на символ, зависящим от скорости передачи данных. Они помещаются на 48 поднесущих OFDM-символа, а на 4 несущих передается пилот-сигналы. Выполняется обратное быстрое преобразование Фурье, после чего формируется циклический префикс. Результативная последовательность модулирует подходящую несущую.

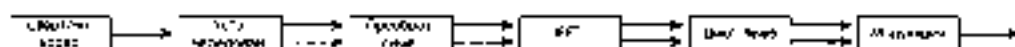


Рис. 3.24. Обобщенная схема передатчика OFDM стандарта 802.11a

В табл. 3.14 показано, как необходимая скорость передачи данных преобразуется в соответствующие параметры уровня передатчика OFDM.

Таблица 3.14. Параметры передатчика стандарта 802.11a

Скорость передачи данных (Мбит/с)	Сигнальные созвездие	Степень сверточного кодирования	Число канальных битов на поднесущую	Число канальных битов на символ	Число битов данных на символ OFDM
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	5/6	6	288	216

Описанное вами ранее поле Signal передается в одном OFDM-символе на скорости 6 Мбит/с, что позволяет передавать 24 бит данных. Это объясняет, почему существует 6 бит поля Tail в конце данного поля. Поле Data передается как ряд последовательных OFDM-символов со скоростью передачи данных, указанной в подполе Rate поля Signal. Вы можете определить число защищающих битов, необходимых для того, чтобы длина поля Data была кратной числу битов кода на OFDM-символ, если знаете длину PSDU.

Что касается деталей устройства передатчика стандарта 802.11a, то скремблер использует такой же полиномиальный генератор, как и применяемый во всех других схемах модуляции стандарта 802.11. Сверточный кодер использует несколько отлич-

ную от 1/2 эффективную степень кодирования, чем применяем опционально и PUSC стандарта 802.11b. Эффективные степени кодирования 2/3 и 3/4 достигаются за счет "прокалывания" (puncturing) или опускания некоторых из закодированных битов в передатчике и замены их нулевыми битами в приемнике. В конечном счете таким образом приводит к повышению степени кодирования, поскольку на каждый вложенный бит передается меньше битов кода. Опускание битов производится организованным способом и систематически.

Устройство чередования — блочного типа с размером блока, определяемым числом битов кода, приходящихся на один OFDM-символ. Чередование выполняется в два этапа.

На первом этапе добавляются нули, чтобы соседние канальные биты передавались несоседними несущими, на втором — чтобы соседние канальные биты преобразовывались инверсионно и менее и более старшие разряды сигналами высшего порядка символов. Этот процесс является важным, потому что в сигналах высшего порядка самые младшие биты (LSB) часто передаются с меньшей надежностью. Эта проблема также для нас более очевидна, если вы рассмотрите сигнальные созвездия на точки, которые ближе и более подвержены искажениям и ошибкам, имеют тенденцию различаться только своими самыми младшими битами.

Преобразования групп битов в символы на комплексной плоскости показаны на рис. 3.25–3.28 для BPSK, QPSK, 16-QAM и 64-QAM соответственно.

#### На заметку

При квадратичной амплитудной модуляции (QAM) осуществляется одновременно модуляция и амплитуды, и фазы синусоидального сигнала. При модуляции типа 16-QAM используется 4 уровня амплитуды в каждом измерении. При модуляции типа 64-QAM — восемь уровней. Можно считать, что за счет изменения фазы определяются значения 2 бит, как при QPSK, амплитуда определяет 2 или 3 бит.

Для того чтобы при всех скоростях передачи данных средняя мощность сигнала была статистически одинаковой, каждый символ умножается на масштабный коэффициент, который зависит от типа модуляции. Значения масштабных коэффициентов приведены в табл. 3.15.

Таблица 3.15. Масштабные коэффициенты, применяемые для нормализации мощности

Тип модуляции	Масштабный коэффициент
BPSK	1
QPSK	$\frac{1}{\sqrt{2}}$
16-QAM	$\frac{1}{\sqrt{10}}$
64-QAM	$\frac{1}{\sqrt{42}}$

<sup>4</sup> Их также называют канальными символами или битами кода (coded bits) - Прим. ред.

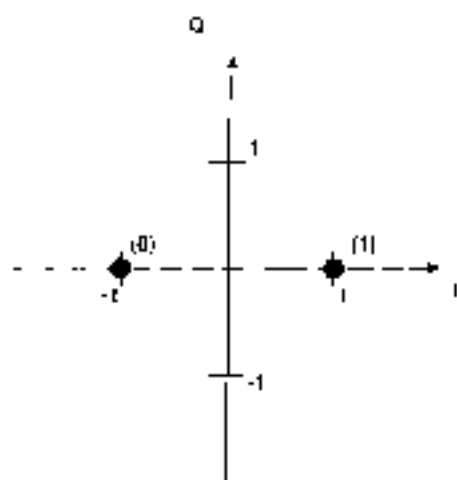


Рис. 3.25. Составные стандарты 802.11a для модуляции типа BPSK

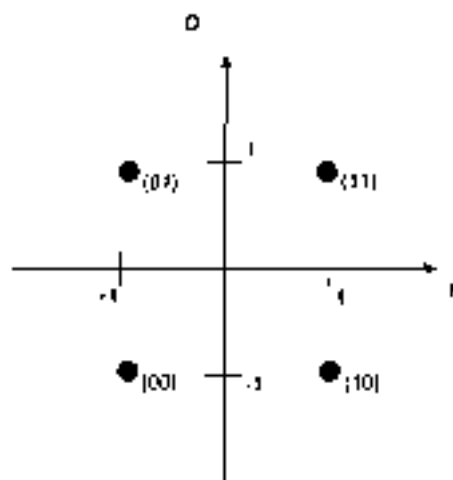


Рис. 3.26. Составные стандарты 802.11a для модуляции типа QPSK

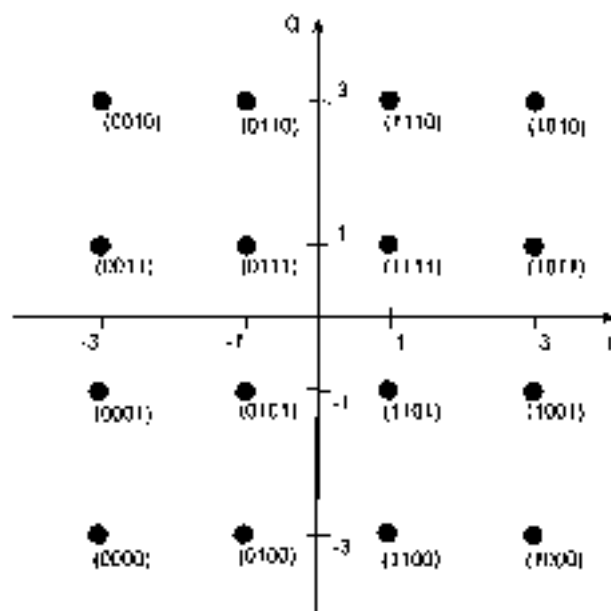


Рис. 3.27. Составные стандарты 802.11a для модуляции типа 16-QAM

Внутри каждого OFDM-символа через регулярные интервалы добавляются 4 пилот-сигнала в обратном БПФ для использования их приемником. Эти пилотные поднесущие кодируются и модулируются последовательностью с использованием BPSK.

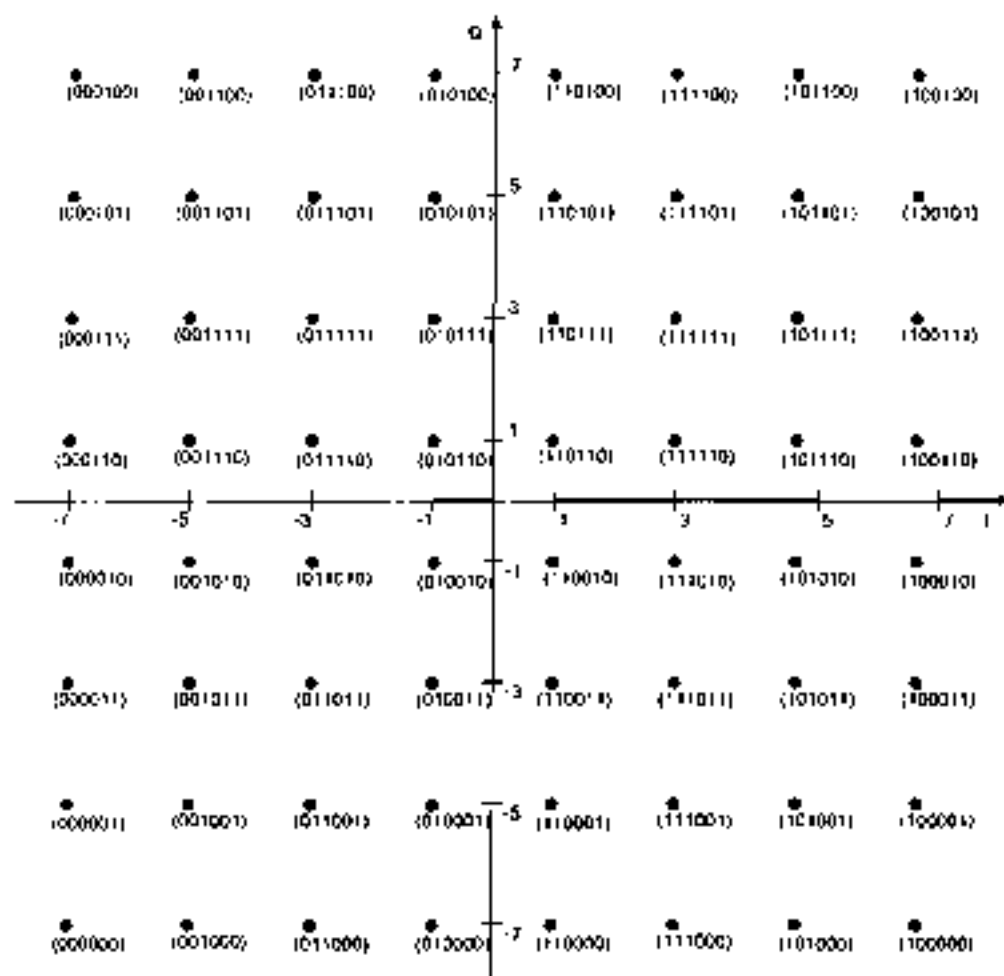


Рис. 3.28. Составные стандарты 802.11a для модуляции типа 64-QAM

## Беспроводные локальные сети стандарта 802.11g

Стандарт IEEE 802.11g, предложенный в июне 2003 года, определил технологию EPR как средство обеспечения скоростей передачи до 54 Мбит/с в диапазоне ISM 2,4 ГГц; он позаимствовал методы OFDM стандарта 802.11a. В противоположность стандарту 802.11a этот обеспечивает обратную совместимость со стандартом 802.11b, поскольку устройства, соответствующие стандарту 802.11g, могут изменять скорость передачи данных до значений, меньших, чем регламентированы стандартом 802.11b. Определены три схемы модуляции: ERP-OFDM, ERP-PBCC и DSSS-OFDM. При использовании ERP-OFDM задействуются специально разработанные для нее механизмы, обеспечивающие скорость передачи 6, 9, 12, 18, 24, 36, 48, и 54 Мбит/с, из них обязательными являются скорости 6, 12 и 24 Мбит/с в дополнение к скоростям пере-

длинных 1, 2, 5,5 и 11 Мбит/с. Стандарт также позволяет опционально использовать режимы RBCC со скоростями 22 и 33 Мбит/с и также опционально режимы DSSS-OFDM со скоростями 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с. В данном разделе описаны изменения, введенные в стандарт для реализации схем модуляции ERP-OFDM, ERP-RBCC и DSSS-OFDM.

## Подуровень PLCP стандарта 802.11g

Стандарт 802.11g определяет пять подуровней PLCP с длинной преамбулой, короткой преамбулой, преамбулой ERP-OFDM, длинной преамбулой DSSS-OFDM и короткой преамбулой DSSS-OFDM. Поддержка первых трех обязательна, двух остальных — опциональна. В табл. 3.16 приведены различные преамбулы и схемы модуляции, а также скорости передачи данных, которые они поддерживают или с которыми взаимодействуют.

Таблица 3.16. Преамбулы

Тип преамбулы	Скорости передачи данных поддерживаются/взаимодействуют
Длинная	1, 2, 5,5 и 11 Мбит/с. DSSS-OFDM на всех скоростях OFDM ERP-RBCC на всех скоростях ERP-RBCC
Короткая	2, 5,5 и 11 Мбит/с. DSSS-OFDM на всех скоростях OFDM ERP-RBCC на всех скоростях ERP-RBCC
ERP-OFDM	ERP-OFDM на всех скоростях
Длинная DSSS-OFDM	DSSS-OFDM на всех скоростях
Короткая DSSS-OFDM	DSSS-OFDM на всех скоростях

Длинная преамбула использует ту же самую длинную преамбулу, что определена для HR-DSSS, но ее поле Service модифицировано так, как показано в табл. 3.17.

Таблица 3.17. Определения полей поля Service для ERP

Бит	Наименование	Что означает
b0	Зарезервирован	0
b1	Зарезервирован	0
b2	Блокировка генераторов (lock status)	0 — не заблокированы; 1 — генераторы тактовой частоты передатчика и символов заблокированы
b3	Выбор модуляции	0 — не ERP-RBCC, 1 — ERP-RBCC
b4	Зарезервирован	0
b5	Расширение длины	Для ERP-RBCC
b6	Расширение длины	Для ERP-RBCC
b7	Расширение длины	Для RBCC

Биты расширения длины определяют число октетов, когда используются режимы RBCC на скорости 11 Мбит/с и ERP-RBCC на скоростях 22 и 33 Мбит/с.

Короткая преамбула так же модифицируется по отношению к таковой HR-DSSS, как указано в табл. 3.16.

Прямбулы ERP-OFDM использует такую же стандарты 802.11a и расширяет сигнал на дополнительные 6 мкс, в течение которых не происходит никакая передача данных, чтобы сделать пакет длиннее для согласования его с более длинным 16-микросекундным таймингом SIFS стандарта 802.11a против 10-микросекундного тайминга SIFS стандарта 802.11b.

Формат длинной преамбулы PPDU, технологии CCK-OFDM представлен на рис. 3.19. В поле **Rate** поля **Signal** устанавливается скорость 3 Мбит/с. Благодаря такой установке обеспечивается совместимость со станциями, не поддерживающими ERP, потому что они по-прежнему считывают значение поля **Length** и ожидают передачу, несмотря на то что не способны демодулировать полезную нагрузку. Заголовок PLCP соответствует таковой предварительно определенной длительности преамбулы, но эта преамбула точно такая же, как для режима HR-DSSS. И заголовок, и преамбула передаются со скоростью 1 Мбит/с с использованием DBPSK, а PSDU передается с использованием подходящей скорости передачи данных OFDM. Заголовок скремблируется посредством скремблера HR-DSSS, а символы данных скремблируются с помощью скремблера стандарта 802.11a.



Рис. 3.19. Формат длинной преамбулы PPDU технологии CCK-OFDM

В формате короткой преамбулы PPDU технологии DSSS-OFDM, аналогично длинной преамбуле DSSS-OFDM, используются короткая преамбула HR-DSSS и заголовок при скорости передачи данных 2 Мбит/с. Посредством скремблера HR-DSSS и символов данных короткая преамбула и заголовок передаются с использованием технологии OFDM и используют скремблер стандарта 802.11a.

## ERP-OFDM

Как уже говорилось, ERP-OFDM обеспечивает механизм для использования скоростей передачи данных стандарта 802.11a в диапазоне ISM таким образом, что обеспечивается обратная совместимость с технологиями DSSS и HR-DSSS. В дополнение к использованию модуляции OFDM стандарта 802.11a по схеме распределения частот лицензия 2,4 ГГц ERP-OFDM также устанавливает, что центральная частота передачи и частота частоты символов определяются тем же генератором, который был опциональным для DSSS. Он использует каналный интервал длительностью 20 мкс, но она может быть уменьшена до 9 мкс, если выяснится, что в ISM находится только устройства ERP.

## ERP-PBCC

Для передачи данных с более высокими скоростями, 22 и 33 Мбит/с, технология двичного пакета с частотным кодированием (PBCC) использует тот же механизм, что и на меньших скоростях, 5,5 и 11 Мбит/с PBCC, но с использованием S-PSK вместо QPSK и BPSK для достижения скорости 22 Мбит/с. Скорость 33 Мбит/с достигается за счет применения генератора с частотой 16,5 МГц вместо генератора с частотой 11 МГц. Схема отображения символов показана на рис. 3.30.

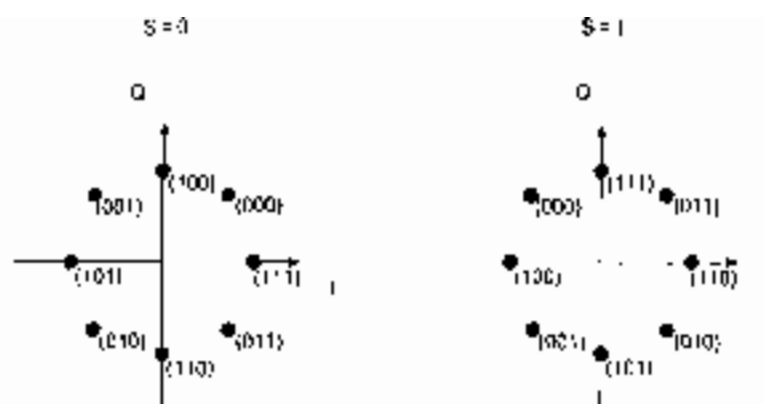


Рис. 3.30. Сигнальные созвездия ERP-PPCC стандарта 802.11g

## Стандарт 802.11g: резюме

Главное, что следует помнить относительно стандарта 802.11g, состоит в следующем. Он увеличивает поддерживаемые скорости передачи данных в диапазоне 2,4 ГГц до 54 Мбит/с сложным, обеспечивающим обратную совместимость со старыми устройствами, соответствующим стандарту 802.11b. Если в локальной сети используются только устройства стандарта 802.11g, передача осуществляется с максимальной возможной скоростью. Однако, если в нее входят устройства стандарта 802.11b, информация закодированная должна передаваться со скоростями стандарта 802.11b, чтобы их могли «понимать» эти старые устройства. Такие сниженные скорости должны выполняться при всех передачах, независимо от того, происходят они между устройствами стандарта 802.11g или 802.11b. Конечным эффектом оказывается общее увеличение накладных расходов, но это — небольшая цена за обратную совместимость, обеспечиваемую стандартом 802.11g.

## Оценка незанятости канала (CCA)

Различные стандарты семейства 802.11 определяют пять режимов оценки незанятости канала (CCA).

- Решение о занятости основывается на выделении в канале энергии, превосходящей некоторое пороговое значение.
- Решение о занятости основывается на обнаружении сигнала несущей, соответствующей стандарту 802.11.
- Обнаружение несущей и выделение энергии (комбинация способов 1 и 2).
- Обнаружение несущей с сообщением таймера о том, что среда не занята, если никакой сигнал не обнаружен в течение 3,65 мс.
- Выделение энергии, соответствующей повышенным скоростям передачи на физическом уровне, и обнаружение несущей по способу 3, но применительно к ERP.

В стандарте указано, что процесс CCA должен применять по крайней мере один из названных методов.

## Резюме

В табл. 3.18 приведены основные параметры различных технологий, применяемых на уровне PHY и рассмотренных в данной главе. Хотя технологии FHSS распространяется очень быстро, ее догоняют технологии DSSS и HR-DSSS. В то время как писались эти строки, промышленность находилась на пике второй революции в технологии, поскольку пользователи переходили к использованию устройств на основе стандартов 802.11a и 802.11g.

Таблица 3.18. Стандарты PHY 802.11

Параметр	802.11 FHSS	802.11 DSSS	802.11b HR-DSSS	802.11a OFDM	802.11g ERP	802.11j
Частотный диапазон (ГГц)	2,4	2,4	2,4	5	2,4	4,9
Максимальная скорость передачи данных (Мбит/с)	2	2	11	54	54	54
Тип модуляции	QPSK	GFSK	OQK	OFDM	OFDM	OFDM

В этой главе кратко рассказывалось об основных составляющих физического уровня и о том, как их можно использовать совместно для создания законченной системы физического уровня. Рассматривались также отдельные параметры каждого из различных физических уровней и компромиссы, на которые приходится идти при выборе необходимой технологии.





В этой главе...

- Безопасность в соответствии со стандартом 802.11 1997 года. Почему в качестве алгоритма шифрования выбран WEP, а в качестве алгоритма аутентификации — алгоритмы с открытым и совместно используемым ключом.
- Уязвимость системы защиты, регламентированной стандартом 802.11 1997 года. Почему WEP неэффективен в качестве алгоритма шифрования, а открытый и совместно используемый ключи — в качестве средства аутентификации.
- Усовершенствования, которые будут внесены в систему защиты беспроводных LAN (WLAN) следующего поколения. Новые технологии, которые будут использоваться для обеспечения безопасности WLAN стандарта 802.11.

## Безопасность беспроводных LAN

Разработчикам, которые уже применили или применят сейчас беспроводные локальные сети стандарта 802.11, множество аббревиатур, которые описывают повышенную защищенность беспроводных LAN стандарта 802.11, напоминает суп с макаронками и виле букв. При обсуждении проблем безопасности локальных сетей стандарта 802.11 часто используются такие термины, как 802.1X, EAP, LEAP, PEAP, EAP-TLS, WEP, TKIP, WPA и AES. Сетевому администратору, привыкшему иметь дело с IP-протоколами и ориентированными на установление соединения технологиями, эти новые, ориентированные на обеспечение безопасности протоколы могут обить с толку.

## Безопасность беспроводных сетей

Представьте длинный кабель вашей внутренней сети Ethernet, который выходит за пределы офиса и проложен в земле под автостанцией. Любой, кто хочет подключиться к вашей сети, может запросить это сделать, сделав шнур от этого кабеля. Подключая незащищенные беспроводные LAN к вашей внутренней сети, вы потенциально представляете точно такую же возможность.

Устройства стандарта 802.11 связываются друг с другом, используя в качестве переносчика данных сигнал, передаваемый в диапазоне радиочастот. Данные передаются по радио-отправителем, полагающим, что приемник также работает в выбранном радиодиапазоне. Недостатком такого механизма является то, что любая другая станция, использующая этот диапазон, тоже способна принять эти данные.

Если не использовать какой-либо механизм защиты, любая станция стандарта 802.11 сможет обработать данные, посланные по беспроводной локальной сети, если только ее приемник работает в том же радиодиапазоне. Для обеспечения хотя бы минимального уровня безопасности необходимыми являются следующие компоненты.

- Средства для принятия решения относительно того, кто или что может использовать беспроводную LAN. Это требование удовлетворяется за счет механизма аутентификации, обеспечивающего контроль доступа к LAN.
- Средства защиты информации, передаваемой через беспроводную среду. Это требование удовлетворяется за счет использования алгоритмов шифрования.

На рис. 4-1 показано, что защита в беспроводных сетях обеспечивается как за счет аутентификации, так и благодаря шифрованию. Ни один из названных механизмов в отдельности не способен обеспечить защиту беспроводной сети.

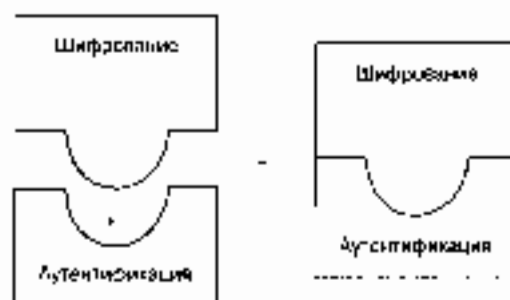


Рис. 4.1. Защита в беспроводных сетях обеспечивается за счет аутентификации и шифрования

В спецификации стандарта 802.11 регламентированы примененные механизмы аутентификации устройств с открытым и с совместно используемым ключом и механизма WEP, обеспечивающего защищенность данных на уровне привязанных сетей. Оба алгоритма аутентификации, с открытым и с совместно используемым ключом, основаны на WEP-шифровании и применении WEP-ключей для контроля доступа. Поскольку алгоритм WEP играет важную роль в обеспечении безопасности сетей стандарта 802.11, в следующем разделе будут рассмотрены основы шифрования и шифры

## Обзор систем шифрования

Механизмы шифрования основаны на алгоритмах, которые рандомизируют данные. Используются два вида шифров.

- Поточный (групповый) шифр.
- Блочный шифр.

Шифры обоих типов работают, генерируя ключевой поток (key stream), получаемый на основе значения секретного ключа. Ключевой поток смешивается с данными, или открытым текстом, в результате чего получается закодированным выходной сигнал, или зашифрованный текст. Названные два вида шифров отличаются по объему данных, с которыми они могут работать одновременно.

Поточный шифр генерирует непрерывный ключевой поток, основываясь на значении ключа. Например, поточный шифр может генерировать 15-разрядный ключевой поток для шифрования одного фрейма и 200-разрядный ключевой поток для шифрования другого. На рис. 4.2 проиллюстрирована работа поточного шифра. Поточные шифры — это небольшие и эффективные алгоритмы шифрования, благодаря которым нагрузка на центральный процессор оказывается небольшой. Наиболее распространенным является поточный шифр RC4, который и лежит в основе алгоритма WEP.

Блочный шифр, наоборот, генерирует единственный ключевой поток шифрования фиксированного размера. Открытый текст делится на блоки, и каждый блок смешивается с ключевым потоком независимо. Если блок открытого текста меньше, чем блок ключевого потока, первый дублируется с целью получения блока нужного размера. На рис. 4.3 проиллюстрирована работа блочного шифра. Процесс фрагментации, а также другие особенности шифрования с использованием блочного шифра выглядят следующим образом, по

связанную с потоковым шифрованием, нагрузку на центральный процессор. В результате производительность устройства, применяющего блочное шифрование, снижается.



Рис. 4.2. Так осуществляется потоковое шифрование

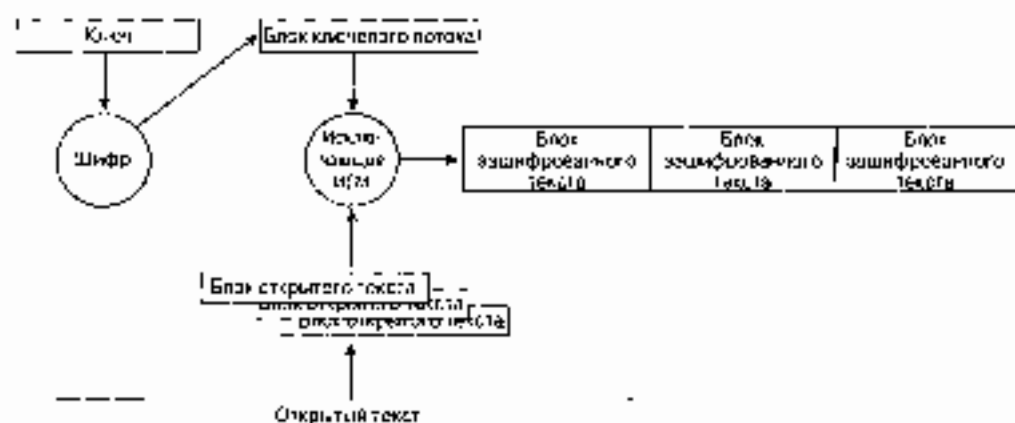


Рис. 4.2. Так осуществляется блочное шифрование

Процесс шифрования, описанный нами для потоковых и блочных шифров, называется *режим шифрования с потоковой ключевой электронной книгой* (First-time Code Book, ECB). Режим шифрования ECB характеризуется тем, что один и тот же открытый текст после шифрования преобразуется в один и тот же зашифрованный текст. Этот фактор потенциально представляет собой угрозу для безопасности, поскольку злоумышленники могут обнаружить образцы зашифрованного текста и выдвигать какие-то предположения об исходном тексте.

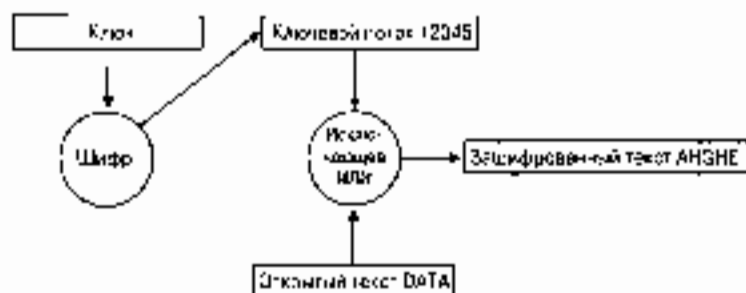
Некоторые режимы шифрования позволяют решить эту проблему.

- Векторы инициализации (initialization vector, IV).
- Режимы с обратной связью (feedback modes).

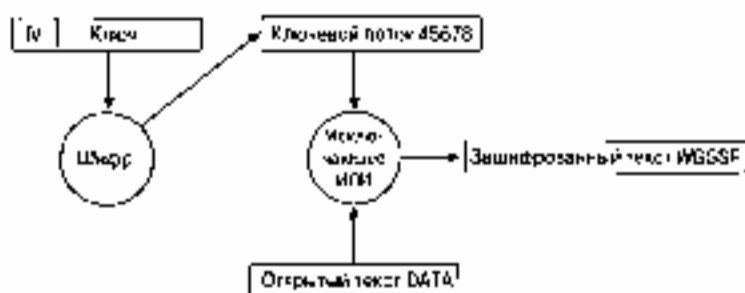
## Векторы инициализации

Вектор инициализации — это номер, добавляемый к ключу, конечным результатом этого является изменение информации ключевого потока. Вектор инициализации связывается с ключом до того, как начнется генерация ключевого потока. Вектор инициализации все время изменяется, то же самое происходит с ключевым потоком. На рис. 4.4 показаны два сценария. Первый относится к шифрованию с использованием потокового шифра без применения вектора инициализации. В этом случае от-

крытый текст DATA после смешения с ключевым потоком 12345 всегда преобразуется в зашифрованный текст AHGHE. Второй пример показывает, как тот же открытый текст смешивается с ключевым потоком, дополненным вектором инициализации для получения другого зашифрованного текста (Обратите внимание на то, что зашифрованный текст во втором случае отличается от такового в первом. Стандарт 802.11 рекомендует использовать вектор инициализации по умолчанию (0000000000000000). Это означает, что если один и тот же файл будет передан дважды, весьма высокой окажется вероятность того, что зашифрованный текст будет разным.



1 Шифрование с использованием логичного шифра без применения вектора инициализации



2 Шифрование с использованием логичного шифра и вектора инициализации

Рис. 4.4. Шифрование и векторы инициализации

## Режимы с обратной связью

Режимы с обратной связью представляют собой модификации процесса шифрования, разработанные во избежание того, чтобы один и тот же открытый текст преобразовывался в ходе шифрования в одинаковый зашифрованный текст. Режимы с обратной связью обсуждаются далее в данной главе.

## Кодирование по стандарту 802.11

Спецификация стандарта 802.11 предусматривает обеспечение защиты данных с использованием алгоритма WEP. Этот алгоритм основан на применении симметрич-

видом потока цифра RC4. Симметричность RC4 означает, что согласованные WEP-ключи размером 40 или 104 байт заранее конфигурируются на клиентских устройствах и в точках доступа. Алгоритм WEP был выбран главным образом потому, что он не требует обмена ключами. Хотя персональные компьютеры с беспроводными сетевыми картами стандарта 802.11 сейчас широко распространены, в 1997 году ситуация была иной. Большинство из устройств, включаемых в беспроводные LAN, составляли специализированные устройства (application specific devices, ASD). Примерами таких устройств могут служить считыватели штрих-кодов, планшетные ПК (tablet PC) и телефоны стандарта 802.11. Приложения, которые выполнялись этими специализированными устройствами, обычно не требовали большой вычислительной мощности, поэтому ASD оснащались слабыми процессорами. WEP — простой и привлекательный алгоритм, для запуска которого в некоторых случаях достаточно 30 строк кода. Малые производственные расходы, возникающие при применении этого алгоритма, делают его идеальным алгоритмом шифрования для специализированных устройств.

Чтобы избежать дешифрования в режиме ECB, WEP использует 24-разрядный вектор инициализации, который добавляется к ключу перед выполнением обработки по алгоритму RC4. На рис. 4.5 показан фрейм, зашифрованный по алгоритму WEP с использованием вектора инициализации.

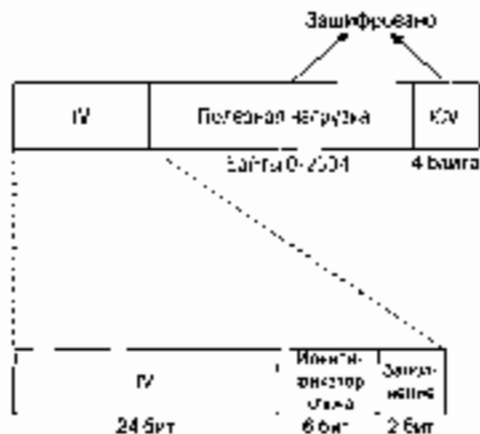


Рис. 4.5. Фрейм, зашифрованный по алгоритму WEP

Вектор инициализации должен изменяться пофреймово по инициализации IV-ключами. Коллизии такого рода происходят, когда используются один и тот же вектор инициализации и один и тот же WEP-ключ, в результате чего для шифрования фрейма используется один и тот же ключевой поток. Такая коллизия представляет двумерным пользователям большие возможности по разгадыванию данных открытого текста путем сопоставления гербибых элементов. При инициализации вектора инициализации можно предотвратить головный сюрприз, поэтому вектор инициализации часто меняют. Большинство производителей предлагают пофреймовые векторы инициализации в своих устройствах для беспроводных LAN.

Спецификация стандарта 802.11 требует, чтобы одинаковые WEP-ключи были сконфигурированы как на клиентах, так и на устройствах, образующих инфраструктуру сети. Можно определять до четырех ключей на одно устройство, но одновременно для шифрования отправляемых фреймов используется только один из них.

На рис. 4.6 показано окно клиента сети Cisco Aironet, предназначенное для конфигурирования WEP.

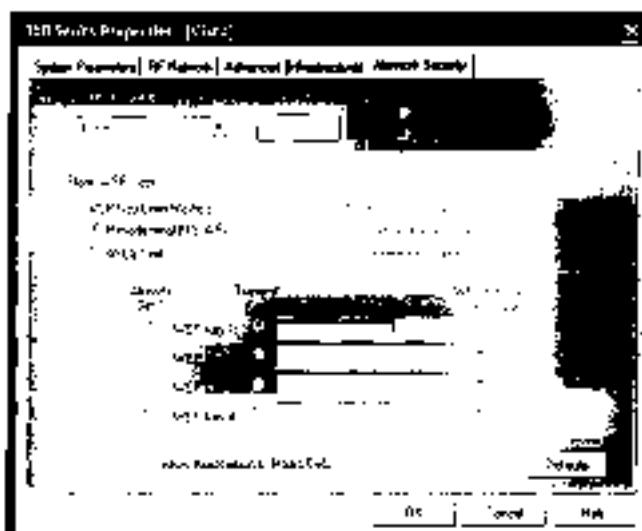


Рис. 4.6. Конфигурирование WEP

WEP-шифрование используется только по отношению к фреймам данных и во время процедуры аутентификации с совместно используемым ключом. По алгоритму WEP шифруются следующие поля фрейма данных стандарта 802.11:

- Данные или полезная нагрузка (payload).
- Контрольный признак целостности (integrity check value, ICV)

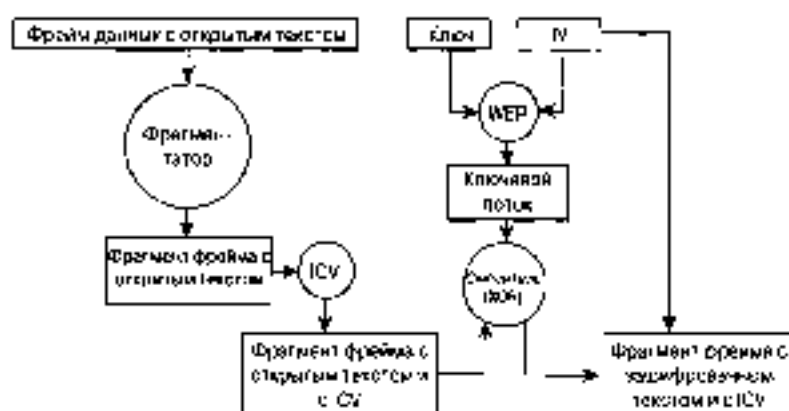
Значения всех остальных полей передаются без шифрования. Вектор инициализации должен быть послан незашифрованным внутри фрейма, чтобы приемная станция могла получить его и использовать для корректной расшифровки полезной нагрузки и ICV. На рис. 4.7 схематично представлен процесс шифрования, передачи, приема и расшифровки фрейма данных в соответствии с алгоритмом WEP.

В дополнение к шифрованию данных спецификация стандарта 802.11 предлагает использовать 32-разрядное значение, функция которого — осуществлять контроль целостности. Этот контрольный признак целостности говорит приемнику о том, что фрейм был получен без повреждения в процессе передачи. Он усиливает действие контрольных последовательностей фрейма (FCS) уровней 1 и 2, назначение которых — выявлять возникающие в процессе передачи ошибки.

Контрольный признак целостности вычисляется по всем полям фрейма с использованием 32-разрядной полиномиальной функции контроля и с помощью избыточного кода (CRC-32). Станция-отправитель вычисляет это значение и помещает результат в поле ICV. Значение поля ICV включается в часть фрейма, шифруемую по алгоритму WEP, так что его не могут просто так "увидеть" злоумышленники. Получатель фрейма дешифрует его, вычисляет значение ICV и сравнивает результат со значением поля ICV полученного фрейма. Если эти значения совпадают, фрейм считается подлинным, неподдельным. Если они не совпадают, такой фрейм отбрасывается. На рис. 4.8 представлена диаграмма функционирования механизма ICV.



### Процесс шифрования



### Процесс дешифрования

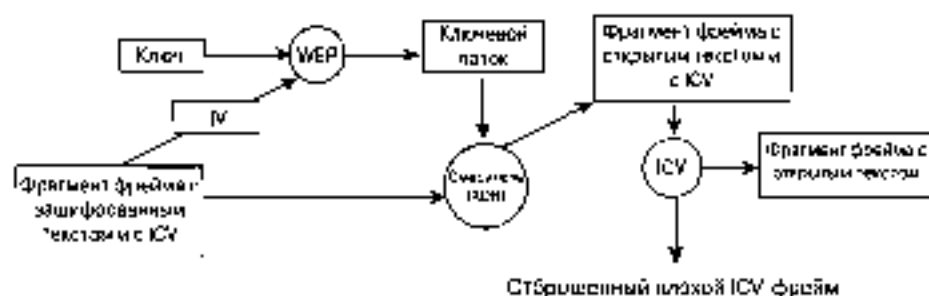


Рис. 4.7. Процесс шифрования и дешифрования

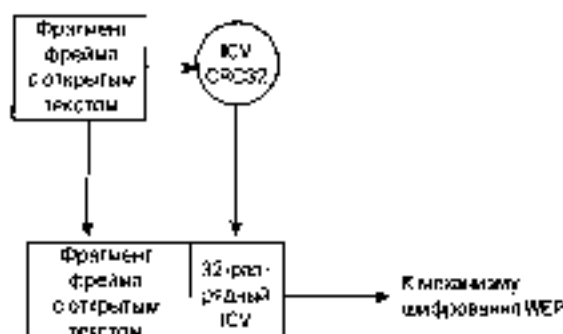


Рис. 4.8. Двухэтапная функционализация механизма ICV

## Механизмы аутентификации стандарта 802.11

Стандартизация стандарта 802.11 оговаривает два механизма, которые могут применяться для аутентификации клиентов WLAN.

- Открытая аутентификация (open authentication).
- Аутентификация с совместно используемым ключом (shared key authentication).

Открытая аутентификация по сути представляет собой алгоритм с нулевыми аутентифицирующей (null authentication algorithm). Точка доступа принимает любой запрос на аутентификацию. Это может быть просто бессмысленный сигнал, используемый для указания на применение именно этого алгоритма аутентификации, тем не менее открытая аутентификация играет определенную роль в сетях стандарта 802.11. Столь простые требования к аутентификации позволяют устройствам быстро получить доступ к сети.

Контроль доступа при открытой аутентификации осуществляется с использованием заранее сконфигурированного WEP-ключа в точке доступа и на клиентской станции. Эта станция и точка доступа должны иметь одинаковые ключи, тогда они могут связываться между собой. Если станция и точка доступа не поддерживают алгоритм WEP, в BSS невозможно обеспечить защиту. Любое устройство может подключиться к такому BSS, и все фреймы данных передаются незашифрованными.

После выполнения открытой аутентификации и завершения процесса ассоциирования клиент может начать передачу и прием данных. Если клиент сконфигурирован так, что его ключ отличается от ключа точки доступа, он не сможет правильно зашифровать и расшифровывать фреймы, и такие фреймы будут сброшены как точкой доступа, так и клиентской станцией. Этот процесс представляет собой довольно-таки эффективное средство контроля доступа к BSS (рис. 4.9).

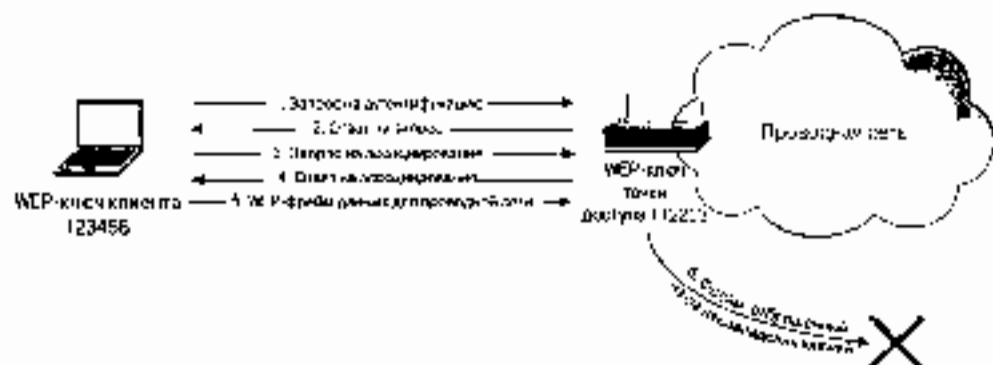


Рис. 4.9. Процесс открытой аутентификации при различии WEP-ключей

В отличие от открытой аутентификации, при аутентификации с совместно используемым ключом требуется, чтобы клиентская станция и точка доступа были способны поддерживать WEP и имели одинаковые WEP-ключи. Процесс аутентификации с совместно используемым ключом осуществляется следующим образом.

1. Клиент посылает точке доступа запрос на аутентификацию с совместно используемым ключом.
2. Точка доступа отвечает фреймом вызова (challenge frame), содержащим открытый текст.
3. Клиент шифрует вызов и посылает его обратно точке доступа.
4. Если точка доступа может правильно расшифровать этот фрейм и получить свой исходный текст, клиенту посылается сообщение об успешной аутентификации.
5. Клиент получает доступ к WLAN.

Предпосылки, на которых основана аутентификация с совместно используемым ключом, точно такие же, как и те, которые предполагались при открытой аутентификации, использующей WEP-ключи в качестве средства контроля доступа. Разница между этими двумя схемами состоит в том, что клиент не может ассоциировать себя с точкой доступа при использовании механизма аутентификации с совместно используемым ключом, если его ключ не сконфигурирован должным образом. На рис. 4.10 схематично представлен процесс аутентификации с совместно используемым ключом.

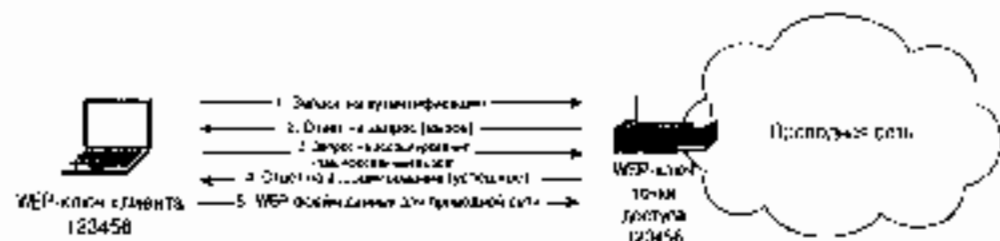


Рис. 4.10. Процесс аутентификации с совместно используемым ключом

## Аутентификация с использованием MAC-адресов

Аутентификация с использованием MAC-адресов не специфицирована стандартом 802.11, но обеспечивается многими производителями. В ходе аутентификации с использованием MAC-адресов проверяется соответствие MAC-адреса клиента локально сконфигурированному списку разрешенных адресов или списку, хранящемуся на клиенте аутентификационного сервере (рис. 4.11). Аутентификация с использованием MAC-адресов усиливает действие открытой аутентификации и аутентификации с совместно используемым ключом, обеспечиваемыми стандартом 802.11, дополнительно снижая тем самым вероятность того, что неавторизованные устройства получат доступ к сети. Например, администратор сети может надеяться ограничить доступ к определенной точке доступа для трех конкретных устройств. Если все станции и все точки доступа BSS используют одинаковые WEP-ключи, при использовании открытой аутентификации и аутентификации с совместно используемым ключом такой сценарий реализовать трудно. Чтобы усилить действие механизма аутентификации стандарта 802.11, он может применить аутентификацию с использованием MAC-адресов.



Рис. 4.11. Процесс аутентификации с использованием MAC-адресов

## Уязвимость системы защиты стандарта 802.11

В предыдущем разделе рассказывалось о том, как осуществляется аутентификация и шифрование при использовании устройств стандарта 802.11. Не секрет, что система защиты, специфицированная в стандарте 802.11, несовершенна. Вскоре после утверждения стандарта 802.11 появились статьи, в которых указывались слабые места механизма аутентификации стандарта 802.11 и шифрования по алгоритму WEP.

### Уязвимость открытой аутентификации

При использовании механизма открытой аутентификации точка доступа не имеет возможности проверить правомочность клиента. Отсутствие такой возможности является недостатком системы защиты, если в беспроводной локальной сети не используется WEP-шифрование. Даже при использовании и клиентом, и точкой доступа стандартного WEP механизм открытой аутентификации не предоставляет средств для определения того, кто использует устройство WLAN. Авторизованное устройство в руках неавторизованного пользователя — это угроза безопасности, равносильная полному отсутствию какой-либо защиты сети.

### Уязвимость аутентификации с совместно используемым ключом

В случае аутентификации с совместно используемым ключом необходимо, чтобы клиент использовал заранее выделенный для совместного использования ключ и зашифровал текст запроса, полученного от точки доступа. Точка доступа аутентифицирует клиента путем расшифровки зашифрованного с помощью совместно используемого ключа ответа и проверки того, что полученный текст вклада полностью соответствует отправленному.

Процесс обмена текстом вызова осуществляется по беспроводному каналу связи и является уязвимым для атаки, возможной при передаче открытого текста. Эта уязвимость в случае аутентификации с совместно используемым ключом обусловлена математическими методами, лежащими в основе шифрования. Ранее в этой главе говорилось о том, что процесс кодирования текста и перемещения открытого текста с ключевым потоком и получения в результате зашифрованного текста. Процесс дешифрирования представляет собой выполнение двоичной математической операции, которая называется "исключающее ИЛИ" (XOR). Если открытый текст перемещать с соответствующим зашифрованным текстом, в результате выполнения этой операции будет получена следующая пара ключевой поток, используемый для WEP-ключа, и вектор инициализации (рис. 4.12).

Дополнительник может захватить как открытый, так и зашифрованный текст ответа. Выполнив над ними значениями операцию "исключающее ИЛИ", он может получить действующий ключевой поток. Затем домысленник может использовать этот ключевой поток для расшифровки фреймов, имеющих такой же размер, как и ключевой поток, поскольку вектор инициализации, используемый для получения ключевого потока, такой же, как и у расшифрованного фрейма. На рис. 4.13 показано, как ата-

хуже, если сеть злоумышленник может проследить процесс аутентификации с помощью используемых ключей и заполнить клиентской эллипс

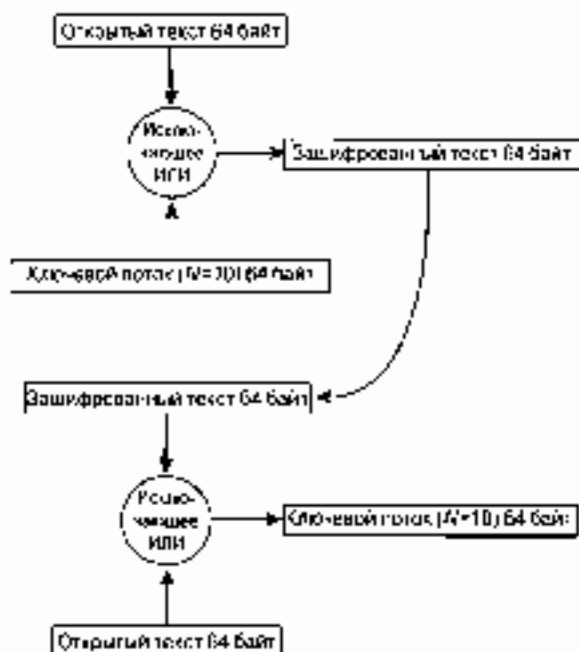


Рис. 4.12. Использование ключевого потока

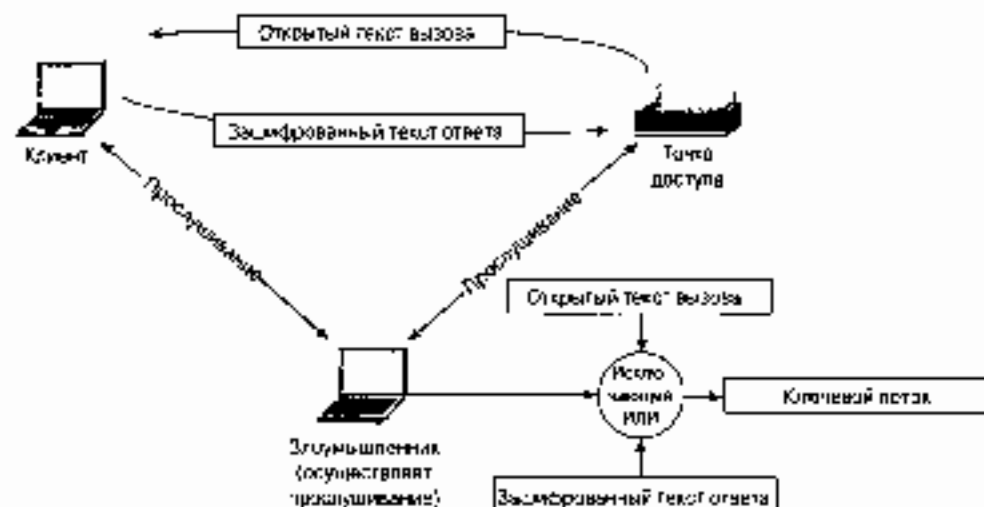


Рис. 4.13. Использование метода MITM для аутентификации с помощью беспроводных ключей

## Уязвимость аутентификации с использованием MAC-адресов

MAC-адреса пересылаются с помощью нешифрованных фреймов стандарта 802.11, как и оговорено в спецификации этого стандарта. В результате беспроводные LAN, в которых применяется аутентификация с использованием MAC-адресов, уязвимы для атак, в ходе которых злоумышленник “подкапывается” под аутентификацию с использованием MAC-адресов путем имитации “законного” MAC-адреса.

Имитация MAC-адреса возможна для сетевых карт стандарта 802.11, которые позволяют заменять универсально-назначаемый адрес (universally administered address, UAA) локально-назначаемым (locally administered address, LAA). Универсальный адрес — это MAC-адрес, жестко закодированный для сетевой карты производителем. Адапционер может переопределить адапционер Препроцессора для определения разрешенности в BSS MAC-адреса и сетевую карту, допускающую локальное назначение адреса, для считывания разрешенного MAC-адреса.

## Уязвимость WEP-шифрования

Наиболее серьезные и непреодолимые проблемы защиты сетей стандарта 802.11 были выявлены криптоаналитиками Флурером (Fluhrer), Маннингом (Mantin) и Шамиром (Shamir). В своей статье они показали, что WEP-ключ может быть получен путем пассивного наблюдения отдельных фреймов, распространяющихся в беспроводной LAN.

Уязвимость обусловлена как раз тем, как механизм WEP применяет алгоритм составления ключа (key scheduling algorithm, KSA) на основе поточного шифра RC4. Часть векторов инициализации (их называют слабым IV - weak IV) могут раскрыть биты ключа в результате проведения статистического анализа. Исследователи компании AT&T и университета Rice, а также разработчики приложения AirSnort весьма успешно этой уязвимости и выяснили, что можно заполучить WEP-ключи длиной 40 или 104 бита после обработки 4 миллионов фреймов. Для первых беспроводных LAN стандарта 802.11b это означает, что они должны передавать фреймы примерно один час, после чего можно вывести 104-разрядный WEP-ключ. Подобная уязвимость делает WEP неэффективным механизмом обеспечения защиты информации.

Атака считается пассивной, если атакующий просто прослушивает BSS и накапливает передаваемые фреймы. В отличие от уязвимости аутентификации с совместно используемым ключом, атакующий, как показали Флурер, Мантин и Шамир, может получить действующий WEP-ключ, а не только ключевой поток. Эта информация позволяет атакующему получить доступ к BSS в качестве аутентифицированного устройства без ведома администратора сети.

Если атака такого типа окажется недостаточной, можно, как показывает теория, перейти на механизм WEP и другую (правда, на практике атаки такого рода не проявлялись). Эта логически возможная атака может быть основана на методах, применяемых для преодоления защиты, обеспечиваемой механизмом аутентификации с совместно используемым ключом: для получения ключевого потока используются открытый текст и соответствующий ему зашифрованный текст.

Как уже говорилось, выведенный ключевой поток можно использовать для дешифровки фреймов для пары “вектор инициализации — WEP-ключ” и для определения длины. Умозрительно можно предположить, что атакующий будет прослушивать сеть с целью накопления как можно большего числа таких ключевых потоков, чтобы создать

базу данных клиент-сервер, изменить сеть и получить возможность расшифровать фреймы. В беспроводной LAN, в которой не используется аутентификация с совместным секретным ключом, атака с применением побитовой обработки фрейма позволяет злоумышленнику вывести большое количество ключевых данных за короткое время.

Атаки с использованием побитовой обработки (или "жонглирование битами", bit flipping) основаны на уязвимости криптоалгоритма признака целостности (ICV). Данный механизм базируется на полиномиальной функции CRC-32. Но эта функция неэффективна как средство контроля целостности сообщения. Математические свойства функции CRC-32 позволяют подделать фрейм и модифицировать значение ICV, даже если исходное содержимое фрейма неизвестно.

Хотя размер полезных данных может быть разным для различных фреймов, многие элементы фреймов данных стандарта 802.11 остаются одними и теми же и на одних и тех же позициях. Атакующий может использовать этот факт и подделать часть фрейма с полезной информацией, чтобы модифицировать пакет более высокого уровня. Сценарий проведения атаки с использованием побитовой обработки может быть следующим (рис. 4.14).

1. Атакующий захватывает фрейм беспроводной LAN.
2. Атакующий изменяет случайные биты (flips packet bits) полезной нагрузки фрейма.
3. Атакующий модифицирует ICV (подробнее об этом — ниже).
4. Атакующий передает модифицированный фрейм.
5. Приемник (клиент или точка доступа) получает фрейм и вычисляет ICV по содержимому фрейма.
6. Приемник сравнивает вычисленный ICV со значением, хранящимся в поле ICV фрейма.
7. Приемник принимает модифицированный фрейм.
8. Приемник передает модифицированный фрейм на устройстве более высокого уровня (повторитель или дост-компьютер).
9. Поскольку в пакете уровня 3 биты изменены, контрольная сумма для уровня 3 оказывается неправильной.
10. Протокол IP приемника выдает сообщение об ошибке.
11. Атакующий получает сведения о беспроводной LAN, анализируя незашифрованное сообщение об ошибке.
12. Получая сообщение об ошибке, атакующий выводит ключевой поток, как в случае атаки с повторением IV.

Основой такой атаки является несоответствие ICV требуемому значению. Значение ICV зашифровано с помощью WEP части фрейма; как атакующий может изменить ее, чтобы согласовать изменения, вызванные жонглированием битов, с фреймом? На рис. 4.15 проиллюстрирован процесс "жонглирования битами" и изменения ICV.

1. Пусть фрейм (F1) имеет ICV, значение которого равно C1.
2. Генерируется новый фрейм (F2) той же длины, какую имеет набор битов фрейма F1.

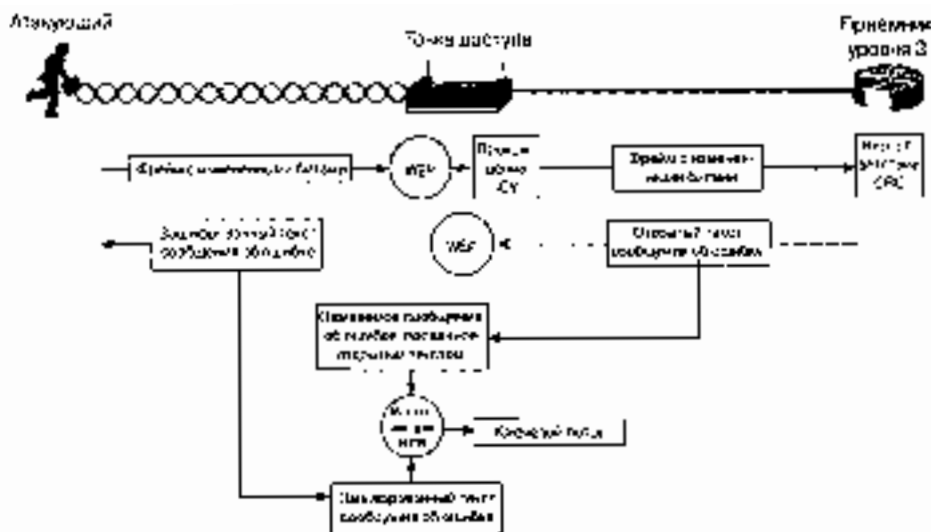


Рис. 4.14. Атака с использованием модифицированной обработки

3. С помощью операции "исключающее ИЛИ" над  $F1$  и  $F2$  создается фрейм  $F3$ .
4. Вычисляется ИСВ для  $F3$  ( $C2$ ).
5. посредством операции "исключающее ИЛИ" над  $C1$  и  $C2$  генерируется ИСВ  $C3$ .

