ВИЛЬЯМС

Cisco Systems

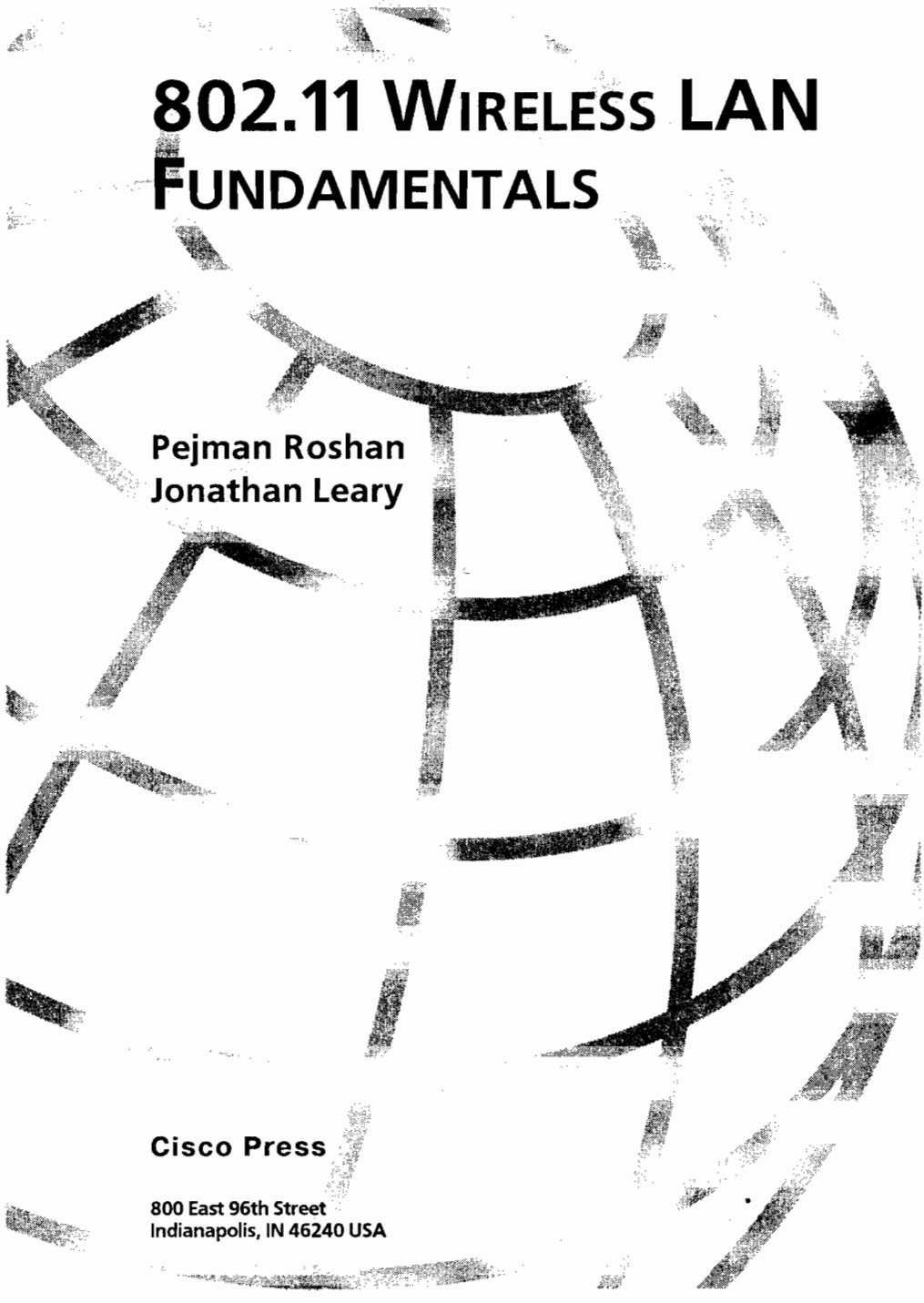
Основы построения беспроводных локальных сетей стандарта 802.11

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

www.williamspublishing.com
www.ciscopress.ru
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 Лиэри

Москва • Санкт-Петербург • Киев
2004

ББК 32.973.26-018.2.75
Р81
УДК 681.3.07

Издательский дом "Вильямс"

Зав. редакцией *С.Н. Тригуб*

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, Педжман, **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 рынком 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

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

ISBN 5-8459-0701-2 (рус.)
ISBN 1-5870-5077-3 (англ.)

Оглавление

Содержание

Об авторах

Педжман Рошан (Pejman Roshan) — 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, Педж проработал шесть лет сетевым инженером, позднее 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 Лиэри (Jonathan Leary) — 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 мостовых соединений, а также обеспечивает помощь и руководство в части развертывания наружных сетей системными инженерами. Джон получил степень доктора технических наук (B.S. degree in engineering science) в Гарвардском университете и степень магистра электротехники (electrical engineering) в Станфордском 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 Aironet 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 Ameritron Amateur Radio Company. Брюс посещает университет в г. 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 за счет учета ими окружающей радиосреды. Будучи активным участником процесса разработки стандартов IEEE серии 802.11, он помогал разрабатывать проект дополнения IEEE 802.11k на радиоизмерения. Ранее он отвечал за управление и технические характеристики систем беспроводной обработки сигналов для базовых станций глобальной системы мобильной связи (GSM) — от пикосот до макросот. До этой коммерческой деятельности Дарил работал с военным подрядчиком, компанией Silicon Valley, разрабатывая заказные алгоритмы для детектирования сигналов и автоматического распознавания.

Брюс Макмэд (Bruce McMurdo), сертифицированный специалист по объединенным сетям Cisco, сотрудничал 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 наши!

Моим родителям, Биджен и Джелэ. Вы всегда верили в меня, гордились мною 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 Лиэри

Моим родителям, Норите и Эдварду, 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 в должности администратора сети, управляя сетями всевозможных размеров, а также их разработкой. Когда в 2000 году WLAN стали основным направлением оснащения предприятий, я сделал то, что всегда делал, когда приходило время изучать новые технологии: попытался найти книгу издательства Cisco Press. Я ничего не нашел и вынужден был обратиться к чтению (ужас!) спецификаций IEEE, чтобы разобраться в этих беспроводных штуковинах. Это не было испытанием, 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 посчастливилось работать с Раулем Ромеро (Raul Romero), моим хорошим другом. Рауль всегда играл положительную роль в моей жизни и карьере и возвращал меня к реальности, когда я собирался наделать глупостей. Эта книга не появилась бы без его повседневных советов и если бы не была написана для него.

Мои руководители — Кристин Фалсетти (Christine Falsetti), Эрик Блауфарб (Eric Blaufarb) и Брюс Александер (Bruce Alexander); именно они дали мне возможность написать эту книгу. Кристин — вечный "сетевой рабочий" с миллионом контактов и еще одним. Ее ободрение и поддержка на протяжении всей моей карьеры в команде беспроводных сетей Cisco были бесконечны.

Вы даже не представляете, как я благодарен Эрику Блауфарбу, 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 идут за ответами на вопросы, касающиеся радиотракта или развертывания сети. Он — ходячая энциклопедия по радиотехнике, и его участие в создании этой книги большая честь для меня.

Брюс Макмэд (Bruce McMurdo) — второй технический редактор этой книги. Брюс — 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 нацеленность 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 802.11 — о качестве обслуживания (QoS), радиотракте или мобильности, — и он ответит просто и доходчиво. К тому же его помощь обходится очень дешево. Все, что я ему должен, — это оплатить ланч в Le Boulanger (тарелка 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) благоразумно отказался от работы над этой книгой, как в качестве соавтора, так и в роли технического редактора. К счастью для меня, я мог задавать ему тысячи вопросов, и он всегда отвечал на них, даже на вопросы, касающиеся технологии. Большое спасибо Тиму за техническую помощь — как в 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 Брету Бартоу и Крису Клевленду, редакторам этой книги и мастерам по части постановки задач. Почему эти два профессионала возились с такими дилетантами, как я и Джон, я не знаю! Большое спасибо им за электронные письма, напоминания, ворчание и поощрение нашей работы.

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

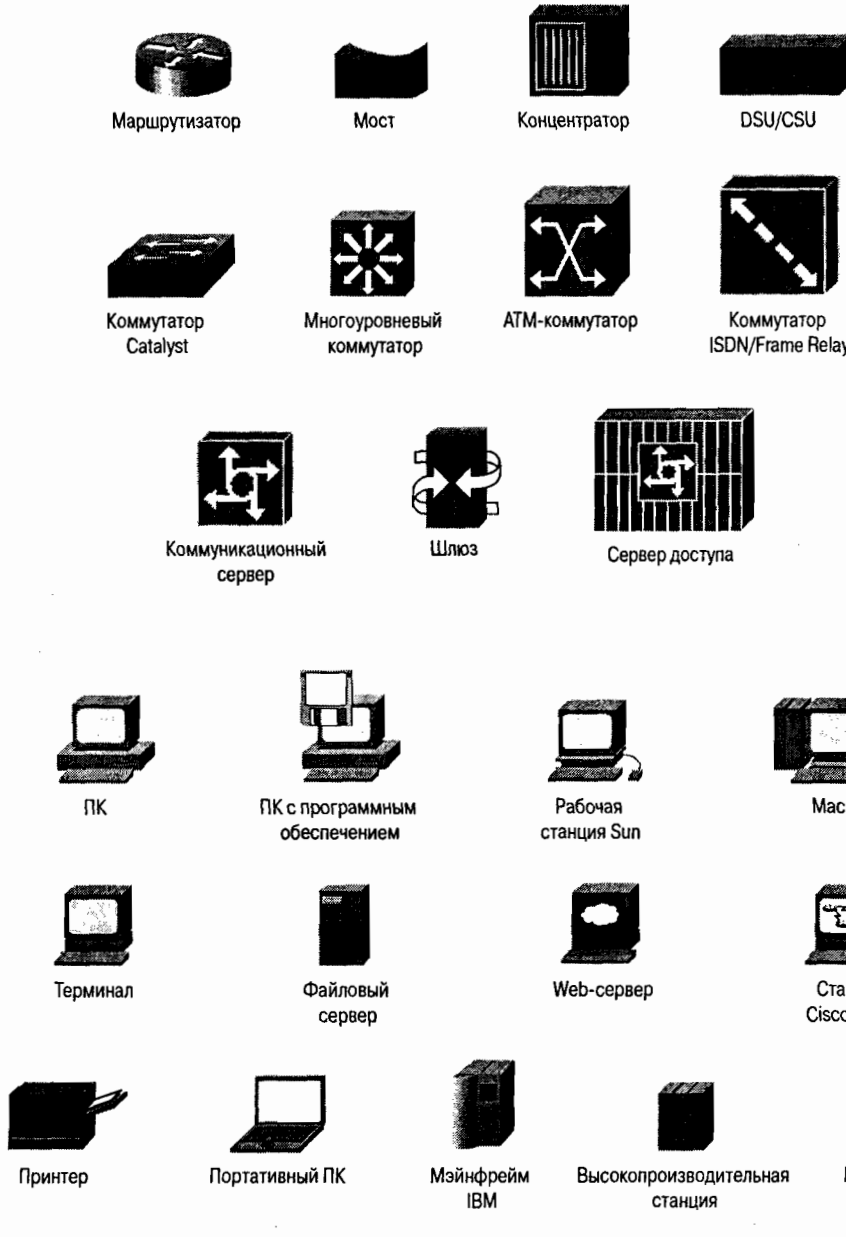
Джонатан Лиэри

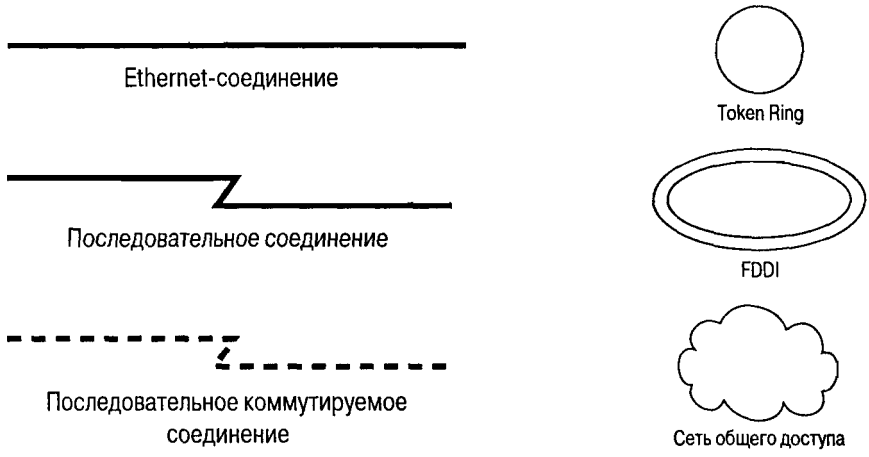
Прежде всего я хотел бы поблагодарить Педжа за предоставление мне возможности "помочь ему подняться". С момента, когда он упомянул о том, что пишет книгу для Cisco Press и нуждается в соавторе, я вдохновился на участие в этой работе.

Работа над этой книгой позволила мне лучше разобраться в том, как пишутся книги, — ведь 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 Александеру, Дарилу Кайзе и Брюсу Макмэду за выявление первых набросков и рисунков, которые не согласовывались с текстом.

Наконец, Педж и я многим обязаны Бретту Бартоу, Гранту Манрою и Кристоферу Кливленду за нашу более-менее постоянную нацеленность на соблюдение сроков и руководство нами в процессе написания книги.

Пиктограммы, используемые в книге





Условные обозначения

Обозначения, используемые в этой книге для представления синтаксиса команд, точно такие же, как используемые в книге *Cisco 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 соответствующих 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 высокоскоростных беспроводных служб работы с информацией. Она позволяет пользователю всегда быть "подключенным", уплотняет 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 отделяют многие часы полета.

Скромно начав в 1997 году как стандарт на беспроводную передачу данных со скоростью 1 и 2 Мбит/с в нелицензируемом 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 технология 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 платят за мобильный телефон. Сравните эту скорость, мобильность и сумму до 700 долларов, которую вы могли бы выложить за модем со скоростью передачи 9600 Кбит/с примерно 10 лет назад, и вы поймете, что технология Wi-Fi развивается с ускорением, которым могли похвастаться лишь немногие технологии прошлого.

Стандарт 802.11, или Wi-Fi, переходит из изначально присущего ему разряда вертикальных приложений для складов, управления запасами и средства связи для кассовых 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, соединяя нас постоянно и без каких-либо усилий с нашей стороны с Internet и нашими офисными приложениями, где бы мы ни находились — в офисе, аэропорту, дома, 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 технологии передачи речи через Wi-Fi для передачи видеосигналов от потребительских электронных устройств на информационное табло, висящее на стене вашего 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, возникает желание соединить эти устройства, не прикладывая для этого никаких усилий. Однажды, придя в свой любимый магазин электронных товаров, вы купите новый аудиовизуальный центр, который без проводов будет передавать через вашу домашнюю сеть видеоизображения на дисплей с плоским экраном, расположенный в другой части дома.

Новые расширения стандарта, мобильность клиента и быстрая эволюция оборудования — все вместе это может привести потребителя в некоторое замешательство. Что означают буквы в разновидностях стандарта 802.11 и какая из этих разновидностей представляет для вас интерес? Сколько точек доступа нужно развернуть и где они

должны быть установлены? Что можно сказать о мобильности пользователя 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 Итон (Dennis Eaton),
председатель Wi-Fi Alliance
(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 хотели тянуть за 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, надомным работникам, связывающимся 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 полосу 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 Ricochet, 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 Fast 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 использовании проводов 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 сетевого администратора решения непривычных для него задач.

Цель этой книги — рассмотреть аспекты стандарта 802.11 с точки зрения специалистов по информационным технологиям и сетевых инженеров. Книга представляет собой справочное руководство по работе сетей стандарта 802.11 и поиску неисправностей 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 некая противоположность 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 уровень управления доступом к передающей среде (Media Access Control, MAC) стандарта 802.11 и достаточно подробно — функции, которые он выполняет.