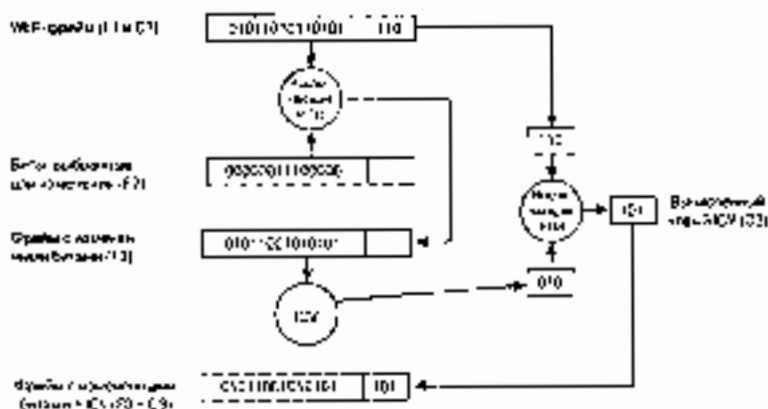


Рис. 4.15. Модифицирование ИСВ по счет выбранных битов

## Проблемы управления статическими WEP-ключами

В спецификации стандарта 802.11 не указан конкретный механизм управления ключами. WEP по определению поддерживает только статические ключи, заранее предназначенные для совместного использования. Поскольку в процессе аутентификации по стандарту 802.11 аутентифицируется устройство, а не пользователь этого устройства, утеря или кража беспроводного адаптера немедленно приводит к имитации



повлечению проблем, связанных с защитой сети. Для ее решения администратору сети придется долго вручную изменить ключи всех беспроводных устройств сети, если исключаются ключи «эквивалентности» из-за утери или кражи адаптера.

Такой риск может оказаться приемлемым для небольших сетей, когда управление пользовательскими устройствами — несложная задача. Но подобная перспектива неприемлема для крупных сетей, куда счет беспроводных подкапитальных устройств идет на тысячи. Без механизма распределения или генерации ключей администратору придется доезжать и починять там, где развернута беспроводная сеть.

## Защищенные LAN стандарта 802.11

Промышленность преодолела слабые места в механизмах аутентификации и защиты сетей стандарта 802.11. Чтобы поддерживать полномочиям решения, обеспечивающие защищенность, масштабируемость и управляемость сетей, IEEE повисил защищенность сетей стандарта 802.11, радиобезопасный механизм аутентификации и шифрования. Эти изменения были введены в проект стандарта 802.11i. На сегодняшний день проект 802.11i не утвержден как стандарт, поэтому Альянс Wi-Fi (Wi-Fi Alliance) собрал набор компонентов, соответствующих стандарту 802.11i, который получил название «защищенный доступ к Wi-Fi» (Wi-Fi Protected Access, WPA). В данном разделе подробно описаны стандарт 802.11i и компоненты WPA.

Хотя до сих пор в этой главе рассматривались в первую очередь детали стандарта 802.11, а также совместного использования WEP-шифрования и аутентификации — открытой сети с совместно используемым ключом, — многие эксперты полагают, что WEP — это единственный компонент, обеспечивающий защиту беспроводных LAN. На самом деле защита беспроводных сетей имеет четыре составляющие.

- **Базовая аутентификация (authentication framework).** Представляет собой механизм, который использует легитимные алгоритмы аутентификации путем организации защищенного обмена сообщениями между клиентом, точкой доступа и сервером аутентификации.
- **Алгоритм аутентификации.** Представляет собой алгоритм, посредством которого подтверждается полномочия пользователя.
- **Алгоритм защиты данных.** Обеспечивает защиту при передаче через беспроводную среду фрейма данных.
- **Алгоритм обеспечения целостности данных (data integrity algorithm).** Обеспечивает целостность данных при передаче их через беспроводную среду, позволяя приемнику убедиться в том, что данные не были изменены.

Названные четыре составляющие показаны на рис. 4.16.

### Первая составляющая: базовая аутентификация

Основной аутентификации стандарт 802.11 является служебный фрейм аутентификации стандарта 802.11. Этот служебный фрейм позволяет реализовать алгоритмы открытой аутентификации и аутентификации с совместно используемым ключом, хотя сам по себе фрейм не обладает способностью аутентифицировать контент. Поскольку о деталях аутентификации стандарта 802.11 мы уже говорили, попробуем разобраться в том, что необходимо сделать для того, чтобы обеспечить проведение защищенной аутентификации в беспроводных LAN.



Рис. 4.16. Четыре составляющие системы защиты беспроводных сетей

В стандарте 802.11 не определены основные компоненты, способные обеспечить эффективную аутентификацию (они перечислены ниже):

- Централизованная аутентификация, ориентированная на пользователя
- Динамично шифруемые ключи
- Управление зашифрованными ключами.
- Взаимная аутентификация.

Аутентификация, ориентированная на пользователя, чрезвычайно важна для обеспечения защиты сети. Аутентификация, ориентированная на устройство, подобная открытой аутентификации и аутентификации с совместно используемым ключом, не способна предоставлять независимым пользователям воспользоваться авторизованным устройством. Из этого следует, что при потере или краже такого устройства для прекращения работы по найму администратор сети будет вынужден вручную изменить ключи всех точек доступа и клиентов сети стандарта 802.11. При централизованном, ориентированном на пользователя управлении через сервер аутентификации, авторизации и учета (authentication, authorization, and accounting, AAA), такой как RADIUS, администратор может запретить доступ к сети отдельным пользователям, а не их устройствам.

Требование проводить аутентификацию, ориентированную на пользователя, имеет положительный побочный эффект: наличие отдельных ключей шифрования для каждого пользователя. Различия аутентификации, которые поддерживают создание динамических ключей шифрования, хорошо подходят для улучшения защиты беспроводных LAN и модели управления ими. Динамические ключи, индивидуальные для каждого пользователя, освобождают администратора сети от необходимости использования статически управляемых ключей. Ключи шифрования динамически создаются и аннулируются, когда пользователь проходит процедуру аутентификации или выходит из сети. Для того чтобы удалить какого-либо пользователя из сети, достаточно аннулировать его учетную запись и он потеряет возможность доступа к сети.

Взаимная аутентификация — это аутентификация двухсторонняя. Ее "двухсторонняя" природа обусловлена тем, что не только сеть аутентифицирует клиента, но и клиент аутентифицирует сеть. При открытой аутентификации и аутентификации с совместно исполь-

здесь ключом точка доступа или сеть аутентифицирует клиента. Пользователь не знает ни адреса, ни идентифицирующую информацию к той сети, к какой нужно, поскольку в стандарте 802.11 не предусмотрен механизм позволяющий клиенту аутентифицировать сеть. В результате принадлежащая злоумышленнику точка доступа или клиентская машина может выдавать себя за "экономную" точку доступа и посылать данные на клиентской машине. На рис. 4.17 представлены диаграммы, иллюстрирующие процессы односторонней и взаимной аутентификации.

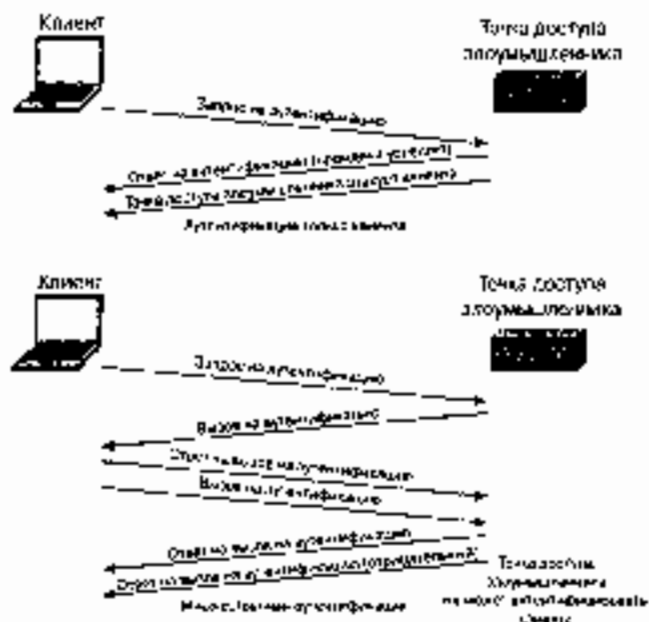


Рис. 4.17. Односторонняя и взаимная аутентификация

Постановщики сетей стандарта 802.11 в IEEE осознают необходимость усиления и замены существующих механизмов обеспечения логина — и аутентификации, и шифрования. Исследовательская группа рабочей группы стандарта 802.11 сейчас работает над этим, и в виде того как изменения будут полностью подготовлены, спецификации по защите будут утверждены как спецификации стандарта 802.11i.

IEEE начал борьбу с дефектами механизма аутентификации стандарта 802.11 с помощью базовой аутентификации, соответствующей стандарту 802.1X. Стандарт 802.1X представляет собой стандарт IEEE, который относится ко всем топологиям канального уровня серии стандартов 802 и позволяет извлекать его механизмы аутентификации до тех пор, обычно реализуемых на более высоких уровнях. Стандарт 802.1X основан на принципах аутентификации, характерных для протокола типа "точка-точка" (Point-to-Point Protocol, PPP), и называется расширенным протоколом аутентификации (Extensible Authentication Protocol, EAP). Подпросту говоря, стандарт 802.1X инкапсулирует сообщения для использования их на уровне 2. Стандарт 802.11i включает базовую аутентификацию стандарта 802.1X, чтобы она применялась для аутентификации пользователей. На рис. 4.18 представлен стандарт 802.1X в части алгоритма аутентификации и топологии канального уровня серии стандартов 802.

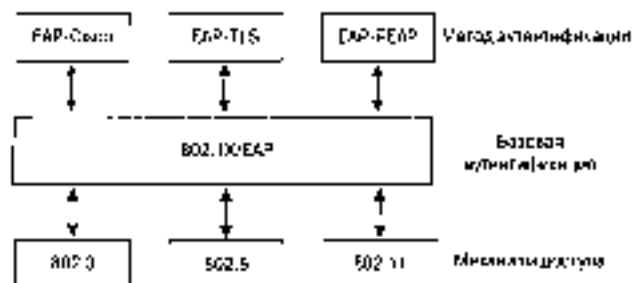


Рис. 4.18. Стандарт 802.1X и реализация клиентского уровня

Протокол EAP (RFC 2284) и стандарт 802.1X не регламентируют использование любого алгоритма аутентификации. Администратор сети может применить соответствующую протоколу EAP разновидность аутентификации — для 802.1X, или EAP Единственное требование — чтобы как клиент стандарта 802.11 (здесь он называется *supplicant*), так и сервер аутентификации поддерживали алгоритм EAP-аутентификации. Такая открытая и расширяемая архитектура позволяет использовать любую аутентификацию в различных условиях, и в каждой ситуации можно применить подходящую разновидность аутентификации.

Ниже приведены примеры типов EAP-аутентификации.

- **EAP защиты транспортного уровня (EAP-transport layer security, EAP-PEAP).** Работает аналогично протоколу защищенных сокетов (secure sockets layer, SSL). Взаимная аутентификация выполняется с использованием цифровых сертификатов на стороне сервера для создания SSL-туннеля для клиента, осуществляющего защищенную аутентификацию в сети.
- **EAP-Message Digest 5 (EAP-MD5).** Аналогично протоколу аутентификации с предварительным согласованием вызова (challenge handshake authentication protocol, CHAP). EAP-MD5 обеспечивает работу алгоритма односторонней аутентификации с использованием пароля.
- **EAP-Sync EAP-аутентификация типа EAP-Cisco,** которую называют также LEAP, была первой, определенной для применения специально в беспроводной LAN. EAP-Cisco — это алгоритм взаимной аутентификации с использованием пароля.

Аутентификация по стандарту 802.1X требует наличия трех составляющих:

- **Проститель.** Размещается на стороне клиента беспроводной LAN.
- **Аутентификатор (authenticator).** Размещается в точке доступа.
- **Сервер аутентификации.** Размещается на сервере RADIUS.

Эти составляющие представляют собой программные компоненты, устанавливаемые на устройствах сети. С точки зрения стандарта 802.11 аутентификатор создает логический порт для устройства клиента, основанный на идентификаторе ассоциации (AID). Этот логический порт имеет два тракта прохождения данных: неконтролируемый и контролируемый. Неконтролируемый тракт прохождения данных позволяет проходить через сеть всему трафику аутентификации стандарта 802.1X. Контролируемый тракт прохождения данных блокирует обычный трафик сети до тех пор, пока не будет осуществлена успешная аутентификация клиента. На рис. 4.19 показаны логические порты аутентификатора стандарта 802.1X.

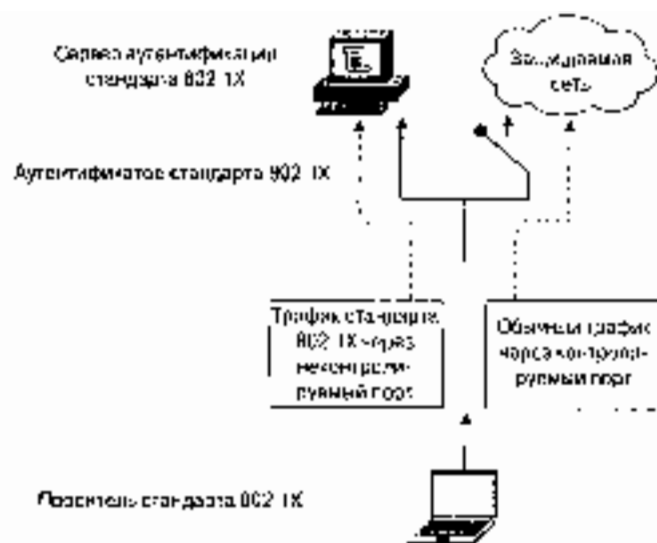


Рис. 4.19. Логические порты аутентификатора стандарта 802.1X

Обмен сообщениями по стандарту 802.1X зависит от алгоритма аутентификации, но в общем случае он осуществляется следующим образом.

1. Клиент-присоединитель становится активным и ассоциируется с аутентификатором точки доступа.
2. Аутентификатор обнаруживает ассоциацию клиента и предоставляет порт пропителя. Он переводит порт в псевдоориентированное состояние, так что пересылается только трафик стандарта 802.1X. Остальной трафик блокируется.
3. Клиент может послать сообщение EAP-Start, хотя инициация клиента не требуется. На рис. 4.20 представлены алгоритмы обмена сообщениями по стандарту 802.1X.
4. Аутентификатор отвечает сообщением с EAP-запросом на идентификацию (EAP-Request (Identify)) клиенту, чтобы удостовериться в идентичности клиента.
5. На сервер аутентификации отправляется пакет EAP-ответа (EAP-Response), содержащий идентификационные данные клиента. Объем ответа на идентификацию зависит от политики от типа CAP, но в общем случае посылается только имя пользователя или его эквивалент, а не какая-либо форма смещенно используемого "секрета", такого как пароль.
6. Сервер аутентификации может быть сконфигурирован так, что он будет аутентифицировать клиентов по особому алгоритму. Но в настоящее время стандарт 802.1X для сетей стандарта 802.11 не регламентирует применение любого алгоритма.
7. В зависимости от регламентированного результата обмена, зависящего от алгоритма аутентификации CAP, последним ориентированном в стандарте 802.1X сообщением может быть пакет RADIUS-ACCEPT или RADIUS-REJECT, направленный от сервера аутентификации к точке доступа.
8. Получив пакет ACCEPT, аутентификатор переводит порт клиента в состояние "авторизован", и через него может идти трафик.

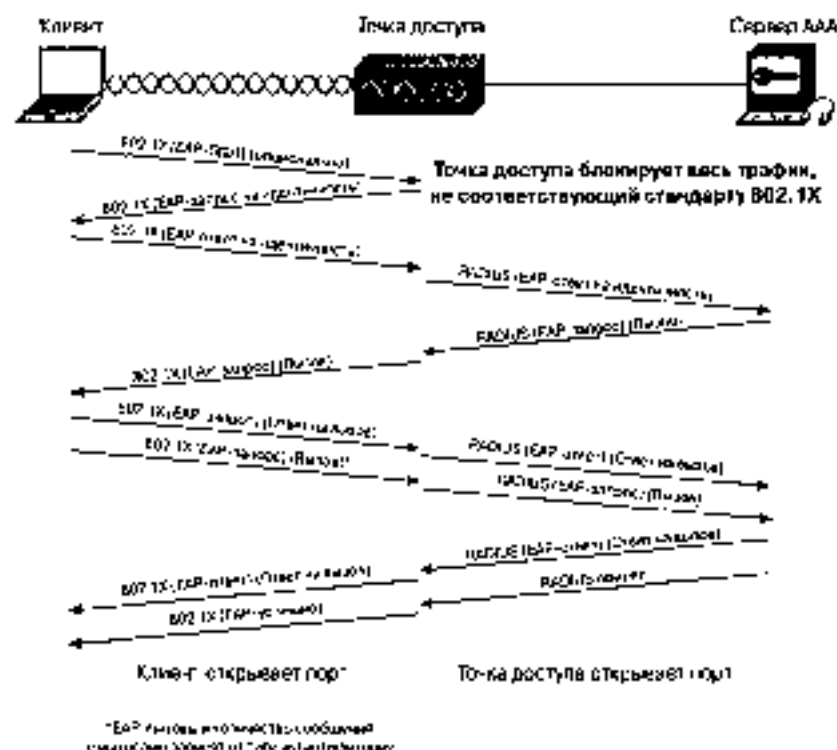


Рис. 4.20. Обмен сообщениями в соответствии со стандартом 802.1X

Стандарт 802.1X не специфицирует и не регламентирует какой-либо конкретный алгоритм аутентификации.

## Вторая составляющая: алгоритм аутентификации

Стандарт 802.11i и WPA обеспечивают механизм, поддерживающий работу алгоритма аутентификации с целью обеспечения связи между клиентом, точкой доступа и сервером аутентификации с использованием механизма базового аутентификации стандарта 802.1X. Ни стандарт 802.11i, ни WPA не регламентируют применение какого-либо алгоритма аутентификации, но оба рекомендуют использовать алгоритм, который поддерживает быструю аутентификацию, генерацию динамических ключей шифрования и аутентификацию пользователя. На рис. 4.21 представлены сообщения, которыми взаимодействуют клиент, точка доступа и AAA-сервер, но быстрее разобраться в этом процессе поможет конкретный пример. В данном разделе рассматривается работа алгоритма EAP-Sisco. Этот алгоритм, более известный как Cisco LEAP, представляет собой простой и эффективный алгоритм, разработанный специально для использования в беспроводных LAN.

На рис. 4.21 проиллюстрирована работа EAP-Sisco. В последующей последовательности выполняемых действий подробно описывается каждая транзакция.

1. Клиент получает возможность доступа к среде и посылает точке доступа сообщение EAP-Start, инициализирующее по стандарту 802.1X.
2. Точка доступа блокирует клиентский порт, позволяя передавать по сети только трафик стандарта 802.1X.

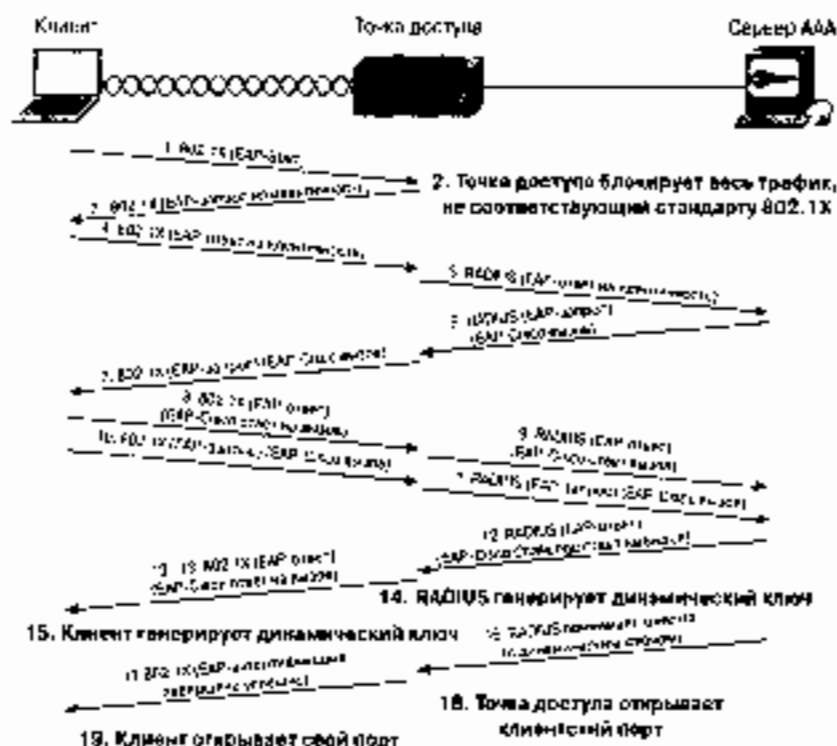


Рис. 4.21. Процесс аутентификации в соответствии с алгоритмом EAP-Success

- Точка доступа посылает клиенту сообщение с EAP-запросом на идентификацию (EAP Request Identity), инкапсулированным по стандарту 802.1X
- Клиент отвечает EAP-ответом (EAP-Response), инкапсулированным по стандарту 802.1X и содержащим пользовательское имя клиента.
- Точка доступа перенаправляет эти пользовательские имя, инкапсулированное в пакет запроса к серверу RADIUS на доступ (RADIUS ACCESS-REQUEST), на сервер аутентификации.
- Сервер RADIUS создает соответствующее алгоритму EAP-Success сообщение с вызовом (challenge message) и посылает его, инкапсулированное в пакет ответа сервера RADIUS на просьбу доступа (RADIUS ACCESS-RESPONSE), клиенту (через точку доступа).
- Точка доступа перенаправляет вызов EAP-Success клиенту, инкапсулированный во фрейм стандарта 802.1X.
- Клиент обрабатывает вызов в соответствии с алгоритмом EAP-Success и посылает ответ на вызов обратно серверу RADIUS через точку доступа.
- Точка доступа инкапсулирует ответ на вызов в пакет запроса к серверу RADIUS на доступ (RADIUS ACCESS REQUEST) и перенаправляет его на сервер RADIUS.
- Клиент посылает вызов в соответствии с алгоритмом EAP-Success на сервер RADIUS (через точку доступа), чтобы аутентифицировать сеть. Этот вызов инкапсулируется во фрейм стандарта 802.1X.

11. Точка доступа инкапсулирует вызов EAP-Cisco в пакет ответа серверу RADIUS на просьбу доступа (RADIUS ACCESS-RESPONSE).
12. Сервер RADIUS посылает ответ на вызов в соответствии с алгоритмом EAP-Cisco обратно клиенту (через точку доступа), инкапсулированный в пакет ответа сервера RADIUS на просьбу доступа (RADIUS ACCESS-RESPONSE).
13. Точка доступа инкапсулирует ответ на вызов EAP-Cisco во фрейм стандарта 802.1X и посылает его клиенту.
14. Сервер RADIUS генерирует динамический ключ шифрования (dynamic encryption key) на основе пароля пользователя и некоторой специфической для сессии обмена информацией.
15. Клиент генерирует такой же динамический ключ шифрования. Клиент способен локально генерировать такой же динамический ключ шифрования, поскольку он имеет доступ к той же самой информации.
16. Сервер RADIUS посылает этот ключ точке доступа, инкапсулированный в пакет RADIUS ACCEPT (принят сервером RADIUS). Пакет RADIUS ACCEPT указывает точке доступа, что процесс аутентификации завершился успешно.
17. Точка доступа устанавливает динамический ключ для данного клиента, инкапсулирует сообщение "EAP-аутентификация завершена успешно" (EAP-Success) во фрейм стандарта 802.1X и отправляет это сообщение клиенту.
18. Точка доступа переводит клиентский порт в состояние, допускающее перенаправление трафика.
19. Клиент открывает свой порт (при условии успеха завершения множественной аутентификации).

Алгоритм EAP-Cisco является патентованным алгоритмом, который работает поверх алгоритма базовой открытой аутентификации. По этой причине детали алгоритма EAP-Cisco, касающиеся содержимого генерируемых вызова и ответа на вызов, а также распределения ключей шифрования, не могут быть разглашены. Алгоритм EAP-Cisco превосполняет требования, предъявляемые к защищенной аутентификации пользователя в беспроводной LAN, за счет применения следующих мер:

- Аутентификация, ориентированная на пользователя.
- Взаимная аутентификация.
- Динамические ключи шифрования.

Если какому-либо пользователю нужно запретить доступ к сети, достаточно удалить его учетную запись на централизованном сервере аутентификации. В результате пользователь не сможет успешно пройти процесс аутентификации, а его устройство — сгенерировать правильную динамический ключ шифрования.

## Третья составляющая: алгоритм защиты данных

Уязвимость шифрования в WEP поставила производителей сетей стандарта 802.11 в исходной версии IEEE в затруднительное положение. Как можно улучшить систему шифрования стандарта 802.11, не прибегая к замене всех точек доступа и сетевых карт клиентов?

IEEE ответил на этот вопрос, предложив являющийся частью стандарта 802.11i (и WPA) временный протокол целостности ключа (temporal key integrity protocol, TKIP).



Этот протокол использует многие основные функции WEP, чтобы оправдать инвестиции, сделанные клиентами в оборудование и инфраструктуру стандарта 802.11, но ликвидирует несколько слабых мест последнего, обеспечивая эффективное шифрование streams данных. Основные усовершенствования, внесенные протоколом TKIP, таковы:

- **Попереймовое изменение ключей шифрования.** WEP-ключ быстро изменяется, и для каждого фрейма он другой.
- **Контроль целостности сообщения (message integrity check, MIC).** Обеспечивается эффективной проверкой целостности фреймов данных с целью предотвращения проведения тайных манипуляций с фреймами и воспроизведения фреймов (подробнее об этом — ниже)

В статье Флурери, Минтца и Шамира обсуждается уязвимость алгоритма RC4, примененного в WEP. Атаки, использующие уязвимость слабых IV, таких, которые применяются в приложении AirSnort, основаны на накоплении нескольких фреймов данных, содержащих информацию, зашифрованную с использованием слабых IV. Простейшим способом сдерживания таких атак является изменение WEP-ключа, используемого при обмене фреймами между клиентом и точкой доступа, до того как атакующий успеет накопить фреймы в количестве, достаточном для вывода битов ключа.

IEEE адаптировала схему, известную как *попереймовое изменение ключа* (per-packet keying). (Ее также называют *изменением ключа для каждого пакета* (per-packet keying) и *частым изменением ключа пакета* (fast packet keying).) Основной принцип, на котором основано попереймовое изменение ключа, состоит в том, что IV, MAC-адрес передатчика и WEP-ключ обрабатываются вместе с помощью двухступенчатой функции перемешивания. Результат применения этой функции соответствует стандартному 32-разрядному WEP-ключу и 24-разрядному IV.

IEEE предложила также увеличить 24-разрядный вектор инициализации до 48-разрядного IV. В нижеследующих разделах объясняется, почему необходимо также расширение IV. На рис. 4.23 представлен образец 48-разрядного IV и показано, как этот IV разбивается на части для использования при попереймовом изменении ключа.

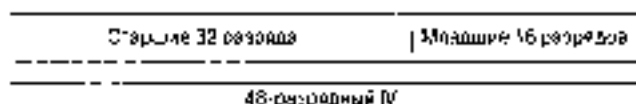


Рис. 4.23 Разбиение на части IV для использования при попереймовом изменении ключа

Процесс попереймового изменения ключа можно разбить на следующие этапы:

1. Базовый WEP-ключ (полученный в процессе аутентификации по стандарту 802.11) перемешивается со старшими 32 разрядами 48-разрядного IV (32-разрядные числа могут принимать значения 0–4 294 967 295) и MAC-адресом передатчика. Результат этого действия называется *ключ 1-й фазы* (phase 1 key). Этот процесс позволяет записать ключ 1-й фазы в кэш и также напрямую поместить в ключ (рис. 4.23).
2. Ключ 1-й фазы снова перемешивается с IV и MAC-адресом передатчика (TA) для выработки значения попереймового ключа.
3. Вектор инициализации (IV), используемый для передачи фрейма, имеет размер только 16 бит (16-разрядные числа могут принимать значения 0–65 535). Оставшиеся 8 бит представляют фиксированное значение, используемое как заполнитель.

4. Пофреймовый ключ используется для WEP-шифрования фрейма данных.
5. Когда 16-битовое пространство IV оказывается исчерпанным, ключ 1-й фазы сбрасывается к 32 старших разряда увеличиваются на 1. (Если значение IV первой фазы было равно 12, оно увеличивается до 13.)
6. Значение пофреймового ключа вычисляется заново, как на этапе 2.

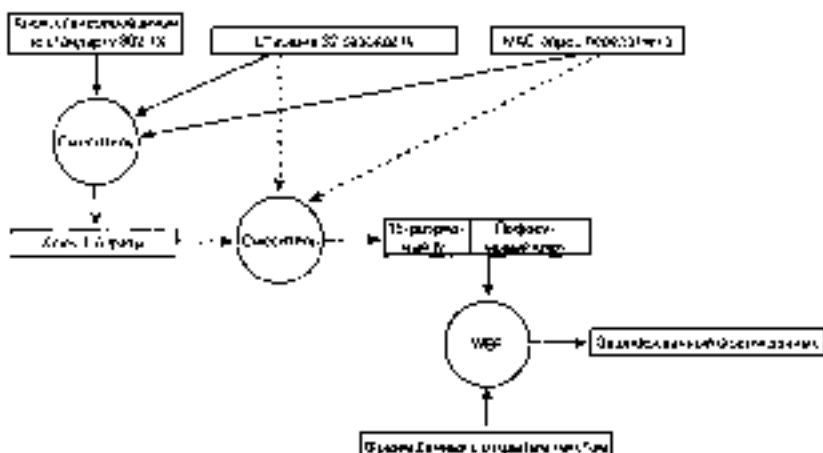


Рис. 4.23 Процесс пофреймового изменения ключа

Пофреймовое изменение ключа имеет одну важную тонкость, когда 16 разрядных значений IV не используются повторно. Если 16-разрядные значения IV используются дважды, происходит коллизия, в результате чего появляется возможность провести атаку и вывести ключевой поток. Чтобы избежать коллизий IV, значение ключа 1-й фазы вычисляется заново путем увеличения старших 32 разрядов IV на 1 и повторного инициализации пофреймового ключа.

#### На заметку

Пофреймовое изменение ключа препятствует проведению статистических атак (таких, которые были возможны по отношению к AirSnort), направленных на пофреймовый ключ, поскольку пара пофреймовый ключ-вектор инициализации получается уникальной.

Процесс пофреймового изменения ключа можно разбить на следующие этапы.

Устройство инициализирует IV, присваивая ему значение 0. В двоичном представлении это будет значение 000.

Первые (старшие) 32 разряда IV (в рассматриваемом случае — первые 32 нуля) перемещаются в выделенный по стандарту 802.1X ключом (имеющим 128-разрядное значение) и MAC-адресом передатчика (имеющим 48-разрядное значение) для получения значения ключа 1-й фазы (88-разрядное значение).

Ключ 1-й фазы вновь перемещается с первыми (старшими) 32 разрядами IV и MAC-адресом передатчика, чтобы получить 128-разрядный пофреймовый ключ, первые 16 разрядов которого представляют собой значение IV (16 нулей).

Вектор инициализации пофреймового ключа увеличивается на 1 (первый IV состоит из 16 нулей, следующие из 15 и т.д., пока все 16 разрядов не примут значение, равное 1).

После того как потенциальные возможности IV будут исчерпаны, IV 1-й фазы (32 бита) увеличивается на 1 бит и теперь будет состоять из M нуля и одной единицы, 00000000000000000000000000000001).

Следующий логично возникающий вопрос таков: "Может ли подобный механизм привести к коллизиям IV?" Правильный ответ "да", но важно понять, когда это может произойти. Предположим, что максимальная скорость перемещения для устройства стандарта 802.11b составляет 1000 фреймов в секунду. Тогда 16-разрядный фрейм IV исчерпает свои возможности через 65 секунд ( $2^{16}$  фреймов/1000 фреймов/с).

Существуют  $2^{48}$  возможных вектора инициализации 1-й фазы (первые 32 разряда 48-разрядного IV), что дает 4 294 967 296 значений. Каждое из этих значений увеличивается в поле ZFPA, как 16-разрядный IV исчерпает свои возможности (а это происходит каждые 65 секунд), так что весь 48-разрядный IV исчерпает свои возможности по истечении  $65 \cdot 4\,294\,967\,296$  с, что составляет примерно 8852 года. Если администратор не потребует повторной аутентификации, для передачи значения ключей вряд ли понадобится провалить во избежание возникновения коллизий IV.

Этот алгоритм усиливает WEP до такой степени, что почти все известные сейчас возможности атак устраняются без замены существующего оборудования. Следует отметить, что этот алгоритм (и TKIP в целом) разработан с целью залатать бреши в системе аутентификации WEP и стандарта 802.11. Он жертвует слабыми алгоритмами, вместо того чтобы заменять оборудование. Следующее поколение оборудования стандарта 802.11 должно поддерживать TKIP, но WEP/TKIP будет постепенно свертываться в пользу алгоритма с большими возможностями шифрования, такого как усовершенствованный стандарт шифрования (advanced encryption standard, AES).

## Четвертая составляющая: целостность данных

В будущем для усиления малоэффективного механизма, основанного на использовании контрольного признака целостности (ICV) стандарта 802.11, будет применяться контроль целостности сообщения (MIC). Благодаря MIC могут быть ликвидированы слабые места защиты, способствующие передаче атак с использованием поддельных фреймов и жонглированием битами, рассмотренные ранее в этой главе. IEEE предложило специальный алгоритм, получивший название *Michael* (Майкл), чтобы усилить роль ICV в шифровании фреймов данных стандарта 802.11.

MIC имеет уникальный ключ, который отличается от ключа, используемого для шифрования фреймов данных. Этот уникальный ключ перемешивается с назначенным MAC-адресом и исходным MAC-адресом фрейма, а также со всей незашифрованной частью фрейма, несущей полезную нагрузку. На рис. 4.24 показана работа алгоритма Michael MIC.

Механизм шифрования TKIP в целом осуществляется следующим образом:

1. С помощью алгоритма пифреймового назначения ключей генерируется пифреймовый ключ (рис. 4.25).
2. Алгоритм MIC генерирует MIC для фрейма в целом.
3. Фрейм фрагментируется в соответствии с указанными MAC-адресными фрагментации.
4. Фрагменты фрейма шифруются с помощью пифреймового ключа.
5. Осуществляется передача зашифрованных фрагментов.

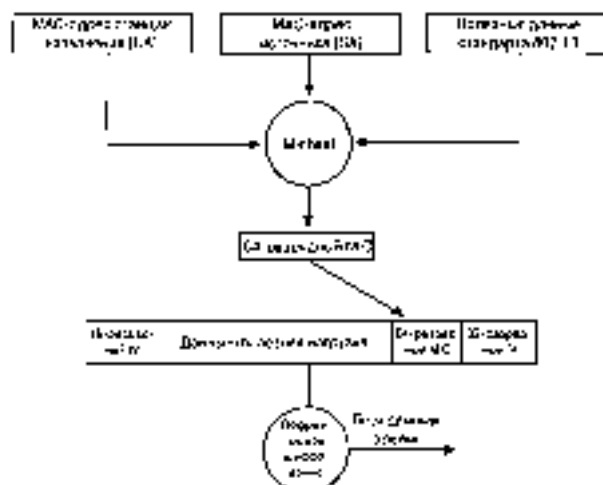


Рис. 4.24. Алгоритм Michael MIC

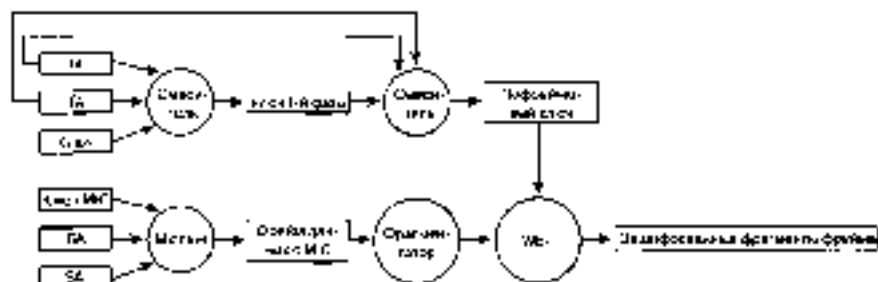


Рис. 4.25. Процесс шифрования по алгоритму TKIP

Аналогично процессу шифрования по алгоритму TKIP, процесс дешифрования по этому алгоритму выполняется следующим образом (рис. 4.26).

1. Предварительно вычисляется ключ 1-й фазы.
2. На основании IV, полученного из предыдущего фрагмента фрейма WEP, вычисляется пофреймовый ключ 2-й фазы.
3. Если полученный IV не тот, какой нужен, такой фрейм отбрасывается.
4. Фрагменты фрейма дешифруются и осуществляется проверка признака целостности (ICV).
5. Если контроль признака целостности дает отрицательный результат, такой фрейм отбрасывается.
6. Дешифрованные фрагменты фрейма собираются, чтобы получить исходный фрейм данных.
7. Приемник вычисляет значение MIC и сравнивает его со значением, находящимся в поле MIC фрейма.
8. Если эти значения совпадают, фрейм обрезается приемником.
9. Если эти значения не совпадают, значит, фрейм имеет ошибку MIC и приемник принимает меры противодействия MIC.

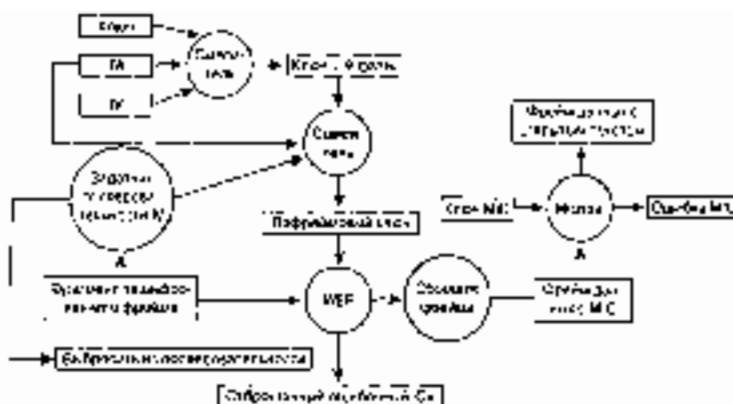


Рис. 4.26. Процесс дешифрования по алгоритму TKIP

Меры противодействия MIC состоят в выполнении приемником следующих задач.

1. Приемник удаляет существующий ключ на ассоциирование.
2. Приемник регистрирует проблему как относящуюся к безопасности сети.
3. Ассоциированный клиент, от которого был получен ложный фрейм, не может быть ассоциирован и аутентифицирован в течение 60 секунд, чтобы замедлить атаку.
4. Если клиент получил ложный фрейм, то он шифрует все фреймы, не соответствующие стандарту 802.1X.
5. Такой клиент также запрашивает новый ключ.

Наше рассмотрение пофреймового назначения ключей и MIC касалось в основном ключа шифрования и ключа MIC. Но мы ничего не говорили о том, как ключи генерируются и пересылаются от клиента к точке доступа и наоборот. В следующем разделе мы и рассмотрим предлагаемый стандартом 802.11 механизм управления ключами.

## Усовершенствованный механизм управления ключами

Алгоритмы аутентификации стандарта 802.11 и EAP могут обеспечить сервер RADIUS и клиента динамическими, ориентированными на пользователя ключами. Но тот ключ, который создается в процессе аутентификации, не является ключом, используемым для шифрования фреймов или проверки целостности сообщений. В стандарте 802.11 WPA для получения всех ключей используется так называемый *мастер-ключ* (master key). На рис. 4.27 представлена иерархия ключей с учетом их зависимости от создания.

Механизм генерации ключей шифрования осуществляется в четыре этапа.

1. Клиент и точка доступа устанавливают динамический ключ (он называется *парный мастер-ключ*, или PMK, от англ. pairwise master key), полученный в процессе аутентификации по стандарту 802.1X.
2. Точка доступа передает клиенту секретное случайное число, которое называется *временным аутентификатор* (authenticator nonce, ANonce), используя для этого сообщение EAPoL-Key стандарта 802.1X.

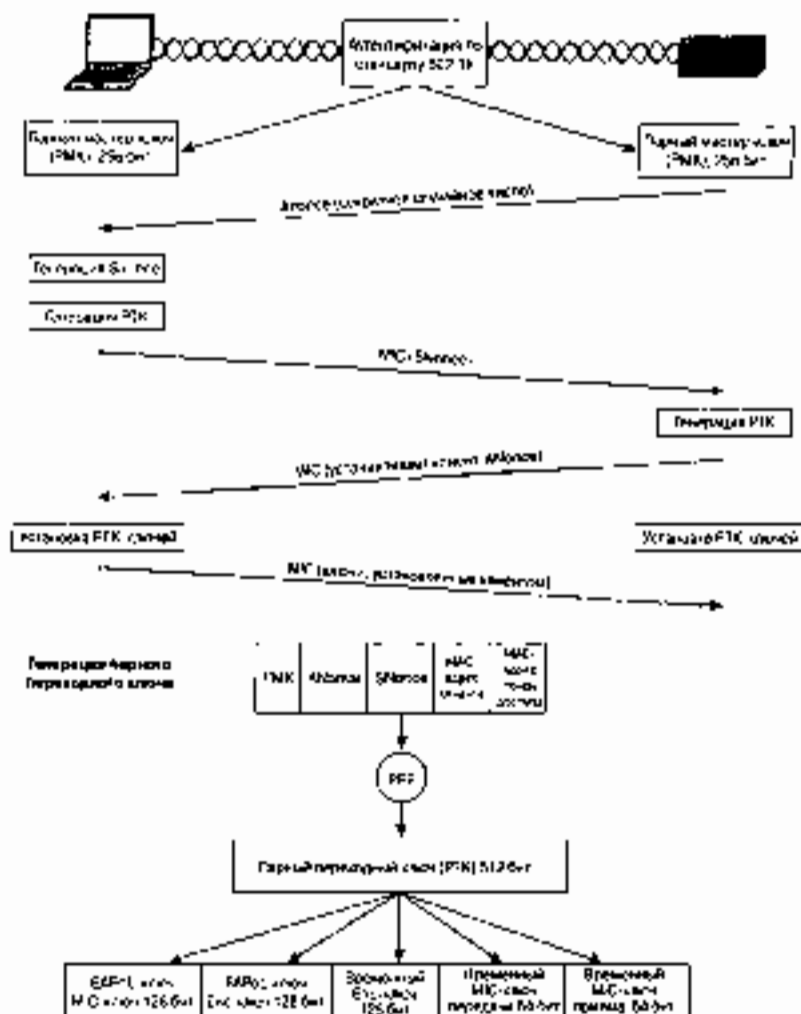


Рис. 4.27. Последовательность создания ключей

3. Этот клиент локально генерирует секретное случайное число, называемое *временный просителем* (surrogate nonce, SNonce).
4. Клиент генерирует парный переходный ключ (pairwise transient key, РТК) путем комбинации РМК, SNonce, Алгоритм, MAC-адреса клиента, MAC-адреса точки доступа и строки инициализации. MAC-адреса упорядочены, MAC-адреса младшего порядка имеют приоритет перед MAC-адресами высшего порядка. Благодаря этому гарантируется, что клиент и точка доступа "выстроят" MAC-адреса одинаковым образом.
5. Это комбинационное значение пропускается через псевдослучайную функцию (pseudo random function, PRF), чтобы получить 512-разрядный РТК.
6. Клиент посылает число SNonce, сгенерированное им на этапе 3, точке доступа с помощью сообщения EAPoL-Key стандарта 802.1X, защищенное ключом EAPoL-Key MIC.

7. Точка доступа использует число *Spnonce* для шифрования РТК таким же образом, как это сделал клиент.
8. Точка доступа использует выведенный ключ *EAPoL-Key MIC* для проверки целостности сообщения клиента.
9. Точка доступа посылает сообщение *EAPoL-Key*, показывающее, что клиент может использовать РТК и его *Spnonce*, зашифрованные ключом *EAPoL-Key MIC*. Данный этап позволяет клиенту удостовериться в том, что число *Spnonce*, полученное на этапе 2, действительно.
10. Клиент посылает сообщение *EAPoL-Key*, зашифрованное ключом *EAPoL-Key MIC*, указывающее, что данные утеряны.

Парный мастер-ключ (РМК) и парный переосновный ключ (РТК) являются одноадресными по своей природе. Они только шифруют и дешифруют одноадресные фреймы, и предназначены для единственного пользователя. Широковещательные фреймы требуют отдельной иерархии ключей, потому что использование с этой целью одноадресных ключей приведет к редкому возрастанию трафика сети. Точке доступа (единственному объекту BSS, имеющему право на рассылку широковещательных или многоадресных сообщений) пришлось бы посылать один и тот же широковещательный или многоадресный фрейм, зашифрованный соответствующими парными ключами, каждому пользователю.

Широковещательные или многоадресные фреймы используют иерархию групповых ключей. Групповой мастер-ключ (*group master key, GMK*) находится на вершине этой иерархии и выводится в точке доступа. Вычисл GMK основан на применении PRF, в результате чего получается 256-разрядный GMK. Входными данными для PRF-256 являются шифровальный секретное случайное число (или полсе), текстовая строка, MAC-адрес точки доступа и значение времени в формате синхронизации (сетевое протокола (NTP)). На рис. 4.28 представлена иерархия групповых ключей.

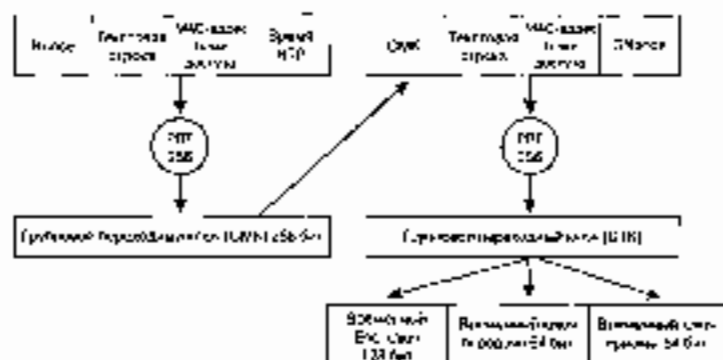


Рис. 4.28. Иерархия групповых ключей

Групповой мастер-ключ, текстовая строка, MAC-адрес точки доступа и *Spnonce* (значение, которое берется из счетчика ключа точки доступа) объединяются и обрабатываются с помощью PRF, в результате чего получается 256-разрядный групповой переходный ключ (*group temporal key, GTK*). GTK делится на 328-разрядный ключ шифрования широковещательных/многоадресных фреймов, 64-разрядный ключ передачи MIC (*transmit MIC key*) и 64-разрядный ключ приема MIC (*MIC receive key*).

С помощью этих ключей шифроадресатные и многоадресные фреймы шифруются и дешифруются точно так же, как с помощью одноадресных ключей, полученных на основе парного мастер-ключа (PMK).

Клиент обменивается с помощью групповых ключей шифрования через сообщения EAPoL-Key. Точка доступа посылает такому клиенту сообщение EAPoL, зашифрованное с помощью одноадресного ключа шифрования. Групповые ключи удаляются и регенерируются каждый раз, когда какая-нибудь станция деаутентифицируется или деаутентифицируется в BSS. Если происходит ошибка MIC, одной из мер противодействия также является удаление всех ключей с имеющей отношение к ошибке приемной станции, включая групповые ключи.

## Шифрование по алгоритму AES

Известно, что шифрование и аутентификация, проводимые в соответствии со стандартом 802.11, имеют слабые стороны. IEEE и WPA усилили алгоритм WEP протоколом TKIP и предлагают сильный механизм аутентификации по стандарту 802.11i, обеспечивающий защиту беспроводных LAN стандарта 802.11. В то же время IEEE рассматривает возможность усиления механизма шифрования. С этой целью IEEE адаптировал алгоритм AES для применения его по отношению к разделу, касающемуся зашифрованных данных предлагаемого стандарта 802.11i. Компоненты WPA не обеспечивают поддержку шифрования по алгоритму AES. Однако последние версии WPA, возможно, будут реализованы в соответствии со стандартом 802.11i и для обеспечения взаимодействия будут поддерживать шифрование по алгоритму AES.

Алгоритм AES представляет собой следующее поколение средств шифрования, одобренное Национальным институтом стандартов и технологий (NIST) США. Названный институт предложил сообществу криптологов разработать новые алгоритмы шифрования. Эти алгоритмы должны быть полностью открыты и использоваться бесплатно. Кандидаты были проверены на предмет "криптографической прочности" и практической применимости. Финалистом и принятым методом стал так называемый *алгоритм Рабиндры* (Rijndael algorithm). Как и многие другие шифры, AES требует режима обратной связи во избежание риска, связанного с режимом ECB (напомним, что режим шифрования с помощью книги электронных жетонов) IEEE разработал режим AES, предназначенный специально для применения в беспроводных LAN. Этот режим называется *режим счетчика шифровальных блоков* (Cipher Block Chaining Counter Mode, CBC-CTR) с контролем аутентичности сообщений в шифровальных блоках шифра (Cipher Block Chaining Message Authentication Check, CBC-MAC), все вместе это обозначается аббревиатурой AES-CCM. Режим CCM представляет собой комбинацию режима шифрования CBC-CTR и алгоритма контроля аутентичности сообщений CBC-MAC. Эти функции скомбинированы для обеспечения шифрования и проверки целостности сообщений в одном режиме.

Алгоритм шифрования CBC-CTR работает с использованием счетчика для питания ключевого потока. Значение этого счетчика увеличивается на единицу после шифрования каждого блока. Такой процесс обеспечивает получение уникального ключевого потока для каждого блока. Фрейм с открытым текстом делится на 16-байтные блоки. После шифрования каждого блока значение счетчика увеличивается на единицу, и так до тех пор, пока не будут зашифрованы все блоки. Для каждого нового фрейма счетчик переустанавливается.



Алгоритм шифрования CBC-MAC выполняется с использованием результата подфункции CBC по отношению ко всему фрейму, к адресу назначения, адресу источника и данным. Результат операций 128-разрядный и выкашивается до 64 бит для использования в пересылаемом фрейме.

CBC-MAC работает с известными криптографическими функциями, но имеет издержки, связанные с выполнением двух операций для шифрования и целостности сообщений. Этот процесс требует серьезных вычислительных затрат и значительно увеличивает "избыточные расходы" шифрования.

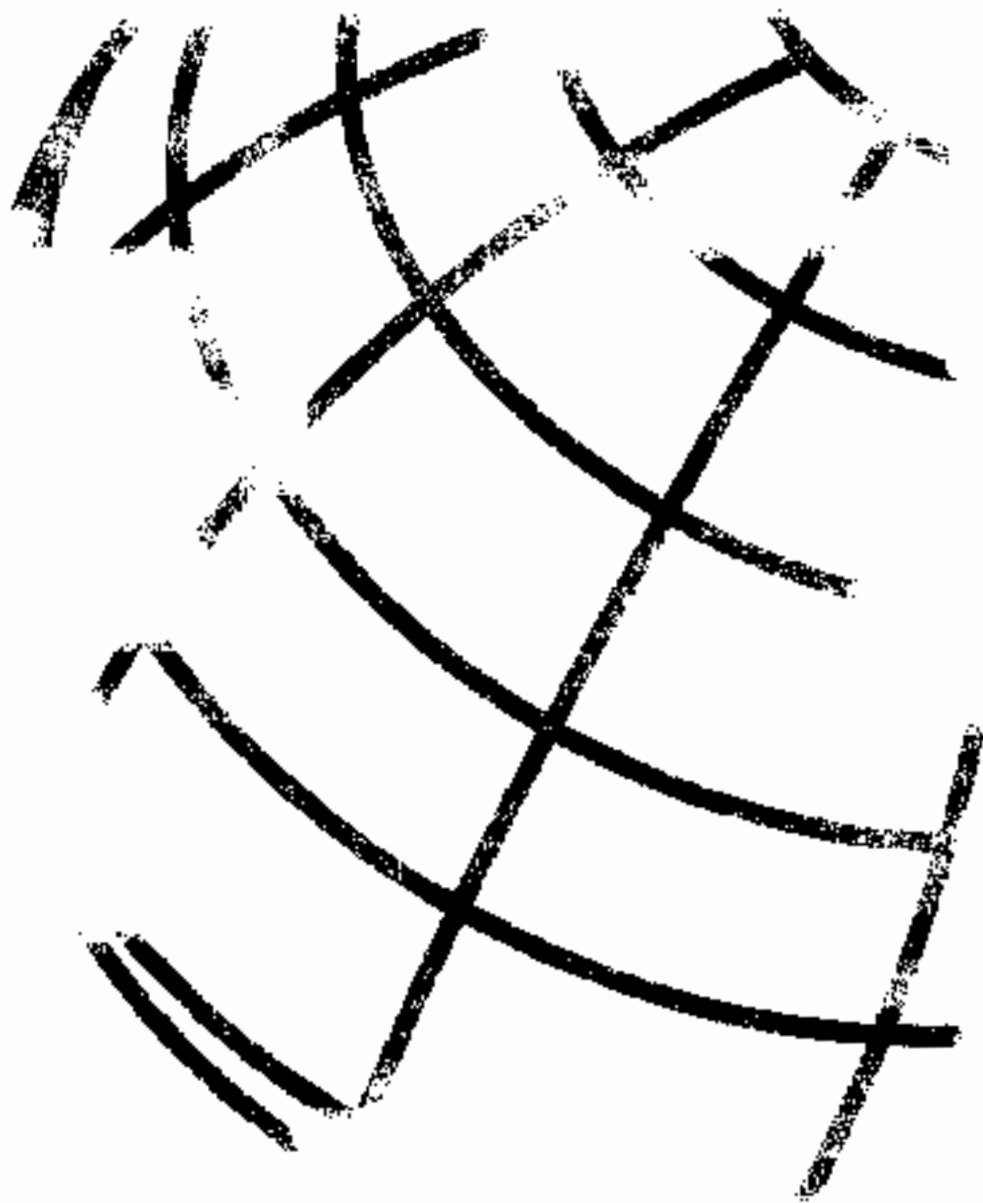
## Резюме

Алгоритмы аутентификации и шифрования, определенные в стандарте 802.11 разработки 1997 года, имеют множество недостатков. Система аутентификации, так же как алгоритм WEP-шифрования, могут быть взломаны за короткое время. Протокол TKIP обещает ликвидировать недостатки WEP-шифрования и системы аутентификации в краткосрочной перспективе, а стандарт 802.1X и AES предоставят долгосрочное решение проблемы безопасности беспроводных сетей.

В этой главе рассказывается о том, как можно защитить беспроводную локальную сеть, и объясняются варианты защиты беспроводных сетей. При развертывании беспроводных LAN важно обеспечить максимальную их защищенность и удобство для пользователей.

В этой главе...

- Характеристики роуминга
- Роуминг на уровне 2
- Роуминг на уровне 3 и некоторые сведения о мобильных IP



## Мобильность

---

В этой книге рассматриваются основные компоненты беспроводных локальных сетей (WLAN) стандарта 802.11. Описанные в предыдущих главах основные концепции, такие как механизмы доступа к среде, форматы фреймов, система защиты и физические интерфейсы, являются основой для понимания других концепций, более приближенных к практическому применению.

В данной главе рассматривается проблема мобильности. *Мобильность* — это свойство сети, позволяющее быстро перемещать ее саму и перемещаться ее пользователям с места на место. Устройства WLAN стандарта 802.11 обеспечивают такую “свободу от проводов”. Но мобильность — это больше чем отсутствие сетевого кабеля. Разбираясь в том, как обеспечивается мобильность в сетях стандарта 802.11, вы узнаете также о том, как можно поддерживать мобильные приложения. Мобильность описывается многими терминами, но в этой главе будут использоваться только два: мобильность и роуминг, для описания процесса перемещения пользователя от одной точки доступа к другой.

## Характеристики роуминга

Определить или охарактеризовать стоящих, осуществляющих роуминг, можно двумя способами:

- Бесшовный роуминг (seamless roaming).
- Качевой роуминг (nomadic roaming).

Ближайшей аналогией *бесшовного роуминга* является звонок по сотовому телефону. Например, представьте, что вы говорите по сотовому телефону и то время как ваш автомобиль мчится по автомагистрали. Типичная базовая станция глобальной системы мобильной связи (GSM) или сотовой, обеспечивающая множественный доступ с временным разделением (TDMA), действует на площади в несколько километров в час, так что с уверенностью можно предположить, что во время такого телефонного разговора базовые станции осуществляют роуминг. Во время роуминга вы не чувствуете ухудшения качества связи (благодаря чему сольные телефоны и стали столь популярными). Не существует заметного промежутка времени, когда из-за роуминга сеть была бы недоступна. Роуминг такого типа называется *бесшовным*, потому что сетевые приложения требуют постоянного подключения к сети в процессе роуминга.

Конечный роуминг отличается от беспроводного. *Конечной роуминг* можно описать как использование ноутбука стандарта 802.11 в офисе. Предположим, что владелец этого ноутбука подключается к сети; когда он сидит на своем рабочем месте, то соединяется с одной точкой доступа. Когда пользователь решает покинуть рабочее место, он берет свой ноутбук и идет с ним в конференц-зал. Здесь он должен доложить о результатах своей работы. Говоря языком технических терминов, клиент стандарта 802.11 перемещается от точки доступа, ближайшей к его рабочему месту, к точке доступа, размещенной поблизости от конференц-зала. Роуминг такого типа принято называть конечным, поскольку пользователь использует службы сети не во время перемещения, а только во его завершении.

Что происходит с выполняемыми приложениями во время роуминга? Ответ на этот вопрос зависит от многих факторов. Рассмотрим следующие.

- Механизм роуминга стандарта 802.11
- Работа приложений. Функционируют ли они только при установлении соединения или способны работать без него?
- Домен роуминга. Осуществляется ли роуминг в одной подсети или сразу в нескольких подсетях?
- Длительность роуминга. Сколько времени занимает процесс роуминга?

## Механизм роуминга стандарта 802.11

Девизом роуминга стандарта 802.11 может быть фраза "сломай, прежде чем строить" (break before make), потому что станция должна завершить сеанс своего обслуживания одной точкой доступа, прежде чем соединиться с новой. Такой процесс может показаться интуитивно неоправданным, поскольку он оставляет возможность потери данных в ходе роуминга, но благодаря этому упрощаются MAC-протокол и радиоконтракт.

Если бы стандарт 802.11 относился к типу "построй, прежде чем сломать" (make before break), т.е. станция должна была бы ассоциироваться с новой точкой доступа, прежде чем диссоциироваться со старой, пришлось бы применять меры безопасности на уровне MAC, препятствующие возникновению топологий с циклом. Станция, подключенная к одному в тому же широковещательному домену уровня 2 через несколько сетевых соединений, потенциально может вызвать широковещательный шторм. Архитектура "построй, прежде чем сломать" потребовала бы алгоритма, подобного связующему дереву стандарта 802.1D, для разрыва потенциальных петель, что привело бы к увеличению непроизводительной нагрузки на MAC-протокол. Кроме того, радиостанция клиента должна была бы иметь возможность прослушивания и установления связи более чем по одному каналу одновременно, что привело бы к ее усложнению, а также снижению общей стоимости устройства.

## Функционирование и применение

Метод работы приложения непосредственно связан с его способностью к восстановлению функций в процессе роуминга. Требуемые устанавливая соединения приложения, например основанные на использовании протокола TCP, более толерантны к утере пакетов, происходящей во время роуминга, потому что TCP

надежны и требующей установки соединения протокол TCP требует дополнительных подтверждений, точно так же как и уровень MAC стандарта 802.11. Это требование позволяет повторно передать любые данные стандарта 802.11, утерянные во время роуминга, посредством TCP – протокола более высокого уровня.

Хотя TCP обеспечивает хорошие решения для приложений, выполняемых в беспроводных LAN стандарта 802.11, некоторые приложения ориентируются на использование пользовательского протокола данных (User Data Protocol, UDP) в качестве транспортного протокола уровня 4. Протокол UDP является минимальным и требует установления соединения. Пакеты UDP использует такие приложения, как IP-телефония (Voice over IP, VoIP) и приложения, обеспечивающие передачу видеонабразжений. Присущая протоколу TCP способность повторной передачи мало помогает при утере пакетов в случае IP-телефонии. Повторно переданные VoIP-пакеты вызовут скорее раздражение пользователя, чем чувство благодарности. Следовательно, роуминг с потерей данных может оказать заметное влияние на работу основанных на протоколе UDP приложений.

## Домен роуминга

В главе 1, “Технология Ethernet”, *ширококоординатный домен* определен как сеть, соединяющая устройства, способные получать и отправлять одно другому ширококоординатные фреймы. Этот домен называют также *сетью уровня 2*. Данная концепция остается справедливой и для сетей стандарта 802.11. О точках доступа, относящихся к одному ширококоординатному домену и сконфигурированных так, что они имеют одинаковый идентификатор зоны обслуживания (SSID), говорят, что они относятся к одному домену роуминга. Вспомните главу 2, “Распределенные локальные сети стандарта 802.11”, в которой расширенная зона обслуживания (ESS) обычно рассматривалась как несколько базовых зон обслуживания (BSS), связанных между собой через службу распределения (проводную сеть). Следовательно, домен роуминга можно назвать ESS. Почему роуминг для устройств стандарта 802.11 ограничен сетью уровня 2? А как насчет роуминга между подсетями уровня 3? Вспомним, что стандарт 802.11 описывает физический интерфейс уровня 1 и технологию канального уровня 2. MAC-протокол стандарта 802.11 “ничего не знает” об уровне 3. Нельзя сказать, что роуминг уровня 3 невозможен в принципе. Но можно сказать, что роуминг уровня 2 изначально поддерживается устройствами стандарта 802.11, а для роуминга на уровне 3 необходимо использовать решения более высоких уровней.

Различие между тем, перемещается ли устройство в пределах домена роуминга или между доменами роуминга, оказывает большое влияние на сеансы связи приложений. На рис. 5.1 показан домен роуминга уровня 2. Перемещающийся пользователь может поддерживать приложение в состоянии подключения, пока находится в пределах домена роуминга и пока поддерживается (не изменяется) сетевой адрес уровня 3.

На рис. 5.2 показано, как осуществляется роуминг между доменами роуминга. Перемещающийся пользователь переходит от точки доступа подсети А к точке доступа подсети В. Поскольку адрес уровня 3 изменяется, сеанс прекращает все сеансы связи приложений. Этот сценарий описан ниже, в разделе “Обзор мобильного IP”.

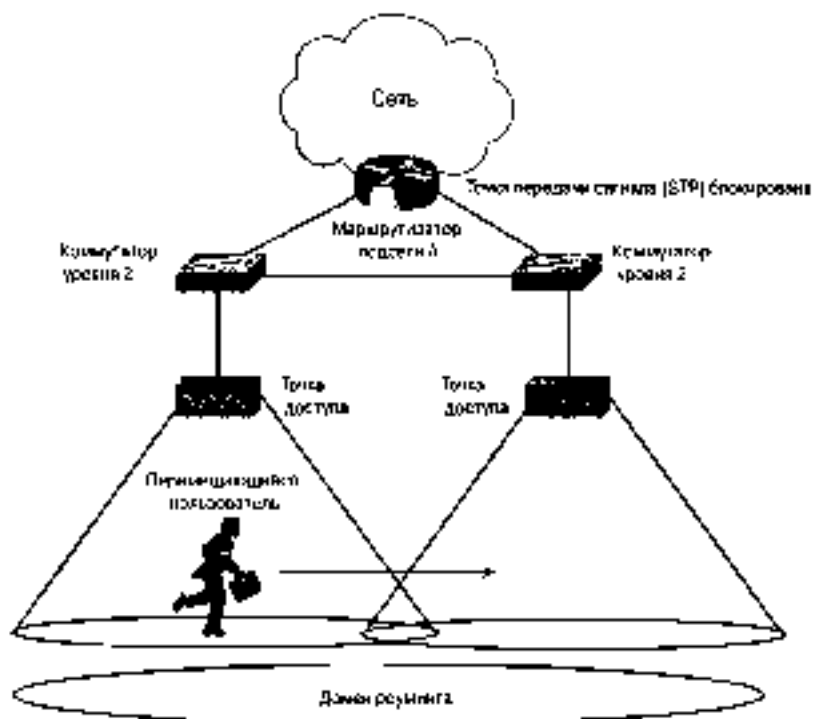


Рис. 5.1. Домашняя сеть уровня 2

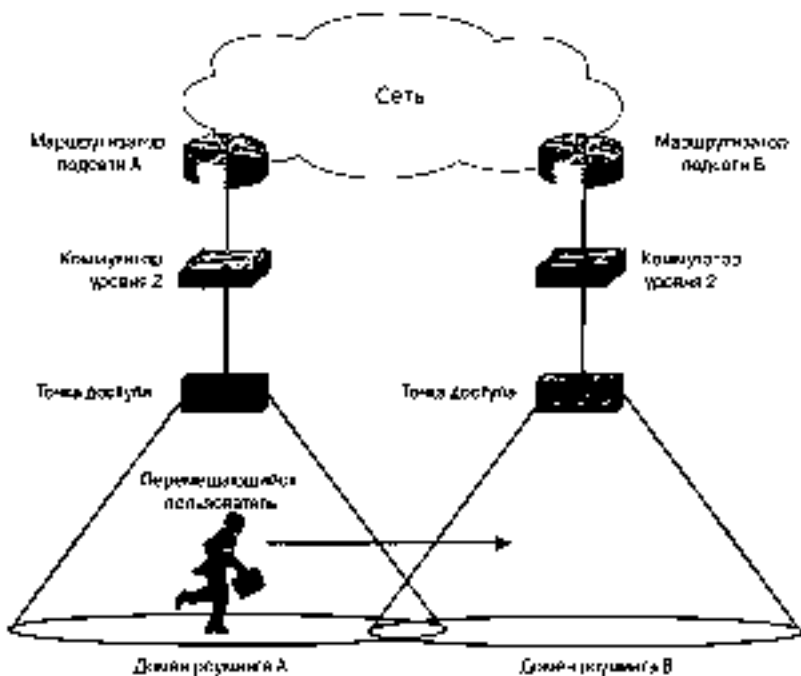


Рис. 5.2. Роуминг между домашними сетями

## Длительность роуминга

Под длительностью роуминга понимается время, необходимое для завершения роуминга. По сути роуминг — это процесс ассоциирования, описанный в главе 2 “Распределенные локальные сети стандарта 802.11”; он зависит от длительности следующих процессов.

- Процесс зонлирования.
- Процесс аутентификации по стандарту 802.11.
- Процесс ассоциирования по стандарту 802.11.
- Процесс аутентификации по стандарту 802.1X.

Суммарная длительность этих процессов и составляет длительность роуминга. Некоторые приложения, такие как VoIP, весьма чувствительны к задержкам и не допускают большой длительности роуминга.

## Роуминг уровня 2

Теперь, после того как были описаны некоторые особенности роуминга, пришла пора рассказать о том, как технически осуществляется роуминг уровня 2. Чтобы мог осуществляться роуминг, должна произойти следующая последовательность событий.

- Клиент должен принять решение о перемещении.<sup>1</sup> Алгоритмы роуминга определяют поставщика оборудования (и являются его собственностью); они зависят от таких факторов, как уровень сигнала, подтверждение приема фрейма, посланные сигнальные фреймы и т.д.
- Клиент должен решить, куда он будет перемещаться. Клиент должен решить, к какой точке доступа он переместится. Это может быть сделано путем сканирования среды на предмет наличия точек доступа или до принятия решения о перемещении, и в таком случае данный процесс называется *предварительное обнаружение точки доступа* (preactive AP discovery), или после принятия решения о перемещении, этот процесс называется *обнаружение точки доступа во время перемещения* (reactive AP discovery).
- Клиент начинает перемещение. Клиент использует фреймы реассоциирования стандарта 802.11, чтобы ассоциироваться с новой точкой доступа.
- Клиент может продолжить сеансы связи выполняемых приложений.

## Алгоритмы роуминга

Механизм определения момента времени, когда необходимо начать процесс роуминга не определен в спецификации стандарта 802.11 и таким образом, оставлен на усмотрение поставщика оборудования. Хотя ранее эта проблема ставила под угрозу возможность взаимодействия первых устройств стандарта 802.11, сейчас поставщики вместе работают над тем, чтобы основы взаимодействия сохранились. Тот факт, что алгоритмы были оставлены на усмотрение поставщиков, для последних возможность

<sup>1</sup> Точнее, в том, что именно начал его перемещать. — *Прим. ред.*

дифференцироваться друг от друга за счет создания новых и лучших алгоритмов, конкурирующих с другими. Алгоритмы роуминга стали “секретным оружием” поставщика, поэтому их особенности не раскрываются.

Не рискуя ошибиться, можно предположить, что в этих алгоритмах учитываются такие параметры, как уровень сигнала, значения счетчиков числа попыток, посланные сфреймами фреймы и другие коэффициенты, рассмотренные ранее в главе 2. Например, алгоритм обнаруживается в той же статье работу распределенной функции координатный (DCF). Двоичный экспоненциальный инвертный алгоритм (binary exponential backoff algorithm), применяющийся для осуществления доступа к среде, увеличивал значения счетчика числа повторных фреймов, если фрейм не мог быть доставлен после нескольких попыток. Это служило предупреждением клиенту, что он выходит из зоны действия точки доступа. Поэтому алгоритм роуминга должен отслеживать показания счетчика числа попыток передачи фрейма, чтобы можно было принять решение о начале роуминга.

Кроме того, алгоритмы роуминга должны искать баланс между коротким временем роуминга и стабильностью работы клиента. Например, чересчур чувствительный алгоритм роуминга может не допускать утери сигнального фрейма или фрейма подтверждения. Такой алгоритм может принять ошибочные случаи за ослабление сигнала и начать процедуру роуминга. Но для BSS подобные события — норма, в результате процедуру роуминга может начать даже стационарный клиент. “Забыв” о том, что он стационарный. Хотя роуминг может осуществляться быстро, результирующая пропускная способность сети для такого пользователя снижается.

## В какую сторону перемещается пользователь

Определение точки доступа, в сторону которой перемещается пользователь, — это второй механизм, отданный на откуп производителям. Вообще говоря, существуют два механизма определения новой точки доступа.

- Предварительное обнаружение точки доступа
- Обнаружение точки доступа во время перемещения

Каждый из этих механизмов может в свою очередь использовать один или оба из следующих механизмов.

**Активное сканирование.** Клиент активно ищет точку доступа. Этот процесс обычно включает отправку клиентом зондирующих запросов по каждому из сконфигурированных на нем каналов (для Северной Америки это каналы 1–11) и ожидание ответов от точек доступа на зондирующие запросы. Затем клиент определяет, какая из точек доступа лучше всего подходит для роуминга.

**Пассивное сканирование.** Клиент не передает ни одного фрейма, а просто прослушивает сигнальные фреймы, передаваемые по каждому из каналов. Клиент продолжает переходить с канала на канал через определенные интервалы времени, как при активном сканировании, но при этом не посылает зондирующие запросы.

Активное сканирование считается наиболее совершенным механизмом поиска точки доступа, потому что при его использовании активно рассматриваются зондирующие запросы стандарта 802.11 по всем каналам. При этом требуется, чтобы клиент оставался на одном и том же канале предопределенное время, обычно от 10 до 20 мс, в зависимости от производителя, ожидая ответа на зондирующий запрос.



При пассивном сканировании клиент медленно проходит по каналам, чем при активном, так как прослушивает сигнальные фреймы, посылаемые пакетами доступа с предопределенной частотой (обычно это 10 сигнальных фреймов в секунду). Такой клиент должен оставаться на каждом канале дольше, чтобы быть уверенным, что получил сигнальные фреймы от максимального числа точек доступа для данного канала. Клиент ищет различные информационные элементы, такие как SSID, указывающие поддерживаемые скорости, а также параметризованные информационные элементы точки доступа, чтобы найти точку доступа. Это мог бы быть более быстрый механизм для сканирования среды, однако так бывает не всегда, потому что некоторые элементы не передаются (в зависимости от конфигурации точки доступа). Например, администратор может заблокировать передачу в сигнальных фреймах имени SSID (в информационном элементе SSID), и тогда клиент не сможет определить, принадлежит ли такая точка доступа к тому же дому/офису.

Идеальный способ сканирования не существует. Пассивное сканирование имеет преимущество, поскольку не требует от клиента передачи зондирующих запросов, но существует вероятность того, что нужная точка доступа будет пропущена, так как клиент не получил ее сигнальный фрейм в отпущенный для этого промежуток времени. Преимущество активного сканирования состоит в том, что клиент активно ищет точки доступа с которыми может ассоциироваться, но при этом он должен передавать зондирующие фреймы. В зависимости от особенностей применения клиента стандарта 802.11 один из механизмов может подходить больше, чем другой. Например, во многих уже внедренных системах в качестве предпочтительного метода выбрано пассивное сканирование, в то время как в телефонах стандарта 802.11, реализующих технологию IP-телефонии (VoIP), и в клиентских картах ПК применяется активное сканирование.

## Предварительное обнаружение точки доступа

Предварительный роуминг — это функция, которая наделяет клиента способностью перемещаться к обслуживанию предварительно определенной точкой доступа после того, как клиент примет решение переместиться. Этот процесс требует минимального общего времени роуминга благодаря чему снижается воздействие роуминга на работу приложений. Однако предварительный роуминг не свободен от недостатков.

Для того чтобы клиент мог определить, к какой точке доступа нужно осуществлять роуминг, он должен сканировать точки доступа в течение периода инициальной, без роуминга, работы. Когда клиент осуществляет сканирование, он должен переходить с канала на канал, чтобы или прослушивать другие точки доступа, или рассылать зондирующие запросы. Такое изменение может потенциально привести к возникновению двух проблем для клиента, которые могут повлиять на работу приложений (рис. 5.3).

- Клиент не может получать данные от точки доступа, с которой он в данное время ассоциирован, пока он сканирует каналы (активно или пассивно). Если точка доступа посылает данные клиенту в то время, когда он сканирует каналы (предполагается, что клиент работает на другом канале, нежели точка доступа), клиент пропустит эти данные и потребуются повторная передача их точкой доступа.
- Приложение клиента может испытать воздействие снижения пропускной способности. Клиент не может передавать данные во время сканирования каналов (эквивалентно либо пассивности), поэтому некоторые приложения, выполняемые клиентом, могут ощутить снижение пропускной способности.

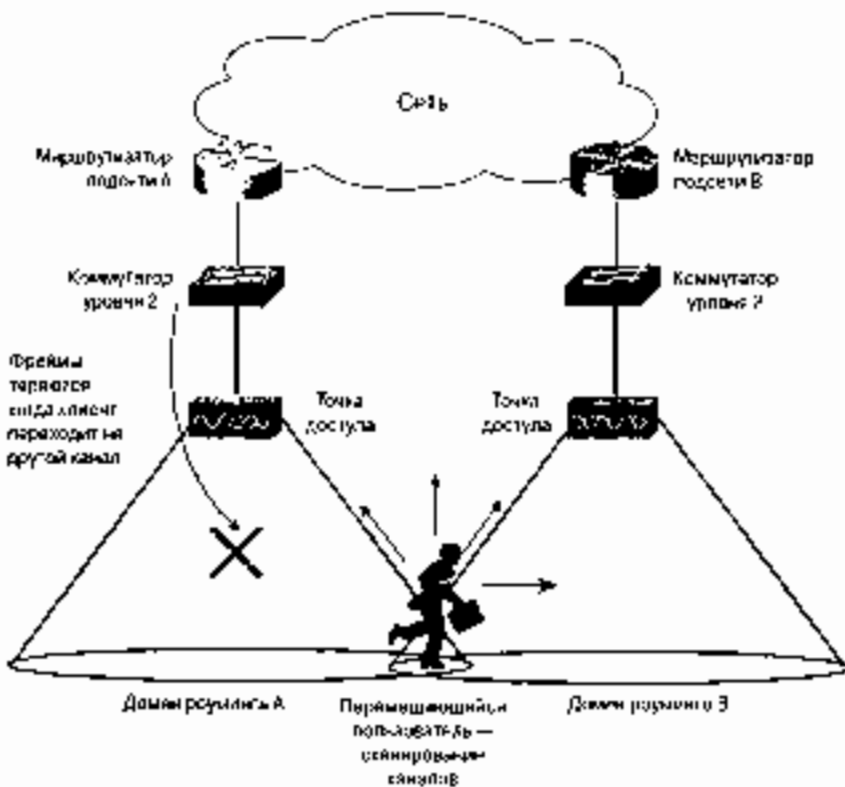


Рис. 5.1. Предварительное обнаружение точки доступа

Для энергосберегающих клиентов существует уникальная возможность практиковать предварительный роуминг и вместе с тем избежать вышеуказанных проблем. Рассмотрим такой сценарий: клиент является энергосберегающей станцией. Такой клиент способен по необходимости переходить в энергосберегающий режим работы. Он может сообщить точке доступа о том, что переходит в энергосберегающий режим, но вместо того чтобы сразу сделать это, начнет сканировать (активно или пассивно) все или определенное число каналов и искать новые точки доступа. Текущая точка доступа выстраивает очередь фреймов, предназначенные для такого клиента, в ожидании, пока он перейдет в активное состояние, поэтому такой клиент не рискует не получить какие-то данные, пока сканирует каналы. Он также может выстраивать очередь предназначенные для передачи фреймы, пока не будет завершено сканирование каналов, избегая потерь к этим данным.

Такое решение приведет к снижению эффективности энергосберегающего режима, поскольку радиостанция клиента проявляет активность по время сканирования каналов, вместо того чтобы соблюдать режим энергосбережения, а приложения клиента могут столкнуться с некоторым запаздыванием, поскольку фреймы будут ожидать своей очереди на передачу.

Работа механизма предварительного обнаружения точки доступа может быть нарушена быстро перемещающимся клиентом. Клиент может двигаться с такой скоростью, что предварительно выбранная точка доступа перестанет быть наиболее предпочтительной с точки зрения роуминга, что приведет к повышению частоты принятия решений относительно роуминга и снижению пропускной способности для приложения.

## Обнаружение точки доступа во время перемещения

Другой вариант обнаружения точки доступа состоит в том, что ее поиск начинается уже после принятия решения о роуминге. Этот процесс похож на таковой, когда клиент осуществляет первоначальное подключение, за исключением того что запрос на ассоциацию, посылаемый клиентом новой точке доступа, является в действительности фреймом запроса на ассоциацию.

Обнаружение точки доступа во время перемещения не приводит к повышению накладных расходов, характерному для предварительного обнаружения точки доступа (в то время, когда роуминг не осуществляется), потому что клиент не знает, с какой точкой доступа он должен ассоциироваться, но зато больше времени тратится на сам процесс роуминга. На рис. 5.4 показан процесс обнаружения точки доступа во время перемещения.

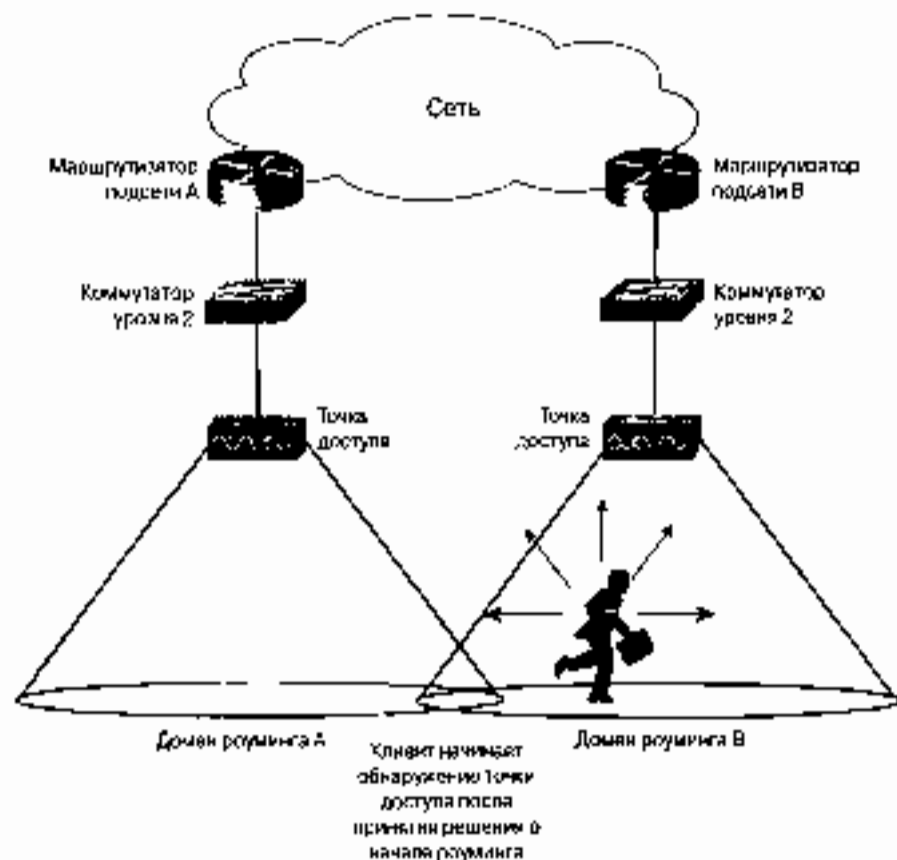


Рис. 5.4 Процесс обнаружения точки доступа во время перемещения

## Процесс роуминга уровня 2

Роуминг включает больше процессов, чем необходимо для поиска точки доступа, с которой можно связаться. Ниже описываются некоторые из задач, решаемых в ходе роуминга уровня 2.

1. Предыдущая точка доступа должна определить, что клиент уйдет из ее области действия.
2. Предыдущая точка доступа должна буферизировать данные, предназначенные для клиента, осуществляющего роуминг<sup>2</sup>.
3. Новая точка доступа должна показать предыдущей, что клиент успешно переместился в ее зону. Этот этап обычно выполняется с помощью одно- или многоадресных пакетов, передаваемых старой точкой доступа для новой и содержащих MAC-адрес источника, указывающий MAC-адрес перемещающегося клиента.
4. Предыдущая точка доступа должна послать буферизированные данные новой точке доступа.
5. Предыдущая точка доступа должна определить, что клиент покинул ее зону действия.
6. Точка доступа должна обновить таблицы MAC-адресов на коммутаторах инфраструктуры, чтобы избежать потерь данных перемещающегося клиента.

На рис. 5.5 и 5.6 представлен процесс роуминга клиента от одной точки доступа к другой, причем обе они находятся в одном домене роуминга. Эти точки доступа подключены к различным коммутаторам уровня 2.

На рис. 5.5 показано, как сервер приложений посылает данные клиенту с MAC-адресом A.B. Коммутатор уровня 3 (L3) перенаправляет фрейм с MAC-адресом назначения A.B коммутатору SW1 через интерфейс 1 (Int1). Коммутатор SW1 проверяет свою таблицу перенаправлений и посылает этот фрейм точке доступа AP1.

На рис. 5.6 показано, как клиент перемещается к точке доступа 2 (AP2) от точки доступа 1 (AP1), но AP1 "не знает", что этот клиент покинул зону ее действия. Сервер приложений продолжает посылать фреймы коммутатору уровня 3 (L3), и L3 возвращает эти фреймы через свой интерфейс 1 (Int1) коммутатору SW1 и точке доступа AP1. Последняя пытается послать эти фреймы клиенту, но заканчивает отбрасыванием фреймов, потому что клиент не отвечает. Точка доступа 2 (AP2) разряжает обставку, послая пакет точке доступа 1 (AP1) с MAC-адресом источника, указанным как MAC-адрес клиентской станции, осуществляющей роуминг, в данном случае A.B. На рис. 5.7 показано, как точка доступа обновляет таблицы перенаправлений коммутаторов.

Точка доступа 2 (AP2) посылает фрейм с клиентским MAC-адресом источника точке доступа 1. Коммутатор SW2 обновляет свою таблицу перенаправлений, поскольку он получил новый MAC-адрес на свой порт входящих (ingress port). Адрес источника, содержащийся во фрейме (MAC-адрес клиента), добавляется в таблицу перенаправлений и сопоставляется входящему интерфейсу (т.е. MAC-адрес A.B сопоставляется с Int 3). Коммутатор L3 обновляет свою таблицу перенаправлений, чтобы показать, что станция назначения теперь доступна через интерфейс 0 (Int 0). Этот фрейм выпрощается на коммутатор SW1, и SW1 обновляет свою таблицу перенаправлений аналогичным образом. Обратите внимание на то, что SW1 убирает запись с MAC-адресом клиента из своей таблицы перенаправлений. Все входящие фреймы для клиента теперь правильно перенаправляются через SW2 к точке доступа 2 (AP2).

<sup>2</sup> Эти данные не регламентированы, потому что они не специфицированы стандартом 802.11 — *Прим. авт.*

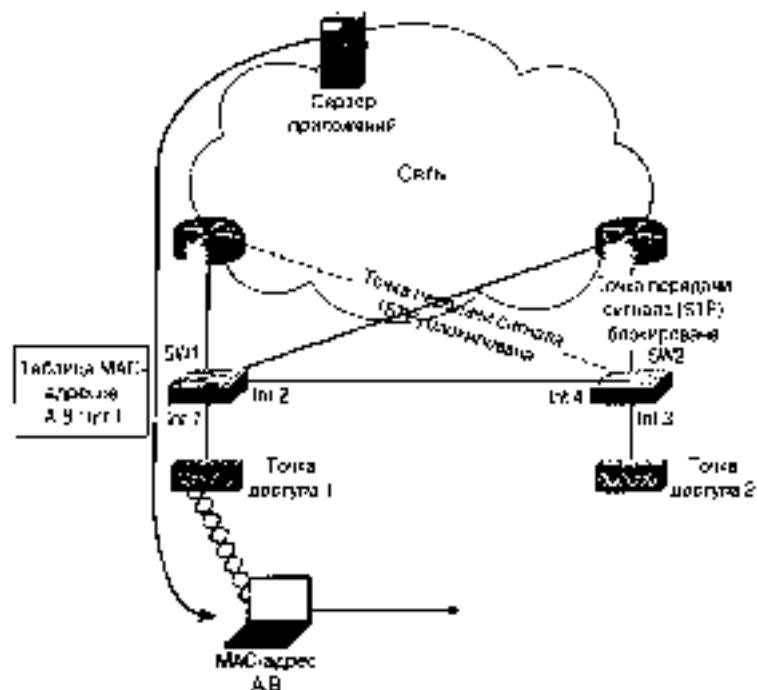


Рис. 5.3. Приложение получает данные перемещающейся станции

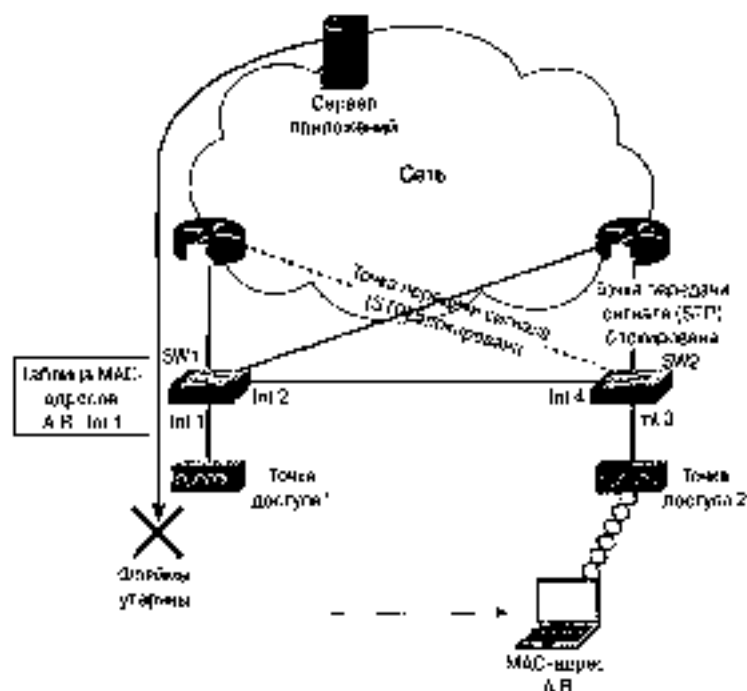


Рис. 5.4. Потери данных в результате разницы уровня 2

Поскольку IEEE и стандарт 802.11 не регламентируют установление связей между точками доступа через распределительную систему (в данном случае проводной интерфейс), поставщики точек доступа применяют эти механизмы по своему усмотрению. В зависимости от поставщика эти механизмы могут основываться на отправке либо многоадресного фрейма с MAC-адресом источника, соответствующим MAC-адресу клиента, и MAC-адресом пункта назначения, соответствующим предыдущей точке доступа, информируя предыдущую точку доступа о том, что клиент переместился, и обновляя в ходе этого процесса таблицу MAC-адресов.

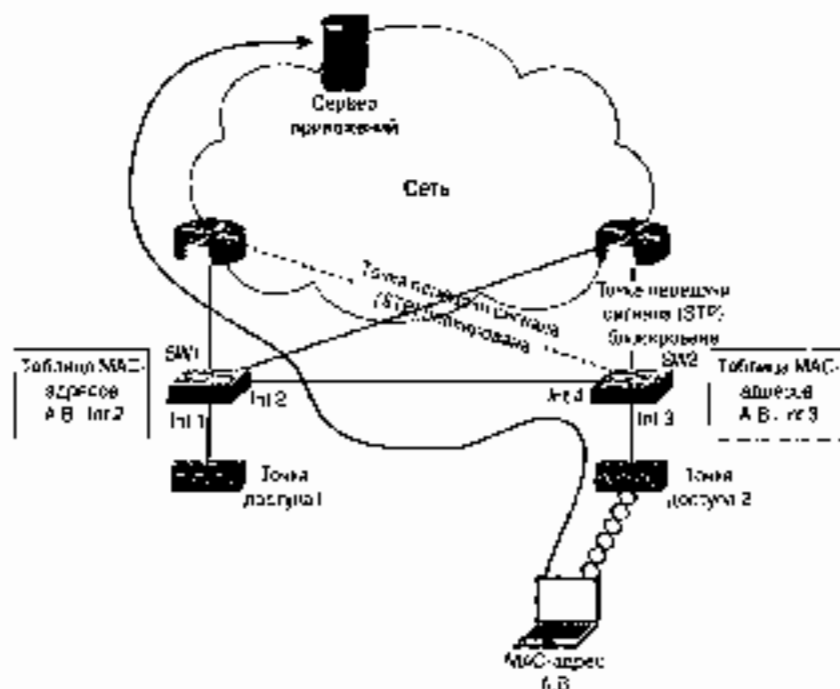


Рис. 5.7. Обновление таблицы MAC-адресов после перемещения клиента

## Роуминг уровня 3

Мобильность уровня 3 основывается на мобильности уровня 2. Клиент стандарта 802.11 должен выполнить роуминг уровня 2, включая обнаружение точки доступа, прежде чем он начнет адаптировать роуминг уровня 3. В данном разделе рассматриваются проблемы, относящиеся к роумингу уровня 3, особенно к протоколу IP и расширениям мобильного протокола IP. В нем рассматриваются следующие темы

- Роуминг между доменами роуминга.
- Обзор мобильного протокола IP.

## Роуминг между доменами роуминга

Как уже говорилось, домен роуминга определяется как совокупность точек доступа, которые относятся к одному и тому же географическому региону и сколапши-

принципы с одним и тем же SSID. Другими словами, клиент может осуществлять роуминг только между точками доступа одной и той же виртуальной локальной сети (VLAN), имеющими один и тот же SSID. Если беспроводная LAN используется в масштабах организации, может возникнуть необходимость в доменах роуминга, распределенных за пределы одного уровня 2 виртуальной локальной сети.

Рассмотрим следующий сценарий. Компания А занимает четырехэтажное здание, в котором развернута беспроводная LAN. Первоначально ее размеры были велики, и беспроводная LAN представляла собой одну подсеть класса С, развернутую в пределах всего здания. Домени роуминга охватывал все четыре этажа здания. Со временем количество пользователей увеличилось настолько, что пропускная способность подсети оказалась исчерпанной и ее характеристики ухудшились из-за увеличения трафика широковещания.

Компания А решила использовать по одной подсети своей беспроводной LAN для каждого этажа. Это вызвало осложнения, поскольку теперь домены роуминга были ограничены отдельными этажами, и не охватывали все здание, как раньше. После внедрения новой модели подсети устойчивость работы приложений при роуминге между этажами была утрачена. Это касалось в основном беспроводных устройств IP-телефонии, видеоконференц и компании А. Когда пользователи перемещались между этажами (и между подсетями) со своими беспроводными телефонами, они теряли возможность разговаривать. На рис. 5.8 проиллюстрирован описанный сценарий. Здесь IP-телефон стандарта 802.11 осуществляет связь с проводным IP-телефоном. Если пользователь перемещается от точки доступа 1 подсети 10 к точке доступа 2 подсети 20, связь прерывается, потому что перемещающийся пользователь попадает в другую подсеть.

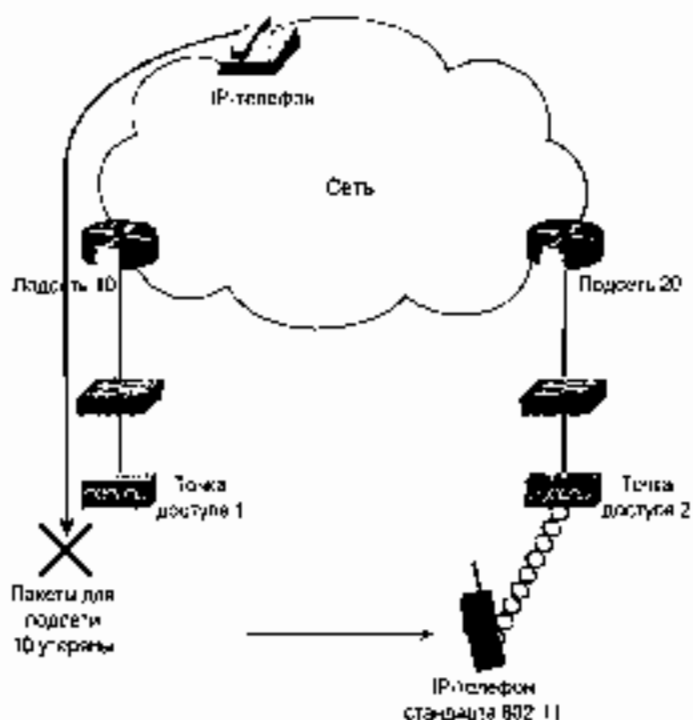


Рис. 5.8 Роуминг между подсетями

## Обзор мобильного протокола IP

Сценарии, описанные ниже для компании А, относятся к числу распространенных. Многие приложения требуют устойчивых соединений и прерывают свои сеансы связи при разрыве между VLAN. Чтобы обеспечить устойчивость сеансов связи, необходимо механизм, который позволит бы станциям поддерживать связь и тот же адрес уровня 3 при разрыве в пределах сети, состоящей из нескольких VLAN. Такой механизм обеспечивает мобильный протокол IP, который представляет собой решение для роуминга уровня 3 в беспроводных LAN, основанное на стандартах, обеспечивающее взаимодействие устройств различных поставщиков.

Сеть, способная поддерживать мобильный IP, должна иметь следующие основные компоненты.

- **Мобильный узел (mobile node, MN).** Представляет собой станцию, осуществляющую роуминг.
- **Внутренний агент (home agent, HA).** Внутренний агент (иногда его называют *домашний агент*) размещается на маршрутизаторах или коммутаторах уровня 3 и следит за тем, чтобы перемещающиеся MN получали свои IP-пакеты.
- **Внешний агент (foreign agent, FA).** Внешний агент размещается на маршрутизаторах или коммутаторах уровня 3, его задача — известить внутреннего агента (HA) о новом местонахождении MN и затем принимать пакеты от HA, предназначенные для MN.
- **Адрес для передачи (care-of address, CoA)** Это временный адрес, выданный FA для MN, на который направляются пакеты, предназначенные HA и предназначенные для MN.
- **Соприженный адрес для передачи (Co-located care-of address, CCoA).** Временный адрес, присвоенный самому MN.

Роуминг в сети, поддерживающей мобильный IP, включает следующие этапы.

1. Считается, что станция находится в своей домашней подсети, если IP-адрес станции принадлежит сети HA.
2. Если MN перемещается во внешнюю подсеть, MN обнаруживает присутствие FA и регистрируется на FA или сам получает временный адрес (CCoA).
3. FA или MN CCoA связывается с HA и создает туннель между HA и CoA для MN.
4. Пакеты, предназначенные для MN, посылаются HA (с использованием обычной IP-маршрутизации), как показано на рис. 5.9.
5. HA перенаправляет пакеты через туннель мобильному агенту.
6. Все пакеты, которые передает MN, отправляются через FA так, как если бы MN был локализован в его подсети (рис. 5.10). (Режим "обратного туннеля" возможен, когда граничные маршрутизаторы (edge routers) применяют фильтрацию входящих пакетов.)

Итак, три основные фазы работы мобильного IP таковы.

- Обновление агента.
- Регистрация.
- Туннелирование.

В следующих разделах каждая из этих фаз рассматривается более подробно.



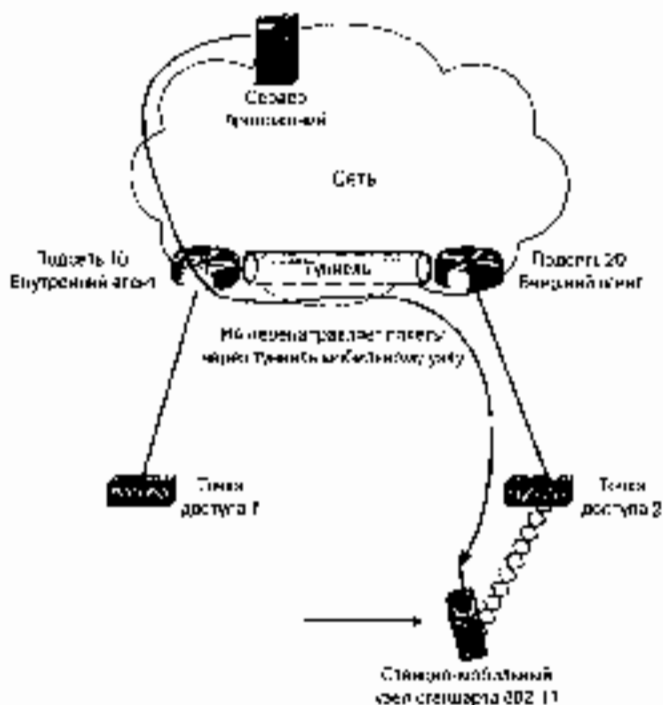


Рис. 5.9 Передача пакетов от стационарного MN

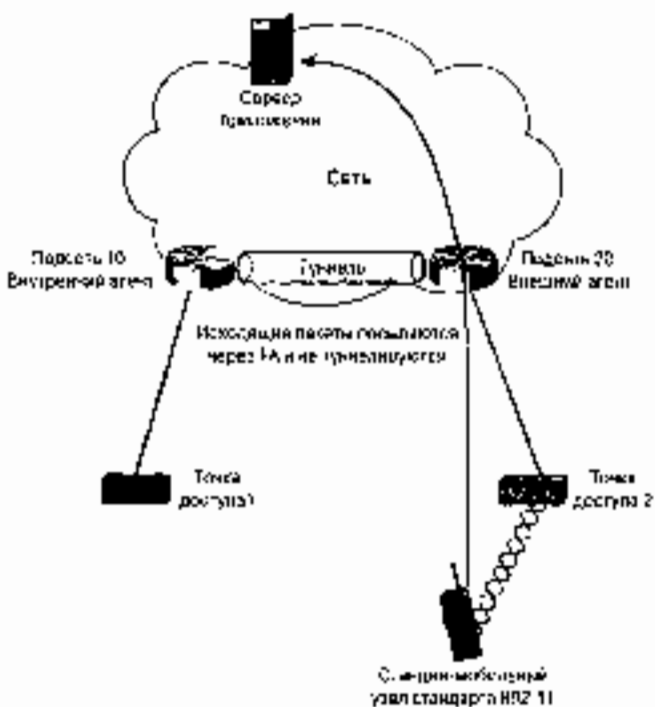


Рис. 5.10 Передача пакетов от перемещающегося MN

## Обнаружение агента

Перемещающийся MN должен своевременно обнаружить, что он находится во внешней сети, чтобы минимизировать задержку и выполнение приложений. Внутренние и внешние агенты оповещают о сменах сервисов, используя сообщения протокола межсетевых управляющих сообщений (Internet control message protocol, ICMP) и принципы обнаружения маршрута влчтра (inter-discovery protocol): вместе эти протоколы называются IRDP) для отправки агенту извещения. Когда MN устанавливает соединение с сетью, в зону действия которой он перемещается, он получает периодически рассылаемые IRDP-пакеты. Эти пакеты рассылаются или многоадресно всем хостам (по адресу 224.0.0.1), или по ограниченному широковещательному адресу (255.255.255.255). IRDP-пакеты не посылаются по широковещательному адресу конкретной подсети, поскольку MN может не знать, в зону действия какой подсети он перемещается. В дополнение к периодически рассылаемым извещениям агент MN может запротестовать извещения после того как обнаружит, что его адрес изменился.

Извещение агента содержит два поля, которые позволяют MN определить, переместился ли он в зону действия другой подсети:

- Поле времени жизни (lifetime field)
- Расширение длины префикса (prefix-length extension)

Поле времени жизни указывает значение времени, в течение которого имеет силу извещение агента. Если, прежде чем время жизни достигнет нуля, ни одно из них не извещено, MN должен повторить процедуру обнаружения нового агента.

Расширение длины префикса указывает на значение адреса сети послатающего извещение агента. Изменение длины префикса (указывающее на изменение адреса сети или подсети) означает для MN, что ему нужно повторить процедуру обнаружения нового агента.

Определяя, что он находится во внешней сети, MN выбирает сведения о CoA из извещения агента. CoA может иметь две формы:

- Адрес внешнего агента
- Сопряженный адрес для передачи. Обратите внимание на то, что CoA не содержится в извещении FA, он скорее всего приобретается мобильным агентом через протокол динамической конфигурации хоста (DHCP).

CoA, указывающий на FA, вынуждает FA (обычно это маршрутизатор подсети) поддерживать управление мобильным IP для всех внешних MN подсети в соответствии с соглашениями, связанными с перенаправлением пакетов. Преимущество этой ситуации состоит в том, что внутреннему агенту приходится создавать только один туннель от HA к каждому уникальному FA.

CoA, временно назначенный мобильному агенту, перекладывает административные обязанности мобильного IP на MN и вынуждает HA создавать уникальный туннель для каждого перемещающегося MN. На рис. 5.11 сопоставлены оба этих метода.

## Регистрация MN

После того как MN получает CoA и устанавливает локального агента мобильности (HA или FA), начинается процесс регистрации. В процессе регистрации создается надежное мобильное соединение между FA и HA, чтобы обеспечить перенаправление пакетов мобильному узлу. Процесс регистрации осуществляется следующим образом (рис. 5.12).

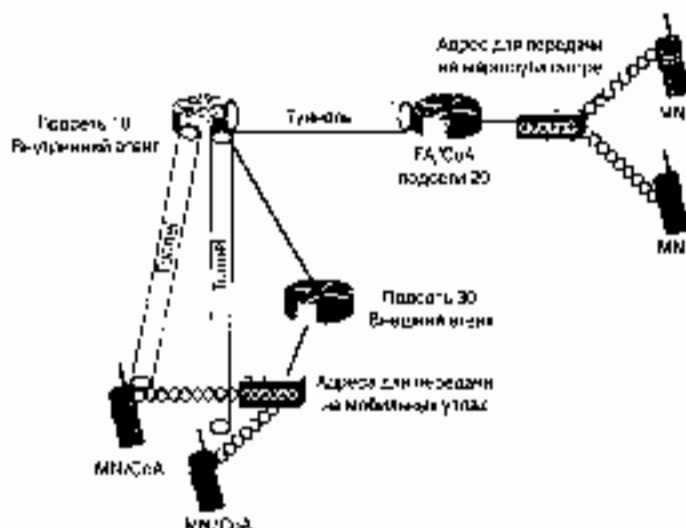


Рис. 5.11. Взаимодействие между MN и CA

1. Мобильный узел посылает запрос на регистрацию внешнему агенту. Если MN имеет CCoA, этот этап пропускается.
2. Внешний агент обрабатывает запрос на регистрацию и перенаправляет его внутреннему агенту.
3. Внутренний агент принимает или отклоняет регистрацию и посылает ответ на регистрацию внешнему агенту.
4. Внешний агент обрабатывает ответ на регистрацию и посылает его MN.

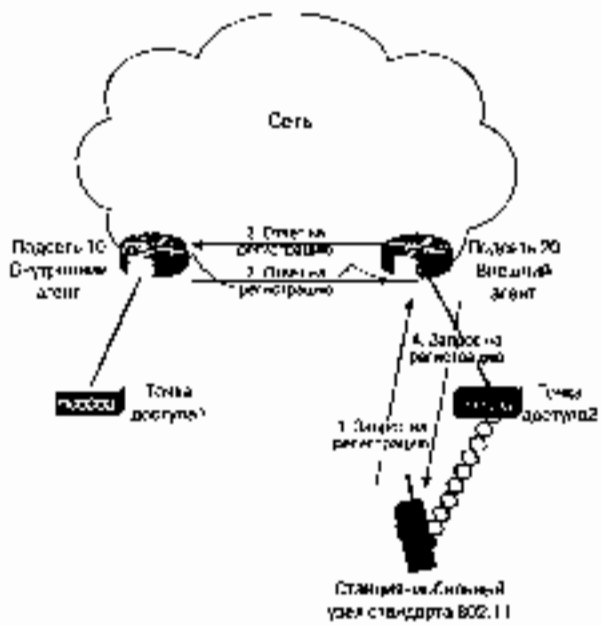


Рис. 5.12. Процесс регистрации в соответствии с мобильным IP

Запрос на регистрацию содержит следующие поля:

- **Синхронные соединения (synchronous bindings)**. MN может запросить, чтобы HA сохранил соединения с предыдущими CoA.
- **Широковещательные пакеты**. MN может запросить, чтобы HA перенаправлял все широковещательные пакеты, которые направляются ему из внутренней сети.
- **Декапсуляция осуществляется мобильным узлом**. MN может запросить, чтобы декапсуляция туннелируемых пакетов осуществлял он сам. Эта опция применяется только в том случае, если MN имеет CoA.
- **Минимальная инкапсуляция**. MN может запросить, чтобы HA применял минимальную инкапсуляцию для туннелируемых пакетов (RFC 2004).
- **Обобщенная маршрутная инкапсуляция (GRE)**. MN может запросить, чтобы HA применял инкапсуляцию по протоколу GRE для туннелируемых пакетов.
- **Реверсное туннелирование**. MN может запросить, чтобы его выходные пакеты туннелировались обратно внутреннему агенту для перенаправления им по назначению.
- **Время жизни**. В этом поле указывается время, оставшееся до конца действия регистрации.
- **Внутренний адрес (home address)**. В этом поле указывается IP-адрес MN.
- **HA**. В этом поле указывается IP-адрес HA, к которому привязан MN.
- **CoA**. В этом поле указывается IP-адрес CoA и точек подключения (connection point) туннеля.
- **Идентификация**. Это поле представляет собой 64-разрядное значение текущего времени: оно используется для поступающих запросов на регистрацию и ответов на них и предшествует проведению эха на пакеты регистрации.
- **Расширения**. Количество доступных расширений, не требуемых для регистрации.

Ответ на запрос относительно регистрации содержит следующие поля:

- **Code**. В этом поле содержится результат регистрации. Значения результата данного поля представлены в табл. 5.1.
- **Время жизни**. В этом поле указывается число секунд, оставшееся до конца действия регистрации.
- **Внутренний адрес (home address)**. В этом поле указывается IP-адрес MN.
- **HA**. В этом поле указывается IP-адрес HA.
- **Идентификация**. Содержимое этого поля меняется в зависимости от основания или сообщения механизма аутентификации, используемого для обработки запроса на регистрацию.
- **Расширения**. Количество расширений, которые допустимы, но не требуются для регистрации.

Таблица 5.1. Значения поля Code

Значение поля Code	Источник	Что означает
0	HA	Регистрация принята
1	HA	Регистрация принята, но синхронные соединения не приняты

Значение поля Code	Источник	Что означает
64	FA	Причина не специфицирована
65	FA	Запрещена администрация
66	GA	Недостаточные ресурсы
67	FA	MN не прошел процесс аутентификации
68	FA	NA не прошел процесс аутентификации
69	FA	Затребованное время жизни через сервер слишком
70	FA	Плохо сформированный запрос
71	FA	Плохо сформированный ответ
72	FA	Запрошенная инкапсуляция невозможна
73	FA	Зарезервирован и недоступен
77	FA	Недействительный CoA
78	FA	Тайм-аут регистрации
80	FA	Внутренняя сеть недоступна (получено сообщение об ошибке от ICMP)
81	FA	Хост NA недоступен (получено сообщение об ошибке от ICMP)
82	FA	Порт NA недоступен (получено сообщение об ошибке от ICMP)
88	FA	NA недоступен (получено другое сообщение об ошибке от ICMP)
128	NA	Причина не специфицирована
129	NA	Запрещена администрация
130	NA	Недостаточные ресурсы
131	NA	MN не прошел процесс аутентификации
132	NA	NA не прошел процесс аутентификации
133	NA	Идентификация регистрации не подходит (Registration identification mismatch)
134	NA	Плохо сформированный запрос
135	NA	Слишком много одновременных мобильных соединений
136	NA	Неизвестный адрес NA

Стандарт мобильного IP требует какого-то используемого ключа и механизма на общепринятых механизмах аутентификации (keyed message-authentication mechanism), защищающего сообщения регистрации, передаваемые между MN и FA (сообщения между FA и NA могут быть аутентифицированы, но обычно этого не делают) и optionally позволяющего также защищать сообщения, передаваемые между MN и FA. По умолчанию доступны хэшированные ключи сообщений аутентификации (hashed message authentication codes) и приритель сообщения (message digest) версии 5 (HMAC-MD5). NA должен использовать секретное значение совместно с MN, или статически сконфигурированное, или хранящееся централизованно на сервере аутентификации, авторизации и учета (AAA). На рис. 5.13 показаны, как выполняется процесс аутентификации сообщений.

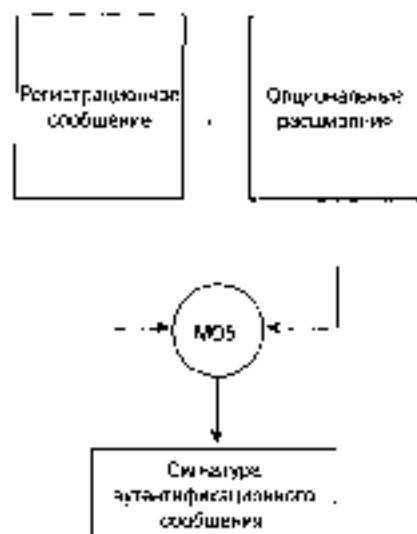


Рис. 5.13. Организация защиты сообщений, полученных в ходе регистрации

Другие проблемы с защитой могут возникнуть, когда вы попытаетесь применить мобильный IP в своей сети. Если на маршрутизаторах FA осуществляется контроль фильтрации адреса источника (source address filtering check, RFC 2827), перенаправление пакетов от MN через FA не может осуществляться. Выходной интерфейс FA способен фильтровать только действительные IP-адреса источника, чтобы предотвратить проникновение в сеть псевдонимных устройств. Такая фильтрация создает проблемы для мобильных узлов, потому что они передают пакеты с IP-адресом своей внутренней сети, и, как результат, все переданные фреймы будут теряться на маршрутизаторе FA.

Чтобы обойти эту проблему, нужно использовать реверсное туннелирование. Реверсное туннелирование несколько увеличивает административные «накладные расходы» для CoA и HA, но обеспечивает функционирование мобильного IP в защищенной сети.

## Туннелирование

Термин «туннелирование» является синонимом термина «инкапсуляция». Туннелирование позволяет двум неравноправным сетям напрямую соединяться между собой, хотя обычно они этого сделать не могут или физически удалены. Такая возможность очень важна для мобильного IP, потому что именно благодаря туннелированию HA может пренебречь обычными правилами маршрутизации и перенаправить пакеты MN.

Для образования туннеля необходимы две конечные точки: входная и выходная. Входная точка инкапсулирует туннелирующие пакеты, добавляя их другим IP-заголовком. Новый IP-заголовок может включать некоторые другие параметры, но основная функция заголовка инкапсуляции состоит в направлении пакета конечной точке туннеля. Пакет, полученный конечной точкой туннеля, освобождается от заголовка инкапсуляции и перенаправляется MN. На рис. 5.14 показан процесс туннелирования пакетов.

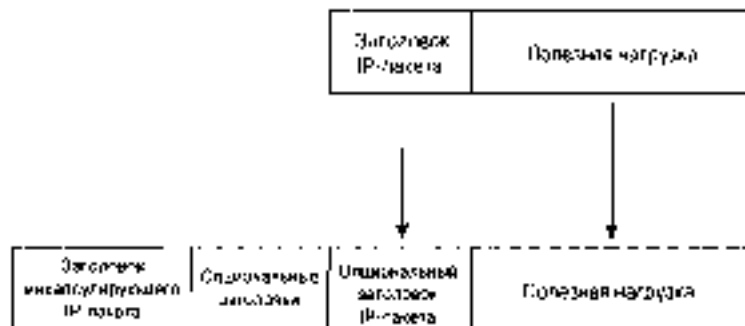


Рис. 5.14. Инкапсуляция IP-пакетов

Мобильный IP поддерживает несколько механизмов туннелирования.

- Инкапсуляция IP в IP.
- Мультикапсуляция.
- Обобщенная маршрутная инкапсуляция (GRE).

Инкапсуляция IP в IP является единственным типом туннелирования, регламентированным спецификацией мобильного IP, но часто используется GRE для мультикапсуляции, потому что каждый из них оказывает несколько других влияний на сеть, и вы можете использовать их, чтобы определить, какой же лучше удовлетворит вашим требованиям.

В некоторых сетях применяется фильтрация в соответствии с RFC 2827 на интерфейсах распределительных маршрутизаторов (distribution router), которые позволяют передавать по сети пакеты только от действительных источников. Например, интерфейс маршрутизатора имеет сеть 10.0.0.0/24 (IP-адреса с 10.0.0.1 по 10.0.0.254). Мобильный узел с внутренним адресом 192.168.10.1 не смог бы послать пакеты через такой маршрутизатор, потому что IP-адрес 192.168.10.1 не относится к подсети 10.0.0.0/24. Для того чтобы MN мог послать пакеты в данном случае, FA должен перенаправить эти пакеты обратно во внутреннюю подсеть через NA. Этот сценарий показан на рис. 5.15. Обратное туннелирование ведет к увеличению дополнительных пакетов и замедлению работы приложений, но оно обеспечивает использование фильтрации в соответствии с документом RFC 2827 для обеспечения защиты сети.

## Резюме

Беспроводные LAN стандарта 802.11 облегчают реализацию беспроводной мобильности, но для приложения развертывания мобильной сети вы должны понимать природу приложений, выполняемых в вашей беспроводной LAN. Многие беспроводные LAN развертываются с прицелом на максимальное покрытие (обычно с большим количеством точек доступа, приходящихся на одну точку доступа), когда главной целью считается обеспечение беспроводных соединений. По мере появления и применения новых приложений, таких как IP-телефония по стандарту 802.11, приходится вносить изменения в уже развернутую беспроводную LAN. Сеть, ориентированная на максимальное покрытие, должна эволюционировать в сторону сети с большей пропускной способностью (малое отношение число пользователей/число точек доступа, но больше точек доступа в зоне покрытия). Развитие в направлении беспроводных LAN с боль-

иной прилуксно́й способно́сти́ требует их развертывания в масштабах предприятия с обеспечением роуминга между доменами роуминга.