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

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 802.11 1997 года, и слабых мест в системе защиты. В этой главе описаны также детали проекта стандарта 802.11i на безопасность беспроводных сетей, кратко рассматриваются 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 краткое рассмотрение мобильного IP-протокола также включено 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 радиоэфир применительно к WLAN. Описаны антенны, приемники и характеристики радиосистем; рассказывается о различных нелицензируемых радиодиапазонах, используемых в разных странах мира. Цель этой главы — вооружить вас знаниями, которые помогут оценить 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 низким уровням, сопровождаемые советами по размещению кон-

кретных сетей. Рассматриваются WLAN, ориентированные на получение максимальной зоны обслуживания, и WLAN, ориентированные на достижение максимальной производительности. В этой главе описано несколько различных подходов к процессу картирования места развертывания сети; показано, что для успешного планирования необходим специальный инструментарий. Описаны аспекты развертывания, связанные с политикой обеспечения безопасности WLAN, и инструментарий, необходимый для управления сетью.

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

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

Одно важное примечание. Индустрия WLAN развивается экспоненциально. Каждый день производители предлагают нововведения, благодаря которым WLAN становятся более защищенными, удобными в развертывании и управлении и, самое главное, более рентабельными. Эта книга не задумывалась как итоговое описание WLAN. Ее задача — предоставить основные сведения сетевому администратору, чтобы он знал, как следует планировать, развертывать WLAN и работать с ними. Мы выбирали темы и примеры из мира реальных проблем, с которыми сами встречались при разработке изделий в компании Cisco Systems и о которых узнали от многих компаний, которые оценивают 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, нравится или нет вам эта книга, а также выскажите свое мнение о том, как сделать наши книги более интересными для вас.

Посылая письмо или сообщение, не забудьте указать название 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 координаты:

E-mail: `info@williamspublishing.com`

WWW: `http://www.williamspublishing.com`

Информация для писем из:

России: 115419, Москва, а/я 783

Украины: 03150, Киев, а/я 152

В этой главе...

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

Глава 1

Технологии Ethernet

Беспроводные локальные сети (WLAN) — это новейшая технология, пытающаяся завоевать сердца потребителей. Сети WLAN, иногда называемые "беспроводные Ethernet", или Wi-Fi (от 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 логических 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 2, 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 необходимы уже обработанные фреймы или пакеты, которые вступают в коллизии на всем "протяжении" уровня. Базовый уровень может быть или уровнем 2 (несегментированный уровень), или уровнем 3.

Хотя технологии Ethernet применимы 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 X3T9 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 взаимодействие 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.
- Технология множественного доступа с контролем несущей и обнаружением коллизий (CSMA/CD).
- Общая среда передачи.

Ethernet 802.3 и модель OSI

Подробное рассмотрение модели OSI не входит в наши задачи, но для оценки перспектив технологии Ethernet нам следует рассмотреть уровень 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 802.5 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.

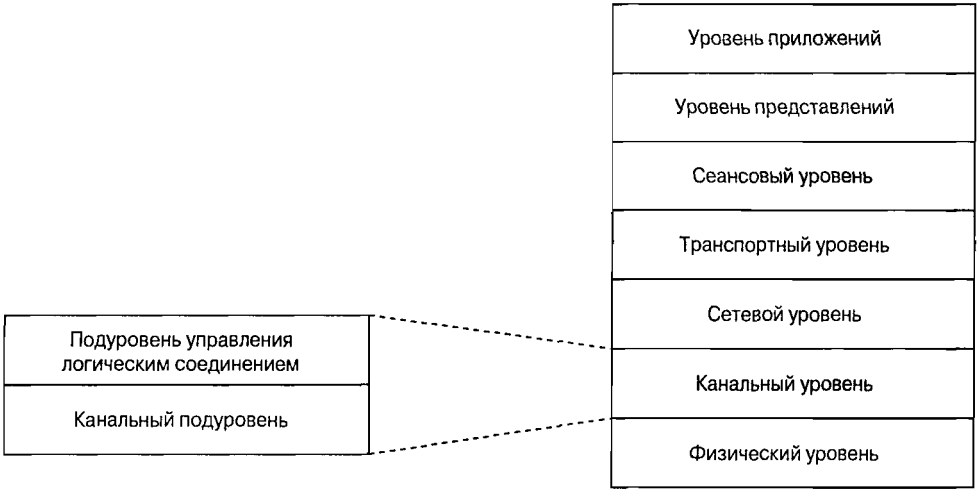


Рис. 1.1. Эталонная модель OSI

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.

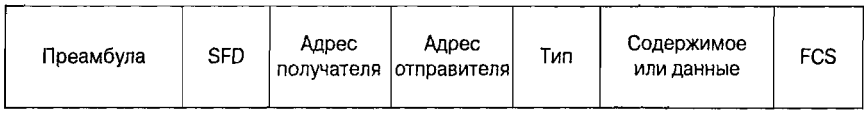


Рис. 1.2. Структура фрейма Ethernet

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

Преамбула. Представляет собой набор из семи октетов (октет содержит 8 битов), т.е. всего 56 бит, поочередно принимающих значение 0 и 1. Каждый 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 преамбулы, хотя нужды в них уже нет.

Флаг начала фрейма (start of frame delimiter, SFD). Представляет собой 8-битовое поле, содержащее битовую комбинацию, аналогичную таковой октетов заголовка, но оба последних разряда имеют значение 1 (10101011). 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/lenth/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* (Ethertype value). В табл. 1.1 представлены некоторые наиболее часто используемые значения режима работы Ethernet.

Таблица 1.1. Некоторые наиболее часто используемые значения режима работы Ethernet

Значение режима Ethernet	Что оно означает
0800	Internet Protocol (IP)
0806	Протокол разрешения адресов (ARP)
0BAD	Banyan Systems
6004	Протокол сетевого виртуального терминала, разработанный Digital Equipment Corporation (LAT)
8037	Internetwork Packet Exchange (IPX) (межсетевой 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)
86DD	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 шанса приема пакета всем станциям. 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 составлял как минимум 46 бит.

Контрольная последовательность 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 величины совпадают, считается, что фрейм не содержит ошибок (рис. 1.3).

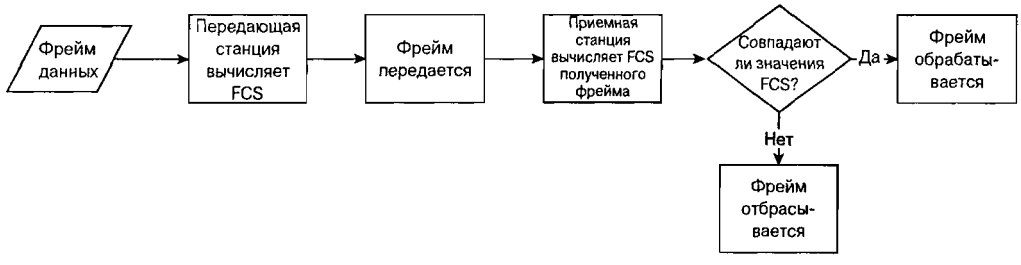


Рис. 1.3. Вычисление значения FCS

Адресация в Ethernet

Адреса Ethernet представляют собой 48-разрядные значения, которые однозначно идентифицируют Ethernet-станции локальной сети. Ethernet-адреса отчасти назначаются в рамках глобальной системы идентификации (курируемой IEEE), отчасти — производителями 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 мира и быть однозначно идентифицирована. Поскольку при такой системе адресации используется физический интерфейс, ее также называют *MAC-адресация*. В большинстве случаев MAC-адреса представляются в шестнадцатеричной форме, причем каждый байт отделяется дефисом или двоеточием, либо каждые два байта отделяются точкой. Например, Ethernet-адрес маршрутизатора Cisco может быть таким:

```
00-03-6b-48-e9-20
```

Это же значение можно представить как

```
00:03:6b:48:e9:20 или 0003.6b48.e920
```

Организация IEEE назначила для Cisco первые 24 бита, `00-03-6b`. Оставшиеся 24 бита, `48-e9-20`, назначаются устройству компанией Cisco. Уникальный организационный идентификатор `00-03-6b` позволяет данному производителю назначать адреса в диапазоне `00-03-6b-00-00-00-00-03-6b-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 говорят одновременно, слушателям трудно их понять, поэтому они должны замолчать и подождать, пока линия освободится, прежде чем вновь начать говорить.

Очень похожим образом функционирует Ethernet. Отвечающая за контроль несущей часть CSMA/CD опирается на возможность станций определять, используется ли среда Ethernet в данный момент. На самом деле никакого сигнала несущей нет, поэтому в действительности станции выявляют отсутствие сигнала; это говорит о 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 *коллизий* фреймов. Коллизия возникает, когда две станции пытаются одновременно передавать информацию через одну и ту же среду. Данные, переданные как одной, так и другой станцией, использовать нельзя, поэтому станции должны повторно передать информацию. Наконец, обнаружение коллизий 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 широковещательного домена. Устройства могут быть соединены с использованием хабов, повторителей, коммутаторов или мостов. Правила, установленные для сетей Ethernet стандарта 802.3, 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 составляет 2800 м. Время, необходимое фрейму Ethernet для преодоления диаметра сети, называется *интервалом Ethernet* (slot time Ethernet).

На заметку

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

Рассмотрим рис. 1.4, на котором представлены две станции, расположенные на противоположных сторонах широковещательного домена.

- Станция А передает фрейм размером менее 512 бит.
- В тот же самый момент времени начинает передачу фрейма станция В.
- Станция А передает последний бит фрейма.
- Станция А не обнаруживает коллизию при передаче и выгружает фрейм из буфера передачи.
- Станция А полагает, 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.

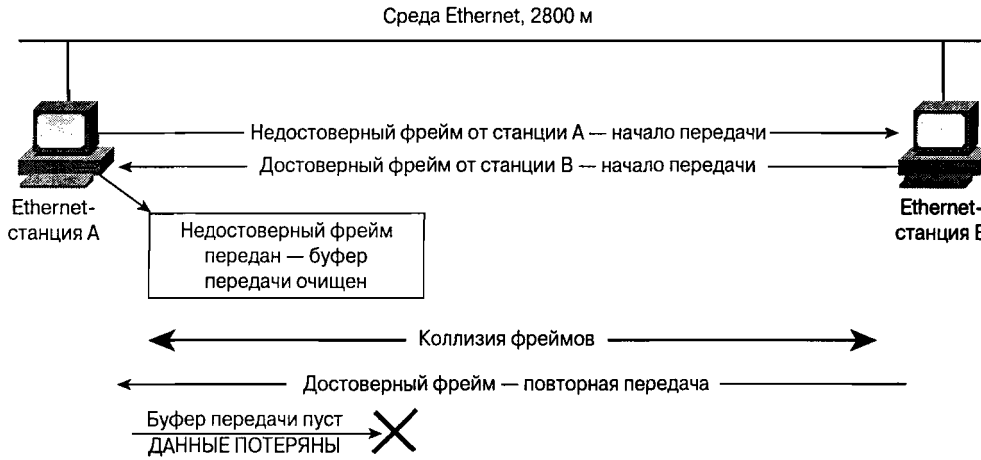


Рис. 1.4. Коллизия в широковещательном домене

Этот сценарий справедлив и для случая, когда протяженность 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 многоадресатная 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. Его называют "адрес все единицы", потому что все его биты имеют значение 1 (или `ff` в шестнадцатеричном виде). Широковещательный адрес может иметь вид `ff-ff-ff-ff-ff-ff` или `ffff-ffff-ffff`. Станция, намеревающаяся передать фрейм всем станциям, посылает фрейм, в котором в качестве адреса приемника указывается широковещательный адрес.

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

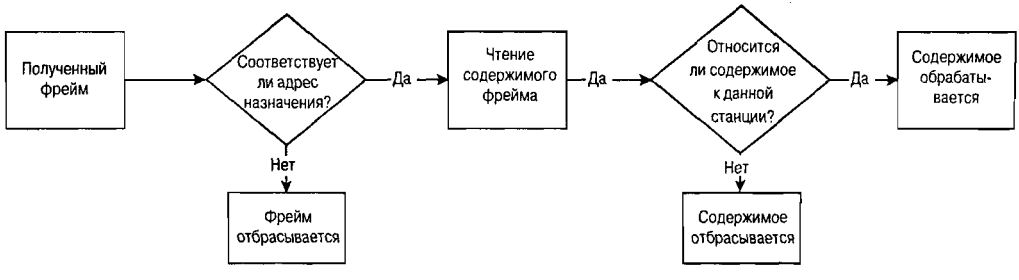


Рис. 1.6. Станция определяет, должна ли она обрабатывать фрейм

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

даря 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 многоадресатные фреймы должна быть "проведена подписка"; это означает, что станция-приемник должна изъявить желание получать их. Если станция-приемник не подписалась на многоадресатные фреймы, предназначенные определенной группе станций, она отвергает эти фреймы.

В качестве примера рассмотрим процесс передачи для станции потокового видеосигнала. Обычно при этом скорость передачи высокая, и если источник передает видеопоток всем станциям широковещательного домена, станция, которая не использует активно видеопоток, тратит большое число тактов ЦП на обработку и отбрасывание содержимого фреймов. Общепринятый механизм работы с содержимым потокового видео — *многоадресатное IP-вещание*. Фреймы многоадресатного IP-вещания передаются по предназначенным специально для этого IP-адресам, содержащим MAC OUI `01-00-5E`. Например, расширенный протокол маршрутизации между шлюзами (EIGPR), или протокол маршрутизации IP, посылает данные об обновлении маршрутов многоадресатной группе IP 224.0.0.10. Эта группа соответствует Ethernet-адресу `01-00-5E-00-00-0A`. Все устройства, которые заинтересованы в получении данных об обновлении маршрутов EIGPR, получают фреймы с этим адресом получателя. Устройства, не подписавшиеся на получение данных об обновлении маршрутов EIGPR, отвергают такой фрейм.

Вообще говоря, многоадресатные и широковещательные фреймы могут снизить нагрузку на сеть, позволяя станциям посылать один фрейм многим станциям-приемникам одновременно. Но если передающая станция направляет фреймы небольшому числу приемных или даже одной станции, широковещательный и многоадресатный трафики могут вызвать ненужную загрузку станций, которым эти фреймы не предназначены.

Одноадресатная рассылка представляет собой простейший и прямой способ передачи данных станции-получателю. 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 все три метода адресации, благодаря чему приложения могут использовать наиболее приемлемый для них метод и тем самым снижать 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 упомянуты нами из-за малости инсталляционной 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 основе неэкранированных витых пар (категории 3), предназначенных для передачи речевого сигнала с использованием только двух пар проводов. Хотя разновидность 10BASE-T требует применения кабелей только категории 3, многие используют в таких сетях кабель категории 5 в расчете на дальнейшую модернизацию сетей до уровней 100BASE-TX или 1000BASE-T. Кроме того, кабели категории 5 имеют более высокие характеристики, что позволяет повысить качество сигнала. Термин 10BASE-T означает способность

среды передавать сигналы со скоростью 10 Мбит/с с использованием основной полосы пропускания 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 2800 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 (такому как повторитель, 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). Преимущество топологии "звезда" (на физическом уровне) состоит в том, что выход из строя кабеля, соединяющего с сетью одну из станций, не влияет на способность других станций работать в сети.

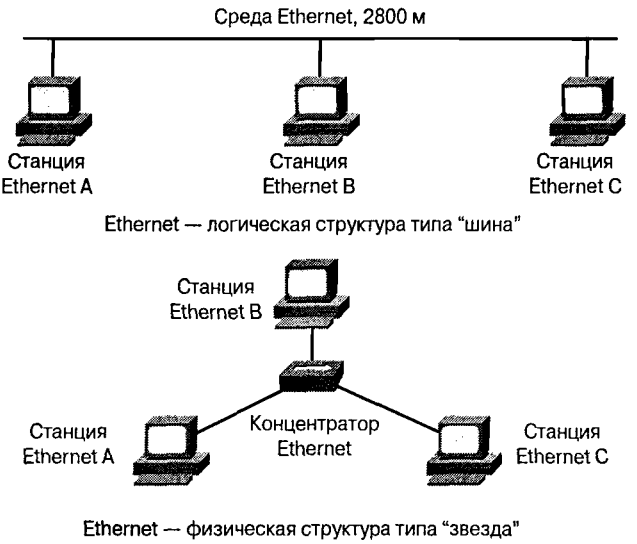


Рис. 1.7. Топология 10BASE-T

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 большую сторону. 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 Т-образных соединителей. Повреждение кабеля на любом участке приводит к выходу из строя всей сети.