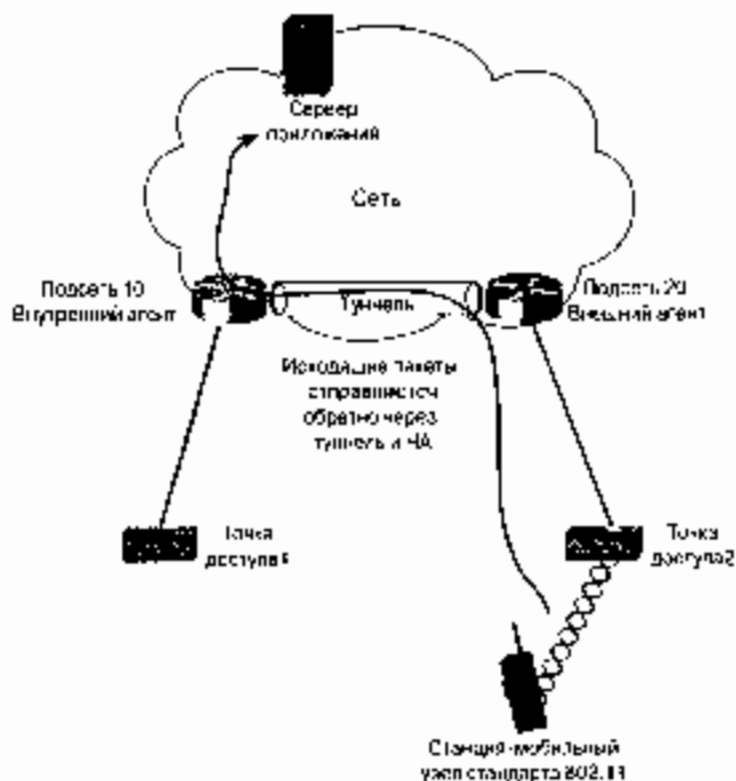
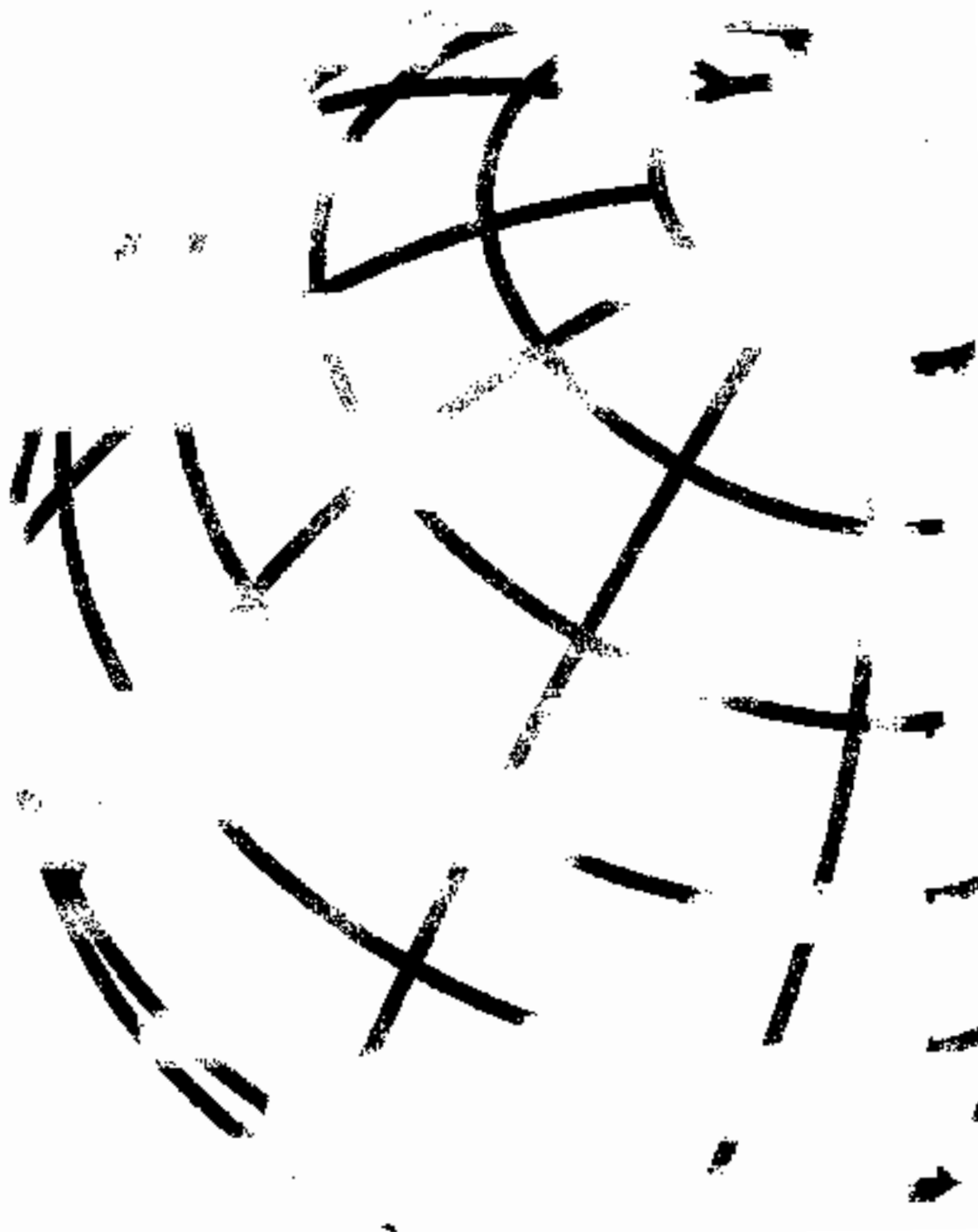


Рис. 5.15. Реверсное проксиирование







## Качество обслуживания беспроводных LAN — стандарт 802.11e

### Задачи по достижению заданного QoS в сетях стандарта 802.11

Рабочая группа 802.11 IEEE организовала исследовательскую группу 802.11e и поставила перед ней задачу улучшить уровень QoS стандарта 802.11 с тем, чтобы он обеспечивал высокое качество обслуживания (QoS) для поддержки чувствительных к задержкам приложений, таких как передача голоса и видео. Кроме того, новые поколения потребителей электроники рассматривают устройства стандарта 802.11 как заменяющие аналоговые приводы. Такие изделия, как кабельные или спутниковые приемники, должны в один прекрасный день начать передавать сигналы телевидения высокой четкости (HDTV) через среду 802.11 бытовым телевизорам. То же самое должны делать цифровые видеоматричные и пишущие DVD-приводы. Представьте, что все это реализовано в жилом доме, где технология стандарта 802.11 используется в домашней сети, а также для связи производных устройств, начиная с DVD-проекторов и спутниковой тарелки и заканчивая телевизором. Новые области применения для технологий стандарта 802.11 требуют эффективного механизма QoS, обеспечивающего приоритет передачи данных, чувствительных к задержкам (таких как аудио- и видеопотоки), по отношению, например, к электронной почте и просмотру Web-страниц. Например, прерывание просмотра фильма из-за того, что пришел электронный письмо или кто-то что-то ищет в Google, вызвало бы раздражение.

В данной главе рассказывается о том, как рабочая группа по внедрению стандарта 802.11 работает над проблемой реализации заданного качества обслуживания путем просмотра запросов на эффективное QoS в сетях стандарта 802.11, обсуждаются QoS-механизмы, предлагаемые в черновых текстах проекта стандарта 802.11e, и обсуждается проблема управления входом в локальную LAN.

Стандарты 802.11 хороши для узкополосных, нечувствительных к задержкам приложений. Сканеры штрих-кодов, персональные цифровые помощники (PDA), сервисы Web или зашифрованной почты могут эксплуатировать беспроводные сети без физических ограничений, вызванных кабелем сети или возможной существенной потерей информации. Но если предприятие начинает развертывать беспроводную LAN (WLAN), которая будет применяться в условиях локального рынка, такого как уход за больными или розничная торговля, ему безусловно потребуется поддержка IP-телефонии (VoIP) и передачи видеоданных через беспроводную среду.

Вы правильно делаете, если задумались над этим. За счет использования IP-телефонии можно уменьшить количество звонков по сотовым телефонам между служащими (когда компания оплачивает эфирное время). Такое снижение степени использования сотовых телефонов даст администратору сети оптимальным образом средства, позволяющие повысить коэффициент окупаемости инвестиций (ROI), сделанных в развертывание WLAN.

Высокое качество обслуживания характерно для зрелых технологий, применяемых в проводных сетях, в таких устройствах, как маршрутизаторы, коммутаторы и оконечные устройства (например, проводные IP-телефоны). Для беспроводных сетей стандарта 802.11 справедливо противоположное утверждение. Это — недавно появившаяся технология, которая горячо обсуждается в IEEE и производителями WLAN. Главные проблемы, стоящие перед механизмом реализации заданного качества обслуживания в сетях стандарта 802.11, следующие.

- **Полудуплексная среда.** Стандарт 802.11 относится к совместно используемой, полудуплексной среде, в то время как большинство проводных сетей Ethernet, обеспечивающих высокое качество обслуживания, является полнодуплексными.
- **Некоторые каналы BSS перекрываются** (иногда это называют “перекрытие по совместному каналу”). В случаях, когда два соседних BSS стандарта 802.11 работают на одном и том же канале, может произойти интерференция сигналов и их затухание.
- **Скрытый узел.** Узлы, находящиеся в зоне действия точки доступа, но “не видящие” один другого, могут вызывать коллизии и оспору конкурентную за доступ к среде в BSS.

В следующих разделах подробно рассматриваются каждая из проблем, подлежащих решению для повышения качества обслуживания в сетях стандарта 802.11.

## Влияние на QoS полудуплексной среды

В главе 2, “Беспроводные локальные сети стандарта 802.11”, описаны основные механизмы доступа для сетей стандарта 802.11, введенные в 1997 году, — с централизованной распределенной функцией координации (DCF) и точечной функцией координации (PCF). Оба механизма позволяют одновременно осуществлять передачу через среду только одной станции, это может быть точка доступа или клиентская станция. Приведенный Ethernet, и, в частности, работающая по стандарту 802.3x в полнодуплексном режиме, создает канал связи типа “точка-точка” между Ethernet-станциями, позволяя одновременно передавать и принимать данные. Такая технология теоретически доминирует Ethernet-среде удваивать свою нормальную полосу пропускания. (Канал Full Ethernet способен передавать и одновременно принимать данные со скоростью 100 Мбит/с, в сумме это эквивалентно потоку пропускания 200 Мбит/с.) Иначе говоря, станция, которая собирается передавать

данных, не конкурирует со станцией, находящейся на противоположном конце канала и также собирающейся передать данные.

Этот сценарий противоположен таковому, характерному для сетей стандарта 802.11. За право доступа к среде состязаются не только станция и точки доступа, но и клиенты между собой. Механизм PCF реализует идею последовательного доступа, когда точка доступа может действовать как точка координации и обрабатывать каждого клиента по очереди *пока*, *нужно* для ему что-то передать. Хотя при небольшом числе клиентов, обслуживаемых BSS, такая методика представляется рациональной, было выяснено, что она приводит к уменьшению пропускной способности среды по сравнению с обычным, основанным на конкуренции доступом в режиме распределенной функции координации (DSSS). При отсутствии механизмов для координации моментов времени передачи клиентов к установлению приоритета между последними поставщиками должны преодолеть серьезные проблемы, чтобы обеспечить работу таких чувствительных к задержкам приложений, как IP-телефония.

## Перекрытие по совмещенному каналу

*Перекрытие по совмещенному каналу (cochannel overlap)* часто происходит в беспроводных LAN диапазона 2,4 ГГц, если они имеют более трех точек доступа. Из-за того что в этом диапазоне можно разместить лишь **три** неперекрывающихся канала, некоторые точки доступа работают вблизи соседних точек доступа на одном и том же канале. Что это означает для клиентов таких BSS? На рис. 6.1 показан клиент, находящийся в зоне перекрытия по совмещенному каналу. Если обе точки доступа начинают передачу одновременно, фреймы вступают в коллизию и обе станции должны ответить средой и повторить передачу. Вы можете рассмотреть и другой сценарий, называемый *черная дыра ширококешательная (broadcast black hole)*. Если в BSS входит энергосберегающая станция, все ширококешательные и многоадресные фреймы посылаются после сигнального фрейма, содержащего карту маршрутизации трафика (DTIM beacon). В большинстве случаев обе точки доступа, входящие в расширенную зону обслуживания (ESS), имеют одинаковый сигнальный интервал и одинаковый интервал рассылки DTIM. Если внутренние таймеры соседствующих точек доступа, использующих совмещенный канал, сработают почти одновременно, обе они могут рассылать ширококешательный и многоадресный трафик одновременно, вызывая коллизию фреймов в зоне перекрытия, из-за чего входящий в этой зоне клиент пропустит эти фреймы. В отличие от одноадресных фреймов, получение ширококешательных и многоадресных фреймов не подтверждается, поэтому повторно они передавать не будут. Перекрытие по совмещенному каналу может нарушить работу механизма QoS из-за увеличения конкуренции за среду в сетях стандарта 802.11, вместе с ситуацией черной дыры это может привести к тому, что клиент не сможет получать потенциально важной для него график.

## Влияние скрытого узла на качество связи

Проблема скрытого узла, описанная в главе 2, осложняет обеспечение высокого качества связи в сетях стандарта 802.11 в целом. Использование сообщений готовности к передаче/готовности к приему (RTS/CTS) для резервирования среды имеет целью решение проблемы скрытого узла, но сообщения RTS/CTS применяются после обнаружения коллизии и после соответствующего возврата к исходному состоянию.

Увеличенная задержка может повлиять -- и ширеет -- на работу чувствительных к задержкам приложений. Устройства, использующие сообщения RTS/CTS при передаче каждого фрейма, также приносят к ухудшению характеристик из-за большого избыточного трафика, сопровождающего каждый фрейм данных.

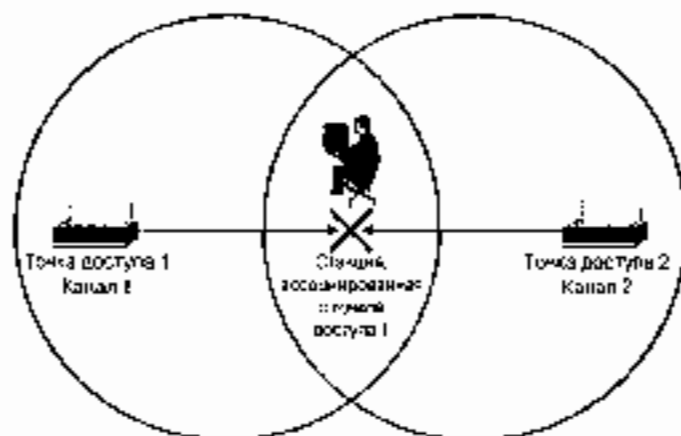


Рис. 6.1. Перекрытие на совместному каналу

## Обзор механизма QoS

Исследовательская группа 802.11e обсуждала многие проблемы, включая описанные в предыдущем разделе. Она предложила два возможных решения для уровня MAC будущих сетей стандарта 802.11. Примите во внимание, что предложенные спецификации еще не утверждены и в них могут быть внесены изменения уже после выхода этой книги. Текущие предложения группы 802.11e решения таковы:

- Гибридная функция координации (*hybrid coordination function*, HCF) с работой в режиме конкуренции. Чаще это решение называют *расширенная распределенная функция координации* (*enhanced DCF*, EDCF).
- HCF с работой в режиме поочередного доступа.

### HCF в режиме конкуренции — механизм доступа EDSF

В проекте спецификации стандарта 802.11e сделана попытка разбить все данные на восемь классов. EDSF и HCF в режиме поочередного доступа используют эти восемь классов, называемые *классы трафика* (*traffic classes*, TC), соотношения которых с сетью классов, определенными в стандарте 802.1D, представлено в табл. 6.1. Трафик от обеспечивающих должно качество связи классом разделен на четыре большие категории, называемые *категории доступа* (*access categories*, AC). Категории доступа 0-3 указывают на приоритет классов стандарта 802.1D.

Таблица 6.1. Соответствие классов трафика категориям доступа

ТС по стандарту 802.1D	Описание	АС и очередность передачи
1	Низкий приоритет	0
2	Низкий приоритет	0
0	Наибольшее благоприятствование (best effort)	0
3	Сигнализация/контроль	1
4	Видеокондиционирование (video probe)	2
5	Видео	2
6	Голос	3
7	Управление сетью	3

Любая система, обеспечивающая высокое качество, нуждается в трех основных компонентах:

- Механизм классификации трафика.
- Механизм пометки трафика соответствующим значением качества связи (QoS).
- Механизм дифференцирования и приоритизации трафика, основанный на значении QoS.

Механизм классификации и пометки фреймов данных не подпадает под действие проекта документа 802.11e, но можно предположить, что приложение (такое как обеспечивающее передачу речи и установленное в телефоне стандарта 802.11) должно по крайней мере отметить биты приоритета IP-действительности или использовать код указателя дифференцированной службы (differentiated services code point, DSCP). Не бойтесь ошибиться, можно также предположить, что клиентское устройство преобразует эти значения уровня 3 в классы трафика стандарта 802.11e. При наличии классифицировочного и служебного метками трафика стандарт 802.11e обеспечивает механизм дифференциации и приоритизации передаваемого трафика.

## Доступ к каналу для дифференцированного трафика

После того как трафик классифицирован и помещен в соответствующую очередь, следующий шаг состоит в передаче фреймов. Проблема состоит в том, как обеспечить приоритет в передаче фреймов для клиентских устройств, но связанных непосредственно одно с другим. IEEE берется за решение этой проблемы, являя несколько новых концепций и реализует новые функции:

- **Благоприятная возможность для передачи (transmit opportunity, TXOP)**. TXOP — это момент, когда станция может начать передачу фреймов и продолжать делать это в течение определенного времени. В отличие от доступа к среде с использованием механизма CS/CF (см. главу 2, "Беспроводные локальные сети стандарта 802.11"), когда каждый фрейм сопровождается еще его подтверждение клиенту жеркут за доступ к среде, механизм TXOP может обеспечить передачу сразу многих фреймов/подтверждений, главное — чтобы они умещались в первом TXOP (табл. 6.2).
- **Арбитражный межфреймовый промежуток (arbitration interframe space, AIFS)**. AIFS арбитрует межфреймовую прикжукку IEEE, рассмотренную нами в главе 2.

но размер JFS изменяется в зависимости от категории доступа (AC). Этот процесс дает возможность станциям с более высоким приоритетом использовать более короткие AIFS, а низкоприоритетным станциям — более длительные AIFS. Чем больше AIFS тем выше шансы получения первоочередного доступа к каналу.

Некоторые уже известные концепции используются по-другому. В главе 2 говорилось о том, что значения окна конкуренции  $CW_{min}$  и  $CW_{max}$  устанавливаются для каждой DCF-станции и изменяются только при повторных попытках доступа к каналу. В случае EDSF различные AC предполагают и различные значения CW, что повышает частоту высокоприоритетных станций на первоочередный доступ к среде.

В табл. 6.2 приведены устанавливаемые по умолчанию параметры, такие как ширина окна конкуренции (CW), AIFS и TXOP для каждой категории доступа (AC).

**Таблица 6.2. Параметры доступа к среде для различных категорий доступа**

AC	$CW_{min}$	$CW_{max}$	AIFS	Предельный TXOP (802.11b)	Предельный TXOP (802.11a/g)
0	Стандартное 802.11 $CW_{min}$	Стандартное 802.11 $CW_{max}$	2	0	0
1	Стандартное 802.11 $CW_{min}$	Стандартное 802.11 $CW_{max}$	1	3,0 мс	1,5 мс
2	$(CW_{min} + 1)/2 - 1$	Стандартное 802.11 $CW_{max}$	1	6,0 мс	3,0 мс
3	$(CW_{min} + 1)/4 - 1$	$(CW_{max} + 1)/2 - 1$	1	3,0 мс	1,5 мс

Необходимые комментарии к табл. 6.2 приведены ниже.

- Категория доступа AC(0) классифицируется как имеющая трафик наибольшего благоприятствования (best effort traffic), поэтому ее параметры приблизительно соответствуют стандартным значениям DCF, за исключением DIFS, который имеет значение канального интервала, равное DIFS + 1. Обратите также внимание на то, что значение предельной длительности TXOP, равное 0, указывает на то, что может быть передан только один фрейм.
- Станция категории доступа AC(1), т.е. с несколько более высоким приоритетом, имеет такие же параметры доступа к среде, как EDSF-станция стандарта 802.11, за исключением длительности TXOP, которая позволяет передать несколько фреймов и подтверждений.
- Станция с категорией доступа AC(2) имеет менее широкое окно конкуренции, чем станции категорий с меньшим приоритетом, и более длительные TXOP. Чтобы проиллюстрировать влияние менее широкого окна конкуренции, отметим следующее.
  - По умолчанию начальное значение  $CW_{min}$  обычно составляет 7 канальных интервалов. DCF-станции случайным образом выбирают значение отсрочки передачи между 0 и  $CW_{min}$  (в данном случае 7) и используют его для инкрементирования значения счетчика. Для категории доступа AC(2) значение  $CW_{min}$  с 7 уменьшается до 3. Такая станция может выбирать значение отсрочки передачи между 0 и 3, т.е. временное окно будет гораздо уже. Значение  $CW_{max}$  также изменяется, теперь для него используется значение  $CW_{max}$ .



равное  $T$ . В данном случае, после того как станция откажется от передачи и ее окно конкуренции достигло значения  $CW_{min}$ , она будет инкрементировать оставшееся значение счетчика прямого быстрого.

- Станция с категорией доступа AC(3) имеет такое узкое окно конкуренции из всех категорий, для нее характерен также самый короткий предел длительности TXOP. Фреймы с категорией доступа AC(3) — это обычно фреймы управления сетью или используемые для передачи речи, они невелики по объему и не требуют много "эфирного времени" для успешной передачи.

Каждая из категорий доступа поддерживается обеспечивающей QoS станцией или точкой доступа. Возможно, что две или несколько станций вступят в коллизии. Станция с менее приоритетной категорией доступа может случайно выбрать короткую очередь и вступить в коллизии со станцией, имеющей более высокую категорию. В этом случае фрейм высокоприоритетной станции имеет преимущество, и низкоприоритетная станция будет вынуждена освободить среду и увеличить ширину своего окна конкуренции.

## Механизм управления входом при использовании EDSF

Целью мер, принимаемых в обеспечение QoS, является защита трафика высокоприоритетных приложений от влияния трафика низкоприоритетных приложений. Например, QoS защищает VoIP-фреймы от фреймов почтового протокола Internet (POP3). В случаях, когда ресурсы сети ограничены (это напрямую относится к WLAN стандарта 802.11), может оказаться необходимым зашиять трафик одних высокоприоритетных приложений от трафика других высокоприоритетных приложений. Это может показаться странным, но рассмотрим конкретный пример. Допустим, что в BSS возможно одновременное проведение не более чем шести разговоров (при использовании IP-телефонии). Любой трафик с данными, который попытается использовать среду передачи, будет иметь приоритет ниже, чем VoIP-трафик, поэтому участники разговоров будут довольны тем, как первоочередной переключат, без накопления фоновых искажений, и смогут плодотворно общаться.

Пусть теперь в BSS делается седьмой телефонный звонок. Независимо от того, какая зона обслуживания способна поддерживать только шесть звонков, в то же время механизм приоритизации должен позволить начаться телефонному разговору, поскольку его трафик относится к числу высокоприоритетных. Хотя разговор и начнется, он негативно повлияет на уже идущие шесть телефонных разговоров, поэтому качество связи для всех семи разговоров будет низким.

Механизм управления входом (admission control) призван решить эту проблему. Точно так же как QoS защищает высокоприоритетный трафик от низкоприоритетного, технология управления входом защищает высокоприоритетный трафик от высокоприоритетного. Механизм управления входом отслеживает различные ресурсы сети и "интеллектуально" разрешает или отказывает новым сеансам связи приложений.

Расширенная распределенная функция координации (EDSF) использует схему управления входом, получившую название *распределенное управление входом* (distributed admission control, DAC). Механизм DAC функционирует на высоком уровне, осуществляя отслеживание и измерение в процентах доли использования среды, приходящейся на каждую категорию доступа. Непользуемая доля пропускной способности среды называется *доступный бюджет* (available budget) для дан-

ной категории. О наличии бюджета сообщается станциям в информационном элементе (IE) параметра QoS, содержащемся в сигнальных фреймах точки доступа. Если бюджет начинает приближаться к нулю, станции, пытающиеся инициировать новые потоки приложений, избегают делать это, и существующим удача не приходится увеличивать или расширять TXOP, которые они уже используют. Данный процесс защищает существующие информационные потоки приложений от влияния со стороны новых потоков.

## НСФ с работой в режиме поочередного доступа

Работа НСФ аналогична работе функции точки координации РСФ (см. главу 2). Точка доступа содержит логический объект (logical entity), называемый гибридным координатором (hybrid coordinator, НС), который отслеживает потоки информации клиентских станций НСГ и передает материалы опросов. Получение доступа в результате опроса НСФ позволяет станциям требовать нужной ей TXOP, а не просто определять, какой из них доступен, как в случае использования EDCF. Работа НСФ, в сочетании с управлением входим НСФ, позволяет гибридному координатору "интеллектуально" определять, какие ресурсы беспроводной среды доступны, а принять либо отклонить информационные потоки трафика приложения. НСФ может функционировать в двух режимах, один из них сосуществует с EDCF, а второй использует период, свободный от конкуренции (CFP), аналогично РСФ.

### Работа НСФ в период, свободный от конкуренции

Работа НСФ в период, свободный от конкуренции, состоит в следующем (рис. 6.2):

1. Посылается сигнальный фрейм точки доступа, включающий IE, устанавливающий набор параметров точечной функции координации (РСФ), в котором определяются момент начала и длительность периода, свободного от конкуренции (CFP).
2. Гибридный координатор (НС) предлагает поддерживающим механизмам НСФ станциям TXOP, посылая им QoS-фреймы опроса (CF-Req).
3. Эти станции могут ответить в течение интервала времени SIFS фреймами данных (QoS Data) или нулевым QoS-фреймом, указывающим, что у станции нет трафика или что фрейм, который она хотела бы передать, слишком велик для того, чтобы она могла сделать это за время, предоставленное ей в период TXOP.
4. Период, свободный от конкуренции, заканчивается, когда НС посылает фрейм конца этого периода CF-End или истекает длительность CFP.

### Взаимодействие EDCF и НСФ

В отличие от работы в режиме РСФ, доступ в результате опроса НСФ может иметь место в период конкуренции и сосуществовать с режимом работы EDCF, а также с режимом работы DCF. Периоды TXOP опросов "распределяются" между гибридными станциями НСФ и способствуют передаче или приему фреймов с данными при обеспечении QoS. НС получает доступ к среде раньше EDCF-станции, потому что должен выждать только в течение интервала PIFS, прежде чем получить доступ к среде. На рис. 6.3 показано, как сосуществуют оба режима.

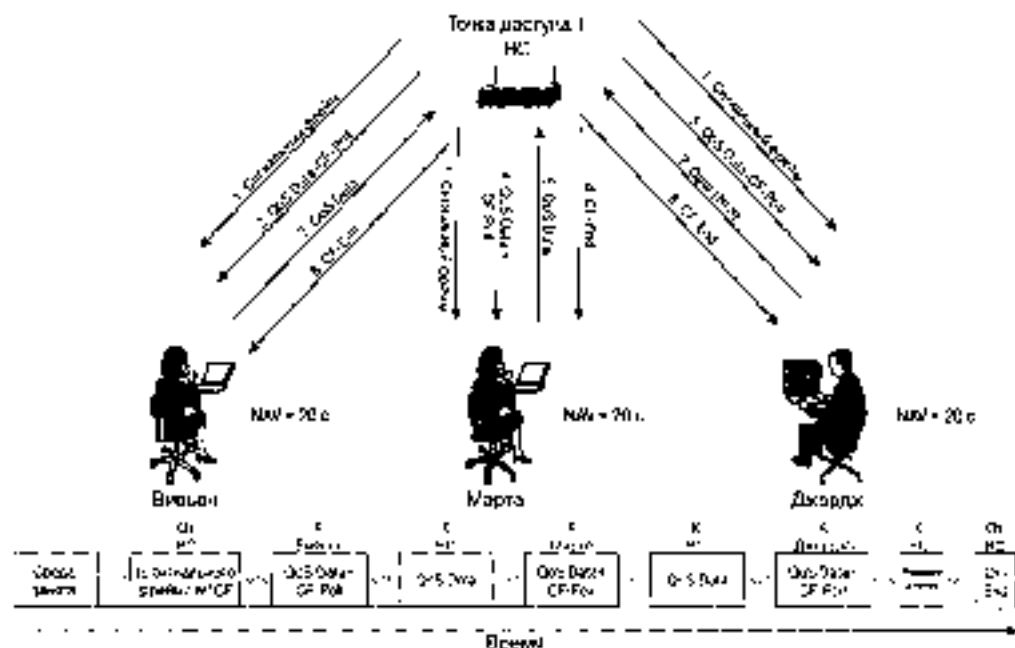


Рис. 6.2. Работа в сети, свободной от конкуренции

## Управление входом с HCF

Что на самом деле отличает работу с доступом, контролируемым HCF, от EDCF — это механизм HCF управления входом. Использование станциями EDCF механизма распределенного управления входом (DCA) основано на том, что станция интерпретирует и соблюдает индивидуальный бюджет для передачи, указываемый в наборе параметров информационного элемента QoS. А вот HCF требует, чтобы станция запрашивала частные параметры резервирования (reservation parameters) для информационного потока трафика приложения, такого как VoIP, от NS. Этот гибридный координатор должен оценить и определить, имеет ли беспроводная среда достаточный бюджет для передачи запрошенного информационного потока. Затем NS должен принять, отклонить или даже предложить своей станции альтернативный набор параметров. Как видите, этот механизм намного более вычислительный и эффективный, чем DCA. Эта вычислительность, однако, не является целью. Гибридный координатор должен строго соблюдать расписание информационных потоков, и в зависимости от реализации NS (который не стандартизован и оставлен на усмотрение производителей) некоторые из них могут оказаться намного менее эффективными, чем другие.

Управление входом HCF концентрируется на информационном элементе с параметрами спецификации передачи (transmission specification IE), который называется также TSPEC. Элемент TSPEC позволяет клиентской станции указать следующие параметры.

- Приоритет фрейма/потока стандарта 802.1D.
- Размер фрейма.
- Скорость передачи фрейма (например, количество пакетов в секунду).

- Скорости передачи данных (например, в бит/с)
- Задержку.

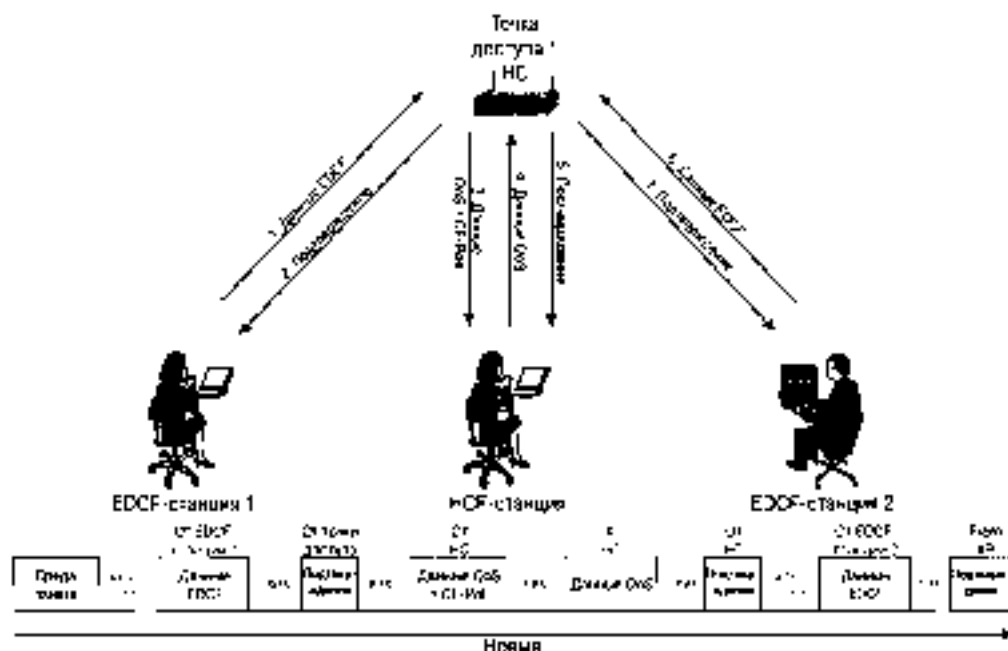


Рис. 6.3. Работа HCF в период коэкзистенции (совместно с EDCF)

На рис. 6.4 представлен информационный элемент TSPEC в том виде, как он определен в проекте 4.0 стандарта 802.11e.

Эта информация необходима HCF для определения, может ли беспроводная среда поддерживать существующие информационные потоки и вновь запрошенный поток без ухудшения условия передачи для уже существующих потоков. Элемент TSPEC указывает также гибриднему координатору, как часто станция предполагает быть опрашиваемой. Такая станция должна генерировать уникальный TSPEC для каждого информационного потока, который она стремится передать и получить с приоритетом и для каждого направления потока (например, двунаправленный VoIP-разговор требует двух информационных потоков).

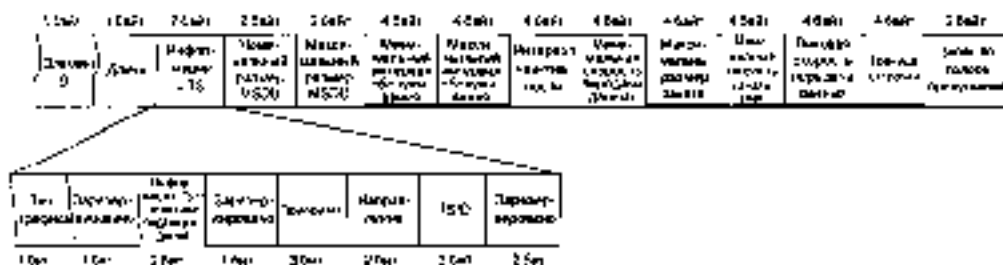


Рис. 6.4. Формат информационного элемента TSPEC

Гибридный координатор может также выполнять одно из трех действий после получения TSPEC.

- Принять TSPEC и гарантировать прохождение нового информационного потока через беспроводную среду
- Предложить клиентской станции альтернативный набор параметров TSPEC.
- Отклонить данный TSPEC.

Чтобы проиллюстрировать сценарий, когда какая-то станция посылает TSPEC, который принимается, предположим, что через точку доступа, через которую уже осуществляется передача трех телефонных разговоров, должен существовать еще один телефонный разговор, а также передаваться некоторый спорадический трафик данных. Спорадический трафик данных классифицируется как “трафик наибольшего благоприятствования”, в то время как VoIP-трафик классифицируется как “высокоприоритетный”.

VoIP-трафик защищен от воздействия трафика данных за счет порядка и частоты запроса HCF. Этот трафик также защищен от воздействия трафика EDCF, потому что он использует HC и должен ожидать доступа к среде только в течение интервала PIFS. EDCF-станция должна ожидать по крайней мере в течение интервала DIFS и, в некоторых случаях, еще одного канального интервала (в предположении использования набора параметров по умолчанию из табл. 6.2).

Процесс присоединения новой станции к BSS и начала передачи ее информационного потока описан ниже и представлен на рис. 6.5.

1. Эта станция должна аутентифицироваться в BSS и ассоциироваться с ним
2. Станция посылает запрос на вход, используя запрос на управляющее действие (management action (MA) request) для QoS, содержащий необходимый ей TSPEC для обеспечения VoIP-разговора.

---

#### На заметку

Необходимо указать TSPEC для каждого направления, как от клиента к HC, так и от HC к клиенту. Клиент должен затребовать оба TSPEC.

---

3. HC принимает TSPEC и отвечает станции ответом на MA для QoS.
4. HC посылает TSPEC посредством фрейма CF-Poll с данными QoS.
5. Станция отвечает фреймом с данными QoS или последовательностью фреймов, в зависимости от длительности TXOP.

В некоторых случаях HC может оказаться не в состоянии поддержать новый TSPEC без ухудшения условий для уже существующих информационных потоков. Гибридный координатор имеет опцию, позволяющую предложить клиенту альтернативный TSPEC или вообще отклонить TSPEC. В первом случае происходят следующие события (см. рис. 6.5).

1. Станция присоединяется к BSS, осуществив процедуры аутентификации и ассоциирования.
2. Станция посылает запрос на вход, используя запрос MA для QoS с указанием необходимого для нее TSPEC.

3. Гибридный координатор передает клиентской станции MA-ответ, содержащий альтернативный TSPEC.
4. Если альтернативный TSPEC приемлем для клиента, процесс продолжается начиная с п. 3 предыдущего сценария.
5. Если альтернативный TSPEC неприемлем для клиента, последний посылает MA для аннуляции TSPEC.

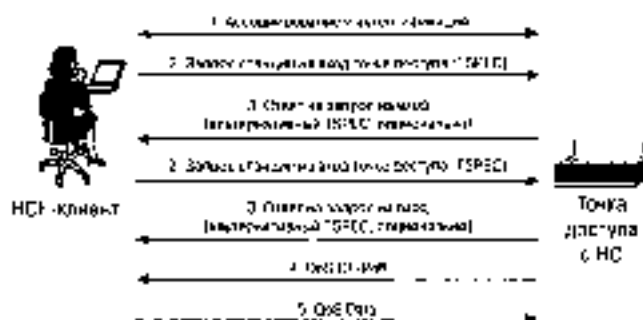


Рис. 6.5 Управляющие сообщения, поступающие для получения потока клиент HCF

Если НС не может принять информационный поток, он посылает MA-ответ, состоящий из TSPEC, и клиентская станция должна повторить попытку, модифицировав запрашиваемый TSPEC.

Информационные потоки могут быть удалены двумя способами

- Истекает тайм-аут TSPEC.
- Станция или точка доступа явно удаляет TSPEC.

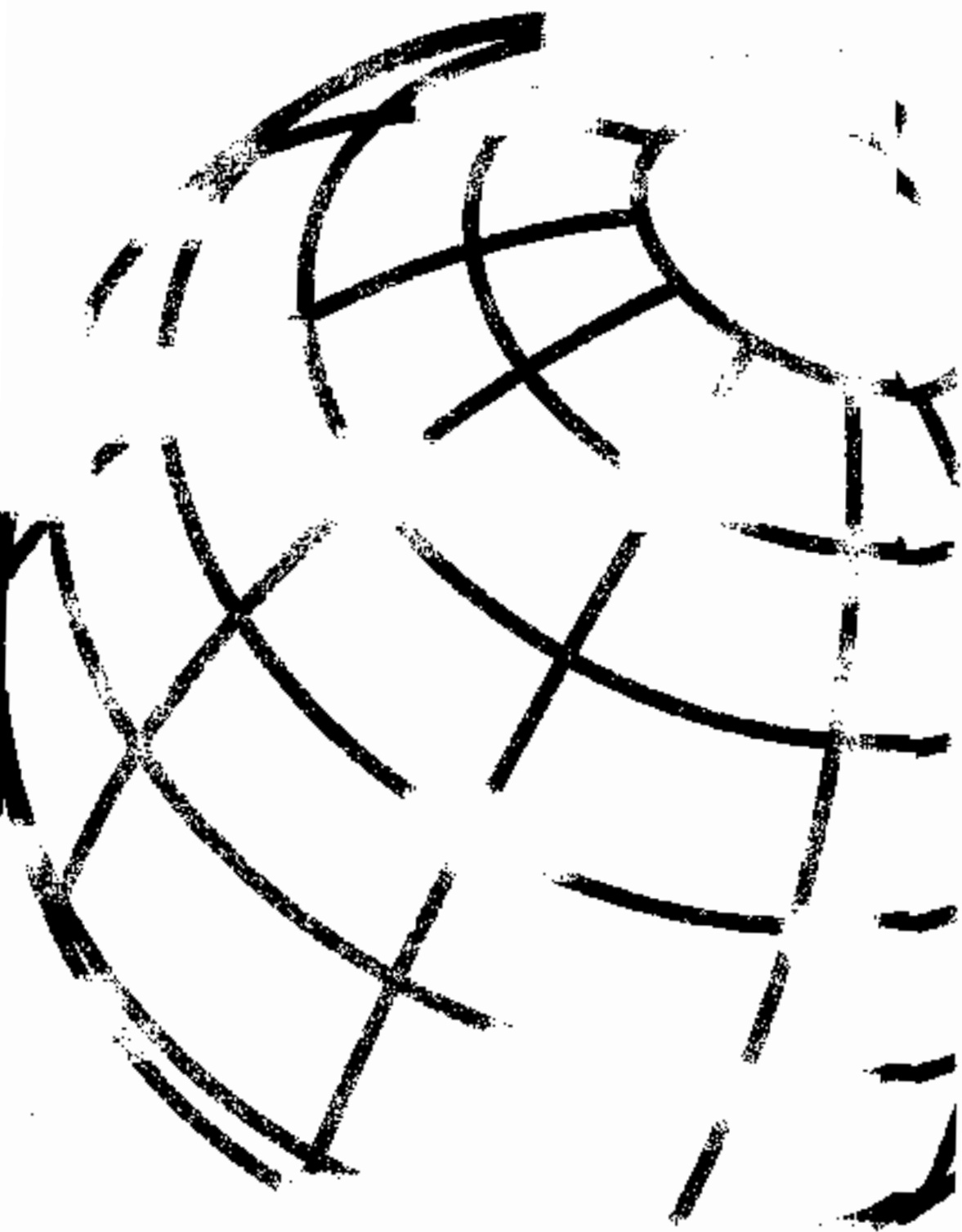
В случае тайм-аута TSPEC после определенного периода тайм-аута для завершения потока НС посылает клиентской станции MA для QoS с целью удаления TSPEC. Этот тайм-аут определяется во время прохода клиентской станции, когда она отвечает пачке QoS-фреймов после нескольких опросов в окне (within a set window), определенном значением тайм-аута, заданным в TSPEC. В случае, когда QoS станция или НС желает "снести" поток, пересылает MA-фрейм для уничтожения TSPEC гибридной координатору для клиентской станции соответственно.

## Резюме. Проблемы, стоящие перед EDCF и HCF

В то время, когда писались эти строки, были сформулированы две основные задачи, над решением которых работала группа по разработке стандарта 802.11e: эффективное, но вместе с тем простое управление входом для EDCF и выполнение операции HCF. Эти вопросы долго обсуждались представителями различных поставщиков и рабочей группе, которые пытались решить проблемы работы приложений.

Механизм распределенного управления входом все еще не обладает нужными характеристиками, потому что не осуществляет строгий контроль входа. Станции потенциально могут осуществлять передачу и тем самым негативно влиять на уже существующие информационные потоки. Решение, по-видимому, может быть найдено пу-

тем параметрического управления входящей также и для EDCF (использование TSPEC для приема или отказа в приеме трафика EDCF). ИСГ имеет свои проблемы. Строптивости приносятся достоинства доступа по опросу как пауза, обеспечивающую эффективное использование среды и почти гарантированное предоставление услуг. Противники полагают, что на практике HCF проявит себя плохо, как это случилось ранее с PCF, из-за перекрытия по совмещенному каналу, который является источником "высокой биты" для многоканальной диапана 2.4 Гц. Эффективность HCF быстро снижается при усилении перекрытия по совмещенному каналу. Хотя рабочая группа еще не закончила работу над стандартом 802.11e, она продолжает продвигаться в направлении создания практического и эффективного набора инструментов для развития и распространения WLAN стандарта 802.11.





## Радиочастотный тракт

Хотя существует только один предмет, который нужно изучить, чтобы разобраться в основных компонентах физического уровня (PHY) стандарта 802.11, это все же совершенно не так же просто — понять, когда и где можно развертывать беспроводные LAN (WLAN) и какие ограничения и положения следует учитывать при их развертывании. Как уже говорилось в главе 3, «Технологии физического уровня стандарта 802.11», использование нелицензируемых частот является одним из главных факторов, способствующих внедрению WLAN почти во всех секторах бизнеса. В этой главе изложены правила, которыми вы должны руководствоваться при проектировании своей беспроводной сети. Важно также знать, с какими проблемами столкнется разработчик радиотракта. Хотя после прочтения этой главы вы не сможете спроектировать радиостанцию стандарта 802.11, заложенный в нее материал поможет вам понять и оценить параметры физического уровня, указываемые в описаниях оборудования большинства производителей. В этой главе описываются основные рабочие параметры приемника и передатчика, из которых состоит каждая радиостанция. Вооружившись этими знаниями, вы сможете сделать разумный и основанный на выборе среди различных типов и типов, предлагаемых поставщиками.

## Основы радиотехники

Термин *радио* относится к передаче электромагнитных волн длиной миллиметр или больше через свободное пространство (эфир). Область применения радио очень широка — от автомобильных радиоприемников диапазонов AM и FM до радиостанций мобильных телефонов и земных цифровых микроволновых радиостанций. Иногда это, как в случае радиоприемников диапазонов AM и FM, — однонаправленные или ширковещательные радиостанции. Передача электромагнитных волн осуществляется только в одном направлении, и часто в конфигурации типа «одно-множество». Альтернативный вариант — двунаправленные радиостанции, позволяющие осуществлять прием и передачу каждой из сторон: они могут осуществлять связь в конфигурации «точка-точка», часто применяемой в телекоммуникационных системах, или в конфигурации «точка-группа точек», характерной для WLAN и сетей мобильной связи.

Важным структурным отличием систем двунаправленной радиосвязи является разницы между дуплексной связью с частотным разделением (frequency division duplex, FDD) и дуплексной связью с временным разделением (time division duplex, TDD). В технологии FDD для передачи информации в каждом направлении используется свой частота, и эти две частоты должны быть достаточно различными, чтобы не возникло

взаимных помех. При достаточном разнесении частот благодаря применению технологии FDD значительно упрощаются конструкция радиостанции и задачи проектировщика системы. Работа осуществляется в полнодуплексном режиме, когда могут одновременно осуществляться и передача, и прием. Однако имеются и проблемы. Выделенный спектр частот приходится делить на две полосы, и он используется неэффективно, потому что полоса частот “простаивает”, когда передача в одном из направлений не осуществляется. В альтернативной технологии, TDD, радиосвязь осуществляется через один и тот же канал, но передача и прием осуществляются попеременно. Хотя при этом на физическом уровне возникает ситуация полудуплексной связи и требуется, чтобы радиостанция могла очень быстро переключаться из режима “прием” в режим “передача”, выделенный диапазон частот используется более эффективно. Благодаря этому упрощается разделение спектра частот на отдельные каналы, и можно по необходимости изменять число частот, выделенную для каждого направления.

Одной из важнейших характеристик радиостанции является мощность ее передатчика. Выходная мощность измеряется в линии передачи, кабеле или антенне и обычно указывается в ваттах (Вт) или милливаттах (мВт). Для сравнения мощностей применяется логарифмическая шкала, отношение мощностей измеряется в децибелах (дБ). Производители радиостанции указывают их мощность в dBm, т.е. в децибелах по отношению к мощности в 1 мВт, или в dBW, т.е. в децибелах по отношению к мощности 1 Вт. В табл. 7.1 приведены соотношения для некоторых значений мощности в абсолютных и относительных единицах.

**Таблица 7.1. Примеры значений мощности, указанной в абсолютных и относительных единицах**

мВт	Вт	dBm	dBW
1	0,001	0	-30
2	0,002	3	-27
5	0,005	7	-23
10	0,01	10	-20
20	0,02	13	-17
50	0,05	17	-13
100	0,1	20	-10
1000	1	30	0
2000	2	33	3
4000	4	36	6

## Основы антенной техники

Что такое *антенна*? IEEE определяет антенну так: “часть передающей или приемляющей системы, предназначенная для излучения или приема электромагнитных волн” (Стандарт IEEE 145-1993). Другими словами, антенной может быть все, что получает радиочастотный сигнал, генерируемый передатчиком, и излучает его в радиэфир, или то, что принимает (захватывает) электромагнитные волны для приемника. Обычно приемные и передающие свойства эквивалентны; это означает, что также параметры антенны, как коэффициент усиления, диаграмма излучения или частота, одинаковы.

Служащий вопрос, который вы могли бы задать, такой: "Как антенна работает?" Согласно учебнику, по которому учат большинство разработчиков антенн, *Теория и конструкция антенн* авторам Штурмана и Сидли (Stutzman and Thiele, *Antenna Theory and Design*), главным свойством антенны является излучение. "...возмущение электромагнитного поля, распространяющегося от источника этого возмущения. ... возмущение создается источником переменного тока". Так что радиосигнал создается источником переменной напряженности определенной частоты, который индуцирует в антенне переменной ток, создающий, в свою очередь, вышеупомянутое электромагнитное поле.

При рассмотрении характеристик антенны следует различать поле в *ближней зоне*, т.е. поле вблизи антенны, и поле в *дальней зоне*. Поле в дальней зоне, в отличие от поля в ближней зоне, характеризуется тем, что расстояние от антенны значительно превышает длину волны и размеры или размеры антенны. При выводе характеристик антенн, указываемых на характеристики, имеют в виду поле в дальней зоне. Покажите об этом, если когда-нибудь вам придется работать в ближней зоне антенны, потому что там ее характеристики будут другими.

Важными понятиями являются *изотропный* излучатель и *изотропная* антенна. Это математическая абстракция, применяемая при описании идеальной антенны, одинаково излучающей во всех направлениях. Если вы воображаете сферу с изотропным излучателем в ее центре, то во всех точках поверхности сферы электромагнитное поле будет одинаковым. Изотропная антенна является удобным эталоном, применяемым при сравнении различных антенн.

## Свойства антенны

Для того чтобы принимать разумные решения относительно антенн, важно разбираться в некоторых их свойствах. Они включают, хотя и не ограничиваются ими, направленность излучения, направленность коэффициента усиления, коэффициент усиления, поляризация и полосу частот.

*Диаграмма излучения* антенны объясняет "угловое изменение радиомощности на фиксированном расстоянии от антенны". Диаграмма излучения часто описывается в терминах направленности или коэффициента усиления. *Направленность* антенны описывает интенсивность излучения в данном направлении по отношению к средней интенсивности излучения, иначе говоря, она указывает плотность мощности излучения по отношению к равномерно распределенной мощности излучения. Коэффициент усиления описывает то же самое, но уже с учетом потерь в самой антенне. Вы можете определить коэффициент помехового действия антенны, который используется для градуировки направленности с целью определения коэффициента усиления антенны; совершенный излучатель имеет к.п.д., равный 1. Поскольку все реальные антенны имеют потери, коэффициент усиления, учитывающий их, является наиболее часто упоминаемым параметром антенны. Единицы измерения, используемые для указания коэффициента усиления, — это или dBi, коэффициент усиления в децибелах по отношению к изотропной антенне, или dBd, коэффициенту усиления в децибелах по отношению к антенне, называемой *полуволновой симметричной антенной* (или *вибратор*, иногда — *диполь*). Следует помнить, что при преобразовании одного значения в другое нужно добавить 2,2 к значению коэффициента усиления, выраженного в dBi, чтобы получить значение коэффициента усиления, выраженное в dBd. Важно знать, как следует осуществлять такое преобразование, поскольку, хотя многие поставщики указывают коэффициент усиления

в dBi, некоторые все же указывают его в dBd. На рис. 7.1 представлен образец диаграммы излучения для направленной антенны.

#### На заметку

Вы можете сделать симметричную дипольную антенну, взяв симметричный кабель и изогнув концы его проводов наружу, чтобы создать противоположно заряженные полюсы, которые будут индуцировать переменный ток в пространстве между собой.

Вспомнив, что излучение осуществляется в трехмерном пространстве, вы скорее всего знаете, что лучистая антенна имеет главный лепесток, или луч, который расширяется в направлении максимального коэффициента усиления, и характеризуется также *второстепенными лепестками*, часто называемыми *боквелами* или *задними лепестками* (диаграммы направленности антенны). — в зависимости от направления или ориентации лепестков относительно главного. Производители часто описывают свои антенны, сообщая коэффициент усиления именно для главного лепестка. Делая это, они также указывают *ширину диаграммы направленности антенны*. Обычно это ширина диаграммы направленности на уровне 0,5 от ее максимальной мощности; она определяется IEEE следующим образом. "В сечении диаграммы излучения, содержащем направление максимума лепестка, угол между двумя направлениями, на которых интенсивность излучения составляет половину максимального значения".

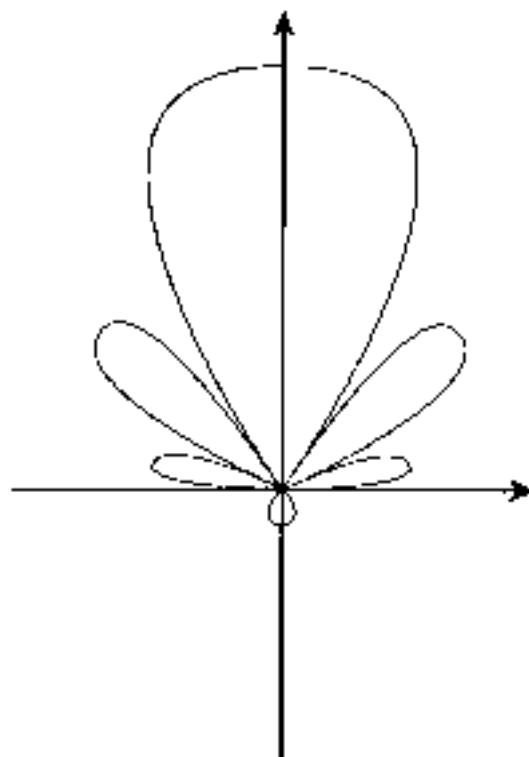


Рис. 7.1 Образец диаграммы излучения

Вернемся к диаграмме направленности антенны (см. рис. 7.1) и отобразим на ней по точке с каждой стороны главного лепестка, где коэффициент усиления на 3 дБ меньше, чем в точке максимума лепестка. В этих точках мощность излучения является меньше. Угол между ними и указывает ширину диаграммы направленности. На рис. 7.2 она обозначена буквами BW (от англ. beamwidth).

Возвращаясь к диаграмме излучения антенны, отметим, что коэффициент обратного излучения антенны определяется путем сравнения максимального коэффициента усиления антенны в ее главном лепестке и коэффициента усиления в направлении, обратном главному лепестку. В случае прямой диаграммы направленности коэффициент обратного излучения антенны может составлять, допустим, 20 дБ (рис. 7.3). Коэффициент усиления главного лепестка составляет 15 дБ, обратного лепестка — 5 дБ. Разница,  $15 \text{ дБ} - (-5) \text{ дБ} = 20 \text{ дБ}$ , и представляет собой коэффициент обратного излучения антенны.

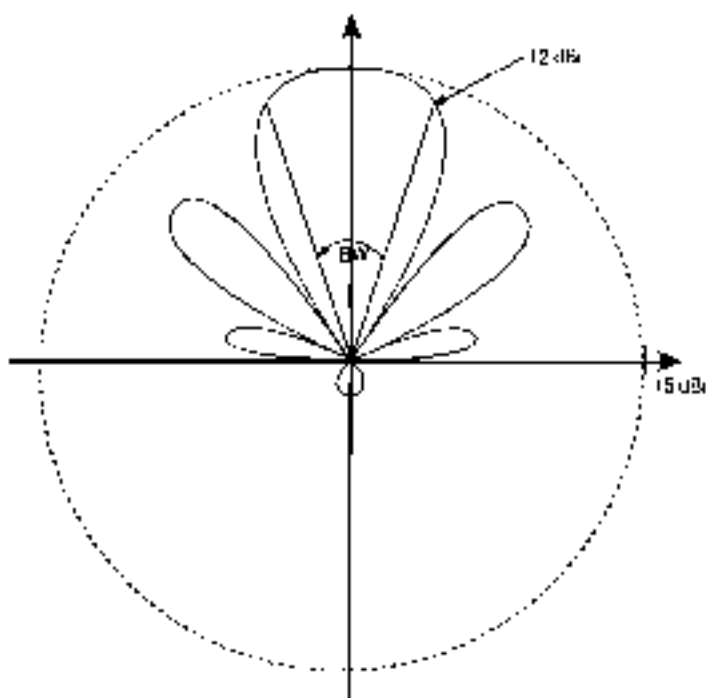


Рис. 7.2. Ширина диаграммы направленности антенны по уровню 3 дБ

Теперь, когда вы знаете, что такое коэффициент усиления антенны, пришло время рассчитать фактическую мощность, переданную радиостанцией, к которой подключена антенна. Эквивалентная излучаемая мощность (ЭИМ, ERP) получается после перемножения коэффициента усиления антенны, измеренного в дБд, т.е. по отношению к полушаровому излучателю, на полезную мощность, подаваемую передатчиком на антенну. Однако часто подобные математические операции проводятся в логарифмической области, или в децибеллах. Это означает, что можно сложить коэффициент усиления антенны с мощностью передатчика. Поскольку чаще всего коэффициент усиления антенны выражают в дБд, наиболее часто употребляемый термин для излучаемой мощности — эффективная изотропно-излучаемая мощность (EIRP),

это то же самое, что EIRP, но с коэффициентом усиления антенны, выраженным относительно изотропного излучателя.

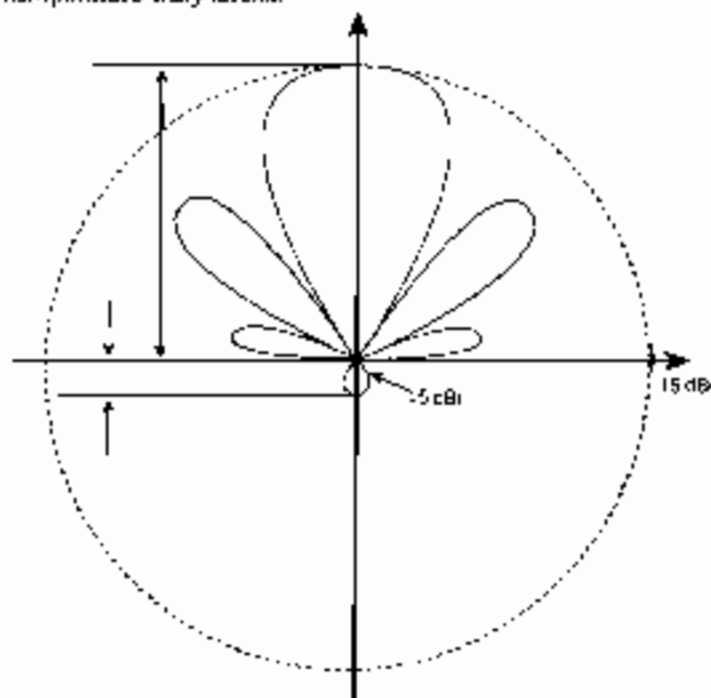


Рис. 7.3. Коэффициент обратного излучения антенны

Электромагнитные волны, излучаемые антенной, могут по-разному распространяться в среде. Особенности распространения зависят от поляризации передающей антенны. Она может быть линейной или круговой.

Большинство антенн, используемых в WLAN, являются антеннами с *линейной* поляризацией, горизонтальной или вертикальной. Первое означает, что вектор электрического поля лежит в вертикальной плоскости, второе — что в горизонтальной. Чаще применяется вертикальная поляризация, хотя в некоторых ситуациях антенны с горизонтальной поляризацией эффективнее. Хотя маловероятно, что в помещениях вы сможете применить антенны с круговой поляризацией, при использовании микроволновое влияние может произойти. Как и в случае антенн с линейной поляризацией, возможны два варианта: левая круговая поляризация и правая круговая поляризация. Если при движении волны в вашу сторону вектор вращается по часовой стрелке, то это левая круговая поляризация.

Аналогично, если вам кажется, что она вращается против часовой стрелки, это правая круговая поляризация. Линии связи, в которых передача осуществляется над водным пространством, когда плоскость поляризации может поворачиваться при каждом отражении, — хороший пример наличия круговой поляризации, потому что она инвариантна по отношению к вращению. При вращении антенны с линейной поляризацией она может изменять ее с вертикальной на горизонтальную.

Вобщем говоря, для линии связи, работающей в пределах прямой видимости, на обоих ее концах нужно использовать антенны с одинаковой поляризацией. Антенны с вертикальной поляризацией, имеющие коэффициент усиления 21 dBi, может

чить коэффициент усиления в горизонтальной плоскости от 1 до -4 дБн, что означает, что уровень кроссполаризационной селекции (выделения поперечной поляризации) составляет обычно 20–25 дВі.

Коэффициент полезного действия антенны — это “отношение общей мощности, излучаемой антенной, к полезной мощности, полученной ею от передатчика”. Все радиоразборки — радиостанции, линии передачи, антенны — имеют характеристику, называемую падением *return loss*, что означает отношение напряжения и тока на экстремальных выводах радиоразборки. Если антенна соединяется с передатчиком посредством кабеля и ее импедансы согласованы с импедансами передатчика и линии передачи, то в антенну передается максимальная мощность. Однако если импедансы не согласованы, часть энергии будет отражаться обратно к источнику, и лишь оставшаяся поступит на антенну. Эти отражения характеризует коэффициент стоячей волны по напряжению (КСВН, VSWR). Если отражения отсутствуют, КСВН равен 1. Увеличение КСВН означает больше отражений с большей амплитудой. КСВН, равный 2, означает, что отражается 11% мощности.

Высокий КСВН и линии передачи с высоким затуханием приводят к потерям существенной части энергии. Более того, при высоком КСВН и больших мощностях может наступить опасная ситуация вследствие повышения напряжения в линии передачи, которое в экстремальных случаях может вызвать искрение. Однако подобная проблема никогда не возникнет перед вами, поскольку уровни мощности в беспроводных LAN весьма невелики.

*Полоса пропускания* антенны определяется диапазоном частот, в котором антенна имеет приемлемые рабочие параметры. Обычно указываются максимальная и минимальная частоты. Термин “приемлемые рабочие параметры” в данном случае означает, что характеристики антенны, такие как ее диаграмма направленности и входной импеданс, не изменяются в рабочем диапазоне частот. Некоторые антенны считаются *широкополосными*. Согласно последнему распространённому определению, таковыми считаются антенны, у которых отношение максимальной частоты к минимальной превышает 2. Однако, поскольку широкополосные антенны часто имеют низкий коэффициент усиления, а уже рассмотренные к настоящему времени WLAN стандарта 802.11 не требуют широкополосных антенн, единственная ситуация, при которой вам могут предложить широкополосную антенну, — это если вы захотите покрыть весь диапазон 2,4 ГГц, выделенный для промышленного, научного и медицинского применения (ISM), а также все близлежащие диапазоны в области 5 ГГц национальной информационной инфраструктуры (I-NII) одной антенной.