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

станции должны быть оснащены недешевыми трансиверами, которые подключаются к среде передачи через ответвления. Как и в случае с 10BASE2, повреждение кабеля на любом участке приводит к выходу 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 используют 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 успокоить массы, в 1995 году IEEE анонсировала 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 ориентируется на спецификацию 100BASE-X и кабели 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 в основном высокочастотных сигналов и требует кабелей более высокого качества, нежели кабель категории 3, используемый в сетях 10BASE-T. Ограничения на расстояния 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 преодолеет 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 2800 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 коллизию 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 средой передачи является многомодовое оптическое волокно. Сетевая карта преобразует электрические сигналы в световые импульсы, которые передаются по волокну сетевой карте приемной станции. Эта сетевая карта осуществляет обратное преобразование световых 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 полудуплексном 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 многомодового волокна с отношением диаметров 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 одномодовое волокно и соответствующие приемопередатчики; в этом случае максимально допустимое расстояние превышает 40 км. Стоимость одномодового волокна и предназначенных для работы с ним приемопередатчиков на порядок превышает стоимость таковых для многомодового, но техническое решение проблемы существует, 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 селекторное 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 802.3x, 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.

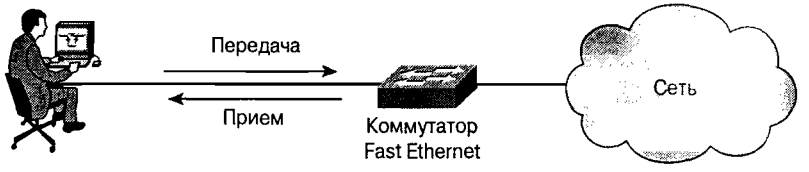


Рис. 1.8. Работа в полнодуплексном режиме

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 станции полнее использовать возможности среды передачи. Доступная станции ширина полосы пропускания теоретически удваивается, поскольку станция имеет полный доступ к среде как при передаче, так и при приеме сигналов. В случае использования техно-

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, которые недоступны конечным станциям. 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, поэтому эти звенья сети способны получить максимальную пользу от расширения полосы пропускания, обеспечиваемого полнодуплексным режимом работы.

Полнодуплексный режим работы позволяет технологиям Ethernet избежать ограничений на расстояние передачи, 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 рассогласования" (duplex mismath errors). Эти ошибки появляются при соединении полудуплексной и полнодуплексных станций. В результате возникает множество ошибок при передаче пакетов, таких как запоздалая 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 сличать 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 пропорций столь же резкий переход для пользователей, 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 10BASE-T и 100BASE-TX, может использовать кабели с неэкранированными витыми парами длиной не более 100 м.
- **1000BASE-X** имеет три варианта.
  - **1000BASE-SX**. Волоконно-оптическая среда передачи на основе стандартных многомодовых волокон, предназначенная для использования на короткие расстояниях (до 200 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 помнят, поначалу 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 разводку, 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 поддержал этот стандарт. Однако когда пришло время предложить гигабитовое решение для стандарта Ethernet, разработчики позаимствовали все лучшее из всех стандартов на 100 Мбит/с и объединили их в спецификации на технологию 1000BASE-T.

Стандарт 802.3z 1000BASE-X

Стандарт 802.3z был утвержден в 1999 году и включен 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, отсюда 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: максимальное расстояние 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 основанное на применении меди решение, в котором используются кабели, выполненные на основе предварительно закрученных (precrimped) экранированных витых пар. Соединитель — не простой RJ-45, обычно используемый в 10/100/1000BASE-T. Вместо него используется или DB-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 ограничена 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 совершенно 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 "набивать" полезную часть фрейма бесполезной информацией, этот стандарт вводит новую характеристику, получившую название *расширение несущей* (carrier extension).

Предположим, 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 станциям 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 передаются также в 7 раз более многочисленные биты расширения несущей. Это — явное расточительство по отношению к полосе пропускания. Для снижения "накладных расходов" стандарт предписывает в качестве дополнительного использовать *пакетный режим* (burst mode), позволяющий решить проблему диаметра сети и неэффективного использования полосы пропускания.

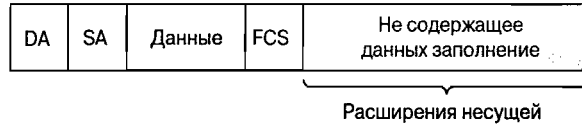


Рис. 1.9. Расширение несущей в Gigabit Ethernet

Пакетный метод позволяет объединять небольшие фреймы; в промежутках между ними передаются биты расширения несущей. Другие станции ожидают очереди на передачу, "глядя" 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. 1.10). Этот механизм, хотя и не свободен от недостатков, все же позволяет полнее использовать возможности среды, чем это происходит при использовании только расширения несущей.

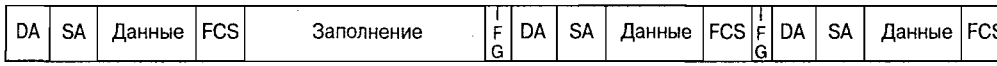


Рис. 1.10. Метод пакетирования в среде Gigabit Ethernet

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 многочисленные комбинации скоростей передачи и дуплексных режимов, для оценки 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 волоконной оптики, не поддерживают автоматическое согласование; это относится ко всем типам волоконно-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 представлена иерархия предпочитаемых 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 станции. Допустим, станция старого образца 10BASE-T может быть подключена

к коммутатору, поддерживающему автоматическое согласование. Коммутатор посылает станции 10BASE-T быстрый канальный импульс, предлагая работу в полнодуплексном режиме со скоростью 100 Мбит/с. Станция 10BASE-T "не понимает", что означает полученный импульс, и игнорирует сигналы автосогласования. Иначе говоря, станция 10BASE-T не способна послать быстрый канальный импульс, поскольку не поддерживает технологию автосогласования. Порт коммутатора "понимает", что его быстрый канальный импульс проигнорирован и что, следовательно, он имеет дело со станцией типа 10BASE-T. В данном случае, поскольку станция 10BASE-T не поддерживает автоматическое согласование, коммутатор возвращается к "наименьшему общему знаменателю", которым и является станция 10BASE-T.

Хорошо, но что будет, если используется станция 100BASE-TX, работающая в полудуплексном режиме и не поддерживающая автоматическое согласование? Неужели она начнет тупо работать в режиме станции 10BASE-T? Ответ отрицателен. Быстрые канальные импульсы основаны на канальных импульсах сети (network link pulse, NLP), описанных в стандарте Ethernet. Канальные импульсы сети — это периодически посылаемые импульсы, своего рода "пульс" Ethernet. Быстрые канальные 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 канальные импульсы, указывающие коммутатору, что данная станция способна работать на скорости 100 Мбит/с. Именно благодаря этой информации устройствам, поддерживающим автосогласование, 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. Использующая 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), единственная возможность — дуплексный режим. В отличие от Ethernet и Fast Ethernet, быстрые канальные 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

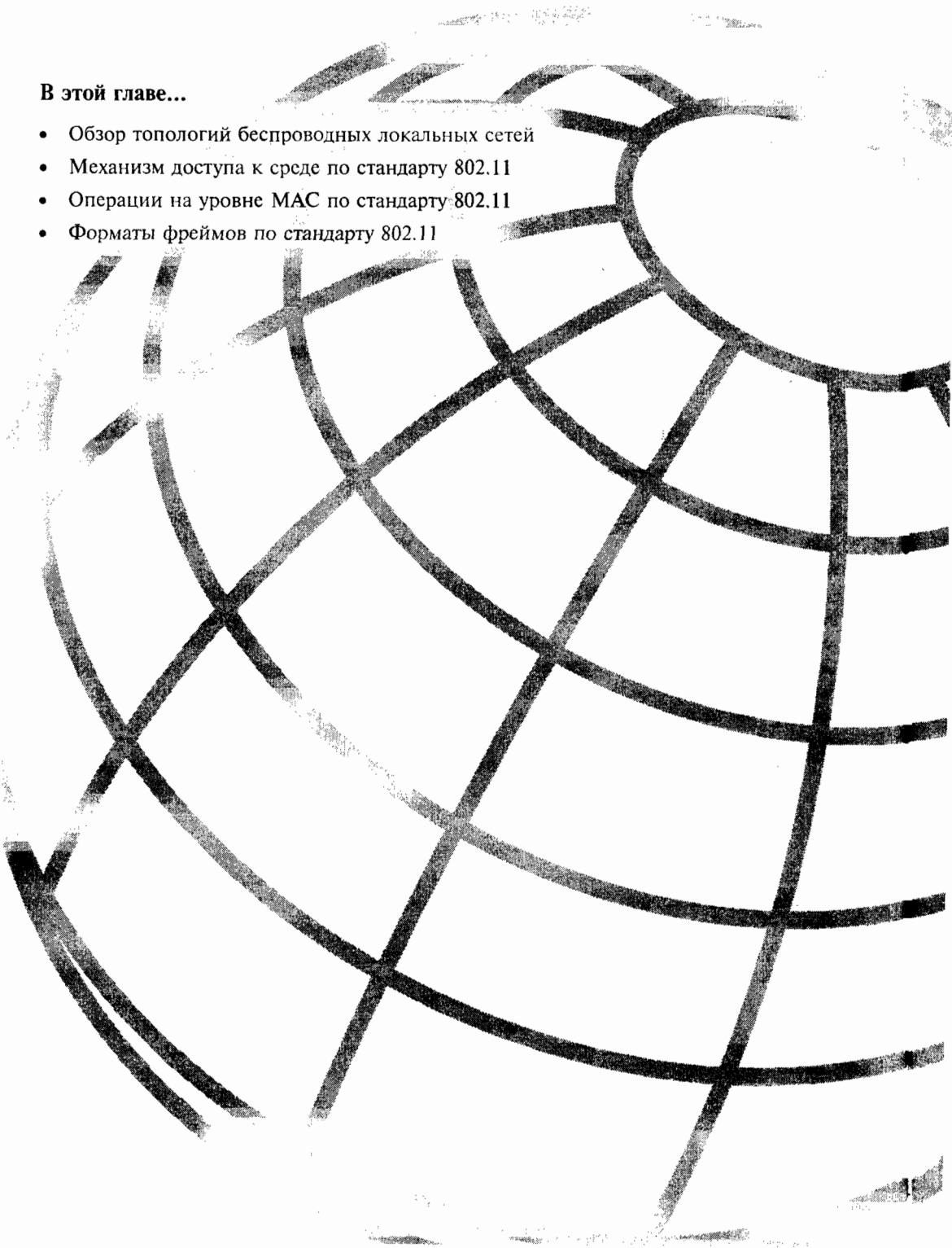
Ethernet эволюционирует, стараясь удовлетворить новым требованиям, предъявляемым к ней пользователями и администраторами сетей. Она продолжает эволюционировать и после появления Gigabit Ethernet — на горизонте уже маячит Ethernet 10 Гбит/с. В табл. 1.3 приведены основные параметры (топология и среда 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 проводного 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	Экранированная витая пара	25
1000BASE-SX	1000	Двухжильный многомодовый волоконно-оптический кабель	
1000BASE-LX	1000	Двухжильный одномодовый волоконно-оптический кабель	10 000

В этой главе...

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



Глава 2

Беспроводные локальные сети стандарта 802.11

Беспроводные локальные сети стандарта 802.11 получают все большее распространение в основном благодаря тому, что они просты в развертывании и удобны в эксплуатации. С точки зрения пользователя их функции и характеристики точно такие же, как и у разделяемых (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 сети с контролем несущей и обнаружением коллизий. Вследствие этого для доступа к среде необходим 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 волен 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 широковещательных сигналов через эфир на несущей в диапазоне радиочастот. Принимающая станция может получать сигналы в диапазоне работы нескольких передающих станций. Передающая станция вначале передает идентификатор зоны обслуживания (service set identifier, SSID). Станция-приемник использует SSID для фильтрации получаемых 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 называют специальной, или неплановой (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 связываться одна с другой.

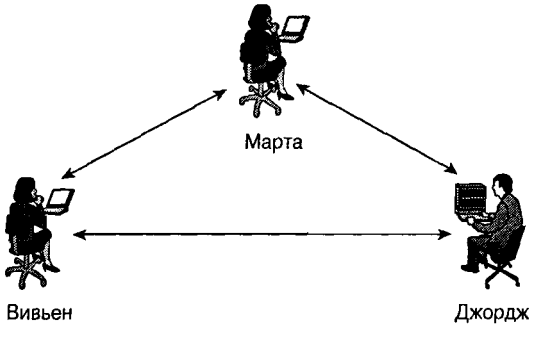


Рис. 2.1. Неплановая (ad-hoc) сеть (IBSS)

Специальная сеть, или независимая базовая зона обслуживания (IBSS), возникает, 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 устанавливают соединения друг с другом, в результате чего создается только одна базовая зона обслуживания (BSS), не имеющая интерфейса для подключения к проводной локальной сети (т.е. отсутствует какая-либо распределительная система, которая необходима для объединения BSS и организации таким образом ESS). Не существует каких-либо оговоренных стандартом 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 один с другим вследствие проблемы скрытого узла (hidden node issue). Несмотря на это, в IBSS не существует какого-либо механизма для реализации фунции ретрансляции.

Поскольку в IBSS отсутствует точка доступа, распределение времени (timing) осуществляется нецентрализованно. Клиент, начинающий передачу в IBSS, задает сигнальный (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) из предыдущего TBTT.
- Определяет новую случайную задержку.
- Если маячковый сигнал поступает до окончания случайной задержки, возобновляет работу приостановленных таймеров задержки. Если никакой маячко-

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

Вы видите, что распределение времени для передачи маячковых сигналов осуществляется в специальных сетях не точкой доступа 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 неплановой сети по клиенту с самым быстрым таймером. В больших распределенных неплановых сетях, когда многие клиенты не могут связываться напрямую, может понадобиться некоторое время для достижения синхронизации всех клиентов.

Базовые зоны обслуживания (BSS)

BSS — это группа работающих по стандарту 802.11 станций, связывающихся одна с другой. Технология BSS предполагает наличие особой станции, которая называется *точка 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 направляет фреймы станции-адресату. Точка доступа может иметь порт восходящего канала (uplink port), через который BSS подключается к проводной сети (например, восходящий канал Ethernet). Поэтому BSS иногда называют инфраструктурой BSS. На рис. 2.2 представлена типичная инфраструктура BSS.

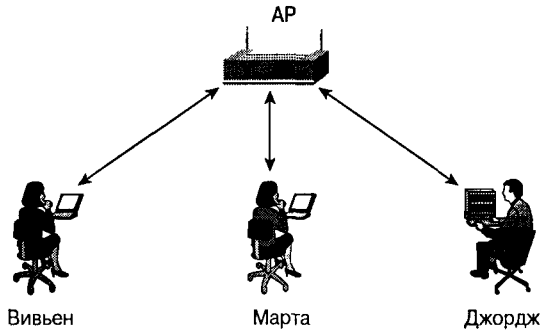


Рис. 2.2. Инфраструктура беспроводной локальной сети BSS

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). Восходящий 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 восходящие каналы к распределительной системе представляют собой каналы проводной Ethernet.

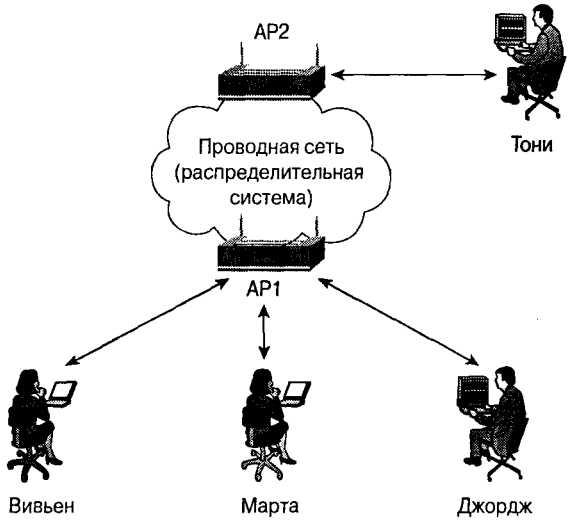


Рис. 2.3. Расширенная зона обслуживания ESS беспроводной локальной сети

Механизм доступа к среде стандарта 802.11

В главе 1, "Технологии Ethernet", описан механизм доступа к среде CSMA/CD, применяемый в сетях Ethernet, функционирующих в соответствии со стандартом 802.3. Основывающиеся на стандарте 802.11 беспроводные сети используют похожий механизм, который называется "множественный 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, увеличивают уровень сигнала в проводнике, и 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, "Технологии Ethernet", технология CSMA/CD сравнивается с селекторным совещанием. Каждый участник, желающий что-то сказать, должен подождать, пока не перестанет говорить другой. Если линия свободна, участник должен попы-

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 селекторного 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 выступающим 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 получают подтверждения того, что были услышаны.

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

Реализация технологии CSMA/CA стандартом 802.11 осуществляется при посредстве распределенной функции координации (distribted coordination function, DCF). Прежде чем описывать работу CSMA/CA, имеет смысл вначале описать 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 намеревается 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 PSY (уровня 1) на предмет наличия несущей.
- Использование виртуальной функции контроля несущей, вектора распределения сети (network allocation vektor, 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 осуществить передачу фрейма и получить подтверждение его приема. 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, хранимое 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.

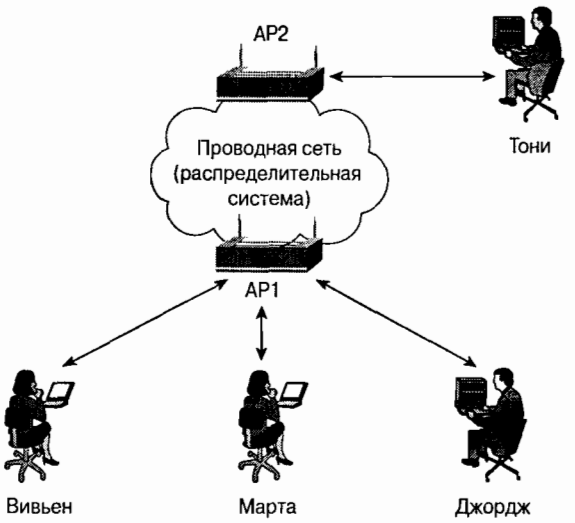


Рис. 2.4. Процесс обновления вектора распределения сети

Распределенная функция координации (DCF)

Утвержденный IEEE механизм доступа 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, намеревающаяся передать фрейм, должна выждать определенное время после того, как среда освободится. Этот интервал времени называется *межфреймовый зазор DCF* (DCF interframe space, DICF). По истечении интервала времени DICF станция может принять участие в состязании за право доступа к среде.

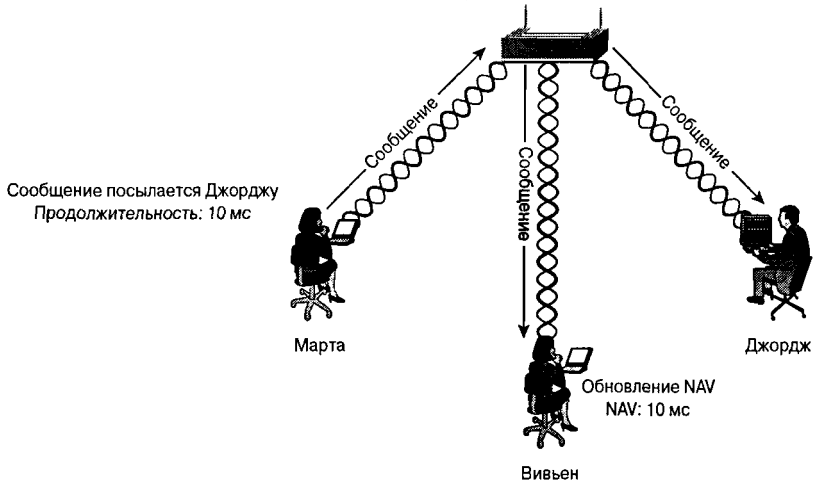


Рис. 2.4. Временная диаграмма доступа к среде с использованием распределенной координирующей функции (DCF)

В случае, проиллюстрированном на рис. 2.5, Вивьен 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 освободится. Существует большая вероятность того, что обе станции одновременно попытаются начать передачу тотчас 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 (contention window, CW). По умолчанию значения CW устанавливаются производителем и хранятся 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 описываемом 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, задаваемой 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 в окне конкуренции, должна воздерживаться от передачи. Канальный интервал (slot time) — это значение времени, определяемое параметрами физического уровня, основанными на характеристиках радиочастотного канала BSS.

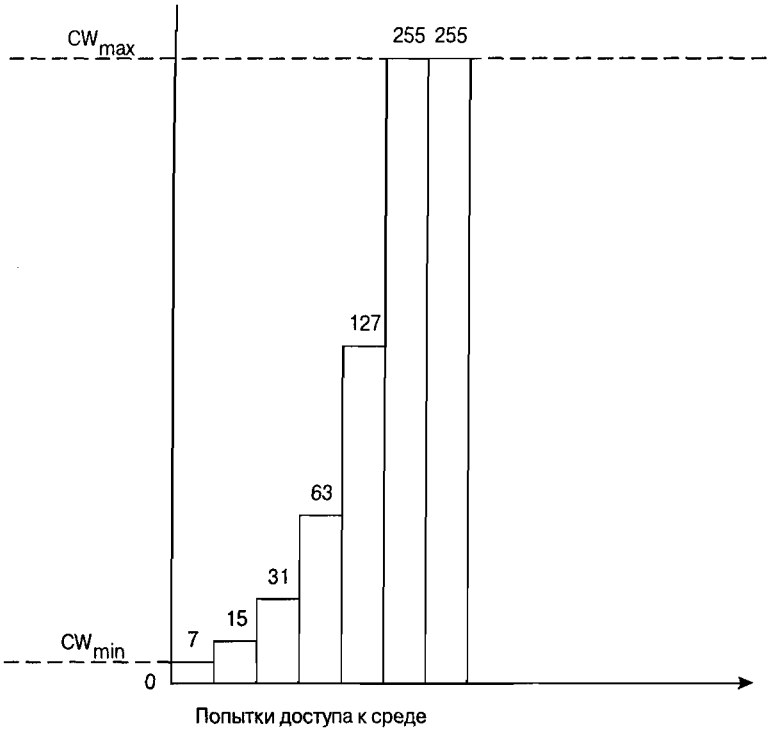


Рис. 2.6. Случайная задержка при доступе к среде с использованием DCF

Возвратимся к нашему примеру. Вивьен готова 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 воздерживается от передачи в течение выбранного количества канальных интервалов. Этот процесс проиллюстрирован на рис. 2.7, где случайное значение задержки составляет 4 канальных интервала.

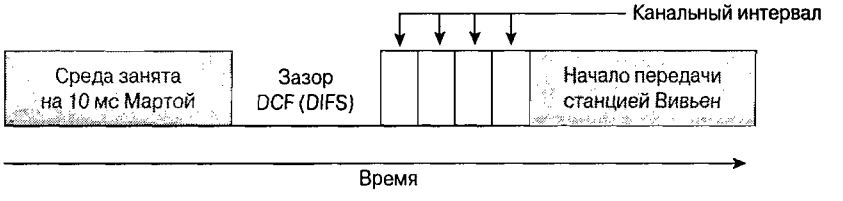


Рис. 2.7. Передача фрейма по истечении времени случайной задержки

По прошествии четырех канальных интервалов Вивьен может начать передачу. Но что произойдет, если станция Джорджа имеет случайное время задержки, равное двум канальным интервалам? Вивьен получает новое значение поля продолжительности из фрейма станции Джорджа, когда она начинает передачу, и обновляет свой NAV, присваивая 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 отложить передачу на все четыре канальных интервала, она передает фрейм. Но как станция Вивьен узнает, что этот фрейм получен станцией назначения? Спецификация 802.11 требует, чтобы принимающая станция передала станции-отправителю фрейм подтверждения. 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, удваивает ширину 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.

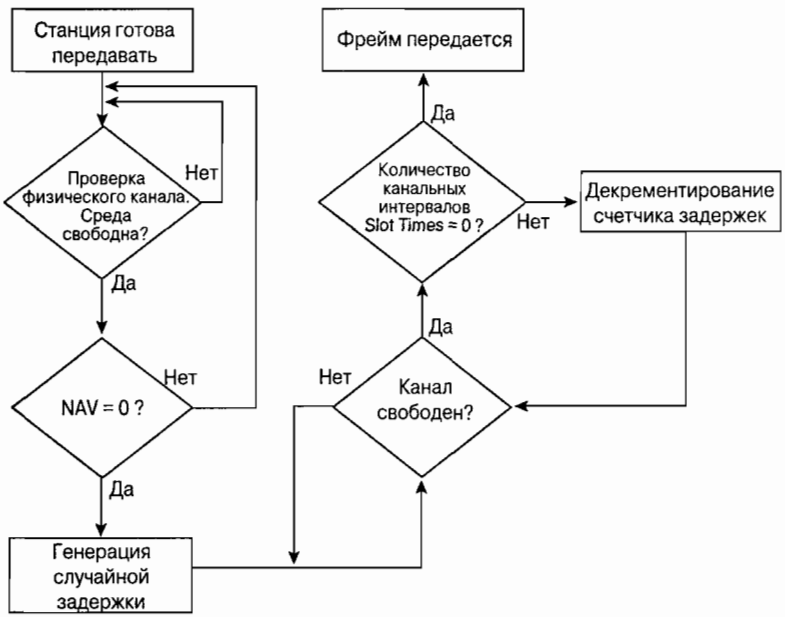


Рис. 2.8. Процесс доступа к среде с использованием DCF

Фрейм подтверждения

Станция, получившая фрейм, подтверждает факт его безошибочного приема путем отправки передающей станции фрейма подтверждения. Узнав, что приемная 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 подтверждения — это особый случай. Фреймам подтверждения разрешается не принимать участия в процессе случайной задержки, долго ждать возможности передать подтверждение после получения фрейма не приходится. Короткий промежуток времени, который приемная станция проводит в ожидании такой возможности, называется *короткий межфреймовый зазор* (short interframe space, SIFS). Интервал SIFS короче, чем интервал DIFS, на два канальных интервала. Это гарантирует принимающей станции наибольший шанс получения доступа к среде для передачи по сравнению с другими станциями.

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

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

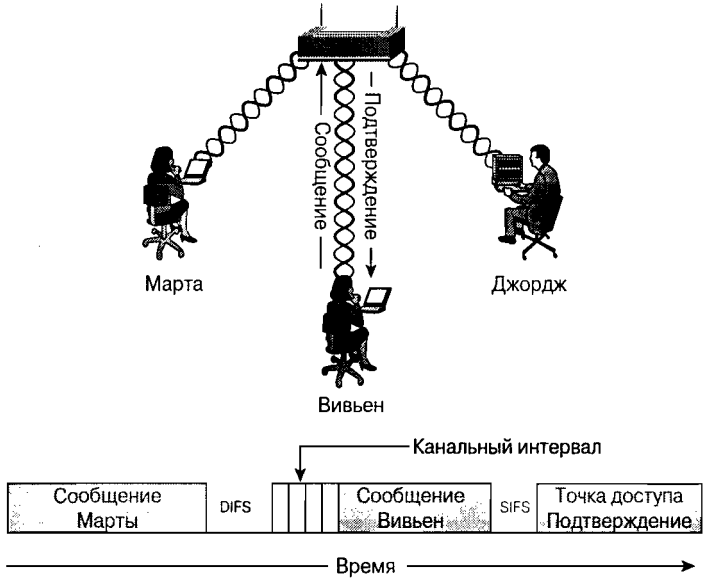


Рис. 2.9. Передача фрейма и подтверждения

Предположим, что станция Вивьен не получила фрейм подтверждения. Тогда она удваивает ширину окна конкуренции CW до 15 и повторяет процесс задержки. При каждой неудачной 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 продолжать 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 получить доступ к среде 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 станция Тони невидима 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.

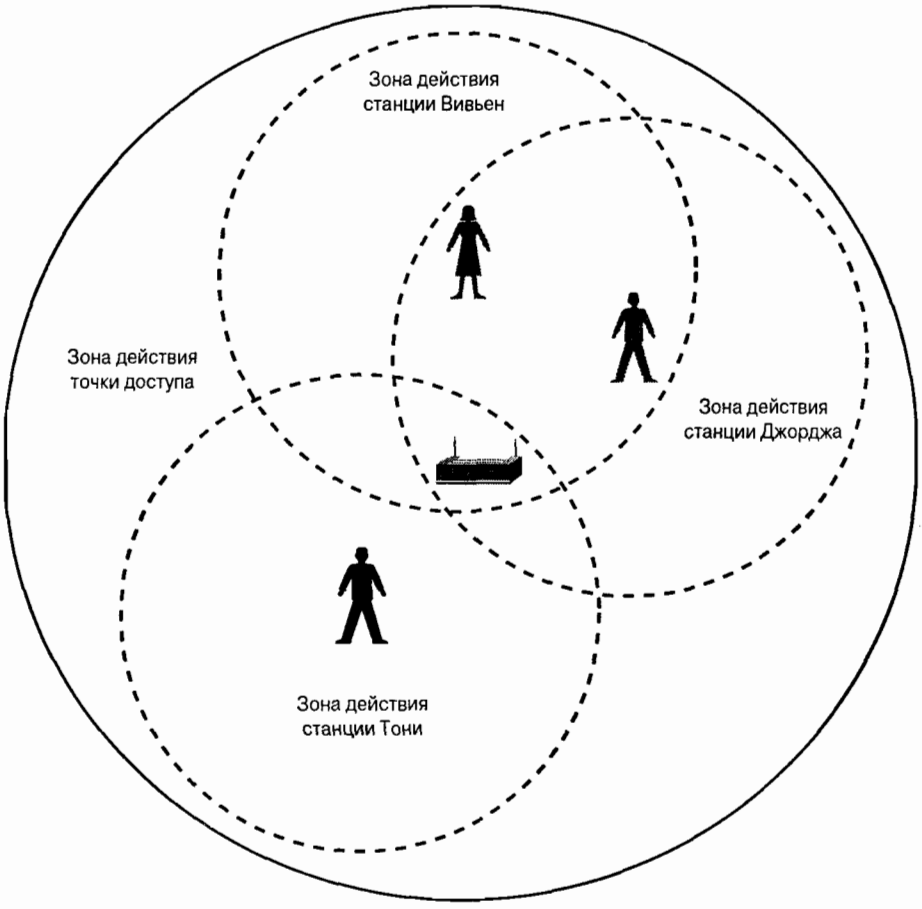


Рис. 2.10. Проблема скрытого узла

Точка доступа получает фрейм RTS от станции Вивьен и отвечает управляющим фреймом CTS (фреймом готовности к приему). Последний содержит поле продолжительности, 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 DCF, как любой другой фрейм. Но, аналогично фрейму подтверждения, соответствующий CTS-фрейм, передаваемый точкой доступа, минует 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. Станции Джорджа и Тони обновляют значения своих NAV одновременно, но фрейм подтверждения, который точка доступа передает станции Вивьен, не обязан подчиняться правилам DCF. После получения фрейма станция Джорджа немедленно отправляет обратно фрейм подтверждения. Хотя значение NAV станции Джорджа не равно 0, она все же посылает фрейм подтверждения точке доступа спустя время, задаваемое интервалом SIFS.