При выборе антенны помните, что многие ее параметры взаимосвязаны, поэтому, хотя оптимальным вариантом, казалось бы, была бы такая антенна, как “идеальная”, характеристик антенны или минимизации всех “отрицательных”, на практике также оказывается невозможным. Например, если вы выберете антенну с очень широким главным лепестком, вам придется пожертвовать коэффициентом усиления; выбор широкополосную антенну, вы можете обнаружить, что ее диаграмма направленности неадекватна. Поэтому важно определить, какие именно характеристики антенны важны для условий конкретного ее применения, и сделать соответствующий выбор.

## Типы антенн

Не исключено, что на своем жезу вам придется применять антенны многих типов. Вместо того чтобы перечислять их все, мы опишем в этом разделе те из них, которые

чаще всего используются в беспроводных LAN. На рис. 7.4 показано несколько антенн различных типов. Как уже говорилось, изотропный излучатель является идеальной, нереализуемой на практике антенной, одинаково излучающей во всех направлениях.

Что касается излучателя диполя, то его длина от одного конца до другого должна равняться половине длины волны для рабочей частоты. Ненаправленная (или всенаправленная) антенна имеет одинаковый коэффициент усиления для всех направлений в заданной плоскости (чаще всего горизонтальной). Дипольные антенны обычно бывают ненаправленными. Ненаправленные антенны обычно используются в беспроводных LAN общего применения, поскольку они обеспечивают покрытие во всех направлениях. Директорная антенна Уда-Яги типа "волновой канал" представляет собой линейную антенную решетку, состоящую из диполей.

Антенны Уда-Яги — один из самых распространенных направленных антенн, потому что они просты в изготовлении. Направленные антенны, такие как антенны Уда-Яги, обычно обеспечивают покрытие в труднодоступных зонах или когда необходим большой радиус действия, чем обеспечиваемый ненаправленной антенной.



Рис. 7.4. Антенны, применяемые в беспроводных LAN

Микрополосковые антенны (*patch antennas*), еще один тип направленных антенн, формируются из двух параллельных проводников с подложкой между ними. Верхний проводник представляет собой излучатель, который может быть вытравлен на печатной плате. Можно относительно просто сформировать решетку, состоящую из излучателей, диаграммы направленности которых комбинируются с целью получения лепестков различной формы. Микрополосковые антенны часто оказываются изотропными, поскольку они имеют плоскую форму, в отличие от антенн Уда-Яги. В обширной категории направленных антенн следует отметить также антенну поперечного излучения, плоскость главного лепестка которой перпендикулярна плоскости антенны; антенну продольного излучения, плоскость главного лепестка которой параллельна плоскости антенны; и антенну с игольчатой диаграммой направленности, которая имеет один, очень узкий и часто с большим коэффициентом усиления лепесток.

В главе 10, "Конструктивные особенности WLAN", рассматриваются вопросы применения антенн различных типов применительно к особенностям их размещения.



## Основные характеристики приемника

Радиоприемники характеризуются прежде всего их чувствительностью, которая определяется как минимальный уровень сигнала, при котором приемник способен удовлетворительно декодировать информацию. Порог приемлемости определяется частотой появления ошибочных битов (BER), частотой появления ошибочных пакетов (packet error rate, PER) или частотой появления ошибочных фреймов (frame error rate, FER). Например, стандарт 802.11a указывает, что минимальной приемлемой характеристикой приемника является чувствительность  $-63$  dBm при скорости передачи данных 34 Мбит/с и PER, составляющей 10%. Обратите внимание на то, что чувствительность приемника указывается для конкретной скорости передачи, поскольку каждая схема модуляции имеет свои требования к отношению сигнал/шум (SNR). В общем случае, чем выше скорость передачи данных, тем больше должны быть отношения сигнал/шум и, следовательно, тем выше чувствительность приемника. Чувствительность приемника радиостанции зависит также от характера шума приемника. Все приемники имеют некоторый базисный, или фоновый, уровень шума, определяемый для точности цифровой обработки, или свойствами аналоговых компонентов. Это — уровень собственных шумов приемника. При возрастании собственного шума приемника растет (ухудшается) и чувствительность приемника, потому что минимально допустимое превышение шума сигналом, SNR, — величина фиксированная для каждой схемы модуляции. Эта концепция визуально представлена на рис. 7.5. Чувствительность приемника — один из важнейших входных параметров для оценки характеристик радиостанции в расчете энергетического потенциала канала, который в конечном счете определяет достижимые скорости передачи данных и радиус действия радиостанции. В общем случае вы должны стремиться приобрести приемник с максимальной возможной чувствительностью, если это позволяют средства.

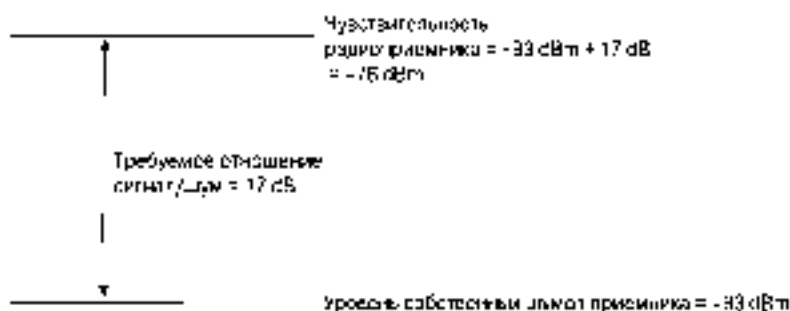


Рис. 7.5. Вычисление чувствительности приемника

## Минимальные характеристики радиостанции стандарта 802.11b

Чтобы вы могли выбрать систему с удовлетворяющими вас характеристиками среды обитания, предлагаемого различными поставщиками, стандарт 802.11b для РНУ-уровня определяет минимальный уровень характеристик радиостанции, которому должно удовлетворять для обеспечения совместимости любое оборудование. Для FER менее 0,08, согласно процедуре определения соответствия требуемым параметрам физического уровня, при длине служебного элемента данных (PSDU) 1024 октета и

скорости передачи данных 11 Мбит/с минимальная чувствительность приемника должна составлять  $-76$  дБм на соединителе антенны, а подавление помех от соседнего канала другого передатчика стандарта 802.11b должно быть 35 дБ на соединителе антенны. Для подавления помех от соседнего канала приемник должен соответственно функционировать или быть способен работать при наличии сигнала соседнего канала с поддержанием 0,6% FER. Для тестирования степени подавления помех от соседнего канала уровень нужного сигнала устанавливается таким, чтобы он на 6 дБ превышал уровень чувствительности приемника, а уровень сигнала соседнего канала устанавливается на 41 дБ больше этого уровня чувствительности. Когда мы будем рассматривать спектральную маску стандарта 802.11b, вы увидите, что похожий результирующий вклад в сигнал канала дает несколько помех.

## Минимальные характеристики радиостанции стандарта 802.11a

Аналогично стандарту 802.11b, стандарт 802.11a также определяет минимально допустимые параметры радиостанции. В табл. 7.2 приведены минимальная чувствительность приемника, степень подавления помех от соседнего канала и степень подавления межкросстных помех от соседнего канала (Adjacent channel rejection) на соединителе антенны для скоростей передачи данных стандарта 802.11a при FER менее 10% и данных PSDU 1400 байт. Что касается характеристик помехоподнесения, то уровень полезного сигнала должен на 3 дБ превышать уровень минимальной чувствительности и уровень сигнала помех, заданный указанным в таблице отношением.

**Таблица 7.2. Минимально допустимые характеристики радиостанции стандарта 802.11a**

Скорость передачи данных (Мбит/с)	Минимальная чувствительность (дБм)	Подавление помех от соседнего канала (дБ)	Подавления перекрестных помех от соседнего канала (дБ)
6	-82	16	39
9	-81	15	31
12	-79	13	29
18	-77	11	27
24	-74	8	24
36	-70	4	20
48	-66	0	16
54	-65	-1	15

Максимальный уровень входного сигнала приемника при тех же условиях составляет  $-30$  дБм. Стандарт 802.11a также регламентирует чувствительность функции оценки занятости канала (CCA); она должна быть такой, чтобы устанавливая среднюю передачу радиостанция могла определять ее занятость с 90-процентной вероятностью в течение 4 мкс в том случае, если уровень полученного сигнала превышает или равен  $-82$  дБм в течение преамбулы. Если преамбула пропущена, то указанный уровень составляет  $-62$  дБм.

## Характеристики системы

Наконец, то, что больше всего интересует нас и производителей сетей WLAN, – это такие характеристики радиостанции, как зона уверенного приема и пропускная способность. Она напрямую связана с радиусом действия и скоростью передачи данных. Для определения радиуса действия мы должны знать, как можно перейти от коэффициента усиления системы, которую вы собираетесь приобрести, к ее радиусу действия и учесть размеры планировки сети. В условиях свободного пространства и прямой видимости это можно сделать относительно просто, поскольку потери на трассе пропорциональны квадрату расстояния или радиусу действия. Радиус действия – это расстояние, на котором потери на трассе становятся равными коэффициенту усиления системы. Другими словами, при каждом удвоении расстояния вам понадобятся дополнительные 6 дБ. Однако обычно WLAN развертываются в помещениях, и приближение сигнала мешают стены, столы, люди и другие объекты, все они уменьшают уровень сигнала и увеличивают потери. В главе 9, “Развертывание беспроводных LAN”, говорится о том, что единственный способ точно определить потери на трассе в конкретных условиях эксплуатации – это провести картирование места развертывания сети. Однако все равно полезно знать механизмы, которые влияют на характеристики системы, и то, как можно определить коэффициент усиления вашей системы и сравнить его с аналогичным параметром других систем.

*Измерительный прибор для связи (link budget)* – это инструмент, который вы можете использовать для определения полного коэффициента системы. Вы должны знать следующие параметры своей системы.

- Мощность радиопередатчика
- Потери в кабеле передатчика, если он используется.
- Коэффициент усиления антенны передатчика
- Коэффициент усиления антенны приемника.
- Потери в кабеле приемника, если он используется.
- Чувствительность приемника при желательной скорости передачи.

*Потери в кабеле* зависят от частоты и должны указываться производителем и спецификации кабеля. В общем случае чем выше частота, тем выше потери в кабеле, поэтому нужно более тщательно выбирать удаленные антенны и длинные радиочастотные кабели в диапазонах U-NII, чем в диапазоне 2,4 ГГц ISM. Например, часто применяемый кабель типа LMR-400 длиной 30,48 м (100 футов) имеет потери 10,5 дБ на частоте 5,3 ГГц и только 6,5 дБ на частоте 2,4 ГГц.

Если вы умножите значение мощности передатчика на коэффициент усиления антенн и затем выделите результат на потери в кабеле и чувствительность приемника, то получите общий коэффициент усиления системы  $K_f$ :

$$K_f = \frac{P_t \cdot G_t \cdot S_{rc}}{L_c \cdot L_{rc} \cdot I_{rc}}$$

Если проложить эти же вычисления с помощью логарифмич. вид. арифметик в качестве единичн. измеренн. децибелы, все вычисления сведется к сложению и вычитанию:

$$K_f = P_t + G_t + G_{rc} - (L_c + L_{rc} + S_{rc}).$$

В табл. 7.3 представлены два примера энергетического потенциала линии связи с низким радиусом действия в диапазоне 2,4 ГГц, в которой применяются два отрезка кабеля длиной примерно по 15 м (50 футов), ведущие к точке доступа. В таблице представлены энергетические потенциалы обеих систем как для нисходящего канала, от точки доступа до клиента, так и для восходящего, от клиента до точки доступа. В системе В применяется точка доступа с невысокими характеристиками, мощность ее передатчика невелика, а чувствительность приемника выше, чем у применяемого в системе А. Вы можете видеть, что параметры нисходящего канала системы В на 3 дБ уступают таковым системы А, а восходящего – на 11 дБ. Для системы А заметно параметры нисходящего канала ограничены малым радиусом действия и скоростью передачи данных, а для системы В ограничивающим фактором является восходящий канал. В условиях свободного пространства система А могла бы иметь преимущество в энергетическом потенциале 5 дБ, что означало бы без малого удвоение радиуса действия при одинаковой скорости передачи данных. Каждый раз, когда энергетический потенциал канала связи увеличивается на 6 дБ, радиус действия при условии распространения радиоволн в открытом пространстве удваивается. Таким образом, вам следует учитывать общий коэффициент усиления системы при оценке зоны действия и пропускной способности, которые могут обеспечить две рассматриваемые беспроводные системы.

**Таблица 7.3. Примеры энергетических потенциалов каналов**

	Система А (нисходящий канал)	Система А (восходящий канал)	Система В (нисходящий канал)	Система В (восходящий канал)
Мощность передатчика (dBm)	20	15	17	15
Потери в кабеле передатчика (дБ)	3,3	0	3,3	0
Коэффициент усиления антенны передатчика (дБ)	6	2	6	2
EIRP (dBm)	22,7	17	19,7	17
Коэффициент усиления антенны приемника (дБ)	2	6	2	6
Потери в кабеле приемника (дБ)	0	3,3	0	3,3
Чувствительность приемника (dBm)	-76	-87	-76	-78
Коэффициент усиления системы (дБ)	100,7	106,7	97,7	96,7

Как уже говорилось, на работу системы влияют и другие механизмы. В их число входят (но не ограничиваются ими) следующие:

- Взаимные помехи (интерференция)
- Многолучевое распространение,
- Фединг (затухание сигнала)

Важным примером взаимных помех, когда какой-нибудь вторичный передатчик излучает электромагнитные волны в канале, где вы пытаетесь работать. Это может быть радиостанция другой WLAN, работающей на том же самом канале, или какое-то дру-

тое устройство, осуществляющее переключ в той же полосе частот. Чем сильнее этот источник внешних помех, тем бо́льшим должен быть уровень полезного сигнала на входе вашего приемника, чтобы вы могли его принять и декодировать. Можно сказать, что ухудшение чувствительности приемника приводит почти к тому же самому эффекту, какой оказывает повышение уровня собственных шумов, и, если уровень нежелательного сигнала слишком велик, вы вообще не сможете работать (рис. 7.6).

*Эффект локального распространения* обусловлен тем, что нужный сигнал достигает антенны приемника различными путями, на которых он испытывает различные задержки и потери на трассе. Различные пути распространения возникают из-за того, что радиоволны отражаются от различных объектов или от неоднородностей атмосферы. Все эти сигналы суммируются в антенне, и в зависимости от задержки и затухания, которые испытывают радиоволны на каждом из путей распространения, может произойти замирание сигнала вследствие конструктивных распределений. На рис. 7.7 представим пример суммирования сигналов, достигших антенны различными путями.

*Замирание сигнала* вызывается изменением с течением времени потерь на трассе, обусловленным, как правило, перемещением каких-то объектов в зоне действия радиостанции, включая перемещение собственно передатчика и приемника. Например, вы можете находиться в конференц-зале с беспроводным звуковым тел. ключом и работать через точку доступа, расположенную в коридоре. Если кто-то закроет двери, ведущую в конференц-зал, потери на трассе возрастут, что приведет к уменьшению уровня принимаемого сигнала. Вот так и получается замирание сигнала.

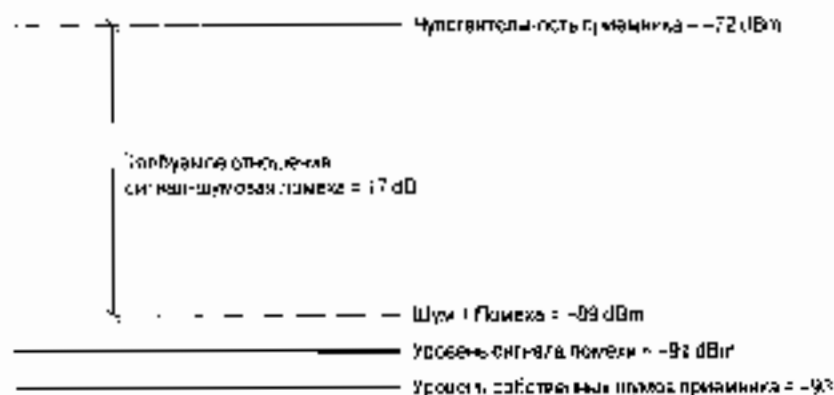


Рис. 7.6. Чувствительность приемника при наличии помех

*Резкое замирание (flat fading)* происходит, когда замирает весь сигнал по всему каналу. В случае широкополосных сигналов, таких, которые используются в устройствах стандарта 802.11, может также наблюдаться частотно-избирательное замирание. Сигнал может существенно ослабевать на определенных частотах, но не во всем диапазоне. Если вы вспомните о методе мультиплексирования с разделением по ортогональным частотам (OFDM), то вспомните и о том, что передача на отдельных частотах происходит независимо, а линии уже осуществляются кодирование и чередование. Этот процесс обеспечивает определенное преимущество технологии OFDM перед другими методами модуляции, например перед кодированием с использованием элементарных кодов (СЕК). Потому что в случае частотно-избирательного замирания может произойти ослабление только нескольких тонов OFDM-сигнала. Следовательно,

но, остается возможность восстановления исходного потока битов за счет кодирования и чередования. В случае же ССК целостность потока битов может быть нарушена.

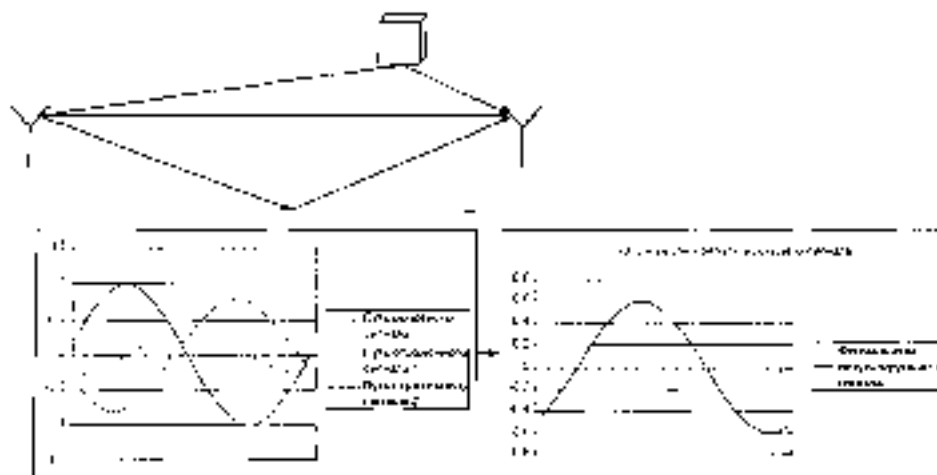


Рис. 7.1. Сигнализация сигнала при равномерном распространении

В зависимости от параметров многолучевого распространения модель потерь на приеме, характерная для свободного пространства, когда потери пропорциональны квадрату расстояния, может измениться на другую, когда потери пропорциональны четвертой степени расстояния. В таком случае при каждом удвоении расстояния потери будут возрастать не на 6 дБ ( $10 \cdot \log(2^4) = 6$ ), а на 12 дБ ( $10 \cdot \log(2^2) = 12$ ). Другими словами, если вы организуете связь в условиях прямой видимости между передатчиком и приемником при обеспечении минимальных отраженных сигналов или попутателей энергии электромагнитных волн, вам нужно увеличивать энергетический потенциал канала связи на 6 дБ при удвоении радиуса действия. Однако при большом числе отражений и, следовательно, существенно многолучевом распространении сигнала энергетический потенциал канала связи должен увеличиваться на 12 дБ при удвоении радиуса действия.

Характер многолучевого распространения изменяется не только с течением времени, он является также функцией местоположения радиостанции. В весьма небольшом отстоянии одна от другой точки может наблюдаться существенно различное замирание сигнала (что говорит об изменении характера многолучевого распространения). Вы можете столкнуться с таким явлением в густой городской жизни, когда слушаете радио в своем автомобиле, стоящем перед светофором. Иногда бивает достаточно сдвинуться на несколько дюймов вперед или назад, чтобы ощутить существенные перемены в условиях приема. Эта пространственная вариация многолучевого распространения является одной из основных причин того, что в беспроводных LAN используются одновременно несколько антенн или радиобитрансы передатчиков и приемные антенны. Если эти антенны отстоят одна от другой хотя бы на расстояние, равное длине волны, принимаемые ими сигналы становятся некогерентными, поэтому если одна антенна может оказаться в зоне замирания сигнала, другая будет принимать его без каких-либо осложнений. В большинстве устройств WLAN предусматривается возможность выбора, когда радиостанция сама определяет, какая из антенн лучше принимает сигнал, и затем использует именно ее.

# Нелицензированная беспроводная связь

Федеральная комиссия связи (FCC) осуществляет контроль за использованием спектра частот беспроводной связи в США. Хотя подобные регулирующие органы имеются во многих странах, нелицензированная беспроводная связь может осуществляться свободно в разных регионах и на разных континентах. В данном разделе рассматриваются основные правила использования спектра частот беспроводной связи.

## Основные стандарты

Три основных органа стандартизации, оказывающих влияние на развитие WLAN, — это Wi-Fi Alliance, IEEE и ETSI.

Институт инженеров по электротехнике и электронике (IEEE) — это некоммерческое профессиональное объединение, которое, помимо прочего, формирует международные стандарты, такие как стандарт 802.11 на беспроводные LAN. Различные группы по разработке стандартов регулярно собираются для того, чтобы обновлять, совершенствовать и предлагать новые стандарты.

В то время как IEEE предлагает стандарты по WLAN, существует еще объединение Wi-Fi Alliance, которое сертифицирует устройства WLAN, произведенные согласно разработанным IEEE спецификациям, на предмет совместимости. Используя устройства, сертифицированные Wi-Fi, вы можете быть уверены в возможности взаимосодействия, превосходящей таковую, оговоренную стандартом IEEE 802.11. Аналогично IEEE, Wi-Fi Alliance — бесприбыльная международная торговая организация, созданная поставщиками и производителями.

Европейский институт стандартов по телекоммуникациям (ETSI) — еще одна бесприбыльная организация, созданная в 1988 году для разработки стандартов по телекоммуникациям для Европы. Что касается WLAN стандарта 802.11, то ETSI решил объединить европейские страны вокруг общего набора документов, регламентирующего передачу. ETSI предложил также конкурирующий набор стандартов для работы в диапазоне 5 ГГц, но во время написания этой книги стандарт 802.11 имел большую «кинетическую энергию».

В США диапазон ISM включает полосу частот 2,4–2,4835 ГГц. FCC определила, что в этом диапазоне может передавать радиоволны соответствующее оборудование. В качестве примера приведем микроволновую печь, излучающую радиоволны в диапазоне 2,4 ГГц, потому что именно этот частотный диапазон используется при приготовлении пищи. FCC позволяет вторичным пользователям работать в этом диапазоне, применяя технологию расширения спектра. Вторичными пользователями считаются таковые, которые не приобрели первичную лицензию на данный набор частот.

В США кодом федеральных правил (Code of Federal Regulations) 47 (CFR47) обозначаются правила, введенные FCC. Часть 15 CFR47 регулирует использование нелицензируемых излучателей, независимо от того, какие они — преднамеренные, непреднамеренные или побочные. Часть 15 правил напрямую регулирует выходную мощность, чтобы вторичный излучатель не создавал помехи для первичного пользователя. В общем случае вторичный пользователь использует частоту (или ряд частот) при уровне мощности, меньшем, чем разрешено для первичного пользователя, такого как оператор радиоловительской связи, имеющий на них лицензию. Что касается микроволновых печей, первичный пользователь на частотах диапазона 2,4 ГГц может излучать радиоволны мощностью при

мерно 600–1000 Вт. Радиостанция стандарта 802.11 обычно имеет мощность 30–100 мВт. Такая разница позволяет домашнему пользователю легко подавить вторичного, если пути их радиоволн пересекутся.

## Частоты диапазона ISM

В диапазоне ISM имеются каналы, предназначенные для использования лицензионными устройствами. Эти каналы и их границы определяются регулятивными органами и могут несколько отличаться в разных странах.

В табл. 7.4 представлены каналы WLAN диапазона ISM и указано, в каких странах какие из них используются. Сведения приведены для четырех регионов: США (FCC), Европы (для тех ее стран, где регулятивным органом признан ETSI), Японии и Израиля.

Таблица 7.4. Каналы WLAN диапазона ISM

Канал	Центральная частота	FCC	ETSI	Япония	Израиль
1	2,412	X	X	X	
2	2,417	X	X	X	
3	2,422	X	X	X	X
4	2,427	X	X	X	X
5	2,432	X	X	X	X
6	2,437	X	X	X	X
7	2,442	X	X	X	X
8	2,447	X	X	X	X
9	2,452	X	X	X	X
10	2,457	X	X	X	
11	2,462	X	X	X	
12	2,467		X	X	
13	2,472		X	X	
14	2,483			X	

Стандарт 802.11b определяет спектральную маску, показанную на рис. 7.8. Относительный пик на центральной частоте спектральные составляющие сигнала должны иметь уровень менее -30 дБ на частотах, отстоящих от несущей на +/-11 МГц и менее -50 дБ на частотах, отстоящих от несущей на +/-22 МГц.

На рис. 7.9 показаны спектральные маски и лучевая диаграмма для 11 каналов, используемых в США. Как вы видите, несмотря на наличие 11 каналов, на самом деле только три из них, 1, 6 и 11, не перекрывают друг друга.

## Уровни мощности передатчика диапазона 2,4 ГГц ISM

В США часть 15.247 правил CFR47 оговаривает уровни передаваемой мощности, которая может быть использована в устройствах диапазона 2,4 ГГц. Для сис-



тем с расширением спектра допустима фиксированная мощность до 1 Вт с антенной, имеющей коэффициент усиления 6 dBi. В результате получается эффективная излучаемая мощность (EIRP) с уровнем 36 dBm. Для каналов типа "точка-точка" с фиксированным размещением, например используемых беспроводными мостами, можно увеличивать коэффициент усиления антенны, но только при условии, что мощность передатчика снижается на 1 дБ при каждом увеличении коэффициента усиления антенны на 3 дБ свыше уровня 6 dBi. Если радиостанция не используется для создания фиксированного канала "точка-точка", то мощность передатчика должна снижаться на 1 дБ при увеличении коэффициента усиления антенны на каждый 2 дБ свыше 6 dBi, таким образом поддерживая ограничение на EIRP значением 36 dBm.

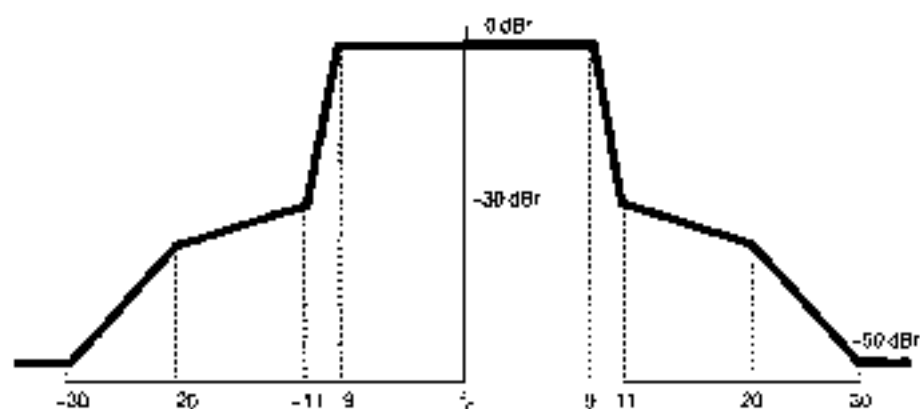


Рис. 7.8. Спектральная маска стандарта 802.11b

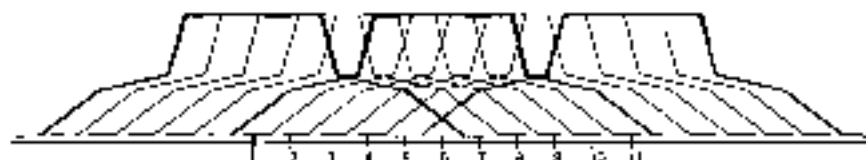


Рис. 7.9. Неперекрывающиеся каналы стандарта 802.11b

Для стран, применяющих правила ETSI, Европейский стандарт на телекоммуникации (European Telecommunications Standard, ETS) инструкции 300328 ограничивает уровень передаваемой мощности, которые могут быть использованы. Она предусматривает мощность EIRP на уровне 100 мВт, или 30 dBm. В Японии статья 49-20 распоряжения МРТ, регулирующего использование радиооборудования, определяет параметры передачи в этом диапазоне. Для сигналов устройств, использующих исключительно расширение спектра методом прямой последовательности (DSSS), может использоваться выходная мощность 10 мВт/МГц. Для передачи сигналов, модулированных за счет расширения спектра путем скачкообразного переключения частоты (FHSS), на частотах 2,471–2,497 ГГц может использоваться та же мощность, 10 мВт/МГц, но на частотах 2,400–2,471 ГГц можно использовать только 3 мВт/МГц. Израиль в настоящее время при определении допустимых уровней выходной мощности также следует правилам ETSI.

# Частоты диапазона U-NII, применяемого в WLAN

Всё же говоря о частотах диапазона U-NII доступны в основном в США и странах, которые приняли правила регулирования спектра FCC-типа. Как уже говорилось, диапазон U-NII 1 простирается от 5,15 до 5,25 ГГц, диапазон U-NII 2 непосредственно граничит с ним и простирается от 5,25 до 5,35 ГГц, а диапазон U-NII 3 занимает участок 5,725–5,825 ГГц. Нумерация каналов начинается с отметки 5,000 ГГц, и номер канала увеличивается на 1 через каждые 5 МГц. Подобный способ обозначения дает схему нумерации каналов, позволяющую охватить все частоты всего диапазона 5 ГГц, которые когда-либо будут использованы в WLAN. На рис. 7.10 представлены непрерывно идущие каналы диапазонов U-NII 1, U-NII 2 и U-NII 3. Обратите внимание на то, что центральные частоты крайних каналов отстоят на 30 МГц от граничных частот диапазона.

Обратите также внимание на то, что, в отличие от двух "низкочастотных" диапазонов области 5 ГГц, центральные частоты диапазона U-NII 3 отстоят лишь на 30 МГц от граничных частот диапазона. Этот факт важно помнить при рассмотрении требований к побочному радиовоздействию и спектральной маске для этого диапазона, потому что выполнить их разработчикам радиотракта сложнее, чем аналогичные требования нижних диапазонов.

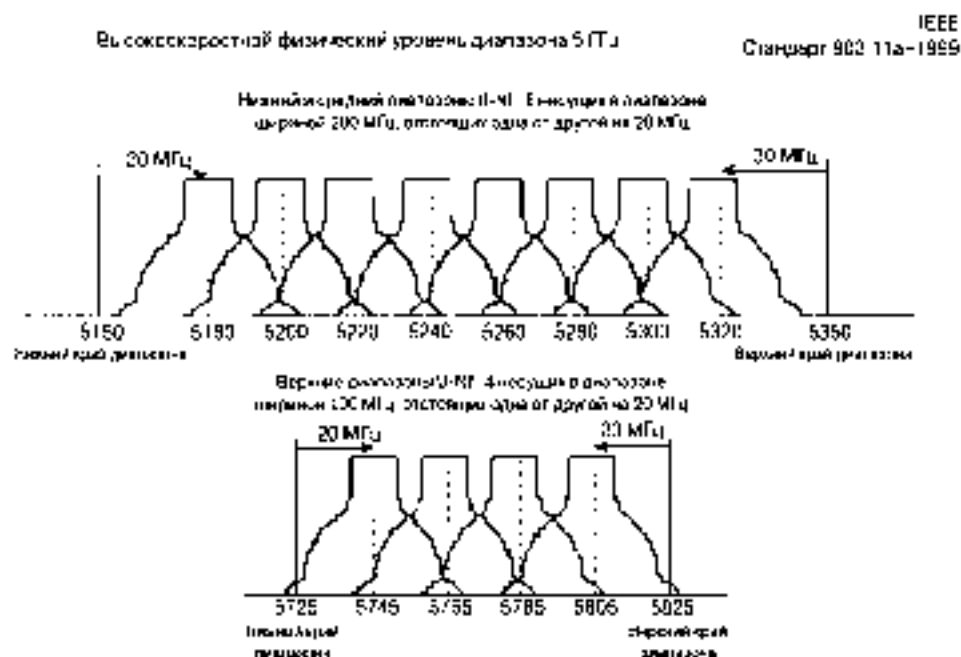


Рис. 7.10. Каналы диапазонов U-NII 1, U-NII 2 и U-NII 3

## Побочное радиоизлучение и спектральная маска диапазона U-NII

В пункте 15.407 документа CFR47 оговариваются требования к побочному радиоизлучению трех диапазонов U-NII. Для диапазона U-NII 1 все излучение вне участка 5,15–5,35 ГГц должно иметь EIRP меньше чем  $-27$  dBm/МГц, передачи должны осуществляться только в помещениях, и должна применяться только направленная антенна. Для диапазона U-NII 2 опционально справедливы точно такие же правила, но можно размещать радиостанцию и вне помещений; они могут иметь не только направленные антенны, но при условии, что все излучение вне диапазона 5,25–5,35 МГц будет иметь EIRP меньше чем  $-27$  dBm/МГц. Для U-NII 3 все излучение вне диапазона 5,725–5,825 МГц должно иметь EIRP меньше чем  $-17$  dBm/МГц; более того, на “расстоянии” 10 МГц от краев диапазона все выходящее радиоизлучение должно иметь EIRP меньше или равный  $-27$  dBm/МГц.

Стандарт 802.11a также определяет спектральную маску для передачи в диапазонах U-NII. Передаваемый спектр должен быть на уровне 0 dBc по отношению к максимуму спектральной плотности сигнала вплоть до максимальной ширины полосы частот 18 МГц, а затем он должен быть меньше 30 dBc “на расстоянии” 11 МГц от центральной частоты,  $-28$  dBc на частотах, отстоящих от центральной на 20 МГц, и  $-40$  dBc для частот, отстоящих от центральной на 30 МГц и более. Эта спектральная маска показана на рис. 7.11.

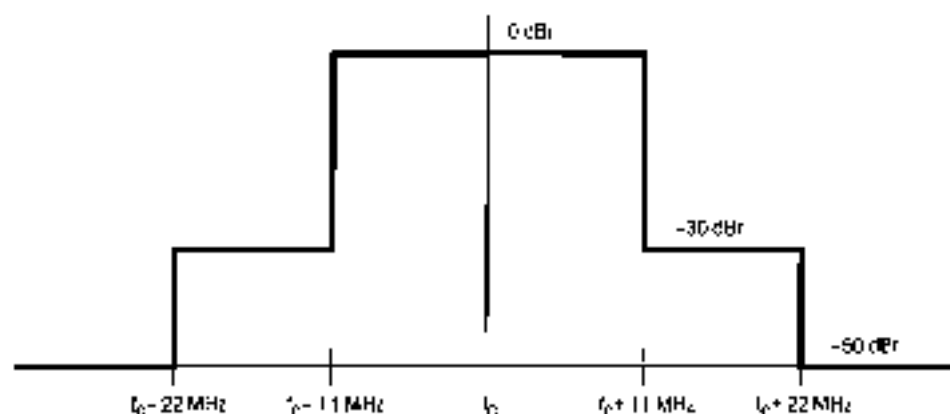


Рис. 7.11. Спектральная маска стандарта 802.11a

Используя свое знание о спектральной маске и подавлении помех от соседнего канала (см. табл. 7.2), вы можете определить, что вклад помех от сигнала соседнего канала по стандарту 802.11a при передаче данных со скоростью 6 Мбит/с мог бы быть на уровне  $-14$  dBc относительно уровня вашего сигнала на центральной частоте (рис. 7.12).

Вы должны иметь это в виду при планировании размещения вашего канала, поскольку помехи от нескольких соседних каналов могут накладываться.

Вам также необходимо иметь информацию о требованиях, предъявляемых к спектральной маске и побочному радиоизлучению, когда вы применяете усиленные антенны. Когда производители сертифицируют свои радиостанции и антенны на пре-

мет соответствия требованиям FCC, они задают уровни, базируясь не только на пределах EIRP, но также на ограничениях, обусловленных этой спектральной маской. Может случиться так, что они установят коэффициент усиления антенны и уровни мощности ниже пределов, оговоренных EIRP, но во многих случаях эти установки будут необходимо привести в соответствие с требованиями спектральной маски. По этой причине вам не следует превышать принятые производителем EIRP-пределы для антенны или радиостанции любого типа.

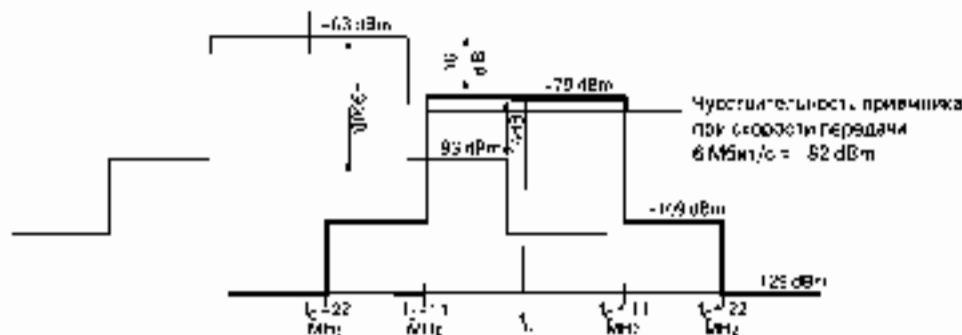


Рис. 7.12. Подача от последователя канала

## Ограничения на передаваемую мощность диапазона U-NII

Три диапазона U-NII имеют различные ограничения на мощность излучения. U-NII 1 предназначен для неиспользования устройствами, рассчитанными на работу только в помехозащищенных, при наименьших условиях излучения. Диапазон U-NII 2 имеет наивысшие уровни, потому что он предназначен для устройств, работающих вне помещений и на больших расстояниях.

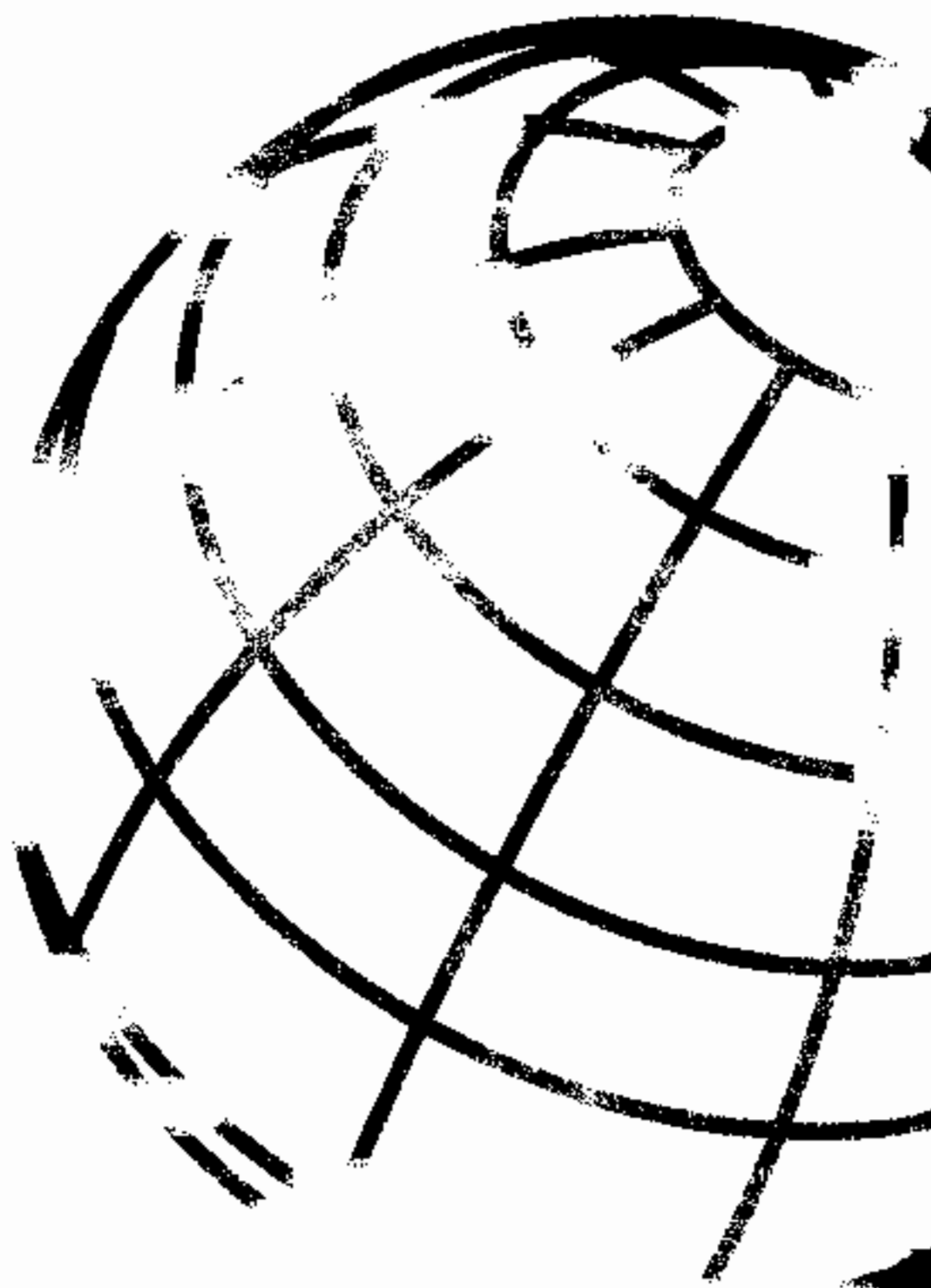
Следующие ограничения на излучаемую мощность установлены стандартом 802.11a для работы в диапазонах U-NII.

- В диапазоне U-NII 1 можно использовать передатчик мощностью до 40 мВт, 16 dBm и антенну с коэффициентом усиления до 6 dBi при максимуме EIRP, составляющем 22 dBm. Кроме того, при каждом повышении коэффициента усиления антенны на 1 дБ свыше 6 dBi излучаемая мощность должна быть снижена на 1 дБ.
- В диапазоне U-NII 2 можно использовать передатчик мощностью до 200 мВт, 27 dBm и антенну с коэффициентом усиления до 6 dBi при максимуме EIRP, составляющем 29 dBm. Кроме того, при каждом повышении коэффициента усиления антенны на 1 дБ свыше 6 dBi излучаемая мощность должна быть снижена на 1 дБ.
- В диапазоне U-NII 3 можно использовать передатчик мощностью до 100 мВт, 29 dBm и антенну с коэффициентом усиления до 6 dBi при максимуме EIRP, составляющем 35 dBm. Кроме того, при каждом повышении коэффициента усиления антенны на 1 дБ свыше 6 dBi излучаемая мощность должна быть снижена на 1 дБ. При работе в диапазоне U-NII 3 можно использовать антенну на 29 dBm без снижения мощности передатчика, но только в фиксированных

каналах типа "точка-точка". При таких условиях максимум LIRP может составлять 52 дБм).

## Резюме

В этой главе обсуждались основные способы оценки физического уровня для радиосистем, а также специфические правила, регламентирующие работу на этом уровне. Главное, что следует запомнить, состоит в том, что качество радиостанции не следует оценивать только по используемой мощности ее передатчика. Следует рассмотреть энергетический потенциал канала в целом, а также рабочие характеристики передатчика и приемника. Только с учетом всего этого можно дать должную оценку радиостанциям, предлагаемым различными производителями.



## Развертывание беспроводных LAN

---

При принятии решений относительно развертывания беспроводных LAN (WLAN) необходимо учитывать особенности работы протокола 802.11, поведение мобильных узлов, вопросы защиты MAC уровня, качество связи (QoS). Для развертывания точек доступа нужно сделать гораздо больше, чем просто проложить кабель и осуществить стандартный монтаж устройств. Физический аспект выполнения картографирования места работ дает возможность администратору понять, какую зону покрытия имеет каждая точка доступа, какое количество точек доступа, необходимое для покрытия заданной области, и установить параметры каждого канала и получаемую мощность. Администратор сети должен также принять во внимание следующее.

- Схемы размещения беспроводных клиентов.
- Приложения, используемые беспроводными клиентами.

На основании этого следует принять следующие важные решения: как много точек доступа придется использовать, какое количество зон перекрытия и местоположение устройств более высокого уровня, таких как серверы аутентификации.

### Развертывание WLAN и влияние приложений

На развертывание WLAN используемые приложения оказывают влияние по-разному. Вам важно разобраться в этом, прежде чем вы начнете планировать развертывание своей WLAN. Ключевые моменты перечислены ниже.

- Расчетная производительность в пересчете на одного клиента.
- Поточные и пульсирующие типы приложений.
- Конкуренция за среду передачи и задержка выполнения приложений.

Расчетная производительность каждого клиента уменьшится с вводом в базовую зону обслуживания (BSS) каждого нового клиента. Поскольку ни один пользователь не занимает гарантированно определенную часть полосы пропускания, механизм доступа к среде, основанный на использовании распределенной функции координации (DCF), обеспечивает удовлетворительный доступ к беспроводной среде; это означает, что каждый клиент имеет одинаковые права доступа к беспроводной среде (и ее части). В мире локальных сетей, где повсеместно применяется Ethernet на 10 и 100 Мбит/с, совместное

использование канала, обеспечивающего скорость передачи данных 11 Мбит/с или даже 54 Мбит/с (стандарт 802.11b и 802.11a соответственно) одновременно 10 или 25 клиентами, рассматривается как шаг назад.

Затывая для сетей стандарта 802.11b скорость передачи 11 Мбит/с и обеспечивая совместный доступ к полудуплексной среде, разумно ожидать реальной производительности не более 6 Мбит/с. Полная доступная производительность для каждого из 25 клиентов составит приблизительно 245 Кбит/с. Принимая те же самые соотношения для BSS стандарта 802.11a со скоростью передачи данных 54 Мбит/с и реальной производительностью 22 Мбит/с, получим среднюю скорость передачи данных 880 Кбит/с на одного клиента. (Это число строго оценочное и получено в предположении, что все клиенты передают и принимают одинаковые объемы данных.)

Типы применяемых приложений существенно влияют на эти объемы. Приложения потокового типа, такие как обеспечивающие передачу речи, имеют характеристики, весьма отличающиеся от приложений пущепроходящего типа, например использующих протокол HTTP или POP3. Типичный двусторонний разговор по технологии G.711 требует средней пропускной способности на уровне MAC 240 Кбит/с. Принимая это во внимание, вы можете ошибочно предположить, что одна BSS может поддерживать 25 таких разговоров ( $25 \times 240$  Кбит/с приблизительно составляет 5,96 Мбит/с).

Но каждый двусторонний разговор требует также обратного направления фреймов со скоростью 200 фреймов в секунду (50 фреймов в секунду и 50 подтверждений по стандарту 802.11 для каждого направления), всего 200 фреймов в секунду. С учетом того что уровень MAC стандарта 802.11b обеспечивает передачу только 200 пакетов в секунду, вы можете поддерживать только шесть телефонных разговоров на одну BSS, и это существенно отличается от расчета, основанного лишь на показателе производительности.

---

#### На заметку

При выводе этой книги не принимались во внимание никакие другие данные, которые могли бы передаваться через точку доступа, — только телефонные разговоры. Любой трафик данных, передаваемых через точку доступа, приведет к ухудшению связи, причем никакого механизма управления входом или механизма приоритетов для обеспечения должного уровня QoS не существует.

---

Плотность размещения точек доступа, т.е. число точек доступа в области покрытия, играет важную роль в поддержке приложений. При развертывании в расчете только на область покрытия сеть не сможет ни обеспечить ни обеспечить для каждого клиента возможность использовать IP-телефонию (VoIP) стандарта 802.11, и то преле как при развертывании, ориентированном на производительность, можно обеспечить необходимую плотность "количество клиентов/количество точек доступа".

Приложения пущепроходящего типа отличаются непостоянством и непредсказуемостью, из-за чего попытки вычисления необходимой плотности размещения точек доступа превращаются в игру на угадывание. Хотя не существует общепринятого эвристического уровня для оценки будущего трафика клиента, использующего Web, получающего электронные письма или работающего с приложениями типа клиент/сервер, пределом считается 25 пользователей на одну точку доступа.

Конкуренция за среду по стандарту 802.11 аналогична конкуренции за среду по стандарту 802.3, относящемуся к полудуплексным проводным сетям. Все станции имеют одинаковые права доступа к среде, и чем больше станций, тем выше шансы на успешное завершение клиентский фреймов, возврат в исходное состояние и повторную передачу. Как говорилось в главе 2, "Беспроводные локальные сети стандарта 802.11", такие же проблемы характерны и для DCF-станций стандарта 802.11.

---



Логическим результатом конкуренции является возникновение задержек в BSS. Ставший трагит больше времени на получение доступа к среде, чем на передачу и получение фреймов. Этот процесс приводит к «индексированию» тайма аутта протокола более высокого уровня и потенциально может привести к прерыванию сеанса связи ближайшего приложения.

Поскольку подобные сценарии вполне вероятны, разумно выбирать высокую плотность размещения, чтобы избежать или уменьшить вероятность возникновения таких ситуаций. С переуплотнением точек доступа при развертывании сети ассоциируется высокая стоимость, но, учитывая дешевизну точек доступа и большое влияние на числа на производительность, имеет смысл сразу же корректно развернуть WLAN, а не выполнять обширные картографические работы и расширять существующую сеть.

У нас есть возможность должным образом настроить клиентские устройства, особенно высокую конкуренцию в BSS.

- **Регулирование порога фрагментации.** Порог фрагментации указывает наибольший размер, который может иметь нефрагментированный фрейм. Как подробно говорилось в главе 2, фреймы меньших размеров имеют больше шансов быть успешно полученными как клиентом, так и точкой доступа.
- **Регулирование порога "готов к передаче" (RTS).** Порог RTS указывает, каким может быть наибольший размер фрейма, прежде чем передатчик посылает RTS. Значение RTS позволяет передатчику (клиенту либо точке доступа) эффективно резервировать среду на время, необходимое для передачи фрейма и получения ожидаемого подтверждения.

В LAN обычно не применяются ни один из этих механизмов, потому что соответствующие настройки следует выполнять вручную на клиентских устройствах, или же выполняются через точку доступа. Пользователь или администратор сети должен сконфигурировать каждую клиентскую станцию на период простоя канала связи, что не практикуется, особенно в больших WLAN. Кроме того, параметры фрагментации и порога RTS нужно устанавливать очень аккуратно. За улучшение характеристик, обеспечиваемые за их счет, приходится платить риком конкуренции и увеличением числа произвольных фреймов.

## Планирование развертывания WLAN

Существуют две основные методологии развертывания WLAN.

- Ориентированная на максимальную зону обслуживания.
- Ориентированная на максимальную пропускную способность.

В данном разделе обсуждаются оба варианта на примере плана этажа типичного офиса (рис. 8.1).

### Беспроводные LAN с максимальной зоной обслуживания

Ориентированные на зону обслуживания WLAN разрабатываются с упором на обеспечение максимального покрытия при минимально возможном количестве точек доступа. (В типичной ориентированной на зону обслуживания сети обеспечивается

связанные качества пользователей к числу точек доступа (25.1.) Некоторые типичные особенности WLAN, развертываемых в расчете на максимальную зону обслуживания, таковы:

- В них применяются приложения пользовательского типа с низкой скоростью передачи пакетов, такие как сканеры штрих-кодов, и приложений, формирующих запросы к базам данных.

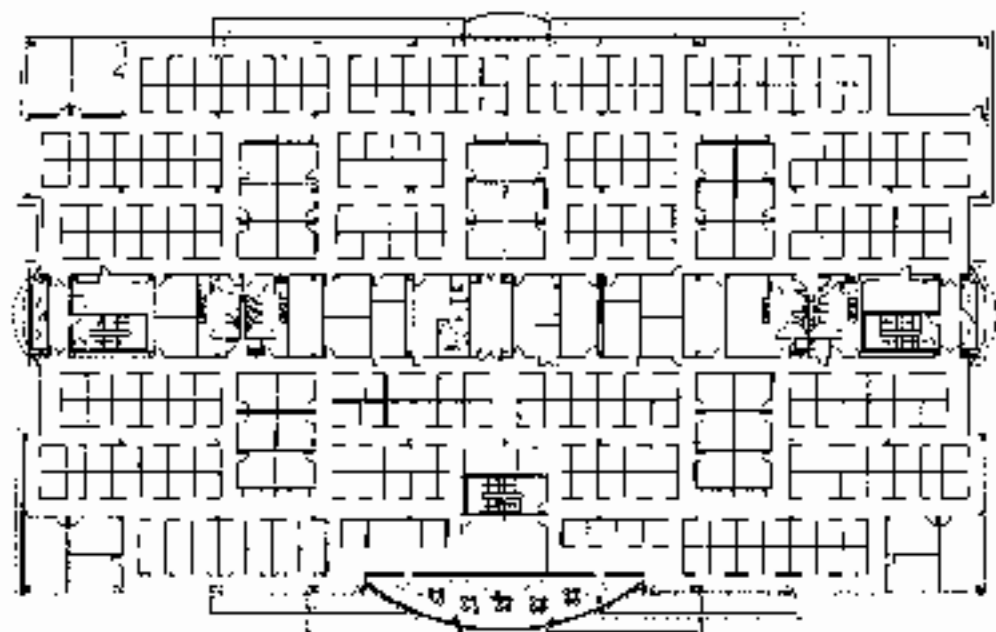


Рис. 8.1 План этажа типичного офиса

- Предъявляются низкие требования к полосе пропускания, благодаря чему скорость передачи данных может быть уменьшена до наименьших значений, таких как 1 и 2 Мбит/с.
- Обеспечивается легкость сопровождения, поскольку персонал обслуживания WLAN нечасто или вообще не обслуживает канал.

В сетях, ориентированных на зону обслуживания, типичные приложения имеют низкую скорость передачи пакетов и предъявляют низкие требования к полосе пропускания. Из-за низких требований, предъявляемых к таким WLAN, пользователи ожидают, что их производительность будет достаточно высокой.

Такой подход позволяет сразу многим пользователям обращаться к услугам WLAN при сохранении последними адекватных характеристик.

Новые варианты развертывания типичны для применений внутри строений или в районной сети, где WLAN не замечены при решении вопроса управления запасами и оперативной закупочной деятельности, когда специалисты по информации и технологиям находятся в центральном офисе, иногда достаточно далеко от места развертывания сети, и не могут оперативно решать возникающие проблемы.

Кроме того, такие варианты обычны для небольших или средних фирм, когда WLAN выбирается в качестве альтернативы проводной Ethernet. В таких случаях

офисы часто переезжают с места на место, и можно сэкономить на прокладке кабелей категории 5. Простые и развертывания WLAN обеспечивают основные соединения и подключения сети, необходимые для совместного использования файлов и принтеров.

На рис. 8.2 показан пример плана этажа, представленного на рис. 8.1, с развернутым на нем WLAN, ориентированным на максимальную зону обслуживания.

Каждая точка доступа WLAN, представленной на рис. 8.2, обслуживает примерно 25–30 пользователей. Для того чтобы зона обслуживания полностью покрывала весь этаж, по плану предлагается развертывание 14 точек доступа. Обратите внимание на то, что предполагается покрытие всех помещений, включая туалеты, комнаты отдыха и лестничные площадки, где в общем случае доступ к WLAN не является обязательным. Разумно предположить, что возможны и другие конфигурации, с меньшим количеством точек доступа, но представленной на рис. 8.2 конфигурацией проще всего проиллюстрировать обсуждаемый вариант размещения.

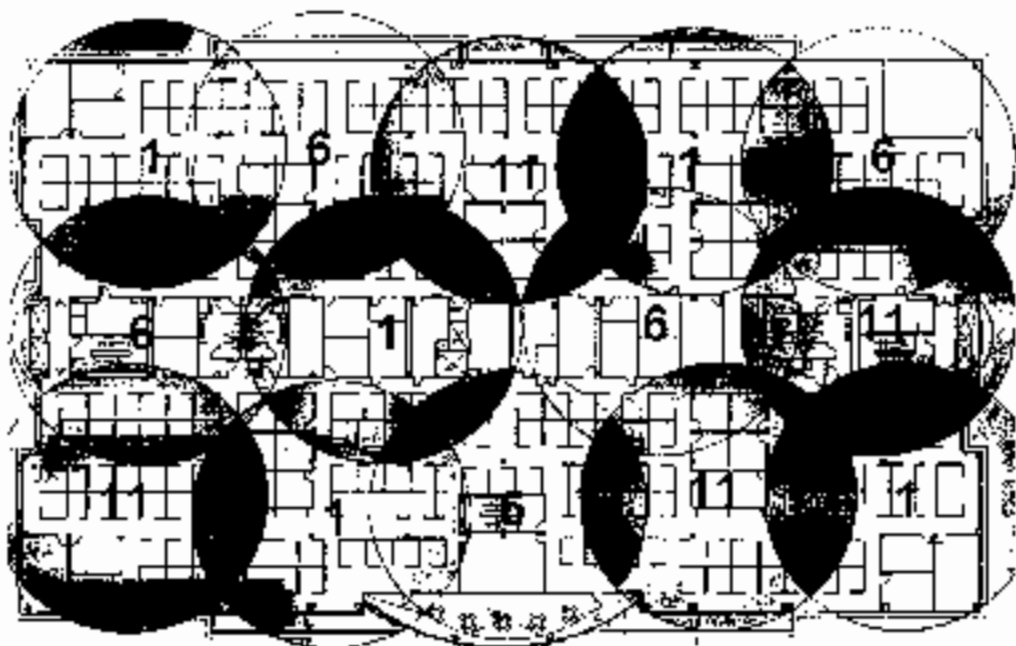


Рис. 8.2. План типового офиса с беспроводной LAN, ориентированной на максимальную зону обслуживания

## Беспроводные LAN с максимальной пропускной способностью

Беспроводные LAN, ориентированные на высокую пропускную способность, должны обеспечивать максимальную приемлемость и скорость передачи пакетов для каждого клиента BSS. Размер сети ориентирован на пропускную способность WLAN меньше, чем таковой для WLAN, назначение которой — обеспечить максимальную зону обслуживания, соответственно плотность размещения точек доступа выше. Ориентированные на высокую пропускную способность WLAN необходимы в случаях, когда:

- используются приложения, требующие высокой скорости передачи пакетов;
- используются приложения, чувствительные к задержкам;
- развертываются подсети меньших масштабов (или несколько подсетей в одной зоне обслуживания);
- наблюдается высокая плотность размещения пользователей.

На рис. 8.1 представлен план все того же этажа, но уже для сети, ориентированной на достижение максимальной пропускной способности. Обратите внимание на то, что количество точек доступа в ней больше чем вдвое превышает число таковых для WLAN, ориентированной на зону обслуживания (30 против 14).

Зона обслуживания каждой точки доступа намного меньше, чем таковая на рис. 8.2: размеры сот примерно вдвое меньше. Каждая точка доступа обслуживает только 12 пользователей, и для полностью развернутой сети необходимы 30 точек доступа, а не 14, как в предыдущем случае.

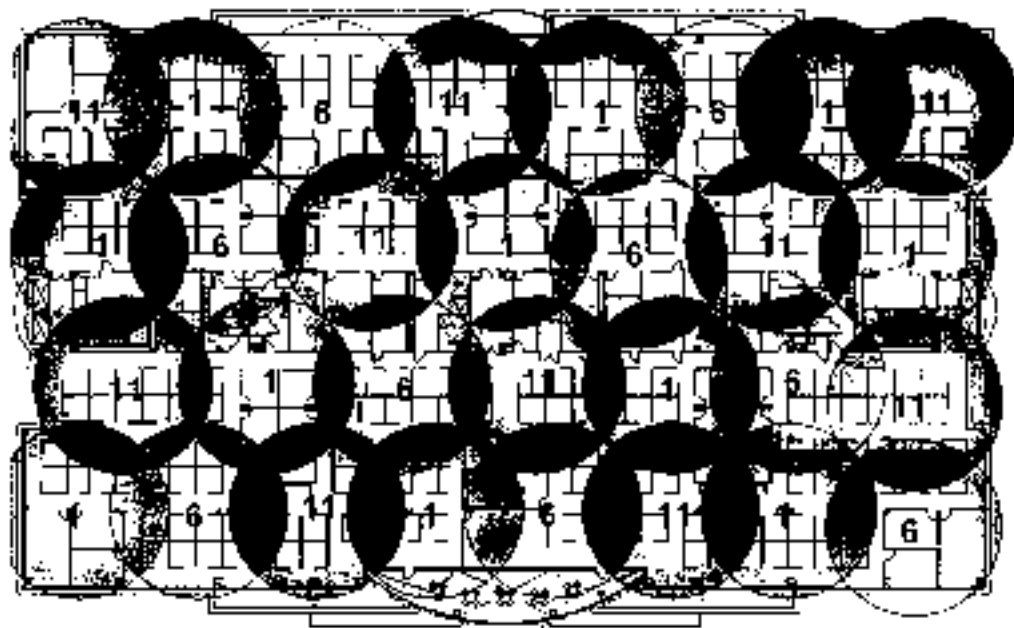


Рис. 8.3. План многоэтажного офиса с WLAN, ориентированным на высокую пропускную способность

## Поэтапное развертывание точек доступа

Очень часто развертывание сети начинается с прицелом на обслуживание каких-то определенных помещений, например конференц-залов. Это приводит к тому, что пользователи, чьи рабочие места располагаются подалека от конференц-зала, могут пользоваться сетью, остальные — нет. Такие варианты развертывания обычно являются переходными к полным вариантам развертывания, когда к сети получают доступ обитатели всех помещений. Требования пользователей рано или поздно вынудят отдел информационных технологий фирмы сделать это, поэтому имеет смысл заранее подготовиться к полночасовому развертыванию сети, даже если первоначально ее задачей является обслуживание лишь нескольких помещений.

Целесообразно провести первоначальное картирование места работ в расчете сразу же на полноразмерном развертывании сети. На рис. 8.4 показан вариант частичного развертывания сети для офиса, план которого был представлен на рис. 8.2 (с приклетом сети, ориентированной на максимальную зону обслуживания). Разворачиваемые точки доступа должны обслуживать конференц-залы и другие помещения, в которых часто бывает много пользователей. Черными точками обозначены места, где в будущем предполагается разместить точки доступа так, чтобы они не вносили помех в работу уже существующих. Обратите внимание на то, что уже развернутые точки доступа находятся в тех же местах, что и на рис. 8.2. Такой подход позволяет в будущем осуществить развертывание новых точек доступа без дорогостоящего дополнительного картирования места работ.

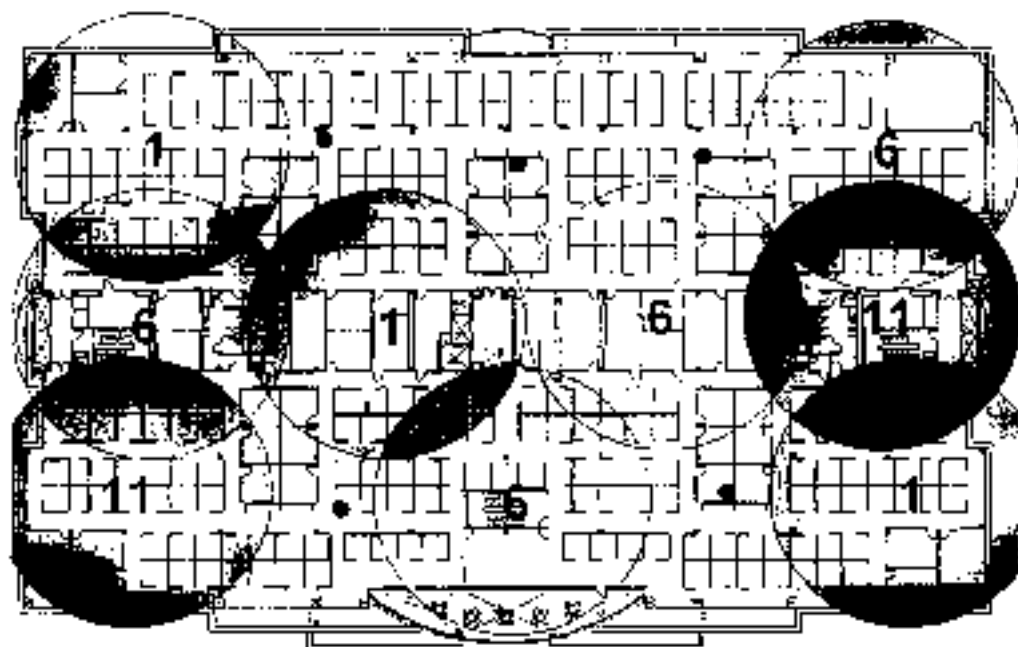


Рис. 8.4. План частичного развертывания сети для офиса

## Картирование места развертывания сети

Все, что вы как системный администратор или картограф места работ должны знать, — это число, расположение и необходимую конфигурацию точек доступа в зданиях компании. Чтобы получить эту информацию, как уже говорилось, сначала необходимо определить, какой будет разворачиваемая сеть — ориентированной на максимальную зону обслуживания, высокую пропускную способность или гибридной, переходной, когда необходимо учитывать оба аспекта. Физический аспект картирования места развертывания должен дать администратору представление о том, какую область покрывает каждая точка доступа, каково количество точек доступа, необходимых для обслуживания всей заданной области, какие каналы и перелатчики какой мощности следует использовать и какой тип или с каким коэффициентом усиления должны быть

антенны. Зная все это, администратор может переделать отношение числа пользователей к числу точек доступа и оценить производительность и скорость перенаправления в расчете на одного пользователя в варианте развертывания, ориентированном на максимальную зону обслуживания. При рассмотрении варианта развертывания, ориентированного на достижение максимальной пропускной способности, следует начать с требуемой производительности и скорости перенаправления и пересчете на одного пользователя, а также вынести планы размещения точек доступа, чтобы определить отношение числа пользователей/число точек доступа. Кроме того, вам необходимо учесть и другие факторы, такие как ограничения, накладываемые пропускной инфраструктурой и возможностями обслуживания ваших точек доступа. В конце концов вы должны разместить и сконфигурировать ваши точки доступа с целью максимизации их характеристик в основной области обслуживания.

## Проблемы, возникающие при картировании места работ

Как инженер, которому поручили провести картирование места работ, вы столкнетесь со многими проблемами и задачами, связанными с планированием. Даже до того, как приступите к изучению места развертывания сети. Например, если вы не знаете, какова инфраструктура помещения, вы можете обнаружить, что разместили свои точки доступа на железобетонных, для покрытия которых недостаточно кабеля категории 5 сети 100BASE-T длиной 100 м. В результате вы можете потратить сотни часов на замеры лишь для того, чтобы доказать, все же нужно начинать сначала. Многие из препятствий, которые вам придется преодолеть, могут оказаться специфичными для отрасли промышленности, в которой вы работаете, как в предыдущем рассмотренном вами примере, когда из-за большого количества помещений могут потребоваться уникальные решения. В данном разделе мы рассматриваем проблемы, с которыми вы можете встретиться в которых должны выжить, в главе 10, "Конструктивные особенности WLAN", эти проблемы рассматриваются применительно к конкретным отраслям промышленности.

Вы должны не только учитывать размеры помещений, но также то, как условия распространения радиоволн могут измениться со временем. Например, для предыдущего примера размещения сети в здании следует учитывать, что характеристики распространения будут существенно разными для случаев, когда полки пусты и полностью заполнены. Вы также должны обратить внимание на объекты, которые отражают микроволны и вызывают многоручежное распространение (см. главу 7, "Раднораспространяющий трафик"), или на объекты, которые могут поглощать радиоволны, мешая их распространению и при этом. Например, полки, заполненные поглощающими энергию буферными продуктами, которые препятствуют распространению радиоволн, иногда создают "тени", в которых прием крайне затруднен. точно так же, как непрозрачные объекты мешают распространению света. Возможен и противоположный случай, когда пустые металлические полки способствуют предельно минимальному распространению. Вы в своем исследовании должны рассмотреть оба названных экстремальных варианта и специфические требования, которым должна удовлетворять сеть при таких условиях. Чтобы развертываемая вами сеть могла оставаться работоспособной как при пустых, так и при, через некоторое время, заполненных полках, вам, возможно, придется перейти к зонам покрытия меньшего размера или более направленным каналам связи, когда энергия радиоволн направляется непосредственно туда, куда нужно, из точки, которая никогда не будет затенена.

В то же время мы должны минимизировать количество энергии, которая просачивается в другие коды, когда пилки рушатся, или уменьшая мощность передатчика, или за счет применения направленных антенн. В любом случае вам придется тщательно измерить уровни сигнала при картировании места работ, чтобы удостовериться в правильности ваших предположений.

В сфере розничной торговли требования к сети могут изменяться от малого использования до интенсивного использования менеджерами небольшого числа телефонов стандарта 802.11 в течение рабочего времени и затем огромного числа обращений к беспроводной сети во время вечеров инвентаризации с использованием сканеров штрих-кодов. Эти сканеры могут потребовать передачи очень большого числа пакетов транзакции, которые должны достигнуть мест сканирования и организационный персонал времени. И наоборот, диспетчер наблюдения могут потребовать очень высокой пропускной способности сети. В первом случае важно, чтобы на EPC покрывались все участки, где могут применяться сканеры. Поскольку возможности использовать небольшие данные, в некоторых зонах достаточно обеспечить высокую скорость передачи данных. Для передачи видеосигналов потребуется, по-прежнему, высокая скорость передачи данных, но камеры находятся скорее всего, в немногих фиксированных точках или лишь в некоторых из зон, где сотрудники работают со сканерами.

Вы не сможете контролировать переданные источники помех, например некоторые беспроводные телефоны, микроволновые печи и даже другие WLAN. Беспроводные телефоны, не соответствующие стандарту 802.11, — наиболее часто встречающиеся источник помех для WLAN. Эти телефоны часто имеют конструкцию, позволяющую им работать или в диапазонах 2,4 ГГц, или 5,8 ГГц ISM, применяя либо технологию скачкообразной перестройки частоты, либо технологию прямой последовательности расширения спектра. Степень ухудшения связи, если это вообще имеет место, зависит от числа и типов используемых телефонов. Некоторые старые телефоны диапазона 2,4 ГГц могут загораживать всю полосу пропускания, другие используют спектр в идиальном режиме. Если используется только один телефон, как это бывает в домашних условиях, наилучшим вариантом будет размещение базовой станции подальше от точек доступа или мест, где предполагается высокая активность клиентов. В случае офиса со многими телефонными линиями шума может вырасти, из-за чего условия передачи для WLAN ухудшатся. Наилучшим выходом будет или использование системы телефонной связи, не мешающей функционированию сетей стандарта 802.11, или использование для разных телефонных сетей и сетей передачи данных разных частотных диапазонов.

Другой повод для беспокойства относительно помех, который часто возникает в компаниях, связанных со здравоохранением, — это ответственное оборудование, для которого ваша сеть может стать источником вредных помех. Поскольку диапазон 2,4 ГГц ISM был выделен для применения в медицине, в некоторых больницах может использоваться оборудование, работающее в этом диапазоне. В общем случае WLAN функционирует с использованием уровней излучаемой мощности, намного меньших, чем характерные для медицинской аппаратуры, и нам следовало бы использовать в сети те каналы, которые не используются медицинскими приборами, или при уровнях мощности, не вызывающих помех в работу медицинской аппаратуры. Первое и главное — вы должны выяснить, где расположены медицинские приборы и каковы их характеристики. Оборудование WLAN, параметры которого не выходят за рамки требований 801-1.2 Международной электротехнической комиссии (МЭК), удовлетворяет промышленным стандартам. Это не означает, что помехи не могут возникнуть, но шансы их появления

снижаются. Если в зданиях размещается ответственные оборудование, работающее в диапазоне 2,4 ГГц, наилучшим выбором может оказаться использование сетей стандарта 802.11, работающих не в диапазоне ISM, а в диапазоне U-NII, только тогда вы будете полностью уверены в отсутствии помех.

Окружающая среда сама по себе может создать проблемы. Если выводу оборудования придется работать при экстремальных температурах, высокой или низкой влажности или в сырости. Например, может оказаться, что в зону покрытия должны войти холодильные камеры. В таком случае может оказаться необходимым разместить точку доступа в обогреваемом кожухе, если температура окружающей среды окажется ниже той, при которой производитель гарантирует ее бесперебойную работу. Аналогичным образом, если вы создаете зону покрытия вне помещений и не хотите гнуть длинный радиочастотный кабель от расположенной внутри помещения точки доступа к месту расположения внешней антенны, вы можете разместить точку доступа в правильно выбранном стальной корпусе NEMA<sup>1</sup>, чтобы предохранить ее от воздействия дождя и прочих погодных условий. Если необходимо охватить локальной сетью несколько этажей здания, например многоквартирного дома, при планировании необходимо помнить о том, что сеть первого этажа может высылать помехи в работу сети второго этажа, и наоборот, в зависимости от конфигурации конструкции здания. Потенциально это может привести к затягиванию процесса картирования зоны работы, потому что нужно будет измерять интерференцию сигнала не только на "своем" этаже, но и на этажах одним выше и одним ниже.

В случае размещения сети на территории ограниченной территории или в образовательном учреждении могут быть предъявлены особые эстетические требования, например по сокрытию инфраструктуры сети, защите ее от вандализма, или какие-то специфические корпоративные требования. В таких случаях точки доступа обычно располагают в пазах подвешенного потолка над потолочными панелями, если там имеется место, и затем размещают антенны на потолке или прямо на стенах. В таких условиях часто бывает удобно использовать микрополосковые антенны, поскольку они маленькие и плоские.

Помимо учета всех этих моментов, необходимо обращать внимание на характеристики клиентских устройств конечных пользователей. При этом необходимо принимать во внимание такие факторы, как типы клиентских устройств, которые должны поддерживать сеть. Каждый человек держит в руках эти клиентские устройства и типы приложений, которые он выполняет с использованием WLAN. В случае стационарных ПК, размещенных в офисе, объем трафика будет невелик, так что основное внимание можно будет уделить уменьшению степени перекрытия каналов. Если даже используются ноутбуки, не обязательно бывает необходимым обеспечить высокую скорость передачи данных валли от рабочих сессий и конференц-залов. Если речь идет об инженерной фирме, в которой широко используются приложения, предъявляющие высокие требования к полосе пропускания, например программы автоматизированного проектирования, необходимо будет максимально увеличить емкость сети, т.е. увеличивать размеры сот и количество пользователей в них. И наоборот, если конечные пользователи применяют в основном такие сеансовые приложения, которые характерны для сканеров штрих-кодов, требования к полосе пропускания могут быть минимальными, но зато понадобится зона покрытия с беспрерывным ретрансляцией и обеспечением возможности связи во всех возможных точках. Помимо телефонных разговоров, такая сеть может быть наполнена множеством мелких пакетов данных, поэтому придется выяснить, насколько устройства инфраструктуры WLAN

---

<sup>1</sup>NEMA — Национальная ассоциация электротехнической промышленности. — *Прим. ред.*



приспособления к поддержанию телефонных разговоров. В таких случаях обычно требуется, чтобы в зоне покрытия сети не были "дыры". Некоторые специализированные клиентские устройства могут не поддерживать высокие скорости передачи данных. Это также следует иметь в виду. После изучения всех этих вопросов у вас появится основа для определения пропускной способности и требования по радиоприемнику пакетов вашей сети — и в общем, и в каких-то ее локальных зонах со специфическими требованиями.

## Сертифицировано Wi-Fi

Наличие ярлычка Wi-Fi CERTIFIED (сертифицировано альянсом Wi-Fi) на клиентских устройствах гарантирует базовый уровень взаимодействия изделий различных производителей. Как точки доступа, так и клиентские устройства должны иметь такой логотип — это императив. Альянс Wi-Fi выполняет тестирование на совместимость (см. главу 7, "Радиочастотный трафик"), так что проверенные им устройства можно использовать, не опасаясь возникновения проблем, связанных с совместимостью.

Как уже говорилось выше, недостаточно изучить только требования, предъявляемые к беспроводным устройствам. Необходимо также рассмотреть инфраструктуру LAN, к которой вы подключаетесь. Одним из наиболее важных вопросов является такой: "Какова топология вашей сети?" Необходимо изучить оборудование сети, ее хабы, коммутаторы и маршрутизаторы, к которым вы будете подключаться и транзиты, где они расположены. Следует также узнать, какие интерфейсы могут использоваться для доступа к сети. Чаще всего это будет неэкранированная витая пара (UTP), но это может быть и оптическое волокно. Помните, что Ethernet 10GBASE-T способен обеспечивать связь на расстоянии не более 100 м по кабелю UTP категории 5. Если используется протокол динамической конфигурации хоста (DHCP), выясните, где находится сервер и каковы периоды его аренды (lease times). Клиенты WLAN могут предъявлять к LAN требования, весьма отличающиеся от таковых ее "проводных" клиентов.

Вы должны также знать, прокладываются ли кабели в зданиях независимо от того, можно ли там разместить устройства инфраструктуры WLAN. Во многих строениях имеются противопожарные перегородки, процедуры прокладки кабелей через них регламентируются Национальным сводом правил по эксплуатации электростанций (National Electric Code). Вы должны отмерить нужные отрезки кабеля, состоящие из прямых сегментов и изгибных участков, когда кабель меняет свое направление на 90 градусов, обеспечить запас для подрезки по прокладке кабеля на случай возникновения непредвиденных проблем. Если используется витая пара, следует минимизировать его длину и не забывать о потерях, которые он вносит для сигнала на рабочей частоте.

## Инструменты, используемые при картировании места работ

После заказа о проблемах, характеристиках и целях развертывания вашей WLAN пришла пора познакомиться как с инструментарием, посредством которого вы будете проводить картирование места работ:

- Клиентские устройства, радиостанция и антенны, которые вы будете обслуживать в своей сети
- Точки доступа с портативными батарейными источниками питания, способными поддерживать их работоспособность до меньшей мере в течение 8 часов.
- По две антенны каждого типа, которые вы предполагаете использовать.

- Монтажный инструмент для точки доступа, портативных батарейных источников питания и антенн. В комплект должны входить накладки для точечного скрепления (brackets), изоляционный лента и т.д.
- Маркеры для указания мест расположения точек доступа.
- Мерные ролики для горизонтальной и вертикальной разметки.
- Радиочастотный кабель или аттенюатор, если предполагается использование уличных антенн.
- Радиорифоры, которые обеспечивают необходимый уровень и качество принятого сигнала, уровни шума и помех, а также характеристики передачи пакетов.

## Проведение картирования места работ

Прежде чем как будет подготовлен весь необходимый инструментарий, потратите время для проведения собственно картирования. Помните, что, как уже говорилось в начале данного раздела, в процессе картирования места развертывания сети вы должны ответить на следующие вопросы:

- Где будут размещены точки доступа?
- Какими образом они будут монтироваться?
- Как они будут подключаться к LAN?
- Где необходимо проложить кабели и установить источники питания?
- Какие антенны используются и где они будут размещены и смонтированы?
- Какими должны быть конфигурационные параметры, чтобы были обеспечены необходимые производительность и скорость передачи данных?
- Какие каналы должны использоваться?

Ответы на них должны быть исчерпывающими настолько, чтобы кто-то помимо вас также смог выполнить установку сети.

В зависимости от того, какой из двух крайних подходов будет выбран — ориентирование на зону покрытия или максимальную производительность, — ваше физическое исследование будет проводиться несколько по-разному. В любом случае распределение каналов должно быть выполнено таким образом, чтобы избежать их перекрытия, каждое исследование должно проводиться именно на том канале, который будет использоваться. Вам следует также провести исследование при минимально необходимой скорости передачи данных. Если речь идет о множественном диапазоне, не забывайте о крайних зонах — этапе над и этапе под рассматриваемым; на них тоже нужно провести все измерения. Проведите все измерения на канале, который вы собираетесь использовать, в противном случае вы можете столкнуться с помехами неизвестного происхождения. Если сети окажутся меньшими, чем ожидалось, попробуйте поменять каналы, поскольку эта проблема может быть вызвана взаимными помехами.

В случае ориентации на максимальную зону обслуживания выберите один из ее краев и поместите там точку доступа. Потом идите к центру предполагаемой зоны обслуживания до тех пор, пока не обнаружите границу зоны покрытия. Переместите точку доступа в это место и исследуйте ее зону обслуживания. Далее возможны два варианта.

- Можно поменять тот же самый способ для других крайних точек доступа и затем заполнить "дыры" в середине.

- ♦ Можно разместить следующую точку доступа на краю только что исследованной зоны обслуживания, найти ее край и переместить точку доступа в этом месте. Аналогичным образом исследуется все здание.

При любом из описанных подходов необходимо определить край сот и предусмотреть приемлемый уровень их перекрытия. На рис. 8.5 представлен подход "от края к середине", а на рис. 8.6 — подход "от одной точки доступа к другой". На каждом из рисунков установленный канал показан в центре каждой окружности ряда. Визуальные точки доступа указывают на потенциальные местоположения, используемые с целью определения центральной точки для размещения в ней точки доступа. Стрелками показано, как от позиционирования одной точки доступа переходят к позиционированию другой.

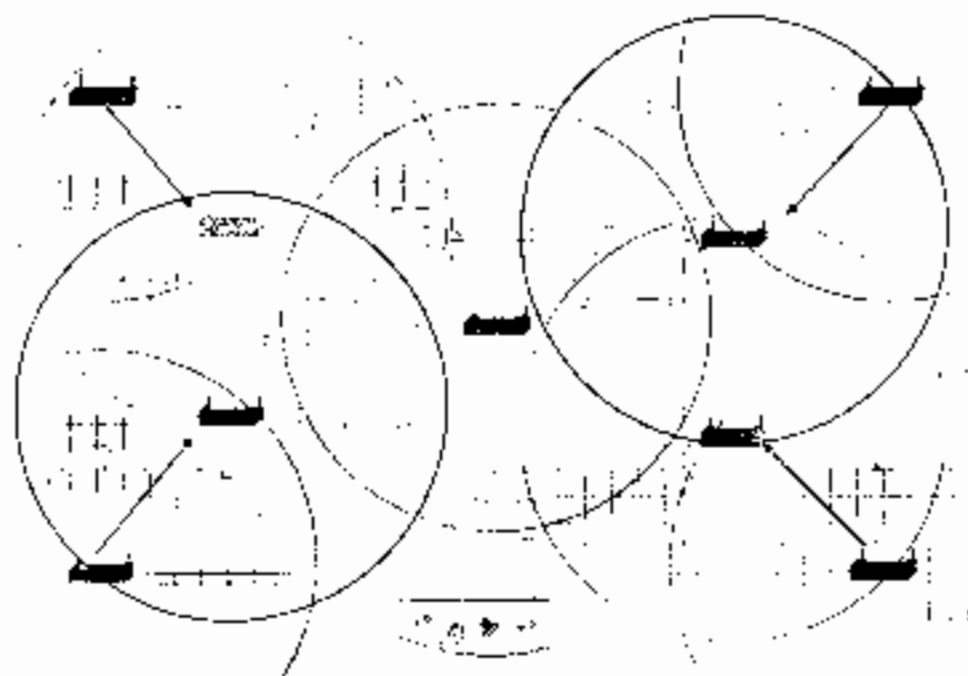


Рис. 8.5 Картирование ориентированной на максимальное покрытие LAN методом "от края к середине" с идентификацией локализации "Дир"

При подходе, ориентированном на достижение максимальной пригодности, следует определить число пользователей, которые будут подключаться к каждой точке доступа, и плотность их размещения (отсюда можно определить желательный радиус сот). Используйте те же способы, что описаны выше, но регулируйте мощность. Ни в коем случае не достигайте желаемых размеров сот. Вероятнее всего, вам придется использовать подход "от края к середине", если пользователи размещаются по некоторой степени изолированными группами, но возможна и другая подоплека, если плотность размещения пользователей фиксирована лишь для области покрытия всей сети.

В зависимости от особенностей места размещения и предъявляемых требований вы можете довольно долго экспериментировать и исправлять ошибки. Следует использовать творческий подход, поскольку существует много вариантов сборки этого "лазилки".

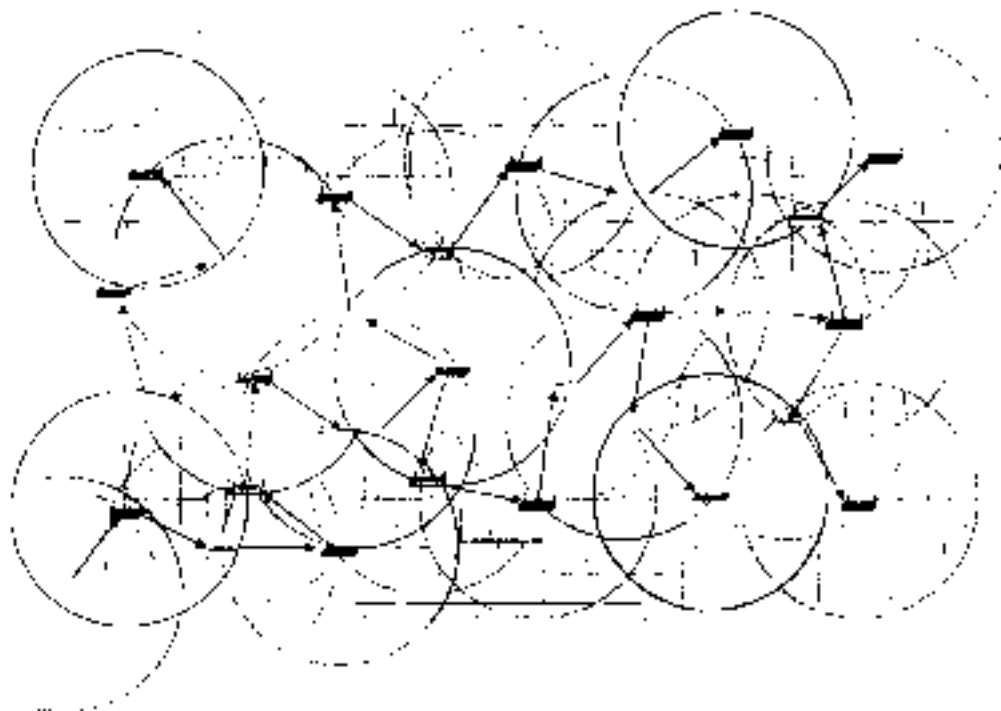


Рис. 8.6. Конфирмирование оптимизированной по локальному покрытию WLAN сетью для точки доступа и другой

---

#### На заметку

Например, вы можете использовать направленные антенны, такие как антенна "волновой канал" для обеспечения покрытия пристройки к зданию, или проложить оптическое волокно к точкам доступа, расположенным в дальних концах.

---

## Исследования более высоких уровней

После того как будет закончено картирование места работ и планирование размещения элементов физического уровня, должна начаться вторая фаза развертывания WLAN. Система безопасности WLAN требует наличия сервера аутентификации, авторизации и учета (AAA), такого как RADIUS, для проведения аутентификации, ориентированной на пользователя. Кроме того, необходимо также развернуть механизм управления WLAN – или путем расширения существующей платформы управления, такой как CiscoWorks, или за счет внедрения платформы управления WLAN, отражающей специфику домена.

## Развертывание LAN стандарта 802.1X

В главе 4, "Безопасность беспроводных LAN", рассматривались проблемы защиты и то, насколько сети стандарта 802.1x соответствуют спецификации защищенного доступа к сети Wi-Fi (Wi-Fi Protected Access, WPA) и грядущему стандарту 802.11i. При-

званию обеспечить безопасность WLAN. Решением, обеспечивающее защиту, требует применения AAA-сервера для проведения организованный на пользователя аутентификации. Возможно, AAA-сервер будет размещен в защищенном информационном центре, "на расстоянии" и несколько маршрутизаторов от края сети. С помощью механизма уровня 3 можно измерить задержку в сети (network latency) между краем сети и информационным центром, которая может составлять несколько микросекунд, если не миллисекунд.

Сети стандарта 802.1X усложняются в случае, если их данные распространяются через канал глобальной сети (WAN). Каналы WAN обычно имеют меньшую полосу пропускания, чем соединения LAN, в результате которые могут оказывать перегрузками. Перегрузка может оказать существенное влияние на процесс аутентификации, если не реализуется на механизмах стандарта 802.1X. В таких случаях утеря RADIUS-пакетов может привести к тому, что клиентские станции не успеют завершить свои процессы аутентификации в отведенное для этого время и завершатся неудачей. Кроме того, потенциально от перегрузки может пострадать и роумтинг (рис. 8.7).

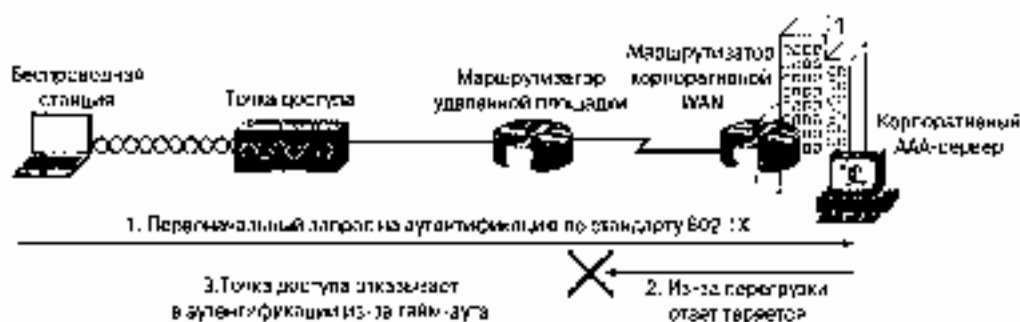


Рис. 8.7. Влияние перегрузки канала WAN на процесс аутентификации по стандарту 802.1X на удаленном клиентском устройстве

Эту проблему можно решить двумя путями.

- Использовать механизмы QoS для задания приоритетов в отрывке RADIUS-пакетов стандарта 802.1X через WAN
- Установить локальный AAA-сервер на удаленной площадке

## Приоритезация RADIUS-пакетов стандарта 802.1x с использованием IP QoS

Использовать механизм QoS для приоритезации RADIUS-пакетов возможно. Он обеспечивает приоритет передачи пакетов стандарта 802.1x в случае перегрузки WAN. Для тех, кто уже применяет механизм QoS для поддержки IP-телефонии, процесс наращивания возможностей маршрутизатора Cisco и конфигурирования коммутатора превращается в формальность.

Приложения VoIP обычно устанавливают приоритет IP-дейтаграмм, равный 5, код указателя дифференцированной службы (DSCP) должен иметь значение, соответствующее срочной передаче (expedited forwarding, EF). Видеосессии обычно имеют приоритет IP-дейтаграмм, равный 4, и значение DSCP в диапазоне от AF41 до AF43. Протокол, управляющий проведением VoIP-разговора (MGCP или H.323), обычно имеет приоритет IP-дейтаграмм 3 и значение DSCP в диапазоне от AF31 до AF33.

Пакеты стандарта 802.1X сервера RADIUS можно рассматривать как пакеты управления трафиком, которые важны для функционирования сети, поэтому разумно классифицировать их наряду с пакетами управления VoIP радиусом с приоритетом IP-дейтаграмм 3 или значением DSCP в диапазоне от AF31 до AF33. Все эти значения приведены в табл. 8.1.

Таблица 8.1. IP QoS

Функция	Приоритет IP-дейтаграмм	Значение DSCP
Передача речи (VoIP)	5	EF
Передача видео	4	AF41-AF43
Сигнализация (управление VoIP-разговором, 802.1x)	3	AF31-AF33
Обычные данные	0	0

Использование механизма QoS для приоритизации трафика сервера RADIUS не решает все проблемы, связанные с аутентификацией на удаленной площадке. Остаются нерешенными следующие:

- Выход из строя WAN.
- Задержка WAN.

Если канал WAN становится недоступным, клиентская станция может не получить доступ к WLAN, в результате чего пользователь лишается возможности работать с локальными ресурсами. Каналы WAN с очень большой задержкой (например, использующие терминалы со световым апертурой луча, VSAT) могут также негативно повлиять на процесс аутентификации, потому что точка доступа для клиента может просто не успеть его завершить из-за тайм-аута. В результате рабочие характеристики станции ухудшаются.

## Локальная аутентификация на удаленных площадках

Локальная аутентификация на удаленных площадках может показаться очевидным способом решения проблемы, но и она не является панацеей. При размещении AAA-серверов на удаленных площадках возникают свои сложности.

- **Дороговизна решения.** Требуется по крайней мере один сервер на площадку, а площадка может быть микроскопической.
- **Управляемость**
  - В некоторых случаях счет числа серверов аутентификации идет на тысячи.
  - Репликация баз данных пользователей на большое число удаленных площадок может оказаться проблематичной.
  - Доступ администратора может оказаться затрудненным, если администраторы удаленных площадок должны постоянно иметь доступ к центральному серверу.

Некоторые производители, такие как Cisco Systems, обеспечивают живучесть механизма аутентификации посредством схожих точек доступа, чтобы клиенты могли избежать излишних затрат и справиться с узкими местами, появившимися в результате использования локальных AAA-серверов (рис. 8.8). Хотя такое решение нельзя назвать совершенным, оно дает возможность администраторам спокойно развертывать WLAN

на удаленных площадках и в то же время поддерживать только одну базу данных с данными аутентификации и управлять ею.

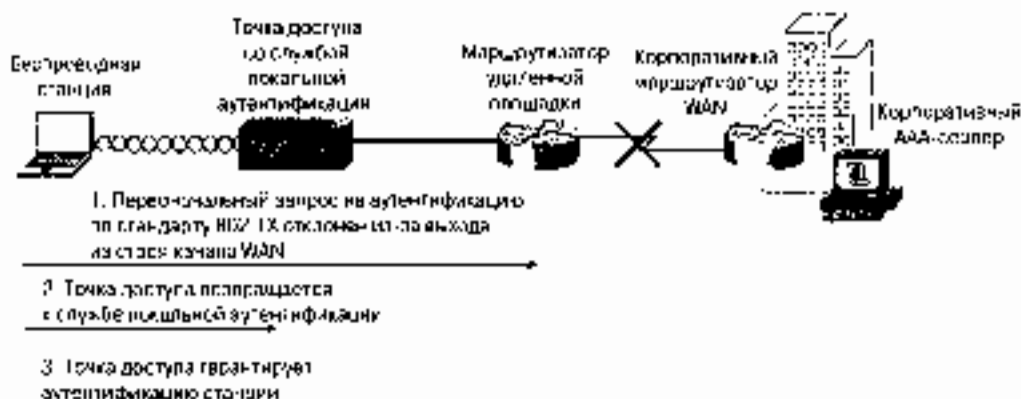


Рис. 4.8. Сеть для локальной аутентификации в точке доступа

## Управление беспроводными LAN

Управление сетями, и в частности управление беспроводными LAN, — это тема, которая требует написания отдельной книги. В данном разделе мы обратим ваше внимание на некоторые ключевые концепции, которые вы должны рассмотреть при развертывании сети.

Для сети любого типа справедливы следующие высказывания.

*Нельзя управлять тем, чего невозможно измерить.*

Во многих больших сетях количество управляемых устройств может достигать тысячи. При развертывании WLAN на типичном большом предприятии достаточно часто количество точек доступа может достигать трех тысяч. Доказанные LAN могут оказаться бесполезными именно по той, как вы управляете своей сетью, а также изменить используемый вами инструментарий. Чтобы добиться от WLAN такой же надежности, какую обеспечивают проводные LAN, и снизить сложность управления вам необходимо решение для механизма управления, обеспечивающее одновременно и управление беспроводной LAN.

Многие первые энтузиасты WLAN с трудом нашли время управления ими. Большинство из недорогих пакетов управления было невозможно масштабировать на управление несколькими тысячами устройств без применения многочисленных управляющих станций, и они не обеспечивали выполнение функций управления, специфичных для радиоприборов. Из-за этого развернутые сети имели недостаточно высокие характеристики, и администраторы были вынуждены разрабатывать собственные инструментальные средства для эффективного управления беспроводными LAN. Однако теперь положение изменилось. Большинство ноутбуков снабжено сетевыми интерфейсными платами (NIC) стандарта 802.11, которые превратились в стандартные устройства, а пользователи начали активно использовать WLAN и ожидают, что они станут столь же доступными, как проводные сети.

Многие системы управления WLAN обеспечивают сервисы, аналогичные таковым проводных сетей: опция и использование простого протокола управления сетью

(SNMP), контроль неисправностей, накопление информации об отказах (trap collection), автоматическую передачу параметров конфигурации (configuration distribution), автоматическое обновление микропрограмм управления устройствами (firmware distribution) и т.д. Ни одно из доступных решений не дает возможности администратору "заглянуть внутрь" собственно радиосети. Характеристики даже однотипных WLAN широко меняются при каждом развертывании. Материалы стен и местонахождение предметов интерьера помещений, таких как микроволновые печи, могут оказывать влияние на характеристики WLAN, а влияние устройств, использующих технологию Bluetooth, беспроводных клиентов (ad hoc clients) и соседей, также использующих WLAN, могут ухудшить характеристики WLAN до уровня, когда она станет вообще бесконечной.

Система управления радиотрактом дает администратору возможность четко видеть все эти проблемы и, в зависимости от применяемого решения, может помочь либо проводить контроль таких параметров радиостанций, как выбор частоты/канала и используемой мощности клиента/точки доступа для адаптации сети к суровой окружающей радиосреде.

Иные решения, обеспечивающие выполнение этих функций, потому что они значительно облегчат вашу работу как администратора. Организация радиочастотных сетей настолько отличается от организации проводных сетей, что при отсутствии многолетнего опыта работы с ними поиск инструментария управления, обеспечивающего комплексное картирование места работ и проведение необходимых расчетов, потерь на трассе, выявление летящих помех и мест возможного размещения служб, определенно имеет смысл.

## Резюме

Решения, которые вы принимаете при развертывании WLAN, весьма важны для достижения ее оптимальных характеристик.

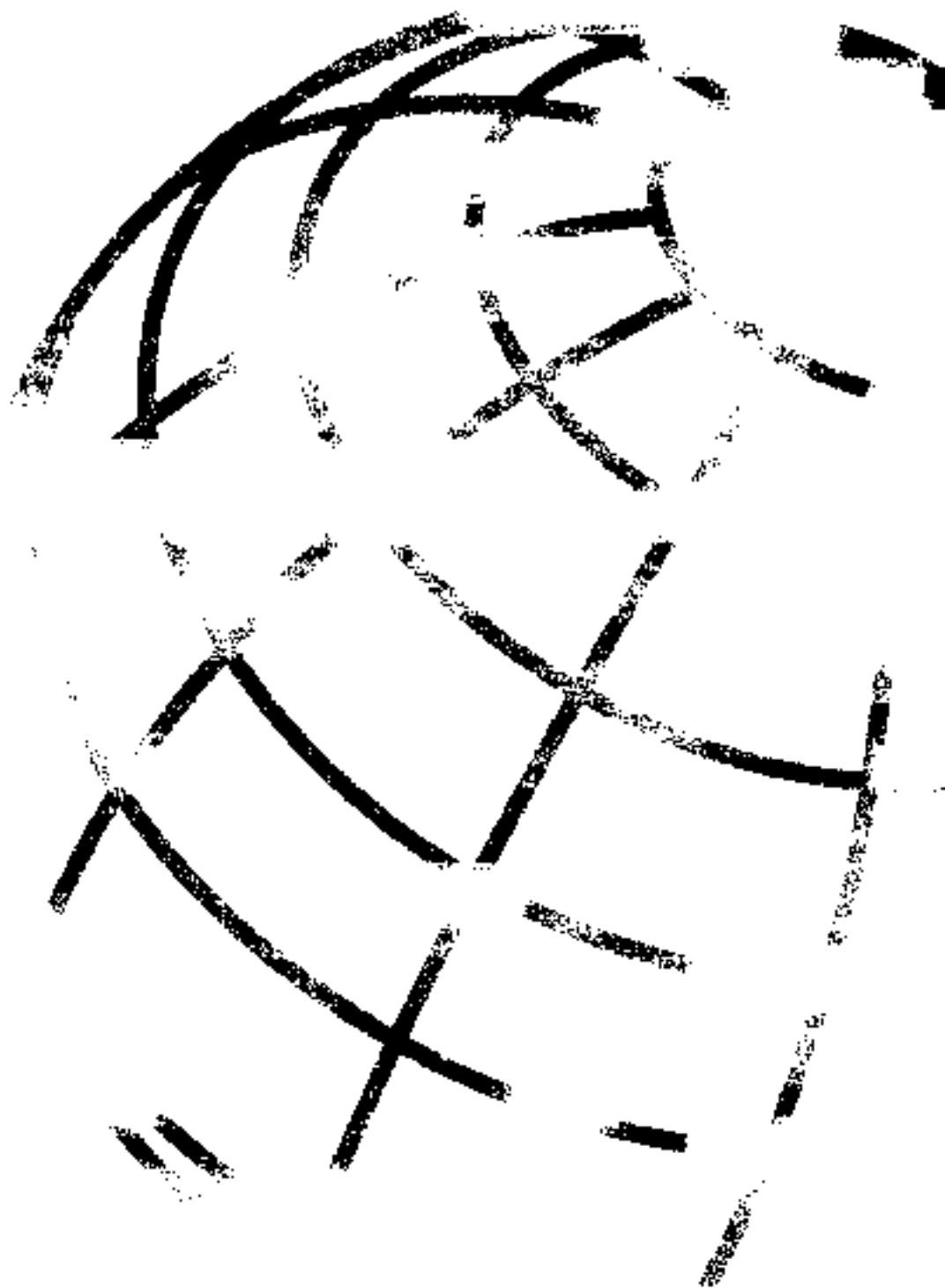
- Какие пользователи будут использовать WLAN (преимущественно мобильные или когнитивные)?
- Приложения какого типа будут выполнять эти пользователи с помощью LAN?

Хотя эти два вопроса являются основными и почти самоочевидными, им обычно не придается значения во время развертывания. Однако они являются основными для экономии средств во время жизни развернутой сети, а именно при выборе сценария развертывания, т.е. при выборе между сетью, ориентированной на максимальную зону обслуживания или максимальную производительность.

Решая, как будет развертываться сеть, вы узнаете, какой инструментарий следует использовать для проведения картирования места работ: лучший метод организации таких работ позволит сэкономить время и средства, необходимые для решения этих трудоемких и отнимающих много времени задач. На сегодняшний день исследование места размещения является задачей, подлежащей решению вручную. Это означает, что все измерения и измерения должен выполнять сотрудник, выполняющий картирование. По мере роста числа WLAN и появления инструментария, позволяющего автоматизировать некоторые из этих процессов, разумно ожидать, что WLAN будут иметь такие же характеристики и надежность, как и проводные сети.







## Будущее беспроводных LAN

---

Предсказывать будущее какой-либо технологии — непростая задача, однако в данной главе мы расскажем о некоторых уже существующих и развивающихся технологиях, которые могут изменить облик WLAN. Некоторые из этих технологий на самом деле не подходят для создания беспроводных LAN (WLAN), но они могут стать хорошим дополняющим решением.

Первая технология, которую мы рассмотрим, — это Bluetooth, разработанная для создания беспроводных соединений небольшой протяженности, в частности для замены кабелей длиной менее 3 м (10 футов). Технологию Bluetooth часто называют *персональная сеть* (personal-area network, PAN). Затем мы рассмотрим *технология сверхширокополосной связи* (ultra wide band, UWB), представляющую собой следующее поколение Bluetooth с намного большей скоростью передачи данных, обеспечиваемой посредством передачи импульсов короткой длительности и малой мощности. На другом конце спектра может развиваться уже давно развиваемая *технология передачи оптических сигналов через свободное пространство* (free space optics, FSO), хорошо приспособленная для установления соединений типа "точка-точка". В ней преобразователи, предназначенные для волоконно-оптических линий связи, используются для передачи гигабитов данных без помощи оптического волокна. Наконец, на ранней стадии разработки дамынок WLAN, рассчитанные на скорость передачи 100 Мбит/с, их назначение — расширить возможности технологий, соответствующих стандартам 802.11. Скорее всего, именно они станут следующим поколением технологий, предназначенных для выполнения приложений, упоминаемых в нашей книге.

Как уже упоминалось, некоторые из названных технологий могут сохранить за собой какие-то сегменты рынка и будут применяться в качестве решений для WLAN, некоторые даже смогут вытеснить устройства стандарта 802.11, а некоторые омертвнут.

### Технология Bluetooth

Из всех технологий, рассматриваемых в этой главе, Bluetooth, по-видимому, является наиболее перспективной. Кроме того, применение устройств и решений Bluetooth для создания персональных сетей расширяется, поскольку эта технология стала доступна потребителям еще несколько лет назад. Как уже говорилось, технология Bluetooth разрабатывалась с целью замены соединительных кабелей различных устройств, находящихся на небольших (менее 10 м) расстояниях одно от другого, например компьютера и клавиатуры или микрофона и сотового телефона, находящихся

в кармане человека. На рис. 9.1 показаны примеры использования беспроводных каналов связи Bluetooth вместо беспорядочно проложенных и перепутанных кабелей для соединения ПК с периферийными устройствами.



Рис. 9.1. Замена кабелей каналами связи Bluetooth

Устройства Bluetooth работают в том же диапазоне 2,4 ГГц, предназначенном для использования в промышленности, науке и медицине (ISM), что и устройства стандартов 802.11 и 802.11b, и многие из той же части 15 правил Федеральной комиссии связи США (Federal Communications Commission, FCC) регламентируют их применение и допустимую излучаемую мощность. Эти правила требуют, чтобы устройства не издавали помех для лицензированных пользователей, и устанавливают, что они не имеют защиты от помех со стороны других пользователей, как лицензированных, так и нелцензированных. Этот момент важен потому, что в будущем такие устройства станут главным источником помех для WLAN, и наоборот, если производители ноутбуков начнут исправлять те и другие устройства в связи с этим. Подобно WLAN, они также будут подвержены воздействию помех со стороны микроволновых печей и беспроводных телефонов.

Каждое устройство сети Bluetooth (или *малая сеть* (piconetwork) — крошечной самоподдерживающейся сети) является или ведущим (master), или ведомым (slave). Ведущий инициирует создание беспроводных каналов, ведомые отвечают ведущему. В общем случае любое устройство Bluetooth может быть как ведущим, так и ведомым, может изменять выполняемую функцию и даже выполнять обе одновременно в разных сетях. Многоточечная сеть Bluetooth может иметь до семи активных ведомых на одного ведущего. Все эти ведомые могут связываться только с ведущим, так что любая связь между ведомыми может осуществляться только через ведущего. Распределенная сеть (scatternet) образуется, когда устройство является ведомым в более чем одной пикосети или когда оно является ведущим в одной и ведомым в другой.

Близлежащие устройства Bluetooth имеют уровень эффективной изотропно-излучаемой мощности 0 дБ относительно 1 мВт (dBm), хотя в спецификации оговорены три класса устройств Bluetooth.

- Передачики класса 1 могут обеспечивать мощность до 20 dBm (100 мВт), но должны иметь систему управления излучаемой мощностью, чтобы использовать лишь мощность, минимально необходимую для установления надежной связи.
- Передачики класса 2 должны иметь максимальную излучаемую мощность 4 dBm (2,5 мВт).
- Передачики класса 3 обеспечивают мощность 0 dBm (1 мВт).

Поскольку технология Bluetooth была разработана для замены кабельных соединений, зачастую для устройств с батарейным питанием, передатчики класса 1 Bluetooth

мало распространены. Схема модуляции, применяемая в технологии Bluetooth, — это модуляция, основанная на гауссовом переключении частот (Gaussian Frequency Shift Keying, GFSK), похожая на применяемую в WLAN модуляцию с расширенным спектром путем скачкообразного переключения частоты (FHSS), со скоростью передачи символов 1 миллион в секунду, что дает в результате базовую скорость передачи данных 1 Мбит/с.

Алгоритмически старый WLAN стандарт 802.11, и технология Bluetooth применяются механизмы доступа на основе дуплексной связи с переменным разделением каналов (time division duplex, TDD), непериодичной FHSS. Диапазон 2,4 ГГц ISM делится на 79 каналов шириной 1 МГц каждый, и каждая пикосеть скачкообразно переходит с канала на канал последовательным образом. Устройства Bluetooth передают каждый пакет на новом канале. Для соединения "точка-точка" при создании пикосети с одним ведомым сдвигаются и нумеруются временные интервалы длительностью 625 мкс, каждый для своего канала: ведущий передает в четные интервалы времени, ведомый — в нечетные. В течение каждого интервала можно передать 366 байт. В случае многоточечной пикосети ведущий тоже осуществляет передачу в четные интервалы, но каждый ведомый может передать данные только в том случае, если в течение предыдущего интервала был передан пакет, адресованный лично ему. Широковещательные пакеты получают все ведомые, но ни один из них не имеет права осуществить передачу в течение интервала времени, следующего за передачей широковещательного пакета. Поскольку данные приходится разбивать на части, чтобы их можно было передать в виде пакетов объемом 366 байт, накладные расходы протокола могут оказаться достаточно большими, поэтому в спецификации Bluetooth предусмотрена передача "многоинтервальных" (multi-slot) пакетов длительностью три и пять интервалов. Они передаются на одном и том же канале, и когда передача заканчивается, следующая осуществляется на канале, который никак никак бы в том случае, если бы многоинтервального пакета не было. Другими словами, некоторые каналы в последовательности скачкообразного переключения частоты пропускаются. Многоинтервальную передачу может осуществлять каждый ведущий или ведомый. На рис. 9.2 представлен образец накладных расходов передачи в многоточечной сети с двумя ведомыми, когда ведущий осуществляет передачу многоинтервального пакета одному из ведомых.

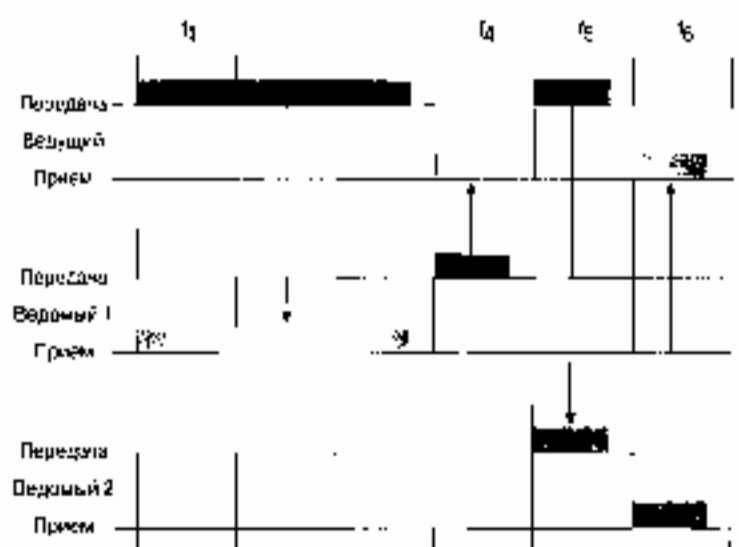


Рис. 9.2 Образец накладных расходов передачи по технологии Bluetooth

В технологии Bluetooth используются физические каналы двух разных типов.

- Асинхронные каналы без установления соединения (*asynchronous connectionless links, ACLs*) чаще всего используются для передачи данных и тех случаях, когда сохранение их целостности оказывается гораздо важнее возможных задержек в передаче. Ошибки при передаче исправляются за счет повторной передачи пакетов.
- Синхронные каналы на основе соединений (*synchronous connection oriented, SCO*) обеспечивают создание коммутируемых, регулярных каналов типа "точка-точка" между ведущим и ведомым без повторной передачи пакетов.

Каждое устройство Bluetooth имеет уникальную 48-битовый адрес Bluetooth-устройства. Активные ведомые получают 3-битовые адреса активных членов от ведущего, а неактивные, или, ведомые (*parked slaves*), получают 8-битовые адреса припаркованных членов. Эти припаркованные ведомые синхронизируются с таймером ведущего и последовательностью переключения частоты и получают широкополосные пакеты, в которых ведущий использует адрес припаркованного участника сети для того, чтобы распарковать его. Ведущий также назначает им адрес запрета на доступ, который указывает особое окно доступа, в течение которого они могут послать запрос на распарковку. Как уже говорилось, устройства Bluetooth могут быть или ведущими, или ведомыми, причем ведущий — не что иное, как устройство, инициирующее создание пикосети, а то время как ведомый — это устройство, контроль которого находится в близости по отношению к ведущему. Ведущий может инициировать переход в энергосберегающий режим, отключить (*sniff*), удерживать (*hold*) и парковать — для экономии энергии, для обеспечения работы в пикосети, включающей более семи ведомых, для предоставления ведомому времени для включения в пикосеть других ведомых или для обеспечения возможности вхождения в несколько пикосетей, т.е. создания распределенной сети.

Поскольку распределенные сети весьма отличны от всех WLAN стандарта 802.11, имеет смысл рассмотреть их несколько подробнее. Три основные сферы применения распределенных сетей таковы.

- Обеспечение механизма для вхождения устройства в существующую пикосеть путем формирования распределенной сети с ее ведущим.
- Обеспечение связи между пикосетями
- Создание обширных сетей с промежуточным хранением (*limited state-and-forward network*).

Хотя эти инструменты могут оказаться весьма полезными, технология Bluetooth сталкивается с некоторыми проблемами. Что касается самих устройств, то они могут поддерживать синхронизацию с двумя независимыми пикосетями. Если говорить о производительности, то ошибки синхронизации между двумя пикосетями снижают их характеристики, а приемы более высоких уровней сталкиваются с проблемами маршрутизации и устранения ошибок. В случае графика ACL участник распределенной сети может использовать режимы *sniff*, *hold* и *park* для управления двумя пикосетями, но в случае графика SCO каждый член распределенной сети должен выбрать между своими двумя пикосетями. Все это может вызвать такие проблемы, что в конце концов вы придете к выводу, что лучше отключить свое устройство от одной пикосети, прежде чем подключаться к другой или установить два Bluetooth устройства на одном месте.

Специальная группа Bluetooth (*Bluetooth Special Interest Group, SIG*), которая разрабатывает спецификацию Bluetooth и, помимо всего прочего, управляет действующей

скими рабочими группами, сейчас определяет несколько моделей использования специфических приложений, применяя устройства от различных поставщиков. В модели использования HMDP (но не ограничиваясь ими) следующие:

- Обеспечение работы cordless и беспроводных телефонов и дополнение к циклически функцией беспроводной радиосвязи (walkie-talkie) по принципу "три в одном".
- Наушники, обеспечивающие аудиоинтерфейс к другим устройствам, таким как телефоны, компьютеры и стереосистемы.
- Мост J2telnet, позволяющий через сотовый телефон создавать мост для доступа к Telnet через сеть сотовой связи и компьютер с интерфейсом Bluetooth.
- Модели использования проталкивания объекта (object push) и преобразования файлов (file transfer), позволяющие осуществлять базовые преобразования данных между неподходящими для этого устройствами.

Преобразуя подходящие профили (совокупности параметров, profiles), которые являются основными "строительными блоками" Bluetooth, создают перечисленные выше модели использования. Эти профили

- позволяют разработчикам свести многие опции, обеспечиваемые Bluetooth, лишь к нескольким, обеспечивающим выполнение необходимых функций;
- обеспечить процедуры для выполнения функций, которые оговорены в основном наборе стандартов;
- обеспечить для пользователей одинаковость навыков работы, даже если они будут применять устройства от различных производителей.

Резюмируя, можно сказать, что Bluetooth умноженно решает иные проблемы, нежели стандарт 802.11, а именно проблему замены кабелей. Поэтому для этой технологии характерны меньшая скорость передачи данных, меньший радиус действия, меньшие потребляемые мощности и, в общем-то, меньшая стоимость. Поскольку и устройства Bluetooth, и устройства стандарта 802.11 работают в одном частотном диапазоне и потенциально являются источниками взаимных помех, будет интересно узнать, как разработчики ноутбуков решат проблему совместного размещения в них устройств стандарта 802.11 и Bluetooth.

## Технология UWB

Технология UWB — это новый метод передачи, для которого FCC определила мода что руководящие принципы использования экстремально широкополосных сигналов, генерируемых при передаче коротких импульсов малой мощности, считается, что они позволят создать широкополосные и мультисервисные системы связи. FCC определяет UWB как сигнал, который имеет относительную ширину полосы частот, т. е. отношение ширины частот сигнала к частоте несущей, превышающую 25%. Принципы использования, разработанные FCC, регламентируют передачу UWB-сигналов в широком диапазоне, используемом многими другими технологиями, но триждыюшиими более узкие диапазоны частот, чем характерные для UWB-сигналов. Это становится возможным потому, что пределы на излучаемую мощность столь строки, даже при большом количестве передатчиков, что они не оказывают ощутимого влияния на существующие технологии и системы. Системы UWB используют очень широкие полосы

частот для того, чтобы избавиться от влияния помех со стороны уже существующих узкополосных систем. В настоящее время не существует никаких стандартов на параметры излучения, частоту их следования, методы модуляции, но, несмотря на это, считается, что у такой технологии большое будущее. Отчет и инструкция FCC (FCC Report and Order) — вот регламентирующие руководства по созданию нескольких классов устройств UWB, для каждого из которых устанавливаются свои пределы на излучаемую мощность.

- Низкочастотная система формирования (сигналов) изображения, состоящая из радаров полупроводящего зондирования (ground penetrating radars, GPR).
- Высокочастотная система формирования (сигналов) изображения, состоящая из GPR, формирования изображения стен (wall imaging) и формирования медицинских изображений (medical imaging).
- Среднечастотная система формирования (сигналов) изображения для видения через стены (for through-wall imaging) и обзорных систем.
- Системы связи и измерительные системы для использования внутри помещений.
- Портативные системы связи и измерительные системы для использования вне помещений.
- Мобильные радарные системы для предотвращения столкновений, улучшенные системы активации или предотвращения столкновений (airbag activation) и подвесные системы (suspension systems).

Предельные классификационные параметры, за исключением мобильных радарных систем, представлены в табл. 9.1.