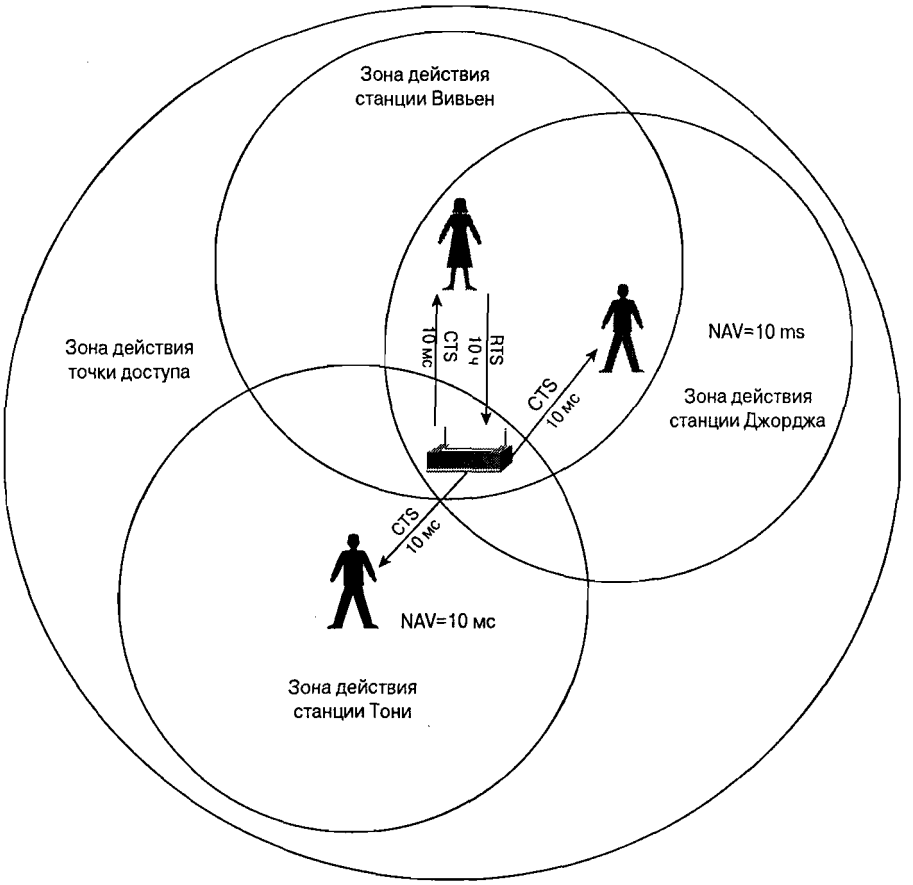


Рис. 2.11. Резервирование среды с помощью фреймов RTS/CTS

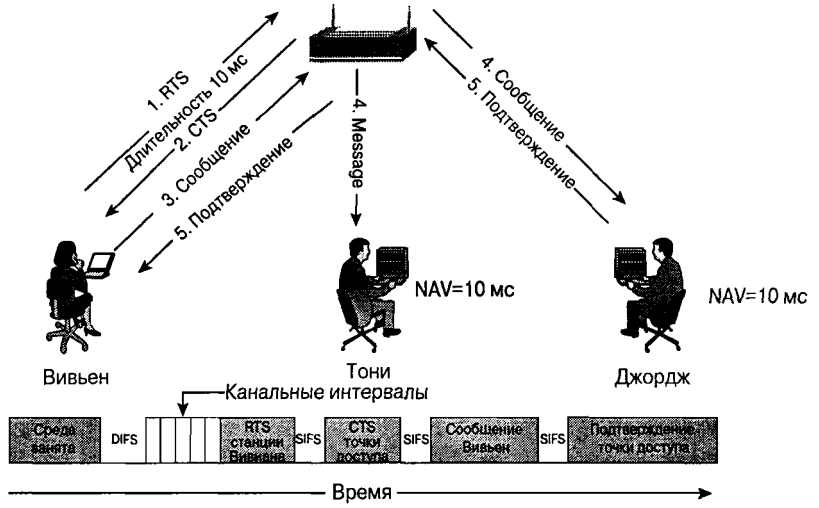


Рис. 2.12. Пример обмена фреймами RTS/CTS

Фрагментация фрейма по стандарту 802.11

Фрагментация фрейма — это выполняемая на уровне MAC функция, назначение которой — повысить надежность передачи фреймов через беспроводную среду. Под фрагментацией понимается дробление 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 передан с ошибкой или вступит в коллизию, только его придется передавать повторно, а не весь фрейм. Это увеличивает пропускную способность среды.

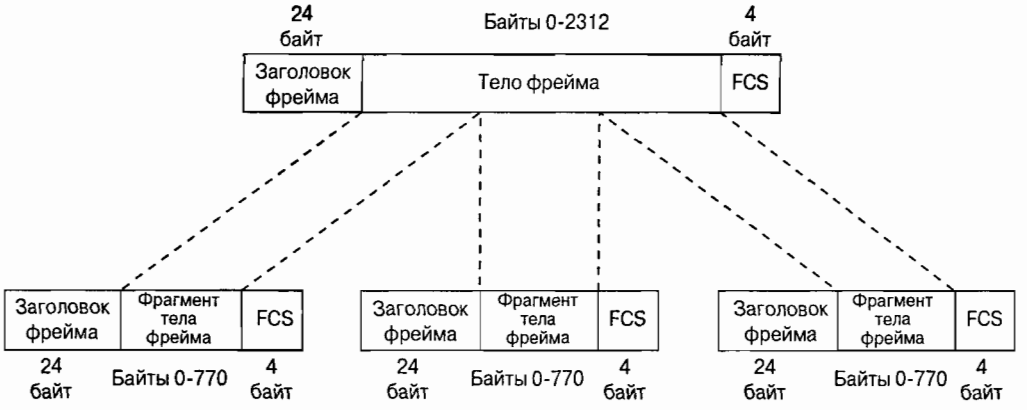


Рис. 2.13. Фрагментация фрейма

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

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, содержащуюся 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 подверженную конкуренции 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. неинформационных, сигналов) на протокол BSS. В результате его распространенность невелика. Предполагается, что с повышением качества и класса предоставляемых услуг передачи дан-

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

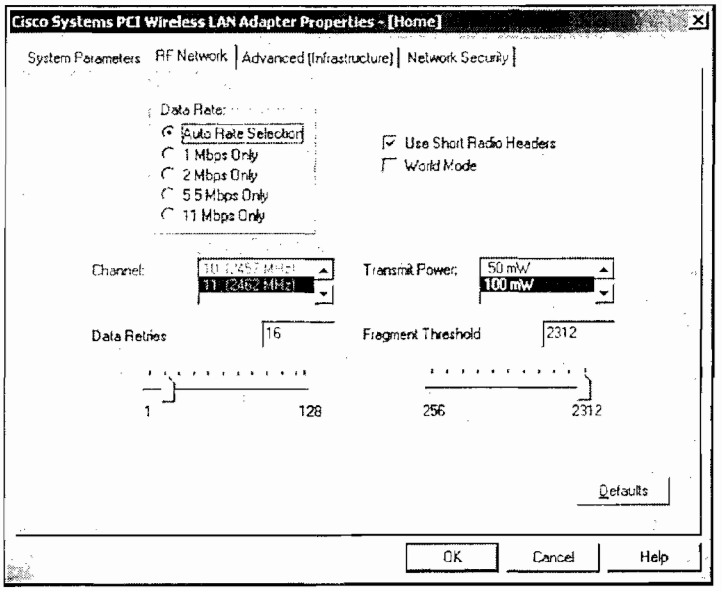


Рис. 2.14. Задание параметров дефрагментации устройств Cisco Aironet Wireless Adapters

В данном разделе рассказывается о работе механизма PCF, а именно о работе точки координации (point coordinator, PC) и реализующих механизм PCF станций (в спецификации 802.11 они называются станции CF-Pollable — станции, опрашиваемые 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 (а это означает, что работа PCF возможна только в инфраструктурах BSS). Каждый клиент 802.11 устанавливает значение NAV равным 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, соответствую-

щим оставшейся продолжительности CFP. На рис. 2.15 представлена временная диаграмма CFP и периода конкуренции (contention period, CP).

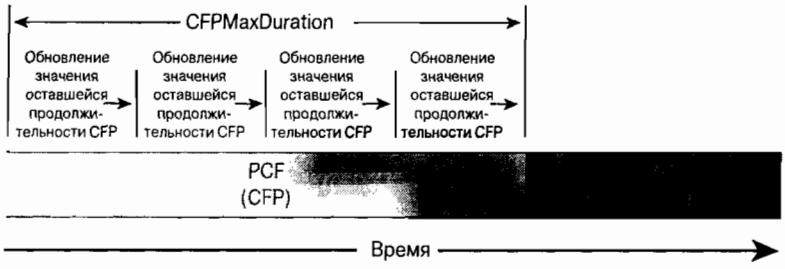


Рис. 2.15. Временная диаграмма CFP и CP

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 опрос. Точка координации может посылать 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 получать 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 *преимущественный межфреймовый интервал* (priority interframe space, PIFS). Интервал PIFS на один канальный интервал дольше, чем интервал SIFS, и на один канальный интервал короче, чем интервал DIFS, что позволяет PCF-станциям получать доступ к среде раньше DCF-станций. Вдобавок они могут использовать управляющие фреймы, такие как фреймы подтверждения, для обеспечения наивысшей 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 начальный 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 посылает 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.

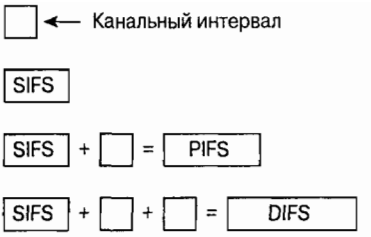


Рис. 2.16. Отношения между SIFS, PIFS DIFS и канальным интервалом

Пример работы PCF

Продолжая рассмотрение нашего примера, предположим, что Вивьен, Марта и Джордж связываются через точку доступа AP1 (рис. 2.17).

Точка доступа AP1 передает сигнальный фрейм, указывающий на начало периода CFP. Продолжительность периода CFP задана равной 20 с. Станции Вивьен, Марты и Джорджа обновляют значения своего NAV с тем, чтобы он соответствовал 20-секундному CFP. После ожидания, равного интервалу SIFS, AP1 передает фрейм, находящийся в ее буфере и предназначенный для станции Вивьен, а также опрашивает станцию Вивьен на предмет того, имеет ли она фреймы, предназначенные для пересылки с использованием комбинации фреймов данных и опроса (Data+CF-Poll). Станция Вивьен получает фрейм Data+CF-Poll и посылает один фрейм данных и не 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 в ответ на получение фрейма CF-Poll.

Точка доступа AP1 продолжает свою работу, посылая опросный лист Марте. AP1 использует другую комбинацию фреймов, для того чтобы послать фрейм данных станции Марты, 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 технология множественного доступа вполне позволяет поступать таким образом. Марта ждет в течение интервала SIFS и посылает фрейм Data+CF-ACK.

Наконец, AP1 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 передавать какие-то фреймы. Поскольку буфер станции Джорджа пуст, она посылает фрейм с нулевыми данными (null data frame). Хотя CFP еще не достиг своей максимально допустимой продолжительности, AP1 посылает фрейм CF-End (конец периода CF) для завершения периода, свободного от конкуренции, и переходит к периоду конкуренции (CP) 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-

ройствах, 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 (repeater aps).
- Универсальные клиенты (мосты рабочих групп).
- Беспроводные мосты.

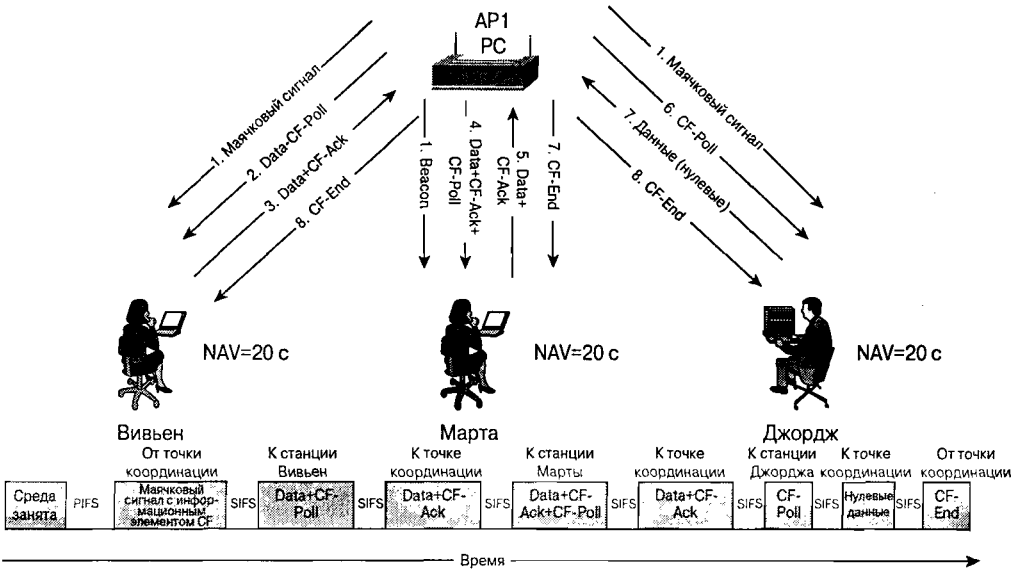


Рис. 2.17. Операция доступа к среде PCF

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 гарантий их способности к взаимодействию, 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 сопрягались с устройствами выбранного вами производителя или устройствами, для которых производитель гарантирует совместимость.

Точки доступа-повторители

Может случиться так, что окажется неудобно или непросто 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 Элейн 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, поступившие на его беспроводной интерфейс. Эта ретрансляция осу-

ществляется через тот же канал, через который пакеты были получены. Точка доступа-повторитель расширяет BSS, а также домен коллизий. Хотя она может оказаться эффективным средством, применять ее следует осторожно; наложение широковещательных доменов может привести к сокращению пропускной способности канала вдвое, потому что начальная точка доступа также "слышит" ретранслированный сигнал. Эта проблема может еще более обостриться при использовании цепочки точек доступа-повторителей. Кроме того, точка доступа-повторитель может ограничить вас в использовании клиентов с расширениями, которые позволяют им поддерживать привязку к службам и их использование через точки доступа-повторители. Несмотря на названные ограничения, весьма вероятно, что вы найдете применение точкам доступа-повторителям в вашей сети.

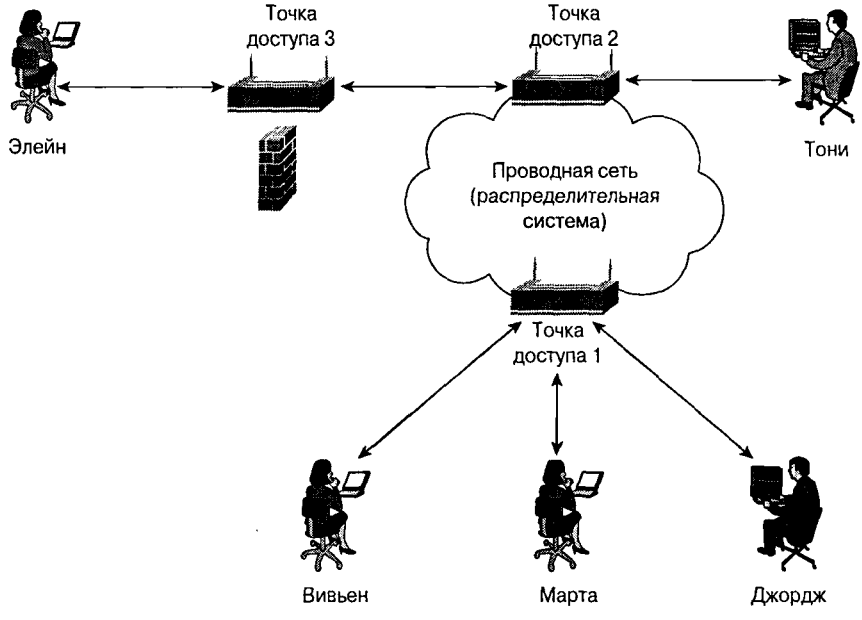


Рис. 2.18. Применение точки доступа-повторителя

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 кассовые терминалы магазинов, принтеры, устаревшие ПК, копировальные устройства и небольшие мобильные сети. Универсальный клиент или мост рабочей группы инкапсулирует полученные 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-

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

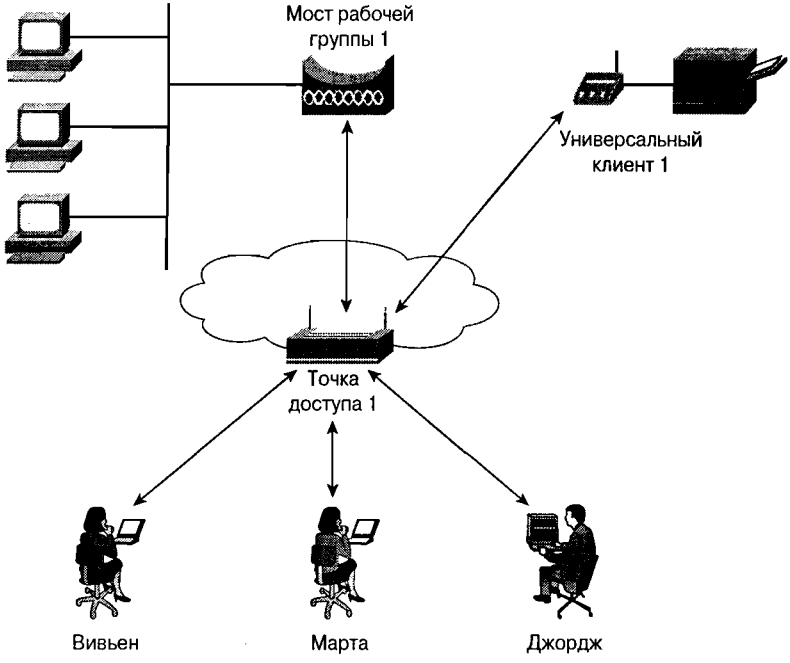


Рис. 2.19. Применение универсального клиента и моста рабочей группы

Беспроводные мосты

Если расширить концепцию моста рабочей группы до точки, в которой вы соединяете две или несколько проводных сетей, мы придем к концепции беспроводных мостов. Аналогично проводным мостам, беспроводные соединяют между собой сети. Вы можете соединять 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 из названных способны соединять большие сети, разнесенные 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 используются в основном технологии подуровней MAC и PHY стандарта 802.11, отдельные производители предлагают собственные патентованные методы инкапсуляции трафика проводной сети и для расширения в перспективе диапазона за ого-

воренный стандартами на подуровни MAC и PHY. Поэтому вам вновь придется проверить, сертифицирован ли ваш беспроводной мост на предмет совместимости.