**Таблица 9.1. Предельные мощности сигналов UWB**

Классификация	Диапазон частот в соответствии с частью 15	Предельная излучаемая мощность в соответствии с частью 15 (dBm/MГц)					
		< 0,960 ГГц	0,960–1,61 ГГц	1,61–1,99 ГГц	1,99–3,1 ГГц	3,1–10,6 ГГц	> 10,6 ГГц
Низкочастотная система формирования изображения	< 960 МГц	-41,25	-65,3	-53,3	-51,3	-51,3	-51,3
Высокочастотная система формирования изображения	3,1–10,6 ГГц	41,25	65,3	-63,3	-51,3	41,3	51,3
Среднечастотная система формирования изображения	1,99–10,6 ГГц	-41,3	-53,3	-51,3	-41,3	-41,3	-51,3
Внутри помещений	3,1–10,6 ГГц	-41,3	-75,3	-53,3	-51,3	-41,3	-51,3
Вне помещений	3,1–10,6 ГГц	-41,3	-75,3	-63,3	-61,3	-41,3	-61,3



В мобильных радарных системах используется полоса частот от 22 до 29 ГГц. В табл. 9.2 представлены предельные и излучаемые мощности для этих систем.

**Таблица 9.2. Предельные и излучаемые мощности для мобильных радарных систем**

Классификация	Диапазон частот в соответствии с частью 15	Предельная излучаемая мощность в соответствии с частью 15 (дБВт/МГц)					
		< 0,950 ГГц	0,950–1,61 ГГц	1,61–22 ГГц	22–29 ГГц	29–31 ГГц	> 31 ГГц
Мобильные	22–29 ГГц	-41,3	-75,3	-61,3	-41,3	-51,3	-61,3

Как видите, уровни излучаемой мощности довольно низкие. В действительности они на уровне или ниже пределов на мощность побочного радиоизлучения для всех преднамеренных источников излучения и на уровне или ниже непреднамеренных источников излучения. Пределы на мощность излучения устройств диапазона ISM по крайней мере на 40 дБ выше, чем объявленные FCC для UWB, поэтому для большинства приемников UWB-сигналы будут представляться случайным шумом. Что касается помех сигналам UWB со стороны других радиопередатчиков, то большой выигрыш от обработки, который позволяет реализовать высокая относительная ширина полосы частот, дает возможность избавиться от помех со стороны узкополосных сигналов. Что касается многолучевого распространения, то высокая относительная ширина полосы частот также позволяет многократно увеличить длительность импульсов по отношению к их длительности, поэтому RAKE-приемники могли бы конструктивно использовать энергию многолучевого распространения.

#### На заметку

В добавок к излучению в нужном канале и рабочей полосе частот все источники генерируют непреднамеренные или побочные излучения на других частотах. В действительности многие электронные устройства, не относящиеся к устройствам микроволновой связи, генерируют побочные излучения. Интенсивность этих излучений жестко ограничивается требованиями на предельные побочные излучения.

#### На заметку

RAKE-приемник получает много экземпляров переданного сигнала, которые создаются в результате многолучевого распространения, и комбинирует их с целью формирования более сильного импульсного сигнала, который мог бы являться одной из отдельных копий. Если длительность импульсов сигналов Bluetooth очень коротка по отношению к временным интервалам между импульсами, RAKE-приемником удобнее разбирать копии.

Основные проблемы, стоящие перед технологией UWB, следующие.

- Для UWB необходимо разработать радиоустройства, работающие в чрезвычайно широком радиочастотном диапазоне; таких устройств на данный момент нет.
- Широкая полоса сигнала предполагает его цифровую обработку со скоростями, которые на данный момент еще не достигнуты.

- Что касается проблем равновесия, то алгоритмы с нужной шириной полосы также пока не разработаны.
- Технология UWB — это пока что инициатива FCC, поэтому потребуются большие усилия по стандартизации ее в глобальном масштабе.

Очевидно, технология UWB находится на переднем крае, и ей предстоит преодолеть множество проблем. Со временем, однако, если исходные принципы были правильными, она может породить беспрецедентную революцию, похожую на ту, которую совершил вышедший техникой стандарта 802.11.

## Технология FSO

Технология FSO пытается использовать преимущества оптики и лазерной техники, достигнутые в сфере волоконной оптики, для создания каналов связи ближнего действия, широкополосных, действующих на расстояниях прямой видимости, на физическом уровне типа “точка-точка” для передачи инфракрасных (ИК) сигналов непосредственно через воздух. Ожидается, что будет реализована беспроводная передача многосигнальных сигналов, но с некоторыми серьезными ограничениями, которые для них еще препятствуют ее широкому распространению и применению. Однако, в зависимости от специфических условий применения, такая технология может обеспечить решения, которые станут хорошей альтернативой беспроводному каналу стандарта 802.11.

Основные технические проблемы, стоящие перед технологией FSO, описаны ниже:

- Туман, состоящий из мельчайших капель воды, которые могут поглощать, рассеивать и отражать свет, — это главная проблема. Другие погодные условия, такие как дождь и снег, меньше влияют на качество связи, хотя сильный дождь или снежная буря также может привести кавал из строя.
- Поглощение, являющееся функцией длины волны используемого излучения, может привести к снижению мощности луча света. Поглощение часто вызывается туманом или наличием в воздухе аэрозолей, таких как пыль, морская соль или антропогенные загрязняющие вещества.
- Рассеяние, особенно когда размеры рассеивающих частиц близки к длине волны, может привести к значительному снижению интенсивности луча, поскольку энергия перенаправляется в различных направлениях случайным образом. Рассеивающими частицами могут быть капли воды тумана, стратосферной пыли или загрязняющие вещества. При увеличении длины канала потери на рассеяние возрастают.
- Физические объекты, такие как птицы, могут временно нарушить работу канала FSO.
- Показания высотных зданий могут нарушить юстировку передатчика и приемника и нарушить работу канала.
- Турбулентность, возникающая, когда нагретые объекты создают перемешивающиеся воздушные ямы различной температуры, вызывает изменяющиеся во времени изменения показателя преломления на границах этих воздушных ям. Луч может отклониться из-за случайных отражений при прохождении воздуш-

ных эм. Это может привести к мерцаниям в виде флуктуаций интенсивности и расширения луча.

К счастью для большинства FSO, две наиболее часты используемые в волоконной оптике длины волны, 850 и 1550 нм, совпадают с окнами прозрачности атмосферы.

Простой FSO передатчик состоит из спонтанно излучающего диода (СИД, LED) или лазерного источника света и телескопа, сформированного из линзы и зеркала. Приемник имеет аналогичную оптическую систему, фокусирующую энергию света на фотодетекторе. При использовании более дешевых СИД скорость передачи ограничивается сотнями мегабит в секунду, что значительно уступает возможностям лазерной. Поскольку полупроводниковые лазеры весьма малы по размерам, имеют большую мощность и широкий спектр излучения в инфракрасной области, большинство производителей FSO создает свои системы на основе именно этих компонентов. Оптическая подсистема, состоящая из зеркала и линзы, обычно занимает большую часть объема системы FSO и требует проведения процедуры очень точной и дорогой калибровки и юстировки, последняя должна сохраняться при колебаниях температуры, из-за которых линзы и зеркала расширяются и сжимаются.

Для достижения финальных радиусов действия необходимо использовать лучи с очень малой расходимостью, порядка миллиардных (мрад)<sup>1</sup>.

Если приемник находится далеко от передатчика, диаметр луча увеличивается и становится больше диаметра телескопа приемника, и результате часть переданной энергии не собирается последним, что приводит к возникновению дополнительных, "геометрических" потерь на трассе (geometric path loss). Например, как показано на рис. 9.3, при расходимости луча 2 мрад и длине канала 500 м диаметр луча составит 1 м. Однако если приемная оптика собирает энергию в круге диаметром 10 см, ею будет получено только 2% переданной энергии, что означает потери 29 дБ для энергетического потенциала линии связи. В чистом воздухе потери возрастают на 3 дБ при каждом удлинении длины канала.

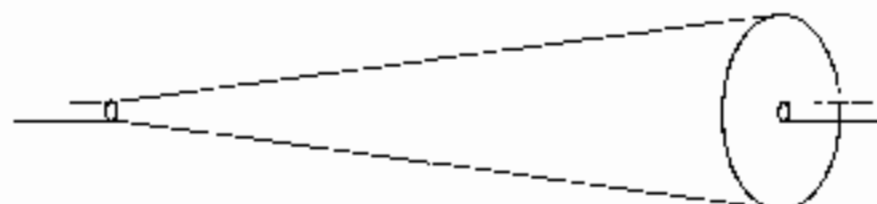


Рис. 9.3. Пример возникновения потерь на трассе, обусловленных расходимости луча

При уменьшении расходимости луча возрастают проблемы, связанные с начальной юстировкой, и канал связи становится более восприимчивым к поворачиваниям зданий, из-за чего возникают потери рассеивания луча. Для преодоления этой проблемы при использовании узких лучей приходится использовать системы автоматического слежения. Они напоминают системы автоматического сопровождения, в которых могут использоваться системы обнаружения отклонения, например линейки детекторов. В таких системах выходной сигнал обрабатывается в реальном масштабе времени и управляет карданным шарниром, с помощью которого осуществляется юстировка в вертикальной и горизонтальной плоскости.

<sup>1</sup> В оригинале — milliradian — прим. ред.

Процесс развертывания канала связи FSO может оказаться более трудоемким, чем беспроводной мостовой линии (bridge link), и основном из-за проблем, рассмотренных выше. Вы должны тщательно проанализировать карьерные места работ, сделав тщательный анализ на замирание сигнала, вызванное воздействием окружающей среды. Во время установки следует позаботиться о том, чтобы канал выглядел как подалеке от источников турбулентности, и сама установка должна быть выделена очень туго. Из-за потенциально опасного влияния на зрение следует избегать излучения мощных лазеров, особенно работающих на длине волны 850 нм, поскольку их излучение легко проникает в глаза.

Всперех всем этим предостережениям, перспектива создания каналов связи с высокой способностью передавать несколько гигабит в секунду без необходимости копать траншеи для укладки оптических кабелей делает эту технологию жизнеспособной. Для внедрения FSO нет необходимости приобретать лицензию (как и для устройств стандарта 802.11), но, в отличие от радиоканалов, они не подвержены влиянию помех. С необходимыми предостережениями и при тщательном планировании вы можете получить решение, которое будет служить вам долгие годы.

## WLAN со скоростью передачи 100 Мбит/с

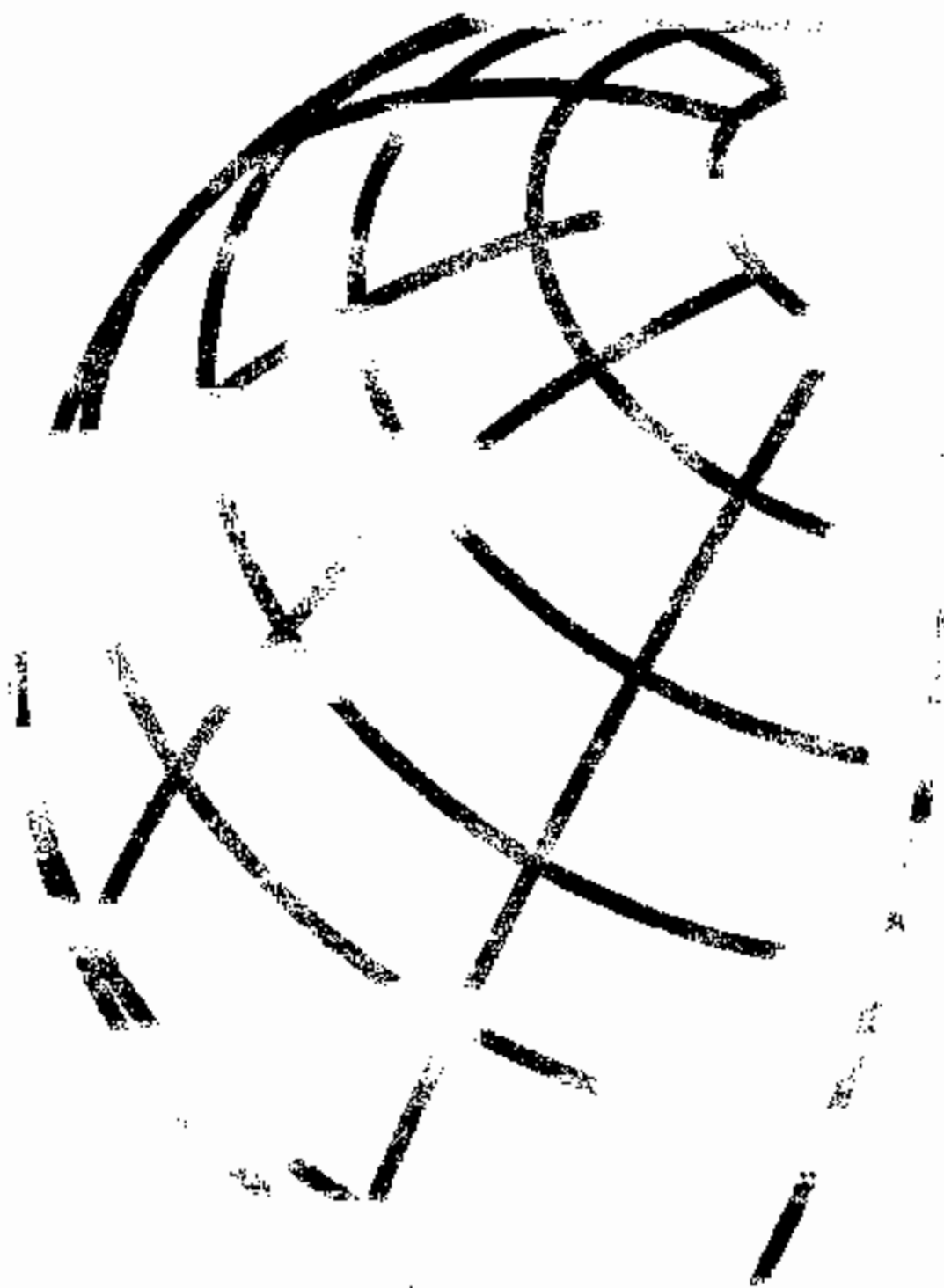
В настоящее время WLAN со скоростью передачи 100 Мбит/с предлагает несколько компаний, но, поскольку они не стандартизованы, то не могут взаимодействовать между собой. В общем случае они комбинируют два из доступных по стандарту 802.11a канала. Формируя один "новый канал", который в два раза шире стандартного. В недалеком будущем мы можем ожидать свидетелями формирования рабочей группы 802.11 по созданию технологии с более высокой пропускной способностью. Ожидается, что они будут заниматься не только внедрением достижения скорости передачи данных 100 Мбит/с, но также прилагать усилия к тому, чтобы эта скорость стала реально доступной для пользователей, — потому что это именно то, что они стремятся получить от проводных LAN. Для реализации такой возможности необходимо будет модифицировать физический уровень (PHY) стандарта 802.11 и уровень MAC стандарта 802.11. В дополнение к основным проблемам, касающимся эффективности использования спектра, расхода действия и потребляемой мощности, эта группа должна также рассмотреть вопросы совместного использования и обратной совместимости.

Что касается стимулов для развития WLAN с пропускной способностью 100 Мбит/с, то их два — это эквивалентность таких сетей с проводной Ethernet 10GBASE-T и перспектива применения беспроводной мультимедиа-технологии для домашнего использования. Первый будет действовать в пользу создания планшета беспроводного офиса, поскольку беспроводная технология будет обеспечивать такую же производительность, как и проводная. Последний будет стимулироваться желанием обеспечить передачу высококачественных аудио- и видеосигналов во все уголки дома без проводов, а также поддерживать Интернет-серфинг.

## Резюме

В этой главе мы рассмотрели три дополнительные технологии. Технология UWB, скорее всего, заменит технологию Bluetooth, поскольку реализует те же возможности, что и Bluetooth, но при значительно более высокой скорости передачи данных. Технология FSO реализует возможность создания каналов типа "точка-точка" при наличии

соответствующих условий. Она еще не получила широкого распространения, но, по-видимому, будет опережать развитие радиоканалов "точка-точка" или использоваться наряду с ними. Реальное будущее стандарта 802.11 – это стандарт на LAN со скоростью передачи 100 Мбит/с, который будет следующим существенным шагом вперед после стандартов 802.11a и 802.11g.



## Конструктивные особенности WLAN

Беспроводные LAN (WLAN) обычно рассматривают как точки доступа, которые подключаются на уровне доступа (access layer) LAN в качестве прозрачного моста, позволяющего беспроводным клиентам работать так, словно они напрямую подключены к проводной сети, но при сохранении мобильности, присущей беспроводным сетям.

Следует помнить о том, что WLAN имеют достаточно сложную структуру: точки доступа и клиенты должны работать, взаимодействуя друг с другом, дабы реализовать возможности беспроводного приложения стандарта 802.11. А это значит, что нужно основательно поработать над планом развертывания и конструктивными особенностями сети, необходимым для того, чтобы предоставить клиентам простой и масштабируемый интерфейс.

В этой главе рассматриваются особенности конструкции WLAN для наиболее часто встречающихся вариантов развертывания: розничная торговля, здравоохранение, филиалы с фиксированными работниками, образование, общественная безопасность и доступ в общественных местах.



### Сфера розничной торговли

К счастью для продавцов WLAN, одним из секторов рынка для которого WLAN является чрезвычайно перспективным, оказался розничная торговля. В будущий раз, когда вы пойдете в хозяйственный магазин, магазин электроники или универсам, обратите внимание на его стены и вывески. Вы обязательно обнаружите точки доступа или как минимум антенны, установленные в обеспеченные зоны обслуживания клиентских устройств стандарта 802.11.

Бизнес также рвется нуждается в приложениях клиент/сервер, обеспечивающих управление запасами и сеть поставщиков. WLAN обеспечивают персоналу мобильность, необходимую ему при работе в магазине для быстрой и эффективной продажи товаров с одновременным обновлением информации на серверах и в базах данных, за счет чего обеспечивается существенная экономия как средств, так и времени, а также уменьшение количества ошибок. Внедрение клиентских стандартов 802.11 способно обеспечить IP-телефонию (Voice over IP, VoIP), также принятое во всемогущими компаниями в качестве замены патентованных узкополосных систем радиодиагностики, систем диапазона 900 МГц или приема передающих радиостанции. Эти новые телефонные трубки наряду с VoIP-переговорами способны обеспечивать выполнение функций, недоступных обычным телефонным трубкам, а также поддерживать двустороннюю подвижную связь и Web приложения. Например, служащий

может начать работу, зарегистрировавшись с помощью своей трубки и через нее же получить рабочие задания. Использование в этих VoIP-трубках интерфейса “тонких клиентов”, способных обрабатывать данные, дает возможность использовать заказные приложения для решения утомительных повседневных задач. Одним из примеров является интерактивный обмен текстовыми сообщениями. Допустим, директор магазина может послать широкополосательное сообщение на все активные трубки с инструкцией одному служащему относительно выполнения какого-то конкретного задания. Все служащие получают эти сообщения, один из них подтвердит получение сообщения и отправится выполнять задание.

Магазины розничной торговли начали применять технологии WLAN задолго до датирующей стандарта 802.11 в 1997 году. Многие компании проинвестировали в беспроводные системы диапазонов 2,4 ГГц и 900 МГц в 1980-х годах и лицензируемые узкополосные системы в 1980-х, наряду с клиентскими устройствами, такими как сканеры штрих-кодов. Вполне очевидно, что большинство приложений для считывания штрих-кодов предъявляло скромные требования к полосе пропускания, поскольку потоки данных были малы и спадали в пути сходящий трафик в силу своей природы. Поэтому многие из этих ранних сетей были ориентированы на достижение максимальной зоны обслуживания, и это вполне естественно. Картирование места работы приходилось с целью минимизации общего количества точек доступа и обеспечения максимальной зоны обслуживания. В типичном большом хозяйственном магазине сейчас можно встретить три-пять точек доступа на все здание.

На сегодняшний день использование VoIP и более диверсифицированной клиентской базы (включающей ноутбуки, персональные цифровые помощники (PDA) и беспроводные принтеры) требует от инфраструктуры большей производительности. Во вновь развернутых сетях сейчас используется 10–20 точек доступа лишь для обеспечения необходимой производительности и создания зоны обслуживания для этих “распределенных” приложений.

Сети розничной торговли имеют много особенностей, отличающих их от других локальных сетей. Предприятия розничной торговли обычно имеют следующее:

- Многочисленные магазины (сотни, иногда тысячи), географически удаленные друг от друга.
- Резервированные, узкополосные соединения через глобальную сеть (WAN) с площадками, где расположены хабы, или центральными узлами.
- Небольшое количество специалистов по информационным технологиям (ИТ) или поддержке сетей, а то и полное их отсутствие в отдельных магазинах.
- Минимальная ИТ-инфраструктура в магазинах.

На рис. 10.1 показана сеть типичного предприятия розничной торговли.

Проблемы, связанные с производительностью сети и ее зоной обслуживания, преодолеваются по мере увеличения плотности размещения точек доступа, однако вместо одних проблем при планировании и развертывании сети магазины могут возникнуть новые. Магазины розничной торговли обычно имеют следующие особенности, которые менеджер сети должен учитывать при разработке WLAN.

- Основные приложения клиент/сервер выполняются локально на территории магазина.



- Остальные приложения (VoIP и обеспечивающие безопасность сети) выполняются централизованно на хостах или центральном узле.
- Решения, относящиеся к управлению, должны легко масштабироваться, т.е. обеспечивать поддержку большого числа точек доступа.

Понятно, что магазин должен продолжать работу даже в случае аварийного отключения системы. Поскольку большинство каналов WLAN перегружены, база данных, размещенная на центральном узле, может оказаться недоступной для служителей магазина в течение всего времени неработоспособности WLAN. По этой причине серверы, обеспечивающие выполнение основных приложений, обычно размещаются в самом магазине.

С целью повышения эффективности использования мобильных средств приложения VoIP обычно выполняется централизованно. Выход из строя WLAN может повлиять на работу VoIP-приложений. Для предотвращения такой проблемы многие производители предлагают режимы повышения живучести. Инфраструктура локальной сети может обнаружить утрату соединения с центральным узлом и перейти в режим автономного обеспечения живучести.

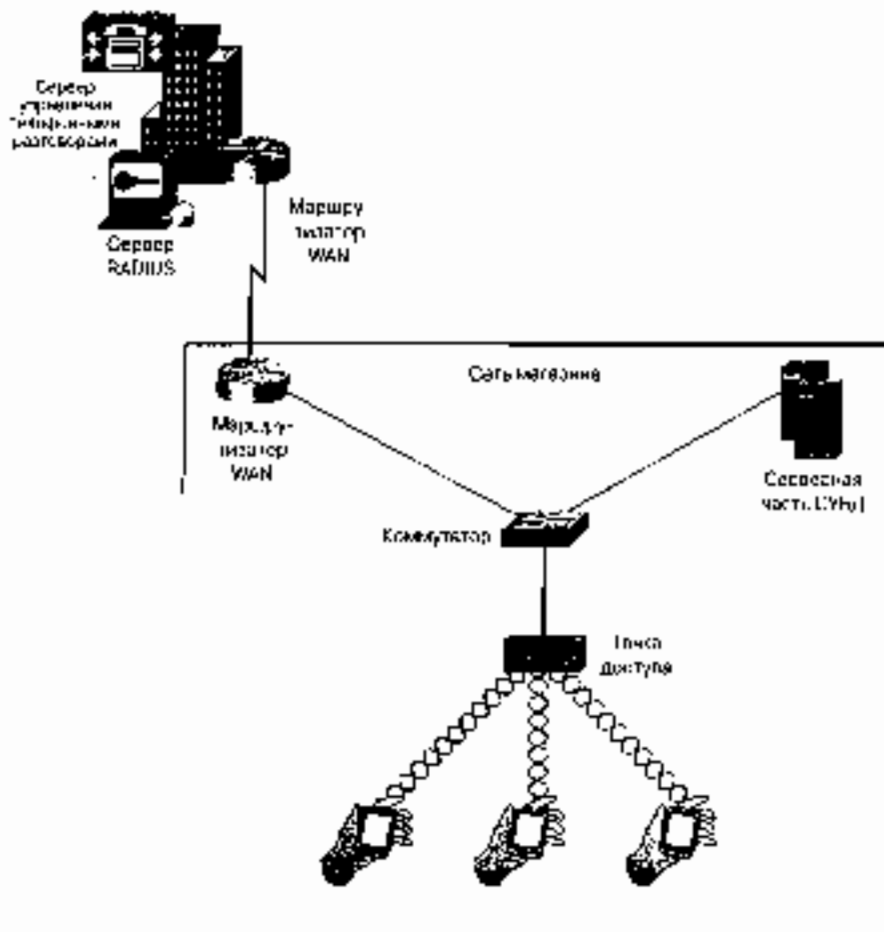


Рис. 10.1 Сеть мобильного предприятия различных торговых

Этот режим позволяет служащему предложить разговор по телефону, несмотря на выход из строя части сети (за исключением случая, когда разговор происходит через канал WAN). То же самое относится и к безопасности сетей. Новые стандарты IEEE 802.11 последней группы IEEE и спецификация на возможность взаимодействия сети (Wi-Fi Protected Access, WPA) требуют использования сервера аутентификации, авторизации и учета (AAA) для проведения аутентификации, привязанной к пользователю. Сервер RADIUS (AAA-сервер, наиболее часто используемый для обеспечения безопасности WLAN) имеет ограниченные возможности управления при децентрализованном развертывании и создает много проблем по части администрирования и синхронизации учетных записей. Многие торговые компании предпочитают децентрализованную службу, дабы минимизировать подобные ограничения. Обратной стороной такого подхода является зависимость от работоспособности канала WAN. Если канал WAN или AAA-сервер становится недоступным, беспроводные устройства не могут выполнить аутентификацию и в результате не могут получить доступ к локальным ресурсам сети магазина. В такой ситуации беспроводной сканер штрих-кодов не может получить доступ к эталонной базе данных, размещенной на сервере в магазине, поскольку он не может аутентифицироваться в беспроводной LAN.

Одним из возможных решений для обеспечения надежной работы службы IP-телефонии в магазинах розничной торговли является использование *беспроводной телефонии для розничной торговли компаниями Cisco* (Cisco Survivable Remote Site Telephony, SRST). Устройство SRST обычно применяется в маршрутизаторах филиалов и контролирует график служебных вызовов VoIP, поступающих на центральный сервер управления телефонными разговорами (Cisco Call Manager). Если центральный сервер становится недоступным из-за отказа WAN или самого сервера, устройство SRST берет на себя управление телефонными разговорами, так что телефонная беспроводная связь внутри магазина продолжает функционировать.

Компания Cisco также предлагает аналогичное решение для повышения живучести механизма аутентификации WLAN. Маршрутизаторы или коммутаторы, на которых работает программное обеспечение Cisco IOS Software с сервисом локальной аутентификации IEEE 802.1X, может оставаться активным и выполнять расширенную аутентификацию даже в том случае, если соединенные с ним рыночные AAA-сервером неработоспособны. Эти решения обеспечивают максимальную готовность WLAN выполнять свои функции и необходимые пользователям приложения при минимизации влияния на работоспособность сети канала WAN и расходов на них. На рис. 10.2 показана сеть магазина розничной торговли, усиленная функциями повышения ее живучести.

Масштабируемые системы управления сетями для адекватности обслуживания большого количества развернутых точек доступа — давняя и все еще нерешенная проблема для WLAN. Широко распространены новые инструменты управления, как правило, разработанные для проводных сетей. При широкомасштабном развертывании WLAN на предприятиях розничной торговли количество точек доступа может составлять сотни и тысячи, и все они требуют элементов управления, аналогичных таковым проводных сетей, включая управление конфигурацией и изображением, составление отчетов и анализ тенденций (configuration and image management, reporting, and trending). Эти инструменты же могут быть применены по отношению к большинству беспроводных сетей. В результате администраторы сети вынуждены сами создавать инструментарий для эффективного управления сетями магазинов. Многие производители, используя, случаем, разрозненные платформы управления, обеспечивающие возможности масштабирования, и инструментарий, необходимый для управления беспроводными сетями. Этим инструментам недостает интеграции

в платформе управления проводными сетями, необходимой для того, чтобы обеспечить цену точки доступа и управления постоянно изменяющейся сетью. Потребители со стороны розничной торговли в последнее время требуют, чтобы необходимые им инструменты предоставляли их текущий доквандж, иначе они сменят его на другое.

## Сфера здравоохранения

Степень использования беспроводных технологий в здравоохранении значительно повысилась в результате распространения устройств стандарта 802.11b и снижения цен на соответствующее оборудование. В сфере здравоохранения от WLAN ждут немедленной окупаемости инвестиций (ROI) за счет отслеживания пациентов, распределения медикаментов, сбора требований к страховым компаниям и повышения мобильности врачей и медсестер (т.е. уменьшения времени ответа пациенту и длительности цикла обработки).

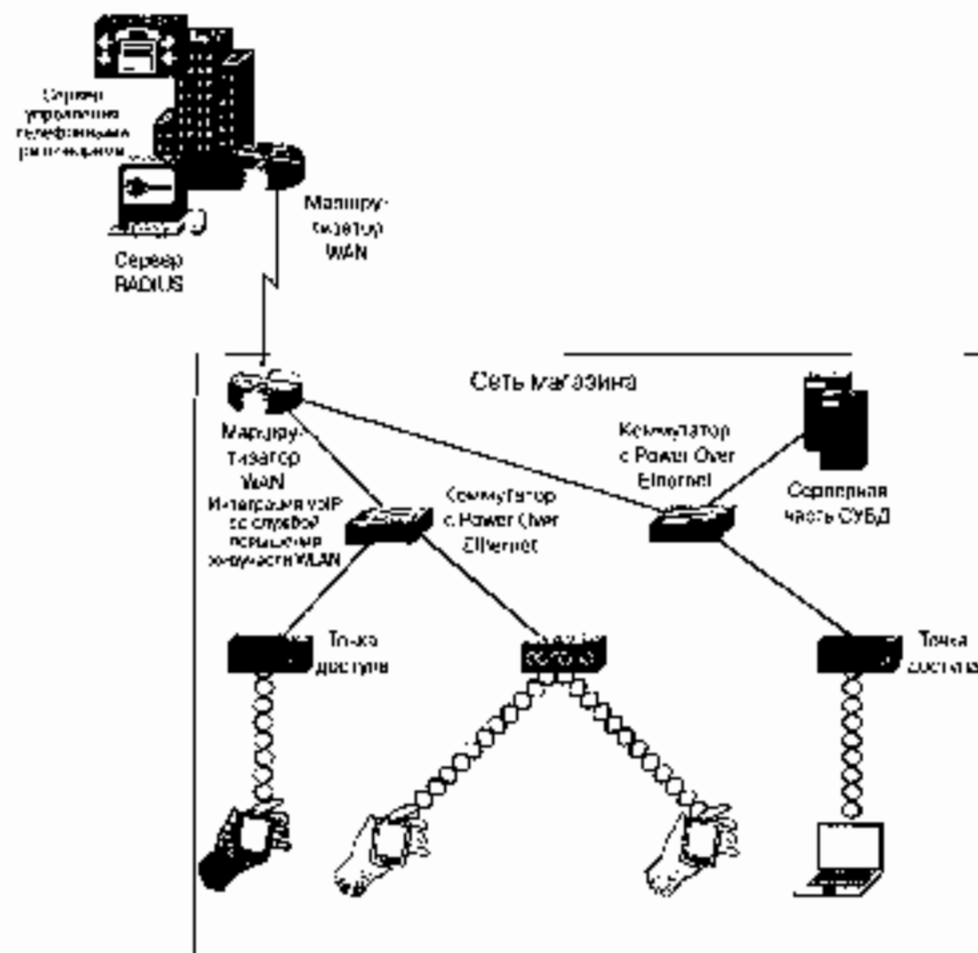


Рис. 10.2 Сеть магазина розничной торговли с механизмами размещения беспроводности

Многие компании начинают развертывать мобильные приложения на PDA, что позволяет врачам и медсестрам быстро обрабатывать формы требований к стационарным компаниям и, что более важно, делать это более точно. Этот процесс уменьшает количество требований, отвергнутых из-за присущего человеку свойства ошибаться, и снижает длительности цикла обработки платежа. Кроме того, многие производители информационных систем для здравоохранения начинают рассматривать WLAN как механизм автоматизации для распространения мобильных приложений.

В целом мобильные приложения для здравоохранения характеризуются теми же особенностями, что и приложения для розничной торговли. Это, в частности, узкополосный пульсирующий трафик. Сети развертываются обычно с ориентацией на максимальную зону обслуживания. Чтобы снизить количество точек доступа, в длинных больничных коридорах нередко используются направленные антенны, а пропускная способность антеннолюбу стандартной ненаправленной антенны "волновой канал" — 2,2 дБм.

Многие медицинские учреждения с уже развернутыми сетями сейчас рассматривают отношение к ним, стараясь оставить сети, ориентированные на максимальную зону обслуживания, выполнять еще и VoIP-приложения. За счет использования VoIP-телефонов медицинский персонал оказывается в досягаемости даже во время его перемещения, благодаря чему опять-таки снижается время реагирования на вызов и длительность цикла обработки. Ориентированные на зону обслуживания сети, существующие в настоящее время, не обеспечивают достаточную пропускную способность для передачи через WLAN трафика VoIP, поэтому сейчас нередко повторно проводят картирование мест развертывания с тем, чтобы сети обеспечивали в первую очередь IP-телефонию.

Аналогично службам VoIP, службы определения местоположения пытаются укрепиться на рынке здравоохранения, хотя большинство из существующих систем нецелесообразно не на стандарте 802.11. Когда эти системы, позволяющие определять местонахождение узла с точностью 1–2 м (от 3 до 6 футов), начнут использовать оборудование стандарта 802.11, возникнет новый рынок приложений для определения местонахождения. Эти приложения будут отслеживать местонахождение медперсонала и пациентов, быстро локализовать оборудование в случае аварий и отображать относящиеся к местонахождению данные, когда медперсонал будет находиться вблизи от пациента.

## Филиалы офисов и надомные работники

Многие из особенностей сетей, предназначенных для крупных предприятий (занимающих несколько зданий, кампус), подробно рассматривались в главе 8, "Развертывание беспроводных LAN". В данном разделе рассматриваются два других типа WLAN — для филиалов предприятий и надомных работников. Количество сетей обоих типов растет, равно как и их популярность, а некоторые из особенностей совершенно нехарактерны для сетей крупных предприятий.

## Развертывание сетей в филиалах

Как уже говорилось, кризис, парализовавший экономику США в конце 2000 года, выдвигает финансовые барьеры на пути развития предприятий. Любые расходы требуются гораздо более серьезных обоснований, чем несколько лет назад. Но технология WLAN

уже полностью сформировалась, и многие из основных барьеров на пути их внедрения (например, проблема защищенности) уже решаются. Предприятия начали применять технологию WLAN не столько на основных площадках или в штаб-квартирах, сколько для замены проводных сетей в небольших филиалах.

В филиалах многих предприятий довольно часто происходят различного рода реорганизации. Основные затраты при привлечении этих реорганизаций связаны с прокладкой кабелей категории 5 для сетей передачи данных. Специалисты по информационным технологиям считают, что при замене проводных сетей филиалов беспроводными LAN будет достигнута существенная экономия средств. Клиентские устройства стандарта 802.11 доступны для любой платформы, включая ноутбуки, PDA, принтеры и серверы, а производителями предлагается все больше моделей VoIP-телефонов. Благодаря этому специалисты по информационным технологиям имеют большой выбор устройств и способов развертывания сетей в филиалах. Беспроводная LAN является в общем смысле объединенной сетью, обеспечивая возможность работы с файлами печати, передачи речи, предоставляя доступ в Internet, и все это при относительно низких затратах.

Развертывание сетей в филиалах предприятий имеет схожие черты с развертыванием их в магазинах розничной торговли, поскольку большое количество филиалов или удаленных площадок подключается к центральному узлу через каналы WAN. Филиалы обычно предъявляют невысокие требования к инфраструктуре, как и магазины, но между ними существуют и отличия:

- Резервированные, высокоскоростные WAN-соединения с забом или центральным узлом
- Присутствие в офисе кого-то из ИТ-специалистов или персонала обслуживания сети.
- Отсутствие важных приложений, для выполнения которых были бы необходимы WLAN.

На рис. 10.3 представлен офис, в котором развернута WLAN. Обратите внимание на существенные различия между сетями офиса и магазина: резервирование WAN минимизирует требования к локальным службам (как AAA-серверам, обеспечивающим защиту WLAN, так и обеспечивающим живучесть VoIP-сервиса), и почти к каждому устройству можно получить доступ через WLAN. Это необходимо для укрепления окупаемости инвестиций, связанных с развертыванием WLAN. Помните, что на большинстве предприятий не выполняются ответственные приложения, для которых не требуется WLAN. В таких условиях WLAN является тем, что за их счет можно снизить стоимость прокладки кабелей и обеспечить мобильность.

Это -- огромное благо для производителей WLAN. Технологии WLAN зарекомендовали на своей зароде. Многие пользователи "пристрастились" к ее гибкости и обеспечиваемой ею свободе и утверждают, что без этого они теперь не могут эффективно работать. Производители ретонно отмечают, что предприятия после развертывания WLAN в филиалах будут вынуждены развернуть их и на своих основных площадках.

Весьма интересно то, что при развертывании WLAN в филиалах возникают многие из тех же проблем, которые встречаются при развертывании их в магазинах. Они связаны со службами защиты (размещение AAA-серверов), надежностью канала WAN и управлением WLAN. Многие из решений, разработанных с целью

удовлетворения потребностей сектора розничной торговли. Были применены в офисах предприятия (важно, однако, отметить, что во многих случаях живучесть WAN обеспечивается за счет его резервирования, а именно за счет резервирования аппаратуры и каналов). В филиалах предприятия обычно используются данные и приложения, размещенные в информационных центрах предприятия на центральном узле. Потери соединения через WAN-канал может вызвать приостановку выполнения операций на удаленных площадках, из-за чего и делаются инвестиции в повышение надежности WAN.

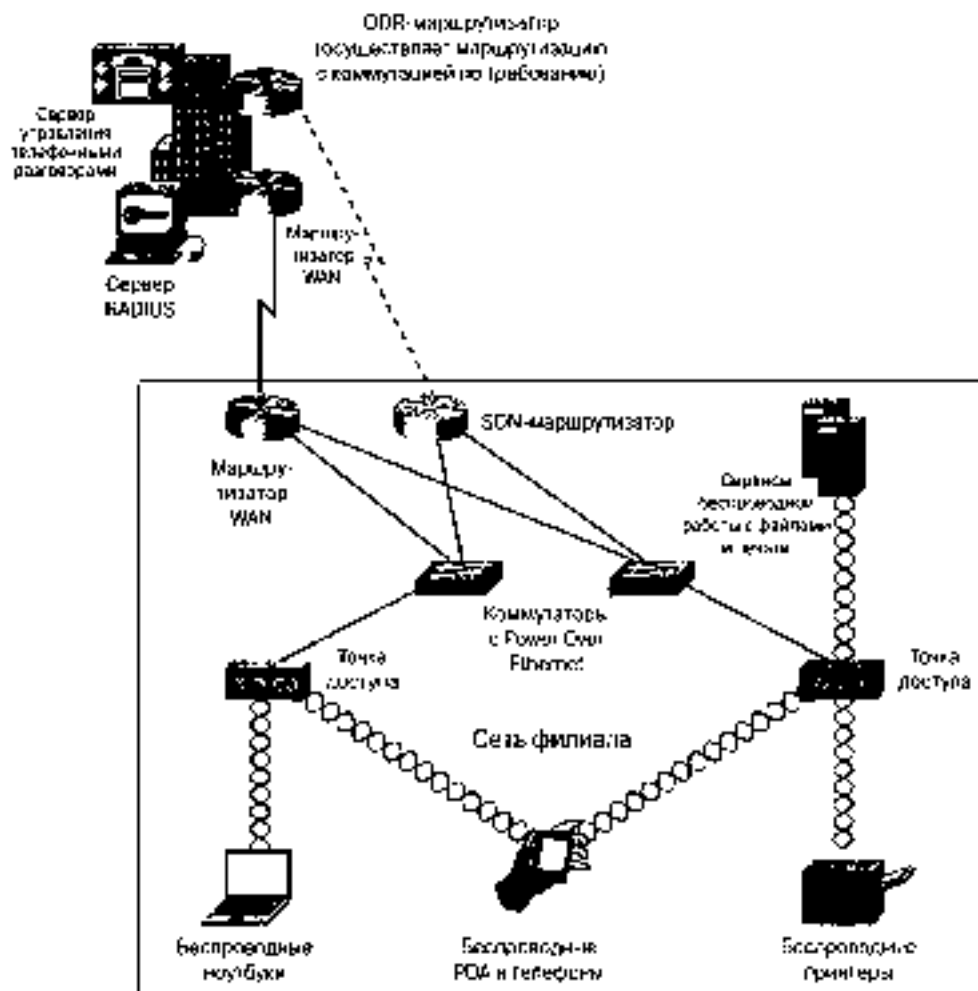


Рис. 10.3. Филиал, оборудованный беспроводной LAN

## Надомные работники

Надомные работники предприятия имеют много рентабельных механизмов для получения доступа к корпоративным ресурсам данных. Если раньше в их распоряжении были лишь дорогие каналы WAN-соединений или информационные сервисы

с коммутацией пакетов, такие как ISDN, представлявшие собой лишь обеспечивающую высокую пропускную способность надстройку над системой автоматической телефонной связи, то сегодня надомные работники могут выбирать между многими широкополосными высокоскоростными решениями. Среди таких решений можно назвать цифровую абонентскую линию (DSL), широкополосные кабельные модемы и высокоскоростные спутниковые службы, все они стоят менее 100 долларов в месяц (для США). Добавив к этим решениям оборудование рентабельной, защищенной и управляемой виртуальной частной сети (VPN), предприятия смогут обеспечить полноценный доступ надомных работников к своим информационным сетям и приложениям. На рис. 10.4 показан вариант сетевого решения для надомного работника, когда VPN через высокоскоростное широкополосное Internet-соединение получает доступ к корпоративной сети.

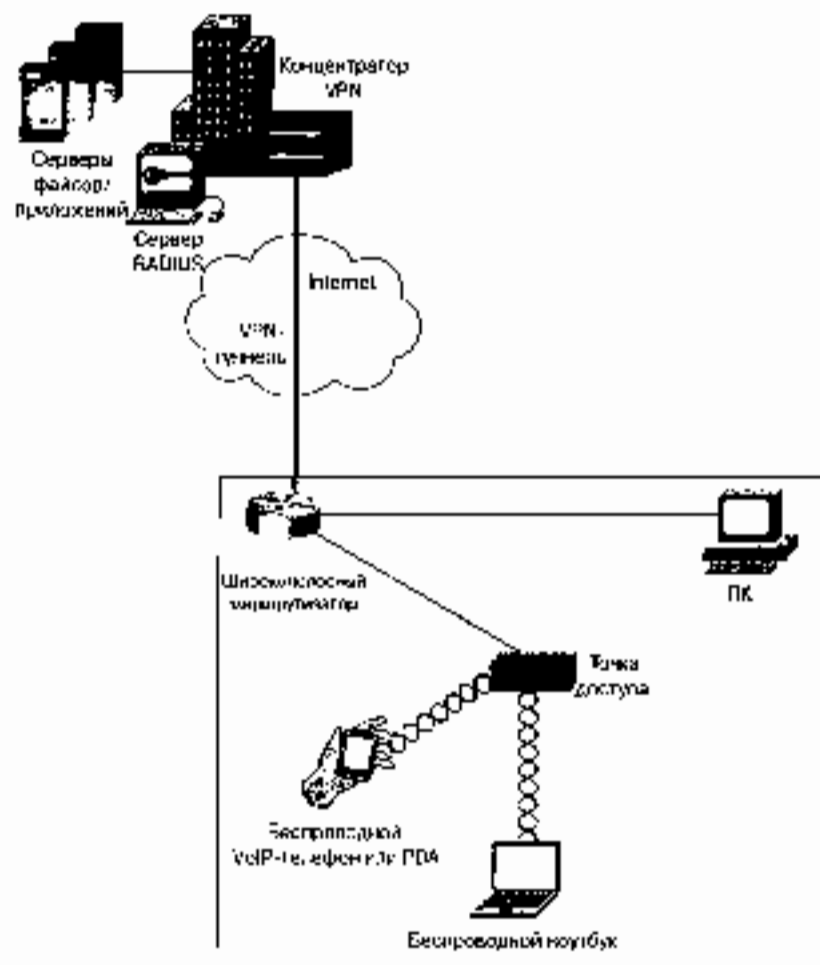


Рис. 10.4 Сеть надомного работника, использующая VPN и высокоскоростное широкополосное Internet-соединение

В некоторых случаях VPN-клиент устанавливается в ноутбуке или ПК пользователя, создавая виртуальный туннель от его машины до концентратора VPN. При такой конфигурации только одно устройство с соответствующим программным обеспечением VPN-клиента имеет доступ к сети предприятия. Можно было бы разрешить такие устройства, как IP-телефоны, в доме служащего. На рис. 10.4 показано, что широкополосный маршрутизатор действует как VPN-клиент к все устройства, расположенные за ним, способны получать доступ к корпоративной сети. Такая конфигурация позволяет администратору сети обеспечивать удаленных работников решениями, которые включают все корпоративные объединенные приложения (consolidated applications).

Хотя на рис. 10.4 представлен пример, когда пользователь имеет доступ ко всем объединенным приложениям, это потенциально опасно возникновением множества "дыр" в системе защиты. Если пользователь создает VPN-туннель, функционирующий в качестве виртуальной точки, такой как ноутбук или ПК, доступ к корпоративным ресурсам получает лишь этот конкретный пользователь или устройство. Однако, согласно сценарию, показанному на рис. 10.4, любое устройство, расположенное за широкополосным маршрутизатором, может получить доступ к корпоративной сети через VPN-туннель. По мере распространения дешевых точек доступа, предназначенных для домашнего применения, вероятность того, что незащищенная точка доступа будет подключена к такой домашней сети, резко возрастает. Если подобная точка доступа не сконфигурирована для работы в защищенном режиме, это эквивалентно тому, что незащищенная точка доступа будет работать в корпоративной сети. Хуже всего то, что администраторы сети не будут иметь никаких возможностей обнаружить такие точки доступа. Рекомендуется, чтобы отделы информационных технологий развертывали на территории корпорации механизмы обнаружения "незаконных" точек доступа и выполняли процедуры "подлинного контроля" с целью обнаружения незаконных точек доступа вручную. По отношению к удаленным работникам такие способы выявления не проходят.

Решить эту проблему позволит разрабатываемый в настоящее время стандарт 802.11i. Поскольку совместимые со стандартом 802.11i точки доступа широко распространены, отделы ИТ могут легко развернуть гибридные, которые دارند сконфигурированы и используют центральные AAA-серверы для аутентифицированного доступа. Хотя это и не соответствует исключительно пользователям персональных устройств, применение стандарта 802.11i на портах коммутатора на широкополосном маршрутизаторе могло бы удерживать их от появления такого рода. Следует учесть, что многие пользователи, включающие незаконные точки доступа к сетям, делают это не из злому умыслу, а из-за удобства получаемого сервиса. Отдел ИТ, развертывающий беспроводную сеть в доме, должен приложить огромные усилия для снижения числа незаконных точек доступа в доме.

## Сфера образования

Подобно здравоохранению и розничной торговле, в образовательных учреждениях, как и в университетах, так и в учебных заведениях первого-второго уровня, широко применяются беспроводные технологии. Институты зачастую не могут позволить себе роскошь обеспечить доступ к сети из каждого помещения, не могут они и постоянно реконфигурировать и переоборудовать свои проводные сети. Беспроводные LAN дают им возможность обеспечить повсеместное покрытие, так что они могут донести сеть



до студентов, вместо того чтобы доставлять студентов к сети. Компьютеры играют все большую роль в учебном процессе: экономия времени и ресурсов – это главное преимущество, которое дает беспроводные технологии.

Но дело не только в удобстве и экономии средств. Многие здания, в которых размещаются учебные заведения, были построены еще до компьютерной революции. В них трудно прокладывать провода к рабочим местам студентов. Беспроводные сети не имеют таких ограничений, поэтому могут быть размещены там, где еще несколько лет назад это представлялось совершенно невозможным. Экономия времени и средств, возникающая из-за отсутствия необходимости прокладывать провода, часто является компенсирующей затрат на беспроводную структуру.

При физическом развертывании беспроводной сети в условиях образовательного учреждения возникают те же проблемы, что и при развертывании ее в офисе предприятия, только здесь в роли клиентов отдельных сегментов выступают учебные аудитории. Зачастую одной обесточенной беспроводной сетью должен стать покрытый травой четырехугольный двор, окруженный зданиями и затененный студентами и преподавателями. Наиболее проблемной, с которой сталкиваются учебные заведения, является необходимость создания инфраструктуры, которая могла бы поддерживать клиентские устройства многочисленных производителей. Даже если приобретение специализированных компьютеров определенной модели планируется на университетском уровне, студенты зачастую все равно приходят со своими собственными компьютерами и, поскольку клиентские оборудование WLAN стало недорогим, используют свои собственные сетевые интерфейсные платы (NIC) беспроводного интерфейса. В учебных заведениях первого-второго уровня нередко случается так, что какая-то группа без доступа группы сетевой инфраструктуры принимает решение по закупке компьютеров. В результате этого создается ситуация, когда студентами используются клиентские устройства с различными (и зачастую разными) операционными системами и беспроводными NIC-устройствами, которые должны взаимодействовать с общей инфраструктурой.

В то время, когда писались эти строки, одновременное использование устройств многих производителей стандарта 802.11b с 40- или 125-разрядным ключом WEP (напомним, WEP – это аббревиатура, эквивалентная ключам проводных сетей) не представляло большой проблемы, поскольку Wi-Fi-сертифицированные устройства стандарта 802.11b были уже широко распространены. Со временем то же самое можно будет сказать и об устройствах стандартов 802.11a и 802.11g. Наиболее проблемной с этой точки зрения является безопасность, поскольку никогда не возникает необходимость ограничить уровень доступа для различных групп пользователей. Например, общий доступ к университетской сети может предоставляться только студентам, преподавателям и персоналу: остальные получают доступ лишь к Интернет. Даже если тех, кто имеет доступ к сети, можно осуществлять “разделение на классы”, и студенты не получают такой же уровень доступа, как профессорско-преподавательский состав.

Технология защищенного доступа к Wi-Fi (WPA) (см. главу 4. “Безопасность беспроводных LAN”) обеспечивает защищенную работу совместимого оборудования, но может оказаться не-прежнему персональной забота поддержки “унаследованных” клиентов, дожившихся еще до внедрения WPA. Если инфраструктура имеет точки доступа, поддерживающие многопользовательские виртуальные LAN (VLAN), вы можете управлять доступом различных групп пользователей, студентов и персонала в соответствии с возможностями VLAN. Аналогичным образом вы можете установить различные уровни безопасности для различных VLAN, так что индивидуумы с компьютерами, не поддержи-

важными аутентификации по стандарту 802.11X, будут все же иметь доступ к части сети. Таким образом можно обеспечить работу устаревшему клиенту не поддерживающего WPA, в операционных системах, не поддерживающих используемый нами механизм аутентификации.

Может также выясниться, что доступ к сети нужно обеспечить не временных учебных аудиториях или в удаленных точках. Вместо того чтобы прокладывать кабель или арендовать линии связи, ведущие к этим точкам, зачастую быстрее и дешевле можно развернуть беспроводные микры, чтобы соединить удаленную сеть с сетью учебного здания (см. главу 2, “Беспроводные локальные сети стандарта 802.11”).

## Доступ в общественных местах

Доступ в общественных местах обеспечивают сети, задача которых — предоставить в определенных зонах доступ к Internet через беспроводную среду широкой публички. Желание обеспечить сервис такой рван растет в отелях, кафе, аэропортах и других местах, где собирается люди. Поскольку, как правило, такие фирмы не собираются предоставлять доступ бесплатно, многие из разработок, обеспечивающих доступ в общественных местах, относятся к механизму аутентификации, который должен работать совместно с системой выписки счетов. Что касается разработок, ведущихся в Европе, то применяется прием аутентификации, основанный на применении смарт-карт с модулем идентификации абонента (Subscriber Identity Module, SIM), оказавшее ключевым решением, поскольку может быть легко осуществлено интегрируя с существующими выписками платежей сетями глобальной системы мобильной связи (GSM). Схема аутентификации должна также определить, какие службы разрешено использовать конкретному клиенту.

Вопрос выписки счетов, который сейчас превращается в самую большую проблему в сфере доступа в общественных местах, возникает из-за roaming. Под roaming в данном случае понимается использование услуг многих провайдеров при заключении абонера только с одним из них. В то время, когда писались эти строки, в большинстве случаев перемещение беспроводного устройства в другую зону обслуживания приходится приобретать эфирное время у поставщика, обеспечивающего этот сервис, хотя гораздо удобнее было бы, если бы платя за услугу включалась в домашний счет. WISPA сформировала комитет Internet провайдеров по беспроводному роумингу (IWISPr). Поскольку не существует набора стандартов, в результате работы комитета, заверше, получила несколько больше, чем просто предложения по наилучшей практике. По мере интеграции систем выписки счетов, основанных на применении SIM-карт, в схемы аутентификации стандарта 802.1X ситуация улучшится, и ожидается, что со временем соглашение относительно roaming между поставщиками услуг станут реальностью.

На рис. 16.5 представлен пример решения для обеспечения доступа в общественных местах со множественным “горячим” зон доступа (access hot spots), подключенных к одной точке присутствия провайдера Internet (point of presence, POP). Интегрированный модуль выбора служб (Service Selection Gateway, SSG) открывает экран с основным пользовательским интерфейсом, управляет процессом аутентификации и затем запрашивает тариф (и управляет им), основанный на оплаченных профилях в сервисе. На рис. 10.5 показаны интерфейс SIM-аутентификации в сети сигнальной системы 7 (signaling system 7, SS7 network), а также Internet соединение.

Что касается реального физического развертывания “горячих” зон общественного доступа, то на сегодняшний день это — самая простая часть проблемы, поскольку

здесь можно с успехом применить многие из методов, уже апробированных другими сегментами рынка. Как уже говорилось, настоящая проблема лежит в области выставления счетов и рингбэка, и именно на ней будет сфокусированы усилия тех, кто будет заниматься развитием этого сектора рынка.

Обозначение Wi-Fi ZONE, предлагаемое Альянсом Wi-Fi, говорит о том, что поставщик услуг, предоставляющий сервис доступа в общественных местах, не требует сертифицированное устройство Wi-Fi для облегчения работы пользователя. Необходимо, чтобы провайдеры Wi-Fi ZONE предлагали высококачественный сервис для потребителей и высокий уровень сервиса, который поддерживают виртуальные закрытые сети (VPN) по отношению к корпоративным сетям.

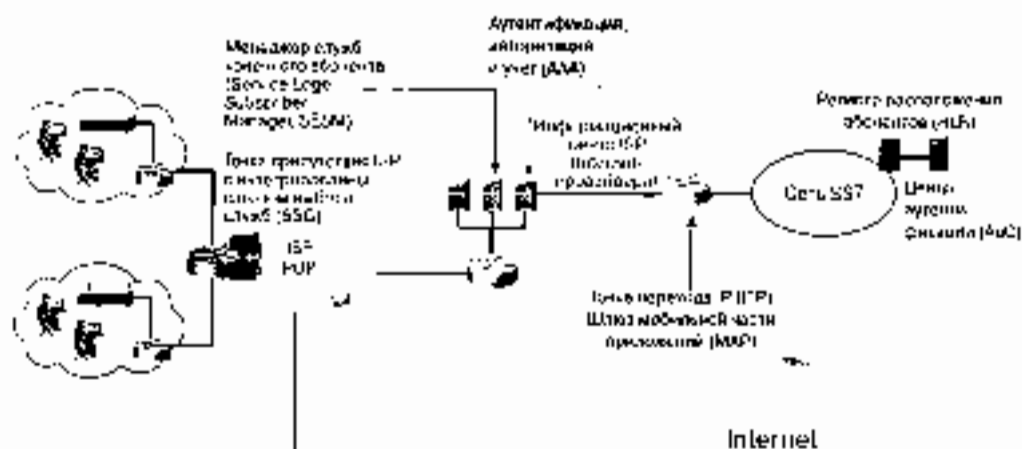


Рис. 10.5. Обзор архитектуры, обеспечивающей доступ в местах общественного пользования

## Сфера общественной безопасности

Органы государственной безопасности используют технологию мобильных радиостанций уже более 70 лет. Однако чаще всего это всего лишь службы высокоскоростной передачи данных, пригодная для передачи речи и (или) небольшого количества данных. С появлением стандарта 802.11 мы очутились на пороге информационной революции, после которой станции конечных пользователей смогут непосредственно получать речь, видео и высокоскоростные данные. В рамках пилотных программ в сфере общественной безопасности офицерам полиции были выданы PDA с беспроводными источниками сигнала стандарта 802.11, поступающих с беспроводных камер, установленных на автомобилях, патрулирующих криминальные зоны, и другие программы облегчают совместное использование информации, имеющейся в базах данных города или всей страны.

С учетом того что частоты стандарта 802.11 не требуют лицензирования, в большинстве случаев зоны обслуживания для устройств стандарта 802.11 формируются как перекрывающиеся зоны покрытия для лицензируемых решений с меньшей скоростью передачи. На рис. 10.6 показан пример с зонами обслуживания устройствами стандарта 802.11 в центральном деловом районе города и областью покрытия низко-

скоростными мобильными радиостанциями в определенной части республ. В сельском хозяйственных районах, при кооперативном использовании спектра частот, более приемлемым может оказаться расширение зоны покрытия службами общественной безопасности, деловыми крутами и провайдерами, обеспечивающими доступ в местах общественного пользования за счет виртуальных LAN. В зависимости от того, необходимо ли соединить множество мобильных сетей или просто предоставить клиентский доступ, можно использовать или беспроводные мосты, или точки доступа. Очевидно, главным является то, что будут использоваться адекватные меры в виде аутентификации и шифрования для защиты информации, касающейся общественной безопасности, или в виде механизмов защиты данных модификация стандарта 802.11, или механизмов VPN.

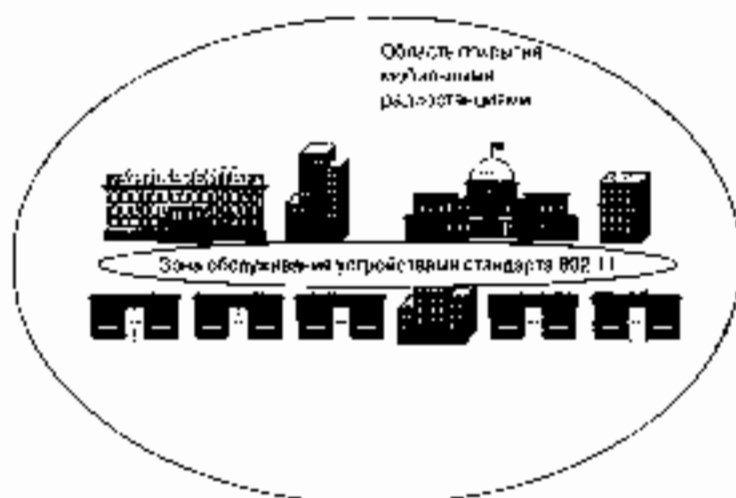


Рис. 10.6. Область покрытия для устройств стандарта 802.11 в сфере общественной безопасности

На рис. 10.7 показан пример сети, в которой применяются беспроводные мосты для соединения машин государственной безопасности с муниципальной сетью, с источниками видеосигнала, когда обеспечивается покрытие "горячей" зоны вокруг автомобиля для ручных устройств (защита обеспечивается с помощью VPN).