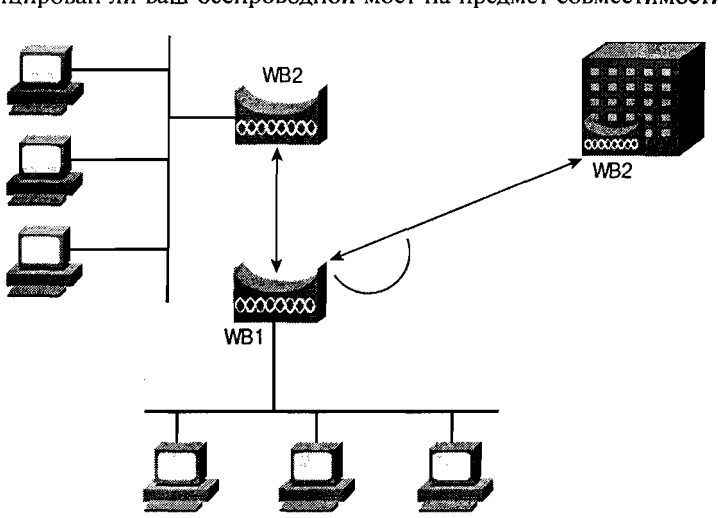


Рис. 2.20. Пример использования беспроводных мостов (WB)

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. Три сеанса обмена происходят между беспроводной станцией и точкой доступа.

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

Процесс зондирования

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

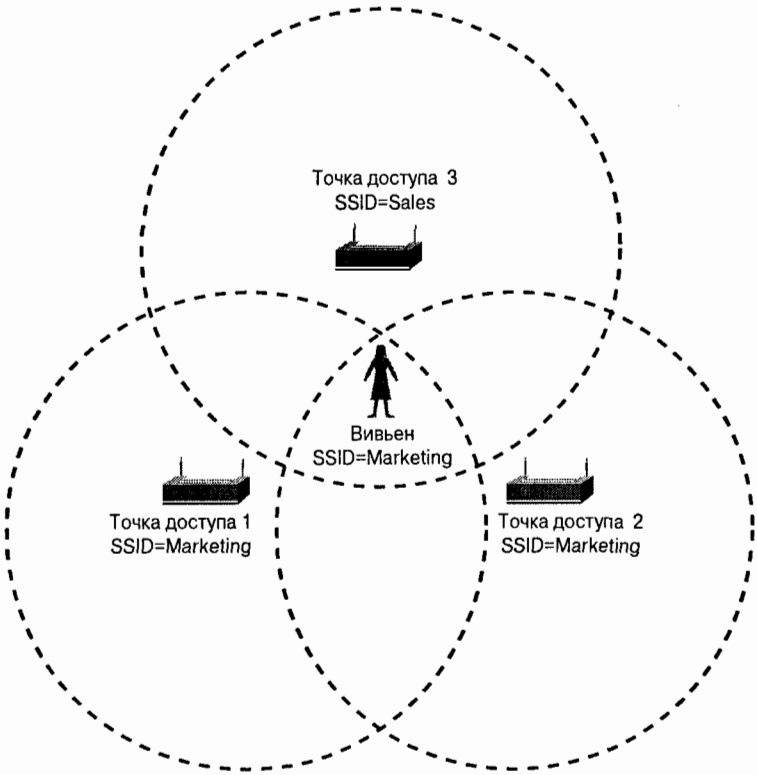


Рис. 2.21. Станция Вивьен и близлежащие точки доступа

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 оговорен 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 раз так, то многие за-

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

```
DLC: Signal level                    = 100%
DLC  Channel                         = 1
DLC: Data rate                       = 2 ( 1.0 Megabits per second)
DLC
DLC: Frame Control Field #1 = 40
DLC                 .... ..00 = 0x0 Protocol Version
DLC:                .... 00.. = 0x0 Management Frame
DLC                 0100 .... = 0x4 Probe request (Subtype)
DLC: Frame Control Field #2 = 00
DLC                 .... ...0 = Not to Distribution System
DLC:                .... ..0. = Not from Distribution System
DLC:                .... .0.. = Last fragment
DLC:                .... 0... = Not retry
DLC:                ...0 .... = Active Mode
DLC:                ..0. .... = No more data
DLC:                .0.. .... = Wired Equivalent Privacy is off
DLC                 0... .... = Not ordered
DLC: Duration                        = 0 (in microseconds)
DLC: Destination Address             = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source Address                  = Station Aironet502F3F
DLC  Basic Service Set ID            = BROADCAST FFFFFFFFFFFF, Broadcast
DLC  Sequence Control                = 0x5690
DLC: .. Sequence Number              = 0x569 (1385)
DLC: ...Fragment Number              = 0x0   (0)
DLC: Element ID                      = 0 (Service Set Identifier)
DLC: ...Length                       = 9 octet(s)
DLC: ...Service Set Identity         = "marketing"
DLC:
DLC: Element ID                      = 1 (Supported Rates)
DLC: .. Length                       = 4 octet(s)
DLC: ...Supported Rates information field = 02
                                0... .... = Not Basic Service Set Basic Rate
DLC:                            .000 0010 =  1.0 Megabits per second
DLC     Supported Rates information field = 04
DLC:                            0... .... = Not Basic Service Set Basic Rate
DLC                             .000 0100 =  2.0 Megabits per second
DLC: ...Supported Rates information field = 0B
DLC                             0... .... = Not Basic Service Set Basic Rate
DLC:                            .000 1011 =  5.5 Megabits per second
DLC: .. Supported Rates information field = 16
DLC:                            0... .... = Not Basic Service Set Basic Rate
DLC.                            .001 0110 = 11.0 Megabits per second
```

Рис. 2.22. Расшифровка протокола зондирующего фрейма запроса

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

Ключевые поля зондирующего фрейма ответа следующие.

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

Поле сигнального 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 модуляцией 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".

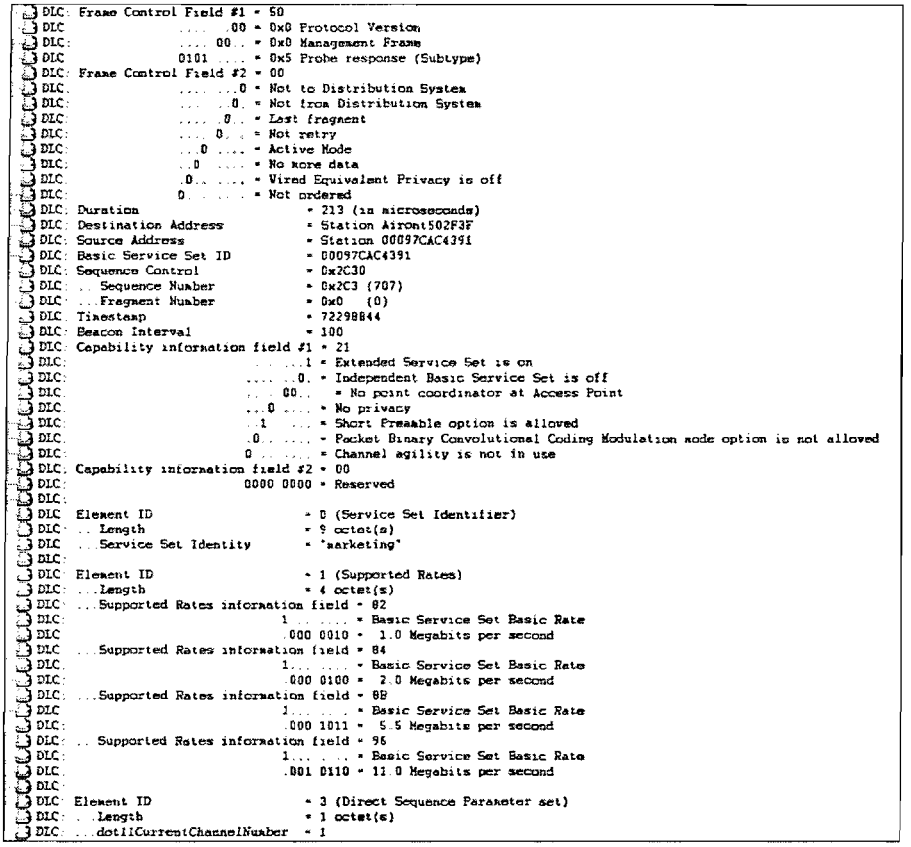


Рис. 2.23. Зондирующий фрейм ответа

Когда 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 критерий выбора точки доступа может включать согласование SSID, уровня сигналов и собственные критерии поставщика.

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

В табл. 2.1 сведены воедино данные из зондирующих фреймов ответа, полученных станцией Вивьен.

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

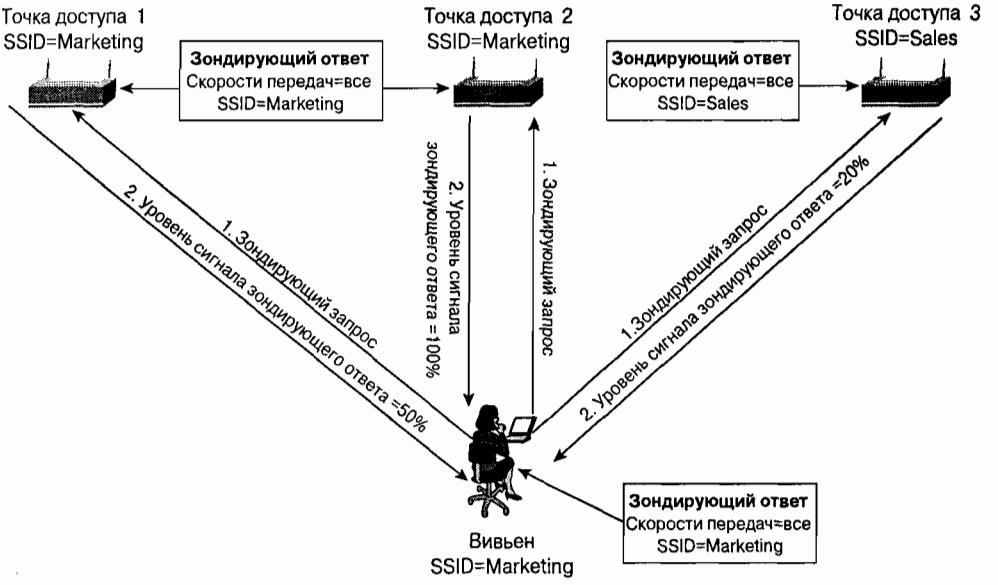


Рис. 2.24. Процесс зондирования

Станция Вивьен намеревается привязаться к точке доступа 2 (AP2). AP2 имеет подходящий SSID, поддерживает все скорости 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 соединения станций — процессу аутентификации.

Процесс аутентификации

Процесс аутентификации по стандарту 802.11 может выполняться в двух режимах: аутентификация с открытым ключом (open authentication) и аутентификация с совместно используемым 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 запроса на аутентификацию и ответа на запрос относительно аутентификации (рис. 2.25).

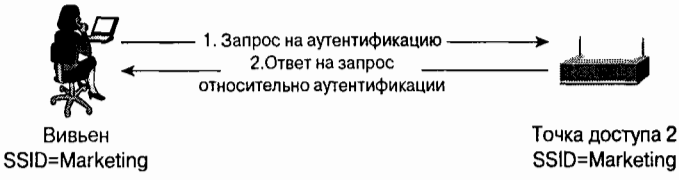


Рис. 2.25. Процесс аутентификации

Процесс привязки

Процесс привязки по стандарту 802.11 позволяет точке доступа выделить для беспроводной станции логический порт или присвоить ей идентификатор ассоциации (association identifier, AID). Процесс привязки начинается беспроводной станцией с фрейма запроса на ассоциирование, содержащего информацию о возможностях клиента, и завершается фреймом ответа на ассоциирование, посылаемого точкой доступа. Ответ на ассоциирование может быть положительным или отрицательным и содержать код, указывающий на причины отказа. На рис. 2.26 представлена расшифровка протокола фрейма запроса на ассоциирование, а на рис. 2.27 — расшифровка протокола фрейма ответа на ассоциирование.

```
DLC: Frame Control Field #1 = 00
DLC:                  ...  ..00 = 0x0 Protocol Version
DLC:                  ...  00.. = 0x0 Management Frame
DLC:                  0000 .... = 0x0 Association request (Subtype)
DLC: Frame Control Field #2 = 00
DLC:                  .... ...0 = Not to Distribution System
DLC:                  .... ..0. = Not from Distribution System
DLC:                  .... .0.. = Last fragment
DLC:                  .... 0... = Not retry
DLC:                  ...0 .... = Active Mode
DLC:                  ..0. .... = No more data
DLC:                  .0.. .... = Wired Equivalent Privacy is off
DLC:                  0... .... = Not ordered
DLC: Duration                   = 314 (in microseconds)
DLC: Destination Address        = Station 00097CAC4391
DLC: Source Address             = Station Aironet502F3F
DLC: Basic Service Set ID       = 00097CAC4391
DLC: Sequence Control           = 0x1720
DLC:  ...Sequence Number        = 0x172 (370)
DLC:  ...Fragment Number        = 0x0   (0)
DLC: Capability information field #1 = 21
DLC:                         ...  ...1 = Extended Service Set is on
DLC:                         .... ..0. = Independent Basic Service Set is off
DLC:                         .... 00..   = STA is not Contention Free-Pollable
DLC:                         ...0 .... = No privacy
DLC:                         ..1. .... = Short Preamble option is implemented
DLC:                         .0.. .... = Packet Binary Convolutional Coding Modulation mode option is not implemented
DLC:                         0... .... = Channel agility is not in use
DLC: Capability information field #2 = 00
DLC:                         0000 0000 = Reserved
DLC: Listen interval            = 200
DLC
DLC: Element ID                 = 0 (Service Set Identifier)
DLC:  Length                    = 5 octet(s)
DLC:  Service Set Identity      = "cisco"
DLC:
DLC: Element ID                 = 1 (Supported Rates)
DLC:  Length                    = 4 octet(s)
DLC:  Supported Rates information field = 02
DLC:                         0... .... = Not Basic Service Set Basic Rate
DLC:                          000 0010 =  1.0 Megabits per second
DLC:  Supported Rates information field = 04
DLC:                         0... .... = Not Basic Service Set Basic Rate
DLC:                         .000 0100 =  2.0 Megabits per second
DLC:  Supported Rates information field = 0B
DLC:                         0... .... = Not Basic Service Set Basic Rate
DLC:                          000 1011 =  5.5 Megabits per second
DLC:  Supported Rates information field = 16
DLC:                         0... .... = Not Basic Service Set Basic Rate
DLC:                         .001 0110 = 11.0 Megabits per second
DLC:
```

Рис. 2.26. Фрейм запроса на ассоциирование

Ключевые поля фрейма запроса на соединение следующие.

- **Интервал прослушивания** (listen interval). Значение интервала прослушивания используется в режиме экономии энергопотребления и сообщается клиентской станцией точке доступа. Оно информирует точку доступа о том, как часто эта станция "просыпается" (выходит из режима экономии энергопотребления), чтобы получить фреймы, буферизированные в точке доступа. Более подробно об этом рассказываются ниже.
- **Элемент SSID**. Описывает SSID клиентской станции для точки доступа. В нормальном режиме работы точка доступа не принимает запросы на ассоциацию от станций с SSID, отличающимся от тех, которые сконфигурированы в точке доступа.

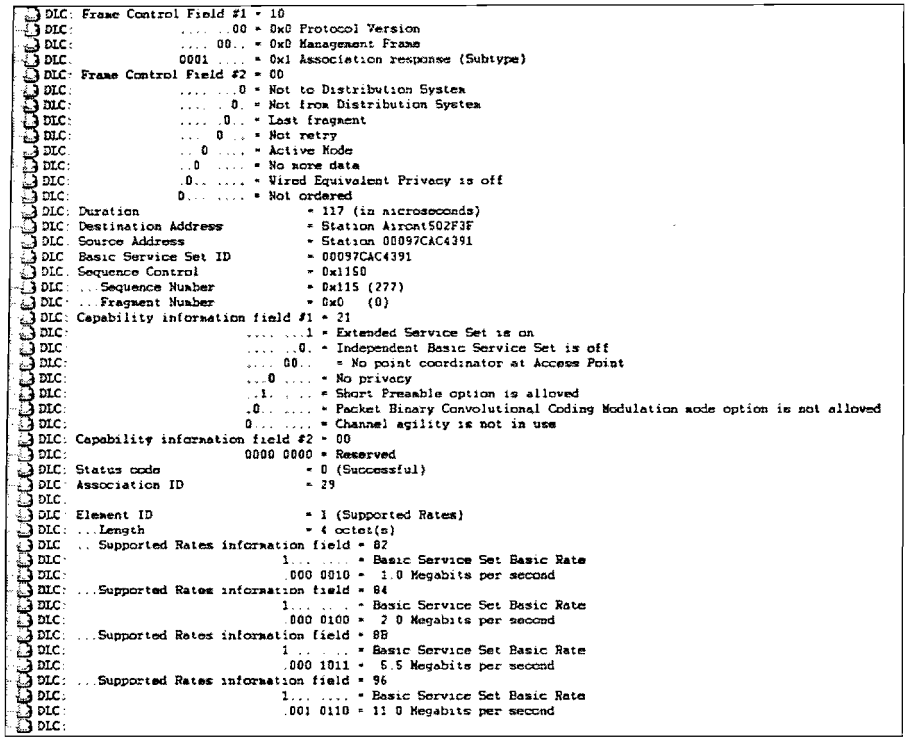


Рис. 2.27. Фрейм ответа на ассоциирование

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

Ключевые поля фрейма ответа на ассоциирование следующие.

- **Код состояния** (status code). Этот элемент указывает код состояния, определяемый 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 знать 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 safe operations). Работа в режиме сниженного энергопотребления осуществляется в двух вариантах.

- Работа с одноадресатными фреймами.
- Работа с широковещательными/многоадресатными фреймами.

Предположения, на которых базируется работа в режиме энергосбережения, просты. 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, показывающий, имеются ли в буфере фреймы для данной клиентской станции.

При работе с одноадресатными фреймами интервал прослушивания или активизации определяется клиентом. И наоборот, при работе в режиме энергосбережения с широковещательными/многоадресатными фреймами интервал прослушивания определяется точкой доступа и объявляется в ее сигнальных фреймах.

Клиент активизируется и принимает сигнальные 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 "спячки".

Работа с одноадресатными фреймами в режиме энергосбережения

Когда клиент связывается с точкой доступа, он указывает значение интервала прослушивания во фрейме 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 всех AID, которые имеют трафик, буферизированный точкой доступа. Может быть до 2008 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. 2.28 представлена расшифровка протокола сигнального фрейма с элементом TIM, указывающим на наличие буферизированного трафика для клиента.

Обратите внимание на то, что нигде в расшифровке протокола не указан в явном виде AID клиентской станции. Чтобы определить AID клиентской станции (или станций), 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 частичной виртуальной битовой карты (the value of partial virtual bitmap field).

```
DLC: Element ID                    = 5 (Traffic Indication Map)
DLC: ...Length                     = 5 octet(s)
DLC: ...Delivery Traffic Indication Message Count  = 5
DLC: ...Delivery Traffic Indication Message Period = 10
DLC: ...Bitmap control field = 03
DLC:                .... ...1 = Traffic Indicator bit
DLC:               0000 001. = 1 Bitmap offset
DLC: ...Partial Virtual Bitmap     = 0020
```

Рис. 2.28. Расшифровка протокола элемента TIM

Стандарт 802.11 регламентирует применение виртуальной битовой карты индикации трафика (traffic indication virtual bitmap) как средство указания на то, идентификаторы ассоциации (AID) каких станций имеют буферизированные фреймы. Виртуальная битовая карта начинается с AID 1 и заканчивается AID 2007. AID 0 зарезервирован для широковещания/многоадресатной 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, используют значение флага 0.

Таблица 2.2. Пример виртуальной битовой карты индикации трафика

AID	1	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 несущественные нулевые значения флага путем их суммирования. Все клиентские станции, для которых имеются буферизированные фреймы (и, 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 производной величиной, обозначенной в нижеследующих примерах буквой X. Все AID со значением флага, равным 0, следующие за частичной виртуальной битовой картой, суммируются с производной величиной, обозначенной в нижеследующих примерах буквой Y. Если мы обратимся к табл. 2.2, то для нее AID с 1 по 15 суммируются с величиной X, а AID с 32 по 2007 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 = (смещение битовой карты) * 2
N2 = (длина − 4) + N1
X = (N1 * 8) − 1
Y = (N2 + 1) * 8

В примере расшифровки, приведенном на рис. 2.28, N1 = (1 * 2) = 2 и N2 = (5 - 4) + 2 = 3. Значение X составляет (2 * 8) − 1, или 15, а Y — это (3 + 1) * 8, или 32. 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.

Неохваченными остаются AID с 16-го по 31-й, и именно здесь вступает в игру частичная виртуальная битовая карта. В нашем 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 по 23), 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 выясняет, что для него буферизированы фреймы, он посылает служебный (management) фрейм уровня MAC стандарта 802.11, называемый *фрейм опроса режима энергосбережения* (power save poll, PS-Poll). На рис. 2.29 представлена расшифровка протокола PS-Poll, посланного клиентской станцией в ответ на сигнальный фрейм. Заметьте, что поле AID имеет значение, равное 29, именно оно 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 указанием 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.

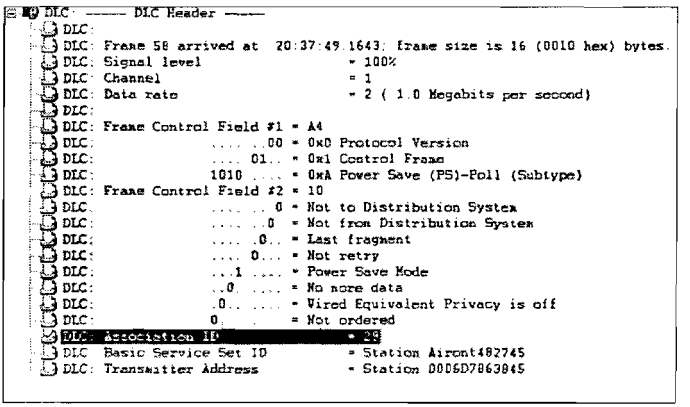


Рис. 2.29. Расшифровка протокола передачи фрейма PS-Poll

Широковещание в режиме энергосбережения

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

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

Информационный элемент TIM имеет два поля, указывающие, буферизирован ли трафик широковещания/многоадресатной 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

TIM 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. 2.30 представлена расшифровка протокола сигнального фрейма, содержащего DTIM. На рис. 2.31 обратите внимание на то, что все фреймы, следующие за сигнальным, являются многоадресатными.

```
DLC: Element ID                          = 5 (Traffic Indication Map)
DLC: ...Length                           = 4 octet(s)
DLC: ...Delivery Traffic Indication Message Count  = 0
DLC: ...Delivery Traffic Indication Message Period = 10
DLC: ...Bitmap control field = 01
DLC:                  .... ...1 = Traffic Indicator bit
DLC:                 0000 000. = 0 Bitmap offset
DLC: ...Partial Virtual Bitmap       = 00
```

Рис. 2.30. Расшифровка протокола элемента DTIM

Рис. 2.31. Многоадресатные 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 похожи 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.

Контроль фрейма	Продолжительность/ID	Адрес 1	Адрес 2	Адрес 3	Управление очередностью	Адрес 4	Тело фрейма	FCS
2 байт	2 байт	6 байт	6 байт	6 байт	2 байт	6 байт	0 - 2312 байт	4 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 одиннадцати подполей. На рис. 2.33 показаны подполя поля контроля фрейма, а на рис. 2.34 дана расшифровка протокола подполей контроля фрейма.

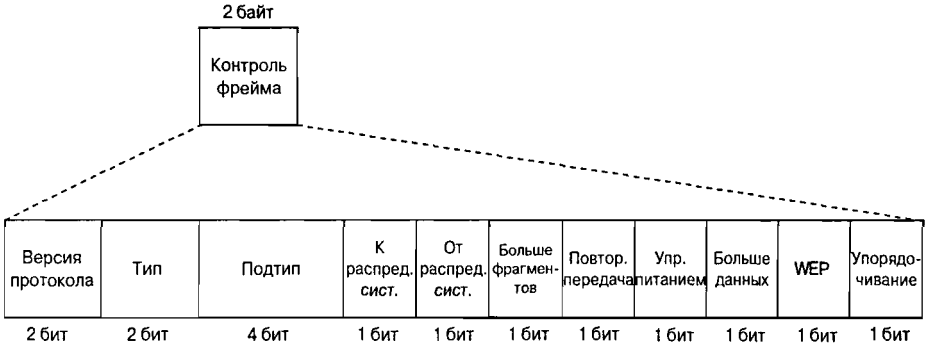


Рис. 2.33. Подполя поля контроля фрейма

```
DLC: Frame Control Field #1 = B0
DLC:                  .... ..00 = 0x0 Protocol Version
DLC:                  .... 00.. = 0x0 Management Frame
DLC:                  1011 .... = 0xB Authentication (Subtype)
DLC: Frame Control Field #2 = 00
DLC:                  .... ...0 = Not to Distribution System
DLC:                  .... ..0. = Not from Distribution System
DLC:                  .... .0.. = Last fragment
DLC:                  .... 0... = Not retry
DLC:                  ...0 .... = Active Mode
DLC:                  ..0. .... = No more data
DLC:                  .0.. .... = Wired Equivalent Privacy is off
DLC:                  0... .... = Not ordered
```

Рис. 2.34. Расшифровка протокола подполей поля контроля фрейма

Ниже перечислены одиннадцать подполей 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	Управление	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
00	Служебный	0000	Зондирующий запрос

Окончание табл. 2.3

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	Объявление карты индикации трафика (announcement traffic indication frame, ATIM)
00	Служебный	1010	Разъединение
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 (данные 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	Зарезервировано	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.
- **Больше данных** (more data). Если бит этого поля установлен, приемная станция оповещается о том, что имеются предназначенные для нее данные, буферизированные в точке доступа.
- **Защищенность, эквивалентная таковой проводных сетей** (wired equivalent privacy, WEP). Указывает, используется ли шифрование WEP для защиты тела фрейма.
- **Параметр упорядочивания** (order). Значение этого поля равно 1, если фрейм данных использует StrictlyOrdered service class, в противном случае оно равно 1.

- **Продолжительность/ID** (Duration/ID). Это поле используется по-разному, 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 во фреймах PS-Poll
1	1	2008–16 383	Зарезервированы

- **Адреса 1, 2, 3 и 4**. Эти поля изменяются в зависимости от типа и подтипа фрейма.
- **Управление очередностью** (sequence control). В этом поле содержатся 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.

```
DLC: Duration                    = 314 (in microseconds)
DLC: Destination Address         = Station Airont31669C
DLC: Source Address              = Station Airont500292
DLC: Basic Service Set ID        = Airont31669C
DLC: Sequence Control            = 0x0A40
DLC:  ...Sequence Number         = 0x0A4 (164)
DLC:  ...Fragment Number         = 0x0   (0)
```

Рис. 2.35. Расшифровка протокола подполей продолжительности, адреса и управления очередностью

Управляющие фреймы стандарта 802.11

В спецификации стандарта 802.11 оговорены шесть уникальных управляющих фреймов.

- Опрос 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, имеющими значение 1.
- **Идентификатор BSS (BSSID)**. MAC-адрес точки доступа к инфраструктуре сети.
- **Адрес передатчика** (transmiccion address, TA). MAC-адрес беспроводной энергосберегающей 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

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 58 arrived at  20:37:49.1643; frame size is 16 (0010 hex) bytes
DLC:  Signal level                    = 100%
DLC:  Channel                         = 1
DLC:  Data rate                       = 2 ( 1.0 Megabits per second)
DLC:
DLC:  Frame Control Field #1 = A4
DLC                  .... ..00 = 0x0 Protocol Version
DLC:                 .... 01.. = 0x1 Control Frame
DLC:                 1010 .... = 0xA Power Save (PS)-Poll (Subtype)
DLC:  Frame Control Field #2 = 10
DLC:                 .... ...0 = Not to Distribution System
DLC:                 .... ..0. = Not from Distribution System
DLC:                 .... .0.. = Last fragment
DLC:                 .... 0... = Not retry
DLC:                 ...1 .... = Power Save Mode
DLC:                 ..0. .... = No more data
DLC:                 .0.. .... = Wired Equivalent Privacy is off
DLC:                 0... .... = Not ordered
DLC:  Association ID                  = 50
DLC:  Basic Service Set ID            = Station Aironet482745
DLC:  Transmitter Address             = Station 0006D7863845
```

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 обменяться 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

```
DLC: Frame Control Field #1 = B4
DLC:                  .... ..00 = 0x0 Protocol Version
DLC:                  .... 01.. = 0x1 Control Frame
DLC:                  1011 .... = 0xB Request To Send (RTS) (Subtype)
DLC: Frame Control Field #2 = 00
DLC:                  .... ...0 = Not to Distribution System
DLC:                  .... ..0. = Not from Distribution System
DLC:                  .... .0.. = Last fragment
DLC:                  .... 0... = Not retry
DLC:                  ...0 .... = Active Mode
DLC:                  ..0. .... = No more data
DLC:                  .0.. .... = Wired Equivalent Privacy is off
DLC:                  0... .... = Not ordered
DLC: Duration                   = 1054 (in microseconds)
DLC: Receiver Address           = Station 00097CAC4391
DLC: Transmitter Address        = Station Aironet502F3F
```

Рис. 2.39. Расшифровка протокола фрейма RTS

Фрейм CTS

Фрейм CTS — это ответ на фрейм RTS. Это указание приемной станции, что среда была зарезервирована на указанное время.

- **Продолжительность** (duration). Величина, полученная из поля Duration предшествующего 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.

Контроль фрейма	Продолжительность	Адрес приемника	FCS
2 байт	2 байт	6 байт	4 байт

Рис. 2.40. Формат фрейма CTS

```
DLC: Frame Control Field #1 = C4
DLC:                   .   00 = 0x0 Protocol Version
DLC:                 .... 01.. = 0x1 Control Frame
DLC:                1100 .... = 0xC Clear To Send (CTS) (Subtype)
DLC: Frame Control Field #2 = 00
DLC:                 .... ...0 = Not to Distribution System
DLC:                 .... ..0. = Not from Distribution System
DLC:                 .... .0.. = Last fragment
DLC:                 .... 0... = Not retry
DLC:                 ...0 .... = Active Mode
DLC:                  .0. .... = No more data
DLC:                 .0.. .... = Wired Equivalent Privacy is off
DLC:                 0... .... = Not ordered
DLC: Duration                  = 836 (in microseconds)
DLC: Receiver Address          = Station Aironet502F3F
DLC: Implied Transmitter Address = Station 00097CAC4391
```

Рис. 2.41. Расшифровка протокола фрейма CTS

Фрейм ACK

Фрейм ACK подтверждает передачу фрейма. Получатель фрейма посылает фрейм ACK отправителю, чтобы сообщить о его успешном приеме.

- **Продолжительность** (duration). Значение этого поля для фреймов ACK обычно равно 0, так как именно этот фрейм подтверждения содержит время передачи для интервала SIFS и фрейма ACK в своем поле Duration.
- **Адрес приемника** (receiver address, RA). MAC-адрес предполагаемого получателя фрейма.

На рис. 2.42 показан формат фрейма RTS, а на рис. 2.43 представлена расшифровка протокола фрейма RTS.

Контроль фрейма	Продолжительность	Адрес приемника	FCS
2 байт	2 байт	6 байт	4 байт

Рис. 2.42. Формат фрейма ACK