Каким образом, устройства стандарта 802.11 могут служить связующим к существующим технологиям мобильной радиосвязи в сфере общественной безопасности, они облегчают совместное использование информации способами, невозможными еще в недавнем прошлом. Из-за отсутствия защиты от помех они не годятся для повсеместного применения, но хороши в качестве добавочной технологии. При правильном применении они могут предоставить удобные и простые в использовании и установке решения.

## Резюме

В данной главе кратко рассматриваются и применяются WLAN в таких различных сферах, как здравоохранение, образование и общественная безопасность. Беспроводные LAN делают доступными пользователям эффективные и новейшие приложения, которые раньше

он выполнять не мог. В данной главе описаны проблемы, которые могут встретиться в каждой из перечисленных сфер применения, такие как связанные с возможностью взаимодействия клиентских устройств разных производителей, и потенциальные решения, такие как использование VLAN для сегментации классов пользователей.

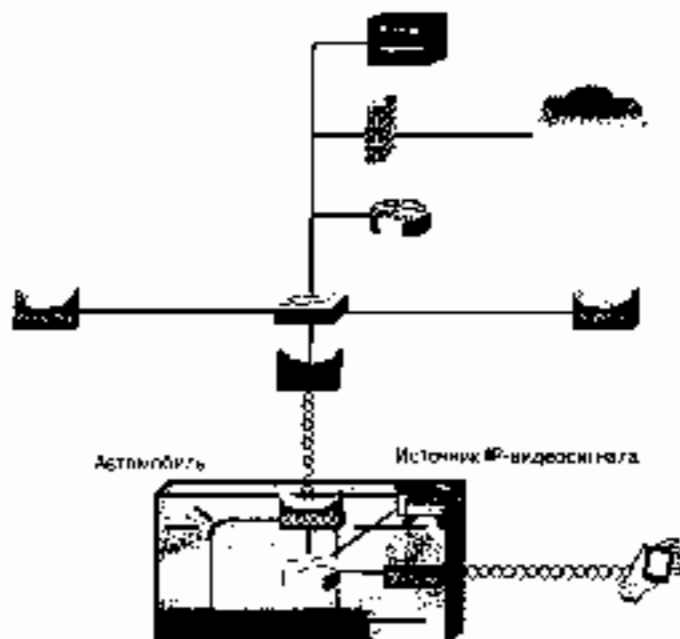


Рис. 10.7 Пример сети в сфере общественной безопасности



## Словарь терминов

---

**3DES (Triple Data Encryption Standard).** Стандарт де-факто безопасности IP-сетей (IP Security, IPSec) и шифрования для виртуальных частных сетей (virtual private network, VPN).

**10BASE2.** Разновидность Ethernet, в которой используется тонкий, RG-58 или RG-59, коаксиальный кабель. Сегмент кабеля 10BASE2 может иметь длину до 185 м.

**10BASE5.** Разновидность Ethernet, в которой используется толстый коаксиальный кабель; максимально допустимая длина каждого сегмента составляет 485 м.

**10BASE-FL.** Разновидность Ethernet, в которой используется оптический кабель на основе многоволоконного волокна. Каждый канал 10BASE-FL может иметь длину до 2 км.

**10BASE-T.** Разновидность Ethernet, в которой используются кабели категории 3 или 5 на основе неэкранированной витой пары (UTP). Каждый сегмент 10BASE-T может иметь длину до 100 м.

**100BASE-CX.** Разновидность Gigabit Ethernet, в которой сигнал передается по кабелю, выполненному на основе экранированной витой пары (STP). Каждый сегмент 100BASE-CX может иметь длину не более 25 м.

**100BASE-FX.** Разновидность Fast Ethernet, в которой используется кабель на основе многомодового оптического волокна. Сегмент 100BASE-FX может иметь длину до 400 м при работе в плуромодовом режиме и до 2 км — в бимодовом режиме.

**100BASE-LX.** Разновидность Gigabit Ethernet, в которой применяется оптический кабель, выполненный на основе одномодового волокна. Каждый сегмент 100BASE-LX может иметь длину до 5 км.

**100BASE-TX.** Разновидность Fast Ethernet, в которой используется кабель категории 5, выполненный на основе неэкранированной витой пары (UTP). Сегмент 100BASE-TX может иметь длину не более 100 м.

**100BASE-X.** Общий термин, используемый для обозначения Fast Ethernet разновидностей 100BASE-TX и 100BASE-FX.

**802.1X.** Стандарт IEEE для сетей стандарта 802, в которых выполняется ориентированная на порты аутентификация на уровне 2.

**802.3.** Стандарт IEEE на проводную Ethernet. Эта спецификация относится к используемым в настоящее время Ethernet, Fast Ethernet и Gigabit Ethernet.

**802.5.** Стандарт IEEE на сети с топологией Token Ring.

**802.11.** Стандарт IEEE на беспроводные, совместимые с Ethernet локальные сети (WLAN).

**802.11i**. Стандарт IEEE на базе стандарта 802.11 с защитой на канальном уровне.

**802.11e**. Стандарт IEEE на базе стандарта 802.11 с качеством обслуживания (QoS), обеспечиваемом на канальном уровне.

**802.11 slot time**. Значение времени, зависящее от характеристик физического уровня (PHY), представляющего собой радиочастотный (RF) канал базовой зоны обслуживания (BSS).

**1000BASE-SX**. Разновидность Gigabit Ethernet, в которой используется оптический кабель на основе мультимодовых волокон. Каждый сегмент 1000BASE-SX может иметь максимальную длину 320 м.

**1000BASE-T**. Разновидность Gigabit Ethernet, в которой используется кабель категории 5, функционирующий на основе скрученных витых пар (UTP). Каждый сегмент 1000BASE-T может иметь длину не более 100 м.

## A

**AAA server**. Сервер, выполняющий функции аутентификации, авторизации и учета.

**AC (access category, категория доступа)**. Очередность передачи для устройств, поддерживающих QoS по стандарту 802.11e.

**Access layer (уровень доступа)**. Термин, используемый при проектировании сетей для обозначения края сети. В LAN уровень доступа обеспечивает подключение к сети конечных станций.

**Acknowledgment frame (фрейм подтверждения)**. Станция, получившая какой-нибудь фрейм, передает спящему ей станции подтверждение этой фрейма.

**Active scanning (активное сканирование)**. Клиент активно ищет точку доступа (AP). Этот процесс обычно включает отправку клиентом зашифрованного запроса по каждому из сконфигурированных на нем каналов и ожидание ответа на зашифрованный запрос от точек доступа.

**AES (Advanced Encryption Standard, усовершенствованный стандарт шифрования)**. Новый стандарт на алгоритм шифрования, предложенный Национальным институтом стандартов и технологий (NIST). AES основан на алгоритме шифрования Рундзель (Rijndael).

**AES-CCM**. Вариант AES, используемый в стандарте 802.11i.

**AID (association Identifier, идентификатор ассоциации)**. Логический порт точки доступа, выделенный для беспроводной станции.

**AIFS (arbitration interframe space, арбитражный межфреймовый промежуток)**. Межфреймовые промежутки переменной длительности, зависящей от приоритета категории доступа (AC).

**Antenna (антенна)**. Часть радиотракта, назначение которой — передавать или принимать электромагнитную энергию.

**AP (access point, точка доступа)**. Центральная точка связи для всех станций в BSS.

**Auto negotiation (автоматическое согласование)**. Позволяет станции и устройству Ethernet которые могут поддерживать один или несколько вариантов Ethernet, таких



как 10BASE-T, 100BASE-TX или 1000BASE-T) автоматически синхронизировать скорость передачи и дуплексный режим.

**Authentication server** (сервер аутентификации). AAA-сервер, выполняющий аутентификацию по стандарту 802.1X или расширяемому протоколу аутентификации (EAP)

**Authenticator** (аутентификатор). Объект, к которому обращается проситель, желающий установить защищенное соединение.

## **В**

**Beacon frame** (сигнальный (или маячковый) фрейм). Служебный фрейм стандарта 802.11, используемый точкой доступа для периодического оповещения BSS о наличии точки доступа и ее параметрах.

**Bluetooth**. Беспроводная технология, разработанная для создания персональных сетей и обеспечивающая радиус действия

**Block cipher** (блочный шифр). Шифр, который преобразует каждый блок (кус текста) фиксированного размера. В ходе операции шифрования незашифрованный текст должен быть фрагментирован для получения блоков определенного размера

**Bridge** (мост). Устройство сети Ethernet, которое физически разделяет два коллизийных домена Ethernet.

**Broadcast domain** (широковещательный домен). Внутренняя сеть устройств, способных посылать друг другу широковещательные фреймы и получать их одно от другого.

**Broadcast frame** (широковещательный фрейм). Один фрейм, адресованный всем станциям широковещательного домена.

**BSS (basic service set, базовая зона обслуживания)**. Группа станций стандарта 802.11, связывающихся одна с другой через точку доступа.

## **С**

**CCK (complementary code keying, последовательность дополнительных кодов)**. Метод расширения физического уровня, используемый в устройствах стандарта 802.11b для достижения скорости передачи 5,5 and 11 Мбит/с

**CFP (contention-free period, период, свободный от конкуренции)**. Период времени, в который для доступа к среде передачи необходим опрос, выполняемый точкой выполнения функции координации (point coordination function, PCF) или гибридной функцией координации (HCF).

**CoA (care of address, адрес для передачи)**. Устройство, получающее пакеты, отправленные внутренним агентом (HA) и адресованные мобильному узлу (MN). Этот CoA должен существовать на самом MN или на внешнем агенте (FA).

**Cochannel overlap** (внутриканальное перекрытие). Перекрытие двух BSS, которые занимают один и тот же канал

**Collision** (коллизия). Результат одновременной передачи двух фреймов в одном коллизийном домене.

**Collision domain** (коллизийный домен). Сеть, состоящая из устройств Ethernet, которые конкурируют за доступ к одной и той же среде передачи.

**Contention period** (период конкуренции). Промежуток времени, в течение которого станции, выполняющие распределенную функцию координации, конкурируют между собой за доступ к среде.

**Core layer** (базовый уровень). Термин, используемый при разработке сетей, обозначает нижестоящий уровень сети. Задачи базового уровня — как можно быстрее пересылать пакеты между маршрутизаторами и коммутаторами.

**CSMA/CA** (carrier sense multiple access with collision avoidance, множественный доступ с контролем несущей и предотвращением коллизий). Основной способ доступа к среде в сетях стандарта 802.11.

**CSMA/CD** (carrier sense multiple access with collision detection, множественный доступ с контролем несущей и обнаружением коллизий). Основной способ доступа к среде в сетях Ethernet.

**CW** (contention window, окно конкуренции). Период времени, когда среда стандарта 802.11 не занята.

## D

**DAC** (distributed admission control, распределенное управление входом). Механизм распределенного распределенного управления входом, при использовании которого станции определяют, должны ли они осуществлять передачу, принимаясь на избыточные, передаваемые точкой доступа.

**Data link layer** (канальный уровень). Второй уровень модели взаимодействия открытых систем (OSI). Состоит из двух подуровней: подуровня канального уровня (data link sublayer) и подуровня логического канала (logical link sublayer).

**Data link sublayer** (подуровень канального уровня, называется также MAC-уровнем). Особенности этого подуровня определяются топологией сети. Например, сети Token Ring стандарта 802.5 имеют MAC-уровень, отличный от такового сетей стандарта 802.11.

**dBi**. Единица измерения коэффициента усиления антенны по отношению к таковому изотропной антенны.

**dBm**. Единица измерения мощности по отношению к 1 мВт.

**DCF** (distributed coordination function, распределенная функция координации). Работа беспроводных LAN стандарта 802.11 в режиме CSMA/CA. DCF — основной механизм доступа, необходимый для всех устройств стандарта 802.11.

**DIFS** (DCF interframe space, межфреймовый промежуток DCF). Количество времени, прошедшее после того, как среда становится доступной, в течение которого станция должна ждать, прежде чем начать доступ к среде по процедуре DCF. Интервал DIFS равен сумме короткого межфреймового промежутка (SIFS) и двух канальных интервалов (slot times).

**Directivity** (направленность). Описывает интенсивность излучения, распространяющегося от антенны.

**Distribution layer** (уровень распределения). Термин, используемый при проектировании сетей, указывает уровень сети, на котором сеть сегментируется на отдель-

ные широкополосные домены уровня 2 с помощью маршрутизаторов или коммутаторов уровня 3. Сетевые службы, такие как списки управления доступом (access control lists, ACL), фильтрация маршрута и трансляция сетевых адресов (NAT), применяются на уровне распределения.

**DQPSK (differential quadrature phase shift keying, относительная фазовая манипуляция с квадратурными (фазовыми) сигналами).** Механизм кодирования символов, используемый при работе станции стандарта 802.11 со скоростью 2 Мбит/с

**DSSS (direct sequence spread spectrum, расширение спектра методом прямой последовательности).** Метод модуляции, используемый в сетях стандарта 802.11.

**Duplex (дуплексный).** Термин, обозначающий возможность одновременно передавать и принимать данные включенными к сети устройствами (см. full duplex) или невозможность делать это (см. half duplex).

## Е

**EAP (Extensible Authentication Protocol, расширяемый протокол аутентификации).** Протокол соединения "точка-точка" (PPP), лежащий в основе механизма аутентификации.

**EAP-MD5 (Message Digest 5, дайжест 5 EAP-сообщения).** Тип аутентификации EAP, основанный на использовании протокола аутентификации с предварительным согласованием вызова (CHAP)

**EAP-TLS (Transport Layer Security, расширяемый протокол аутентификации ... защита на транспортном уровне).** Тип аутентификации EAP, основанный на TLS-аутентификации. Цифровые сертификаты используются для взаимной аутентификации на стороне клиента и стороне сервера

**ECB (electronic code book, книга электронных кодов).** Режим шифрования, при использовании которого из одного зашифрованного текста всегда получается тот же зашифрованный текст.

**EDCF (Enhanced DCF, расширенный DCF).** Регламентируемый стандартом 802.11e метод доступа к среде и приоритезации трафика на основе конкуренции

**EIRP (effective isotropic radiated power, эффективная изотропно-излучаемая мощность).** Реальная мощность, получаемая антенной

**ESS (extended service set, расширенная зона обслуживания).** Несколько базовых зон обслуживания (BSS), которые связываются одна с другой через распределительную систему (distribution system), обычно это мост принципов Ethernet в точке доступа.

**Ethernet.** Стандарт IEEE 802.3, регламентирующий работу проводной сети со скоростью передачи 10 Мбит/с. Другими высокоскоростными вариантами Ethernet являются Fast Ethernet и Gigabit Ethernet.

**Ethernet slot time (критичный интервал Ethernet).** Время, которое необходимо фрейму Ethernet для преодоления диаметра сети.

**Ethertype (тип фрейма Ethernet).** Данные, содержащиеся в поле полезной нагрузки MAC-фрейма.

## Ф

**FA (foreign agent, внешний агент).** Агент на маршрутизаторах или коммутаторах уровня 3, который докогает MN в определении, куда он переместился, и в получении пакетов от внутреннего агента (НА).

**Fading (фэдинг, затухание сигнала)** Проявление, когда уровень мощности сигнала падает под воздействием различных внешних факторов.

**Fast Ethernet.** Стандарт IEEE 802.3u для сетей, в которых информация передается со скоростью 100 Мбит/с.

**FCS (frame check sequence, контрольная последовательность фрейма).** Поле в MAC-фреймах, используемое для определения того, не произошла ли ошибка во время передачи. Значение FCS вычисляется и вставляется во фрейм передающей станцией. Принимающая станция заново вычисляет значение FCS и сравнивает его с аналогичным значением, указанным во фрейме. Если эти значения совпадают, считается, что фрейм получен без ошибок.

**FDD (frequency division duplex, дуплексная связь с частотным разделением).** Дуплексный метод передачи, при использовании которого для передачи информации в каждом направлении применяется своя частота.

**FDDI (fiber distributed data interface, распределенный интерфейс передачи данных по волоконно-оптическим каналам)** Стандарт ANSI X3T9.5, регламентирующий передачу со скоростью 100 Мбит/с. FDDI использует топологию, аналогичную Token Ring, с волоконно-оптическими кабелями.

**FHSS (frequency hopped spread spectrum, расширение спектра путем скачкиобразного переключения частоты).** Метод модуляции с переключением передачи с одного канала на другой.

**FSK (frequency shift keying, частотная манипуляция).** Метод модуляции, при котором для передачи нулей и единиц используются сигналы двух разных частот.

**Full duplex (полнодуплексный).** Топология сети, при которой станции могут передавать и принимать данные одновременно.

## Г

**Gigabit Ethernet.** Стандарты IEEE 802.3z и 802.3ab, регламентирующие работу сети со скоростью передачи 1000 Мбит/с.

**GMK (group master key, групповой мастер-ключ).** Мастер-ключ, используемый при шифровании широковещательных и многоадресных фреймов, обеспечивающий шифрование и проверку целостности сообщений.

**GSM (global system mobile, глобальная система мобильной связи).** Общепринятый стандарт сотовой связи.

**GTK (group transient key, групповой переходный ключ).** Ключ канального уровня, используемый для шифрования широковещательных и многоадресных фреймов GTK выводится из группового мастер-ключа (GMK).

## Н

**NA (home agent, внутренний агент).** Агент на маршрутизаторах или коммутаторах уровня 3, обеспечивающий получение перемещающимся MN его IP-пакетов.

**Half duplex (полудуплексный).** Топология сети, при которой станции в каждый из моментов времени могут или передать, или принимать данные.

**HCF (hybrid coordination function, гибридная функция координации).** Опциональная функция механизма доступа к среде по результатам запроса (стандарт 802.11e).

**Hidden node (скрытый узел).** Когда две станции находятся вне радиуса действия каждой из них, но в пределах радиуса действия точки доступа, говорят, что эти станции скрыты одна от другой.

**Hub (хаб).** Устройство полудуплексной Ethernet со многими портами. Хаб позволяет передать один сигнал Ethernet сразу со многих портов.

## I

**IAPP (Interaccess Point Protocol, протокол обмена служебной информацией между точками доступа).** Протокол, используемый точками доступа для связи между собой.

**IBSS (independent basic service set, независимая базовая зона обслуживания).** Группы станций стандарта 802.11, напрямую связывающихся между собой. IBSS также называют спонтанными, или независимыми (ad hoc), сетями, поскольку она представляет собой одноранговую WLAN.

**ICV (integrity check value, контрольный признак целостности).** Слабая функция контроля целостности сообщения (MIC), определенная в стандарте 802.11. ICV использует CRC-32 для обеспечения целостности сообщений во фреймах стандарта 802.11.

**IGMP (Internet group management protocol, протокол межсетевых управляющих сообщений-протокол обнаружения маршрутизатора).** Протокол, используемый внешними и внутренними агентами для рассылки оповещений (agent advertisements)

**Isotropic antenna (изотропная антенна).** Идеальная антенна без потерь, коэффициент усиления которой одинаков для всех направлений.

**IV (initialization vector, вектор инициализации).** Числовое значение, которое связывается с ключом для генерации ключевого потока во избежание того, чтобы один и тот же ключ генерировал один и тот же поток.

## L

**LEAP.** Разработанный компанией Cisco тип аутентификации EAP, основанной на аутентификации Microsoft CHAP (MS-CHAP).

**Logical link sublayer (подуровень логического канала).** Будучи стандартом для всех разновидностей сетей семейства 802, этот подуровень содержит простой протокол передачи фреймов, который обеспечивает доставку фреймов без установления соединений.

## М

**MIC (message integrity check, контроль целостности сообщения).** Гарантирует получателю фрейма, что фрейм направлен именно получателем (а не злоумышленником) и не был подменен по пути передачи.

**MN (mobile node, мобильный узел).** Перемещающаяся станция, на которой сконфигурирован мобильный IP-протокол.

**Mobile IP (мобильный IP).** Протокол, позволяющий мобильному узлу сохранять статический IP-адрес при перемещении его в пределах VLAN.

**Multicast frame (многоадресный фрейм).** Единственный фрейм, адресованный сразу многим станциям широковещательного домена.

**Multipath (многолучевое распространение).** Возникает, когда многие экземпляры переданного сигнала достигают приемника, распространяясь по различным путям.

**Mutual authentication (взаимная аутентификация).** Аутентификация, в процессе которой не только сеть аутентифицирует клиента, но и клиент аутентифицирует сеть. Проведения именно такой аутентификации требует стандарт 802.11i.

## Н

**NAV (network allocation vector, вектор распределения сети).** Виртуальная функция слуховой станции (virtual carrier-sense function) стандарта 802.11. NAV – это таймер, имеющийся на каждой станции, значение которого обнуляется фреймами данных, передаваемыми через среду. Станция, желающая начать передачу, должна иметь NAV, равный 0, прежде чем она начнет выполнять DCF-операции.

**Network diameter (диаметр сети).** Расстояние между Ethernet-станциями, находящимися на противоположных концах широковещательного домена.

**Nonce (от nonce – спец. временное число).** Число, которое используется только один раз, в основном в криптографии, например при аутентификации и шифровании.

## О

**OFDM (orthogonal frequency-division multiplexing, мультиплексирование с разделением по ортогональным частотам).** Метод модуляции, используемый для обеспечения высокой скорости передачи данных по стандартам 802.11a и 802.11g.

**Open authentication (открытая аутентификация).** Тип аутентификации, регламентируемый стандартом 802.11. Открытая аутентификация является аутентификацией нулевого типа, когда доступ гарантируется каждой станции.

## Р

**Passive scanning (пассивное сканирование).** Сканирование, при котором клиент не передает никакие фреймы, а лишь получает сигнальные фреймы по каждому каналу. Клиент продолжает переходить с канала на канал через определенный промежуток времени, но не посылает зондирующие кадры.

**PBCC (packet binary evolutionary coding, двоичное пакетное эволюционное кодирование)**. Опциональный метод кодирования, используемый в устройствах стандарта 802.11b.

**PCF (point coordination function, точечная функция координации)**. Режим доступа в BSS стандарта 802.11, при котором точка доступа (или точка-координатор) опрашивает PCF-опрашиваемые станции на предмет передачи ими данных.

**PEAP (Protected EAP, защищенный EAP)**. Тип аутентификации 802.1X, при которой на стороне сервера используется цифровой сертификат, а на стороне клиента place ставляется аутентификация по стандарту 802.1X другого типа, такая как EAP-MD5.

**PIFS (PCF interframe space, преимущественный межфреймовый интервал)**. Промежуток времени между моментам, когда среда становится доступной, но станция должна ожидать начала доступа к среде по алгоритму PCF. Интервал PIFS равен SIFS плюс один канальный интервал.

**PMK (pairwise master key, парный мастер-ключ)**. В сетях стандарта 802.11i PMK — это динамический ключ, генерируемый в ходе аутентификации по стандарту 802.1X.

**PTK (pairwise transient key, парный переходный ключ)**. Ключ, используемый при шифровании на канальном уровне в сетях стандарта 802.11i.

## R

**Radio (радиостанция)**. Устройство связи, используемое для передачи электромагнитных или через эфир.

**RADIUS server (сервер RADIUS)**. Специальная разновидность AAA-сервера.

**RC4 (Rivest Cipher 4)**. Криптографическая машина, используемая при WEP-шифровании.

**Receiver sensitivity (чувствительность приемника)**. Минимальный уровень сигнала приемника, при котором он способен декодировать принятый сигнал.

**Repeater (повторитель)**. Устройство, используемое в полудуплексной Ethernet. Повторитель воспроизводит Ethernet-сигнал с целью увеличения диаметра сети при заданной топологии Ethernet. Например, повторитель можно использовать для увеличения расстояния, на которое передается сигнал в сети 10BASE-T, со 100 до 200 м.

**Roaming domain (домейн роуминга)**. Точки доступа, которые находятся в одном широковещательном домене и сконфигурированы с одним и тем же идентификатором зоны обслуживания (SSID).

## S

**Shared Key authentication (аутентификация с совместно используемым ключом)**. Аутентификация подражатель/подражаемый, включенная в стандарт 802.11, при которой WEP-ключ является совместно используемым секретным ключом.

**SIFS (short interframe space, короткий межфреймовый промежуток)**. Наименьший период времени, в течение которого станция ожидает, прежде чем попытается получить доступ к среде. Обычно SIFS используется при передаче служебных фреймов. Напри-

мер, после того как станция получает фрейм данных, она выжидает в течение промежутка SIFS и затем посылает фрейм подтверждения.

**Spectral efficiency** (эффективность использования спектра). Эффективность использования частотного канала. Измеряется количеством битов, которые могут быть переданы в данном частотном диапазоне, или шириной спектра, которая используется для передачи заданного количества информации.

**SSID (service set identifier, идентификатор зоны обслуживания)**. Логическое группирование устройств стандарта 802.11.

**Stream cipher** (поточный шифр). Шифр, который генерирует ключевой поток для шифрования в соответствии с размером незашифрованного текста или незашифрованного фрейма данных.

**Supplicant** (присутитель). Устройство, которое пытается получить доступ к LAN, используя механизм аутентификации стандарта 802.1X.

**Switch** (коммутатор). Многопортовый Ethernet-мост, который обычно использует электронные схемы для повышения скорости коммутации фреймов Ethernet между коллизийными доменами.

## T

**TC (traffic class, класс трафика)**. Восемь различных классов трафика определены в стандарте 802.11e.

**TDD (time division duplex, дуплексная связь с временным разделением каналов)**. Схема модуляции, в которой используются различные промежутки времени для передачи информации в каждом из направлений.

**TKIP (temporal key integrity protocol, временный протокол целостности ключа)**. Алгоритм шифрования и контроля целостности сообщения, введенный в стандарте 802.11i, в котором используются пофреймовые ключи и облегченная проверка целостности для преодоления слабостей функций WEP и TKV стандарта 802.11.

**Token Ring**. Технология типа "кольцо" с predetermined, не основанным на конкуренции доступом к среде. Типичные скорости передачи данных — 4 и 16 Мбит/с.

**TXOP (transmission opportunity, благоприятная возможность для передачи)**. Момент времени, когда станция может начать передавать фреймы в течение определенного интервала времени. Механизм TXOP может обеспечить передачу сразу многих фреймов/подтверждений их получения; они могут передаваться, пока не истечет интервал TXOP.

## U

**Ultra-wide band (сверхширокополосный)**. Новая технология, которая обеспечивает очень высокую скорость передачи данных за счет использования очень коротких импульсов малой мощности.

**Unicast frame (одноадресный фрейм)**. Один фрейм, предназначенный для конкретной станции широковещательного домена.



## V

**VLAN** (virtual LAN, виртуальная LAN). Широковещательный домен.

**VSWR** (voltage standing wave ratio, коэффициент стоячей волны по напряжению (КСВН)). Мера отражения, возникающая при рассогласовании импедансов линий передачи.

## W

**WEP** (wired equivalent privacy, конфиденциальность, эквивалентная проводимых сетей). Алгоритм шифрования уровня 2, основанный на алгоритме RC4, обеспечивающий защиту данных в сетях стандарта 802.11.

# Предметный указатель

---

## I

1000BASE-CX, 35  
1000BASE-LX, 35  
1000BASE-SX, 34  
1000BASE-T, 34; 35  
1000BASE-X, 34  
100BASE-FX, 32  
100BASE-T2, 35  
100BASE-T4, 35  
100BASE-TX, 32  
10BASE-X, 32  
10BASE2, 31  
10BASE5, 31  
10BASE-FL, 32  
10BASE-T, 30

## 4

4-QAM, 119

## A

AAA, 146  
AC, 190  
Access categories, 190  
Access hot spot, 266  
Access layer, 23; 255  
Access point, 43  
ACL, 246  
Ad-hoc client, 249  
Ad-hoc network, 42  
Admission control, 193  
ADSL, 120  
Advanced encryption standard, 155  
AES, 155

AES-CCM, 160  
AID, 65; 66; 148  
AIFs, 191  
AirSnort, 159  
A-Nonce, 157  
Arbitration interframe space, 191  
Association identifier, 65  
Asynchronous connectionless link, 246  
Authentication framework, 145  
Authentication, authorization, and  
accounting, 146  
Authenticator, 145  
Authentication nonce, 157  
Available budget, 193

## B

Backoff timer, 42  
Basic service set, 41  
Beacon, 45  
Beacon frame, 54  
Beacon interval, 42  
Beacon interval field, 62  
Bandwidth, 205  
BER, 209  
Best effort traffic, 192  
Bit flipping, 147  
Bitmap control, 60  
Bitmap offset field, 67  
Bluetooth, 247  
режимы работы, 246  
Bluetooth Special Interest Group, 246  
Brackets, 234  
Bridging link, 252  
Broadcast black hole, 189  
BSS, 47; 48

BSSID, 77  
Burst mode, 36  
BW, 305

## C

Capability information field, 62  
Care-of address, 176  
Carrier extension, 36  
Carrier sense/clear channel assessment, 97  
CBC-CTR, 160  
CBC-MAC, 160  
CCA, 97; 210  
CCA engine, 97  
CCK, 112  
CCoA, 176  
CFP, 54  
CFP count, 79  
CFP period, 79  
CFR47, 215  
Challenge frame, 138  
Challenge handshake authentication protocol, 148  
Challenge message, 157  
Channel numbering scheme, 117  
Channel-equalization scheme, 119  
CHAP, 148  
Chip, 119  
Cipher Block Chaining Counter Mode, 160  
Cipher Block Chaining Message Authentication Check, 160  
Circular convolution, 119  
Cisco Call Manager, 258  
Cisco IOS Software, 258  
Cisco Survivable Remote Site Telephony, 258  
CoA, 176; 177  
Cochannel overlap, 189  
Code of Federal Regulations, 215  
Code rate, 99  
Coding, 98  
Co-located care-of address, 176  
Complementary code keying, 112  
Complex clip, 114  
Configuration distribution, 240  
Constellation, 101

Constraint length of a code, 99  
Contention free period, 54  
Contention period, 55  
Contention window, 47  
Control frame, 70  
Converged applications, 264  
Convolutional coder, 99  
Core layer, 23  
CP, 55  
CRC, 26  
CRC-32, 136, 143  
CS/CCA, 97  
CSMA/CA, 44  
CSMA/CD, 27  
CW, 47

## D

DAC, 193  
Data frame, 70  
Data integrity algorithm, 145  
Data link sublayer, 24  
Data primitives, 47  
DBPSK, 109; 111  
DCF, 45; 46  
DCF interframe space, 46  
Delay spread, 118  
Delivery traffic indication map, 54  
Descrambler, 98  
DIFS, 46  
Differential binary phase shift keying, 109  
Differentiate services code point, 191  
Distributed coordination function, 45  
Distributed admission control, 193  
Distribution layer, 23  
DQPSK, 111  
DSCP, 191; 237  
DSSS, 102, 110  
DTIM, 54  
DTIM count, 80  
DTIM count field, 69  
DTIM period, 80  
DTIM period field, 70  
Duration, 75  
Duration field, 46  
Dwell time, 79  
Dynamic encryption key, 152

## E

EAP, 147  
EAP-Cisco, 148  
EAP-MD5, 148  
EAP-Message Digest 5, 148  
EAPol -Key, 157  
EAP-PEAP, 148  
EAP-Request Identity, 149, 151  
EAP-Response, 149, 151  
EAP-Start, 149  
EAP-transport layer security, 148  
ECB, 133  
Edge router, 176  
EDSF, 190, 193  
EF, 237  
EIGRP, 30  
EIRP, 205  
Electronic Code Book, 133  
Enhanced DSF, 190  
Equalizing, 118  
ERP, 205  
ESS, 41, 43  
Ethernet value, 25  
ETSI, 215  
Expedited forwarding, 237  
Extended service set, 41  
Extensible Authentication Protocol, 147

## F

FA, 176  
Fast Ethernet, 32  
Fast link pulse, 37  
Fast packet keying, 153  
FCC, 102, 244  
FCS, 26, 63  
FDD, 201  
FDDI, 32  
Feedback mode, 133  
FER, 209  
FHSS, 102  
File transfer, 247  
Finite memory code, 99  
Firmware distribution, 240  
Fixed field, 77  
Flat fading, 213  
FLP, 37

Foreign agent, 176  
Frame error ratio, 209  
Free space optics, 243  
Frequency division duplex, 207  
Frequency offset, 104  
Frequency-shift keying, 105  
FSK, 105  
FSO, 243

## G

Gaussian frequency shift keying, 105, 245  
Geometrical path loss, 251  
GFSK, 105, 245  
Gigabit Ethernet, 34  
GMK, 159  
GPR, 248  
GRE, 189  
Ground penetrating radars, 248  
Group master key, 159  
Group transient key, 159  
GSM, 266  
GTK, 159  
Guard time, 119

## H

HA, 176  
Handshaking layer, 96  
HC, 194  
HCF, 190  
Hidden node issue, 42  
HMAC-MD5, 181  
Hold, 245  
Home address, 180  
Home agent, 176  
Hop index, 79  
Hop pattern, 79  
Hop set, 79  
HR-DSSS, 112  
Hybrid coordination function, 190  
Hybrid coordinator, 194

## I

IBSS, 41, 42  
ICMP, 178  
ICV, 136

IF, 77  
IEEE, 215  
IFS, 197  
Independent basic service set, 41  
Information element, 77  
Initialization vector, 133  
Integrity check value, 136  
Interframe gap, 36  
Interleaving, 98  
Internet control message protocol, 178  
Intersymbol interference, 118  
IRDP, 178  
ISI, 118  
ISM, 102  
IV, 133

## K

Key scheduling algorithm, 142  
Key stream, 132  
Keyed message-authentication mechanism, 181  
KSA, 142

## L

LAA, 142  
LBT, 44  
LEAP, 148  
LED, 251  
Length extension bit, 113  
Length field, 67  
Lifetime field, 178  
Limitless store-and-forward network, 246  
Link budget, 211  
Listen before talk, 44  
Listen interval, 65  
LLC, 24  
Locally administered address, 142  
Logical link control, 24  
Long Sync, 117  
LSB, 122

## M

MA, 197  
MAC protocol data units, 96  
MAC-адрес, 25

Management action request, 197  
Management frame, 70  
Master, 244  
Master key, 157  
Media Access Control, 24  
Message digest, 181  
Message integrity check, 153  
MIC, 153, 155  
MIC receive key, 159  
MN, 176  
Mobile node, 176  
MPDU, 96  
Multichannel modulation, 119  
Multicast packet, 245

## N

NAV, 45  
Network allocation vector, 45  
Network interface card, 42  
Network latency, 237  
Network link pulse, 38  
NIC, 42  
NIST, 160  
NLP, 38  
Nomadic roaming, 163  
NTP, 159  
Null authentication algorithm, 138  
Null data frame, 56

## O

Object push, 247  
OFDM, 116  
Open authentication, 64, 135  
Orthogonal frequency division multiplexing, 116  
OSI, 24  
OUI, 26

## P

Packet binary convolutional coding, 112  
Packet error rate, 209  
Packet timing, 104  
Pairwise master key, 157  
Pairwise transient key, 158  
PAN, 243

Park, 246  
Parked slave, 246  
Partial virtual bitmap, 80  
Partial virtual bitmap field, 67  
Partial-rate half-rate encoder, 115  
Payload, 136  
PBCC, 112  
PBSS, 115  
PC, 54  
PCF, 53  
PER, 209  
Per-frame keying, 153  
Per-packet keying, 153  
Personal-area network, 243  
Phase 1 key, 153  
PHY parameter set element, 62  
Physical Layer Convergence Procedure, 96  
Physical Medium Dependent, 96  
Piconet, 244  
PIFS, 55  
PLCP, 96  
PLCP data unit, 97  
PLCP service data unit, 104  
PLW, 193  
PMID, 96  
PMK, 157  
Point coordination function, 53  
Point coordinator, 54  
Point of presence, 266  
Point-to-Point Protocol, 147  
POP, 266  
Power save operation, 66  
Power save poll, 69  
PPDU, 97  
PPP, 147  
Preemptive AP discovery, 167  
Prefix-length extension, 178  
PRF, 158  
Priority interframe space, 55  
Probe request frame, 61  
Probe response frame, 62  
Profile, 247  
PSDU length word, 105  
Pseudo random function, 158  
PSG, 103  
PS Poll, 69  
PTK, 158  
Puncturing, 122

## Q

QoS, 187  
QPSK, 101, 169  
Quadrature amplitude modulation, 119  
Quadrature phase shift key, 109  
Quadrature phase-shift keying, 101

## R

RA, 75  
RADIUS, 146  
RAKE-приемник, 249  
Random backoff timer, 47  
Receiver address, 75  
Repeater AP, 57  
RFC 2284, 146  
Rijndael algorithm, 160  
Roam time AP discovery, 167  
Router discovery protocol, 178  
RTS/CTS, 50

## S

Scatternet, 244  
SCO, 246  
Scrambling, 98  
Seamless roaming, 163  
Secure sockets layer, 148  
Service Selection Gateway, 266  
Service set, 41  
Service set identifier, 41  
SFD, 25, 104  
Shared key authentication, 138  
Shared-key authentication, 64  
Short interframe space, 49  
Short Sync, 117  
SIFS, 49  
SIG, 246  
Signaling field PLCP, 105  
Signaling system 7 network, 266  
SIM, 266  
Simultaneous bindings, 180  
Slave, 244  
Slot time, 27, 47  
Sniff, 246  
SNonce, 158  
SNR, 269

Source address filtering checks. 152  
Spectral efficiency. 98  
SRST. 258  
SS7. 266  
SSG. 266  
SSID. 41  
SSL. 148  
Start of frame delimiter. 25, 104  
Status code. 66  
Stuff symbol. 105  
Subscriber Identity Module. 266  
Supplicant. 148  
Supplicant nonce. 158  
Symbol mapper. 111, 115  
Symbol mapping. 101  
Symbol mapping and modulation. 98  
Synchronous connection-oriented. 246

## T

TA. 74  
TBTT. 42  
TC. 190  
TCP. 165  
TDD. 245  
Temporal key integrity protocol. 152  
TDM. 67  
Time division duplex. 245  
Time unit. 62  
Timer synchronization function. 43  
Timestamp. 84  
Timestamp field. 62  
Timing. 42  
TKIP. 152  
TLV-кодирование. 25  
Traffic classes. 190  
Traffic indication map. 67  
Traffic indication virtual bitmap. 68  
Training sequence. 117  
Transmit MIC key. 159  
Transmit opportunity. 191  
Transmitter address. 25  
Trap collection. 240  
TSF. 43  
TSPEC. 195  
TU. 62  
TXOP. 191  
Type/length value. 25

## U

UAA. 142  
UDP. 165  
Ultra wide band. 243  
U-NI. 116  
Universally administered address. 142  
Unauthorized national information  
infrastructure. 116  
User Data Protocol. 165  
UWB. 243, 247

## V

VPN. 263  
VSWR. 207

## W

WAN. 237  
WECA. 266  
Whitening. 98  
Wi-Fi. 23  
Wi-Fi Alliance. 215  
Wi-Fi Protected Access. 145, 216  
Wi-Fi ZONE. 267  
Wireless Fidelity. 23  
WISPs. 266  
WPA. 145, 236, 265

## A

Автоматическое согласование. 37  
Адрес  
внешний. 176  
внутренний. 176  
домашний. 176  
обнаружение. 178  
Адрес  
Ethernet. 26  
внешнего агента. 178  
исс единицы. 29  
для передачи. 176  
для передачи сопряженных. 176  
пересылки. 25  
присылки. 25  
интерковенсательный. 29

## Алгоритм

AES, 160

Michael, 155

аутентификации, 145, 150

защиты данных, 145, 152

контроля аутентичности сообщений  
CBC-MAC, 160

обеспечения целостности данных,  
145

Ривингла, 160

ривингла, 167

шифрования CBC-CTR, 150

шифрования WEP, 134

Ангстена, 202

изотропная, 203

полосы пропускания, 207

полуволновая, 203

поляризация, 206

поперечного излучения, 203

продольного излучения, 208

с излучателем диаграммы  
направленности, 208

Уда-Яги, 208

ширина диаграммы  
направленности, 203

широкополосная, 207

эквивалентная излучаемая  
мощность, 205

Арбитражный межфреймовый  
промежуток, 191

Аутентификатор, 146

временный, 157

Аутентификация

базовая, 145

взаимная, 146

на удаленных площадках, 238

ориентированная на пользователя,  
146

ориентированная на устройства, 146

открытая, 138

расширяемый протокол, 147

с использованием MAC-адресов,  
139

с открытым ключом, 64

с предварительным согласованием  
вызова, 148

с совместно используемым ключом,  
64, 138

## Б

Базовая зона обслуживания, 43

Благоприятная возможность для  
сервера, 191

Блочный шифр, 132

БПФ, 119

Быстрый канальный импульс, 37

Бюджет наличный, 194

## В

Ведомый

активный, 246

неактивный, 246

принорированный, 246

Ведущий, 244

Вектор

инициализации, 133

распределения сети, 46

Взаимные помехи, 212

Вибратор, 207

Виртуальная битовая карта индикации  
трафика, 68

Внешний агент, 176

Внутренний агент, 176

## Г

Гибридная функция кодирования, 190

Гибридный координатор, 194

Главный депесток антенны, 204

## Д

Дескремблер, 98, 117

Дескриптор последовательных  
последовательностей, 117

Диаграмма излучения, 203

Диаметр сети Ethernet, 27

Диполь, 203

Домашний агент, 176

Домен

рутинга, 165

широковещательный, 165

ДПФ, 119



- Защитное, 213
  - равномерное, 213
  - частотно-избирательное, 213
- Зона обслуживания, 41
  - базовая, 41
  - базовая независимая, 41
  - расширенная, 41

## И

- Идентификатор
  - ассоциации, 65; 66; 145
  - зоны обслуживания, 41
- Изотропный излучатель, 203
- Импеданс, 207
- Инкапсуляция, 182
  - IP в IP, 183
  - минимальная, 183
  - обобщенная маршрутная, 183
- Интервал
  - Ethernet, 27
  - Gigabit Ethernet, 36
  - мачтовый, 42
  - прослушивания, 65
  - сигнальный, 42
- Информационный элемент, 77
  - SSID, 78
  - TIM, 80
  - TSPEC, 196
  - изменяющегося текста, 81
  - набора параметров CF, 79
  - набора параметров IBSS, 80
  - набора параметров
    - распределительной системы, 79
    - набора параметров скачкообразного переключения частоты, 79
    - поддерживаемых скоростей передачи, 78

## К

- Канал
  - FSO, 250
  - асинхронный без установления соединения, 246

асинхронный на основе соединений, 246

- Канальный импульс сети, 39
- Канальный интервал, 47
- Карта индикации трафика, 67
- Категория доступа, 190
- Квадратурная ось, 101
- Класс трафика, 190
- Кэши
  - групповой переходный, 159
  - парный переходный, 159
  - первой фазы, 153
  - передачи MTC, 159
  - приема MTC, 159
  - цифровая асимметричная, 152
- Ключевой поток, 132
- Кол
  - блуждающий без памяти, 99
  - с конечной памятью, 99
  - сверточный, 99
  - состояния, 66
  - указателя дифференциальной службы, 191; 237
- Кодирование, 98
  - двоичное пакетное сверточное, 112; 115
  - с блочным чередованием, 110
  - с использованием
    - комплементарных кодов, 112
- Кодовое ограничение, 99
- Коллизия, 27
- Контроль
  - несущей, 45
  - целостности сообщения, 153; 155
- Контрольная последовательность фрейма, 26
- Контрольный признак целостности, 136
- Короткий межфреймовый зазор, 49
- Коэффициент
  - кодирования, 99
  - полезного действия антенны, 207
  - стычей волны по напряжению, 207
  - усиления антенны, 203
- КСВН, 207

**Л**

Лепесток  
 второстепенный, 204  
 главный, 204

**М**

Манипуляция  
 двоичная относительная фазовая, 109; 111  
 квадратурная фазовая, 109  
 частотная, 105

Мастер-ключ, 157  
 групповой, 159  
 главный, 157

Межсимвольная интерференция, 118  
 Межсимвольные помехи, 118  
 Межфреймовый зазор DCF, 46  
 Межфреймовый пробел, 56

Механизм  
 дифференцирования и  
 приоритезации трафика, 191  
 классификации трафика, 191  
 пометки трафика, 191  
 распределенного управления  
 входом, 193  
 управления входом, 193  
 управления входом ИСГ, 195

Многослужбовое расширение, 213

Мобильный узел, 176

Модуляция  
 DSSS, 108  
 FHSS PMD-GFSK, 105  
 GFSK, 105  
 квадратурная относительная  
 фазовая, 111  
 многоканальная, 119  
 основанная на гауссовом  
 переключении частот, 245  
 с расширением спектра методом  
 прямой последовательности, 108

Мног  
 беспроводной, 59  
 рабочей группы, 58

Мультиплексирование с разделением по  
 ортогональным частотам, 116

**Н**

Наличный бюджет, 193  
 Направленность антенны, 203  
 Настроенная последовательность, 117  
 Незащищенная базовая зона  
 обслуживания, 42  
 Незплановая сеть, 42

**О**

Ожог конкуренции, 47  
 Отбеливание, 98

**П**

Пакет многоинтервальный, 245  
 Перекрытие по совмещенному каналу,  
 189; 199

Период  
 конкуренции, 53  
 свободный от конкуренции, 54

Персональная сеть, 243

Пикосеть, 244  
 многоточечная, 245  
 с одним узлом, 245

Побочное радиопомешание, 219

Подполе  
 CRC, 109  
 Length, 109; 117  
 Pad, 118  
 PSDU, 118  
 Rate, 117  
 Service, 109; 117  
 SFD, 109  
 Signal, 109  
 Sync, 104; 109  
 Tail, 117; 118  
 Флага начала фрейма, 104

Подуровень  
 PLCP, 96  
 PLCP структура 802.11g, 123  
 PLCP технологии HR-DSSS, 112  
 PLCP технологии OFDM, 117  
 PMD, 96  
 PMD технологии OFDM, 121  
 канальный, 24

- управления логическим соединением, 24
  - Полоса**
    - AID, 83
    - CFF Duration Remaining, 80
    - CFF MaxDuration, 79
    - Data, 117
    - FCS, 26
    - TLV, 25
    - адреса отправителя, 25
    - адреса приемника, 25
    - аптечки в ближней зоне, 203
    - аптечки в дальней зоне, 203
    - времени жизни, 178
    - времени пребывания, 79
    - временной метки, 62
    - длиных, 26
    - длина, 67
    - индекса канала, 79
    - интервал прослушивания, 83
    - информационной способности, 62, 82
    - кода причины, 83
    - кода состояния, 83
    - контроля битовой карты, 80
    - контроля фрейма, 70
    - метки времени, 84
    - набора схем скачков, 79
    - номер алгоритма аутентификации, 81
    - перкода CFF, 79
    - периода DTIM, 70, 80
    - подсчета DTIM, 69
    - порядкового номера транзакции аутентификации, 81
    - продолжительности, 46
    - сигнального интервала, 62; 82
    - сигнальное PLCP, 105
    - смещения битовой карты, 67
    - сплержимого, 26
    - схемы скачков, 79
    - счетчика CFF, 79
    - счетчика DTIM, 80
    - текущего адреса точки доступа, 82
    - типа фрейма Ethernet, 25
    - фиксированные, 77
    - частичной виртуальной битовой карты, 67; 80
  - Полоса пропускания антенны, 207
  - Поляризация антенны, 206
  - Помехи взаимные, 212
  - Проп**
    - RTS, 225
    - фрагментации, 225
  - Последовательность Barker, 110
  - Потери в кабеле, 211
  - Потоковый шифр, 132
    - RC4, 132
    - симметричный, 135
  - Пофреймовое изменение ключа, 153
  - Прямбула, 25
  - Преимущественный межфреймовый интервал, 55
  - Преобразующие символы, 101
  - Преобразователь символов, 111; 115
  - Приближа к скрытому узлу, 42; 50
  - Продолжительность, 75
  - Прямитель, 148
    - временный, 158
  - Прослушивание перед передачей, 44
  - Протокол**
    - EAP, 148
    - IRDP, 178
    - TCP, 165
    - UDP, 165
    - аутентификации с предварительным согласованием ключа, 148
    - замкнутых сокетов, 148
    - межсетевых управляющих соединений, 178
    - обнаружения маршрутизатора, 178
    - целостности ключа временный, 152
  - Профиль, 247**
  - Процесс**
    - аутентификации, 64
    - лонгирования, 61
    - привязки, 65
- Р**
- Радиовылучение побочное, 219
  - Разброс задержек, 118
  - Распределенная сеть, 244
  - Распределенная функции координации, 45; 46

Распространение микроволновое, 213  
Расширение несущей, 36  
Расширение спектра  
методом прямой  
последовательности, 102; 103  
путем скачкообразной перестройки  
частоты, 102  
Расширенная зона обслуживания, 43  
Расширенная распределенная функция  
координации, 190  
Расширяемый протокол  
аутентификации, 147  
Режим  
CSM, 160  
автоогласования, 37  
локальный, 36  
работы Ethernet, 25  
энергосбережения, 66  
Роуминг, 163; 266  
бесшлюховый, 163  
кочевой, 163  
между доменами роуминга, 174  
предварительный, 169  
стандарта 802.11, 164  
уровня 2, 167  
уровня 3, 174

## С

Связь  
дуплексная с временным  
разделением, 201  
дуплексная с временным разделением  
каждой, 245  
дуплексная с частотным  
разделением, 201  
сверхширокополосная, 243  
Сервер  
RADIUS, 148  
аутентификации, 148  
Сеть  
ad-hoc, 42  
Bluetooth многоточечная, 244  
тепловая, 42  
одноранговая, 42  
переносимая, 243  
распределенная, 244  
с промежуточным хранением, 246

Сигнальное созвездие, 101  
СИД, 251  
Синхронная ось, 101  
Система распределительная, 43  
Сканирование  
активное, 168  
пассивное, 168  
Скремблирование, 98  
Скрытый узел, 42; 189  
Сота, 163  
Спектральная маска, 216  
диапазона U-NII, 219  
Специальная сеть, 42  
Стандарт  
802.11a, 116  
802.11b, 112  
802.11g, 124  
802.11i, 145  
802.11j, 117  
802.1X, 147  
802.3ab, 35  
802.3u, 32  
802.3z, 35  
ANSI Fibre Channel, 35  
Ethernet 802.3, 23  
шифрования  
усовершенствованный, 155

## Т

Таймер случайной задержки, 42; 47  
Технология  
Bluetooth, 243  
FSO, 250  
UWB, 247  
передача оптических сигналов  
через свободное пространство,  
247  
Точечная функция координации, 53  
Точка доступа, 43  
обнаружение во время  
перемещения, 167; 171  
предварительное обнаружение, 167;  
169  
Точка доступа-повторитель, 57  
Точка координации, 54  
Трафик ближайшего  
благоприятствования, 192

Туннелирование, 182  
реверсное, 183

## У

Узел  
мобильный, 176  
скрытый, 189  
Универсальный клиент, 58  
Управление  
беспроводными LAN, 239  
входом, 193  
входом распределенное, 193  
входом с HCF, 195  
Уровень  
MAC, 24  
PHY, 97  
PHY, 98  
базовый, 23  
доступа, 27; 255  
канальный, 24  
обеспечения взаимодействия, 96  
распределения, 27  
физический, коуровни, 96

## Ф

Фединг, 212  
Физический уровень  
полуронни, 96  
составляющие, 98  
Флаг заглава фрейма, 25  
Фрагментация фрейма, 53  
Фрейм  
ATIM, 99  
CF-Ack, 93  
CF-Ack+CF-Poll, 93  
CF-End, 77  
CF-End+CF-ACK, 77  
CF-Poll, 93  
CTS, 75  
DSSS PPDU, 109  
Ethernet, 25  
PLCP, 104  
PPDU, 104; 117  
PS-Poll, 74  
RTS, 75  
аутентификации, 86

вызова, 138  
готовности к передаче, 59  
готовности к приему, 51  
данных, 70, 91  
деаутентификации, 88  
дисциплинирования, 99  
запроса на ассоциирование, 88  
запроса на ассоциирование, 85  
запроса на зондирование, 86  
запроса на реассоциирование, 89  
зонадирующий запроса, 61  
зондирующий ответа, 62  
маячковый, 85  
многоадресный, 29  
нулевых данных, 92  
опроса режима энергосбережения,  
69  
ответа на ассоциирование, 65  
ответа на ассоциирование, 89  
ответа на зондирование, 86  
ответа на зондирующий фрейм  
запроса, 62  
ответа на реассоциирование, 89  
подтверждения, 49; 56  
с нулевыми данными, 56  
сигнальный, 85  
служебный, 70  
упреждающий, 70  
фрагментация, 53  
широкоадресный, 29

Функция  
координатки гибридная, 190  
координатки распределенная, 46  
координатки распределения  
расширенная, 190  
координатки точечная, 53  
оценки незабитости канала, 97  
синхронизации таймера, 47

## Ц

Циклическая свертка, 119  
Циклический избыточный код, 26

## Ч

Частица  
появления ошибочных битов, 209

количество ошибочных пакетов, 209  
поисления ошибочных фреймов, 209  
Чередование, 49  
Черная дыра широкополосная, 189

### Ш

Широковещание в режиме  
энергосбережения, 69  
Шифр  
блочный, 132  
поточный, 132  
Шифрование, 132  
в режиме с обратной связью, 134  
по алгоритму AES, 169  
с помощью книги электронных  
ключей, 137

### Э

ЭИМ, 205  
Эквивалентная излучаемая мощность,  
205  
Элемент  
SSID, 62, 65  
данных протокола PLCP, 97  
данных служебный PLCP, 104  
набора параметров PHY, 62  
поддерживаемых скриптов  
передачи, 62, 66  
Элементарный сигнал, 110  
Энергетический потенциал линии  
связи, 211  
Эффективная изотропно-излучаемая  
мощность, 205  
Эффективная степень кодирования, 99

*Научно-популярное издание*

**Педжман Рошан, Джонатан Лиэри**

## **Основы построения беспроводных локальных сетей стандарта 802.11**

Литературный редактор *И.А. Цытова*  
Верстка *О.В. Липкина*  
Художественные редакторы *В.Г. Павлюков, Г.А. Тарихурова*  
Корректоры *З.В. Александрова, Т.А. Гарденина*

Издательский дом "Вильямс".  
101509, Москва, ул. Лермонтова, д. 43, стр. 1  
Над. лист ЛР № 090210 от 22.06.99  
Госкомитета РФ для печати.

Подписано в печать 14.09.2004. Формат 70×100/16.  
Тиражирование Times. Печать офсетная.  
Усл. печ. л. 34,51. Уч.-изд. л. 20,9.  
Тираж 3000 экз. Заказ № 555.

Отпечатано с диапозитивов в ФГУП "Ленский литьер"  
Министерства РФ по делам печати,  
телерадиовещания и средствам массовой коммуникации  
197110, Санкт-Петербург, Чкаловский пр., 15

# Основы построения беспроводных локальных сетей стандарта 802.11

- Обзор основных разновидностей технологии Ethernet — от Ethernet на 10 Мбит/с до Gigabit Ethernet
- Основы передачи информации по радиоканалу с рассмотрением характеристик приемников антенн и передатчиков
- Основные концепции, используемые при создании беспроводных ЛВС стандарта 802.11, включая описание функций, выполняемых на беспроводном подуровне управления доступом к носителю (MAC) и технологий, применяемых для создания физического уровня
- Проблемы безопасности беспроводных сетей, в том числе методы аутентификации и шифрования, а также проект стандарта 802.11i и технология защищенного доступа к беспроводным сетям (Wi-Fi Protected Access, WPA)
- Концепции мобильности, с рассмотрением проблем, вызываемых мобильностью клиента, а также краткое описание мобильного IP
- Вопросы, связанные с выполнением в ЛВС приложений чувствительных к задержкам, таких как IP-телефония, и обзор средств обеспечивающих высокое качество обслуживания (QoS) при использовании технологий стандарта 802.11
- Картирование места развертывания беспроводной ЛВС
- Схематички, связанные с применением беспроводных ЛВС в конкретных условиях
- Перспективы развития беспроводных ЛВС на основе таких технологий, как Bluetooth, сверхширокополосная связь, передача оптических сигналов через свободное пространство и технологий стандарта 802.11, обеспечивающих более высокую скорость передачи

Эта книга является частью серии **Networking Technology Series**, которая предоставляет по предметным областям информацию по созданию многофункциональных сетей, в которой вы можете найти новейшие технологии и ресурсы. Выберите свой

[www.it-ebooks.com](http://www.it-ebooks.com)  
[www.ciscopress.ru](http://www.ciscopress.ru)  
[ciscopress.com](http://ciscopress.com)

По мере расширения скорости передачи данных в беспроводных ЛВС (WLAN) и снижения их стоимости преимущества этой технологии становятся все более очевидными. Поддержка все большего числа устройств, работающих в одной и той же сети, делает Ethernet, в отличие от беспроводных LAN, менее гибким и более дорогостоящим. За счет применения WLAN можно резко увеличить производительность групп сотрудников и сэкономить значительные средства при развертывании сети, обладающей высокой гибкостью. Однако по мере того как все больше и больше компаний начинают преимущества WLAN, приступают к их развертыванию, возникает все больше вопросов относительно того, как лучше предоставить, развернуть сеть стандарта 802.11 и работать с ней. Беспроводные ЛВС и их взаимодействие с другими сетями, проблемами имеют дело с применением технологий, уникальные возможности. Сначала мы рассмотрим возможности в области мобильности, в области радиотехники, и проблемы безопасности, и вопросы обеспечения качества обслуживания, а также проектирования сетей и картирование места их развертывания.

Книга **Основы построения беспроводных локальных сетей стандарта 802.11** дает читателю необходимые знания для выбора, разработки, развертывания и эксплуатации беспроводной ЛВС, а также предоставляет множество практических сведений. Начиная с обзор технологии Ethernet, стандартов серии 802.11 и технологий физического уровня (это сведения необходимы читателю для того, чтобы быстрее разобраться в других материалах книги). В последующих главах рассмотрены все проблемные моменты, связанные с безопасностью, мобильностью и качеством обслуживания. Далее основное внимание уделено радиоканалу и описаны методы картирования места развертывания сети. Рассмотрен ряд конкретных случаев применения беспроводных ЛВС в реальных условиях, благодаря чему концепции, описанные в книге, воплотятся в реальном содержании. Независимо от того, являетесь ли вы специалистом по вопросам работы беспроводных ЛВС или просто любите руководить работой по их развертыванию, в книге **Основы построения беспроводных локальных сетей стандарта 802.11** вы найдете множество практических сведений, которые помогут вам, включая базовый курс проектирования сетей, это поможет вам быстрее развернуть WLAN и эффективно управлять ею.

**“Эта книга поможет вам разобраться в основах построения сетей Wi-Fi и подготовит вас к грядущим переменам”**

— Дэвид Пинк, редактор Wi-Fi Alliance

**Педжман Ринган** — менеджер линейки продуктов подразделения беспроводных сетей (Networking Business Unit) корпорации Cisco Systems. Он руководит подразделением прикладных продуктов для беспроводных LAN корпорации Cisco, а его целью является обеспечение безопасности в удаленных сетях.

**Джонатан Лиари** — менеджер линейки продуктов подразделения беспроводных сетей корпорации Cisco Systems. Джонатан занимается в основном проектированием и развертыванием WLAN для компаний.

ISBN 5-8459-0701-2



**Классификация.**  
Cisco Press — беспроводные сети  
**Предмет рассуждения.**  
Беспроводные ЛВС стандарта 802.11