```
DLC: Frame Control Field #1 = D4
DLC:                   .   00 = 0x0 Protocol Version
DLC:                 .... 01.. = 0x1 Control Frame
DLC:                1101 .... = 0xD Acknowledgment (ACK) (Subtype)
DLC: Frame Control Field #2 = 00
DLC:                 .... ...0 = Not to Distribution System
DLC:                 .... ..0. = Not from Distribution System
DLC:                 .... .0.. = Last fragment
DLC:                 .... 0... = Not retry
DLC:                 ...0 .... = Active Mode
DLC:                  .0. .... = No more data
DLC:                 .0.. .... = Wired Equivalent Privacy is off
DLC:                 0... .... = Not ordered
DLC: Duration                  = 0 (in microseconds)
DLC: Receiver Address          = Station Aironet502F3F
DLC: Implied Transmitter Address = Station 00097CAC4391
```

Рис. 2.43. Расшифровка протокола фрейма ACK

Фреймы CF-End и CF-End+CF-ACK

Фреймы CF-End и CF-End+CF-ACK специфичны 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.

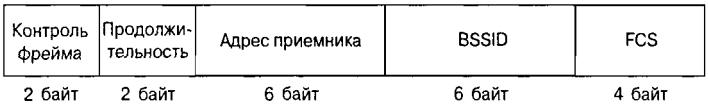


Рис. 2.44. Формат фреймов CF-End и CF-End+CF-ACK

- **Продолжительность** (duration). Установлена равной 0.
- **Адрес приемника** (receiver address, RA). MAC-адрес предполагаемого получателя фрейма. В случае фреймов CF-End это широковещательный 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, отличающиеся от описанного ранее исходного фрейма MAC, и используют структуры данных, которые называются *информационные элементы* (information elements, IE) 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).

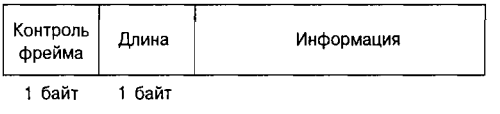


Рис. 2.45. Формат информационного элемента

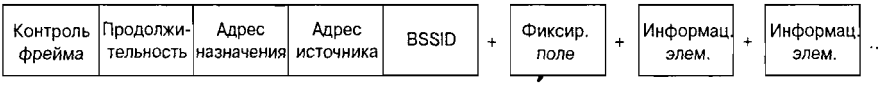


Рис. 2.46. Структура служебного фрейма, использующего информационные элементы и фиксированные поля

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

Таблица 2.5. Информационные элементы, определенные в стандарте 802.11

Информационный элемент	Элемент ID
SSID	0
Поддерживаемые скорости передачи	1
Набор параметров скачкообразного переключения частоты	2
Набор параметров DS	3
Набор параметров CF	4
Набор параметров IBSS	6
Зарезервированы	7–15
Изменяющийся текст	16
Зарезервированы для расширения изменяющегося текста	17–31
Зарезервированы	32–255

Информационный элемент SSID

SSID может иметь размер до 32 бит, а если его размер равен 0, то данный SSID является SSID широковещания.

На рис. 2.47 показан формат фрейма информационного элемента SSID, а на рис. 2.48 приведена расшифровка протокола информационного элемента SSID.

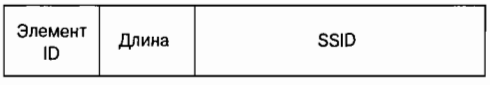


Рис. 2.47. Формат информационного элемента SSID

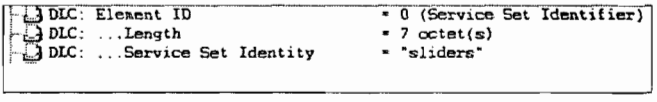


Рис. 2.48. Расшифровка протокола информационного элемента SSID

IE поддерживаемых скоростей передачи

Информационный элемент поддерживаемых скоростей передачи указывает, какие скорости передачи способна поддерживать данная беспроводная станция. Двоичные значения отображают приращения по 500 Кбит/с. Например, поддерживаемая скорость передачи 11 Мбит/с будет представлена в виде `0x16`, что эквивалентно в десятеричном представлении 22,22/500 Кбит/с (или 0,5 Мбит/с) = 11 Мбит/с.

На рис. 2.49 показан формат фрейма информационного элемента поддерживаемых скоростей передачи, а на рис. 2.50 приведена расшифровка протокола IE поддерживаемых скоростей передачи.

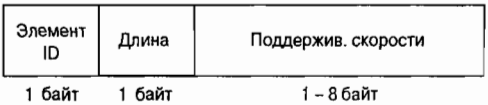


Рис. 2.49. Формат фрейма информационного элемента поддерживаемых скоростей передачи

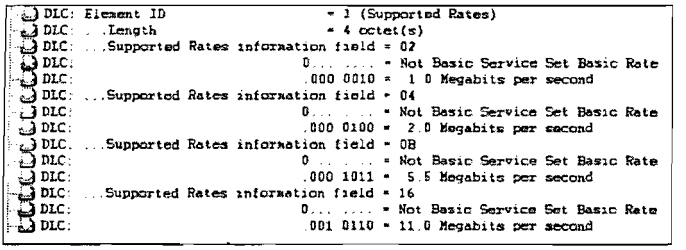


Рис. 2.50. Расшифровка протокола IE поддерживаемых скоростей передачи

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, отсчитывается в тактах (TU).
- **Набор схем скачков** (hop 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-sequencing).

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).

- **CFP DurationRemaining**. Продолжительность (измеряется в TU), оставшаяся до конца текущего CFP.

Элемент ID	Длина	Счетчик CFP	Период CFP	Макс. продолжит. CFP (в тактах)	Оставш. продолж. CFP (в тактах)
1 байт	1 байт	1 байт	1 байт	2 байт	2 байт

Рис. 2.53. Формат информационного элемента набора параметров CF

Информационный элемент TIM

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

- **Счетчик DTIM** (DTIM count). Подсчитывает, сколько пройдет сигнальных фреймов (включая текущий фрейм), прежде чем придет следующий DTIM. Значение 0 свидетельствует о том, что текущий фрейм и есть DTIM.
- **Период DTIM** (DTIM period). Количество интервалов DTIM между фреймами DTIM. Значение 1 указывает на то, что все TIM 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 TIM со значением 0 в поле счетчика DTIM, когда в точке доступа буферизированы один или несколько фреймов широковещания либо многоадресатных фреймов. Оставшиеся 7 бит этого поля формируют смещение битовой карты (bitmap offset).
- **Частичная виртуальная битовая карта** (partial virtual bitmap). Постанционная индикация состояния буфера фреймов точки доступа. Индикация для AID 0 указывает, что буферизированы фреймы широковещания или многоадресатные фреймы.

Элемент ID	Длина	Счетчик	Период	Контроль битовой карты	Частичная виртуальная битовая карта
1 байт	1 байт	1 байт	1 байт	1 байт	1 — 251 байт

Рис. 2.54. Формат фрейма информационного элемента TIM

```
DLC: Element ID                        = 5 (Traffic Indication Map)
DLC: ...Length                         = 5 octet(s)
DLC: ...Delivery Traffic Indication Message Count  = 5
DLC: ...Delivery Traffic Indication Message Period = 10
DLC: ...Bitmap control field = 03
DLC:                  .... ...1 = Traffic Indicator bit
DLC:                  0000 001. = 1 Bitmap offset
DLC: ...Partial Virtual Bitmap      = 0020
```

Рис. 2.55. Расшифровка протокола информационного элемента TIM

Информационный элемент набора параметров IBSS

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

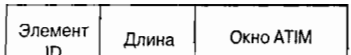


Рис. 2.56. Формат информационного элемента набора параметров IBSS

Информационный элемент изменяющегося текста

На рис. 2.57 представлен формат информационного элемента изменяющегося текста.

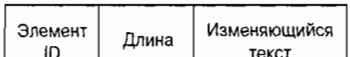


Рис. 2.57. Формат информационного элемента изменяющегося текста

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 совместно используемым 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, важные только 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**. Станции из IBSS устанавливают значение этого подполя равным 1 и подполя ESS — равным 0 для сигнальных фреймов и фреймов ответа на зондирование.
- **Подлежит опросу CF** (CF-Pollable). Это подполе используют 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 применять WEP-кодирование. Подполе включается в сигнальный фрейм, во фреймы ответов на зондирование, ассоциацию и реассоциацию. Если применять WEP-кодирование не нужно, значение данного подполя устанавливается равным 0.

ESS	IBSS	Опрашивается ли CF	Запрос на опрашивание CF	Конфиденциальность	Зарезервированы
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

Подверженность 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	Ответ на запрос CF-Poll	Значение
0	0	Точка доступа не поддерживает PCF 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 активизируется для того, чтобы принять сигнальный фрейм.

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) IBSS 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 (ре)ассоциации, не аутентифицирована отвечающей станцией
10–65 535	Зарезервированы

Поле AID

Данное поле указывает значение, назначенное точкой доступа для представления 16-разрядного ID для беспроводной станции. Это значение представляет собой логический порт для беспроводной станции.

Поле кода состояния

Это поле в служебных фреймах ответа содержит значение, указывающее на успешность или неуспешность реагирования на служебный фрейм запроса. В табл. 2.10 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	Не в состоянии поддерживать все запрошенные возможности, указанные в поле информационной способности
11	Реассоциация 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 соответствующим 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
19–65 535	Зарезервированы

Поле метки времени (Timestamp)

Это поле указывает значение TSFTIMER отправителя фрейма.

Служебные фреймы стандарта 802.11

К числу служебных 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 реассоциирование.
- Фрейм ответа на реассоциирование.
- Фрейм диссоциирования.
- Фрейм индикации объявленного трафика (announcement traffic indication frame, ATIM).

В следующих разделах каждый из служебных фреймов описан более подробно.

Сигнальный фрейм

Сигнальный (маячковый) фрейм — это служебный фрейм, который точка доступа (или отправитель сигнала в IBSS) передает с частотой, определяемой сигнальным интервалом. Сигнальный фрейм (его в данной книге часто называют просто "маяк" (beacon)) обеспечивает временную синхронизацию между точкой доступа и беспроводной станцией, а также синхронизацию специфичных для физического канала параметров. Кроме того, энергосберегающие станции оповещаются о том, что точка доступа имеет для них буферизированные фреймы. В дополнение к определенным в стандарте 802.11 полям и информационным элементам в сигнальные фреймы могут быть также включены специфичные для конкретного производителя информационные элементы.

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

Контроль фрейма	Продолжительность	Адрес назначения	Адрес источника	BSSID	Управление очередностью	Поле метки времени	Поле сигнального интервала	Поле информационной способности	SSID IE	IE поддерживаемых скоростей	IE с набором параметров FH/DS (переключ. частоты/ прям. последов.)	IE с набором параметров CF (опционально)	IE с набором параметров IBSS (опционально)	IE TIM (опционально)

Рис. 2.59. Формат сигнального фрейма

```
DLC: Frame Control Field #1 = 80
DLC:                .... ..00 = 0x0 Protocol Version
DLC:                .... 00.. = 0x0 Management Frame
DLC:                1000 .... = 0x8 Beacon (Subtype)
DLC: Frame Control Field #2 = 00
DLC:                .... ...0 = Not to Distribution System
DLC:                .... ..0. = Not from Distribution System
DLC:                .... .0.. = Last fragment
DLC:                .... 0... = Not retry
DLC:                ...0 .... = Active Mode
DLC:                .0.. .... = No more data
DLC:                .0.. .... = Wired Equivalent Privacy is off
DLC:                0... .... = Not ordered
DLC: Duration                    = 0 (in microseconds)
DLC: Destination Address         = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source Address              = Station Aironet482745
DLC: Basic Service Set ID        = Aironet482745
DLC: Sequence Control            = 0x0070
DLC:   .Sequence Number          = 0x007 (7)
DLC:   .Fragment Number          = 0x0   (0)
DLC: Timestamp                   = 16385154 (in microseconds)
DLC: Beacon Interval             = 2000
DLC: Capability information field #1 = 21
DLC:                         ...0 = Extended Service Set is on
DLC:                         ..0. = Independent Basic Service Set is off
DLC:                         00.. = No point coordinator at Access Point
DLC:                         ...0 = No privacy
DLC:                         .1.. = Short Preamble option is allowed
DLC:                         0... = Packet Binary Convolutional Coding Modulation mode option is not allowed
DLC:                        0.... = Channel agility is not in use
DLC: Capability information field #2 = 00
DLC:                        0000 0000 = Reserved
DLC:
DLC: Element ID                  = 0 (Service Set Identifier)
DLC:   Length                    = 9 octet(s)
DLC:   Service Set Identity      = "powersave"
DLC:
DLC: Element ID                  = 1 (Supported Rates)
DLC:   Length                    = 4 octet(s)
DLC:   Supported Rates information field = 82
DLC:                           1... .... = Basic Service Set Basic Rate
DLC:                           .000 0010 =  1.0 Megabits per second
DLC:   Supported Rates information field = 84
DLC:                           1... .... = Basic Service Set Basic Rate
DLC:                           .000 0100 =  2.0 Megabits per second
DLC:   Supported Rates information field = 8B
DLC:                           1... .... = Basic Service Set Basic Rate
DLC:                           .000 1011 =  5.5 Megabits per second
DLC:   Supported Rates information field = 96
DLC:                           1... .... = Basic Service Set Basic Rate
DLC:                           .001 0110 = 11.0 Megabits per second
DLC:
DLC: Element ID                  = 3 (Direct Sequence Parameter set)
DLC:   Length                    = 1 octet(s)
DLC:   dot11CurrentChannelNumber = 1
DLC:
DLC: Element ID                  = 5 (Traffic Indication Map)
DLC:   Length                    = 4 octet(s)
DLC:   Delivery Traffic Indication Message Count  = 2
DLC:   Delivery Traffic Indication Message Period = 10
DLC:   Bitmap control field = 00
DLC:                        .... ...0 = Traffic Indicator bit
DLC:                        0000 000. = 0 Bitmap offset
DLC:   Partial Virtual Bitmap     = 00
```

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.

Контроль фрейма	Продолжительность	Адрес назначения	Адрес источника	BSSID	Управление очередностью	SSID IE	IE поддерживаемых скоростей

Рис. 2.61. Формат фрейма запроса на зондирование

```
DLC: Frame Control Field #1 = 40
DLC:                  ...  .00 = 0x0 Protocol Version
DLC:                  ..  00   = 0x0 Management Frame
DLC:                0100  ...  = 0x4 Probe request (Subtype)
DLC: Frame Control Field #2 = 00
DLC:                  ..  ..0  = Not to Distribution System
DLC:                  ....  ..0  = Not from Distribution System
DLC:                  ....  .0.  = Last fragment
DLC:                  ....  0...  = Not retry
DLC:                  ..0  ....  = Active Mode
DLC:                  .0.  ....  = No more data
DLC:                  0...  ....  = Wired Equivalent Privacy is off
DLC:                  0...  ....  = Not ordered
DLC: Duration                      = 0 (in microseconds)
DLC: Destination Address           = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source Address                = Station Aironet500292
DLC: Basic Service Set ID          = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Sequence Control              = 0x6F30
DLC:  .. Sequence Number           = 0x6F3 (1779)
DLC:  ..Fragment Number            = 0x0   (0)
DLC: Element ID                    = 0 (Service Set Identifier)
DLC:  .. Length                    = 7 octet(s)
DLC:  .. Service Set Identity      = "sliders"
DLC:
DLC: Element ID                    = 1 (Supported Rates)
DLC:  .. Length                    = 4 octet(s)
DLC:  ..Supported Rates information field = 02
DLC:                               0  ...  ....  = Not Basic Service Set Basic Rate
DLC:                               .000 0010  =  1.0 Megabits per second
DLC:  .. Supported Rates information field = 04
DLC:                               0...  ....  = Not Basic Service Set Basic Rate
DLC:                               .000 0100  =  2.0 Megabits per second
DLC:  ..Supported Rates information field = 0B
DLC:                               0...  ....  = Not Basic Service Set Basic Rate
DLC:                               .000 1011  =  5.5 Megabits per second
DLC:  ..Supported Rates information field = 16
DLC:                               0...  ....  = Not Basic Service Set Basic Rate
DLC:                                001 0110  = 11.0 Megabits per second
```

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.

Контроль фрейма	Продолжительность	Адрес назначения	Адрес источника	BSSID	Управление очередностью	Поле метки времени	Поле сигнального интервала	Поле информационной способности	SSID IE	IE поддерживаемых скоростей	IE с набором параметров FH/DS (переключ. частоты/ прямы. последов.)	IE с набором параметров CF (опционально)	IE с набором параметров IBSS (опционально)

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.

```
DLC: Frame Control Field #1 = 50
DLC:                 ..  . 00 = 0x0 Protocol Version
DLC:                 .... 00.. = 0x0 Management Frame
DLC:                 0101 .... = 0x5 Probe response (Subtype)
DLC: Frame Control Field #2 = 00
DLC:                 .... ...0 = Not to Distribution System
DLC:                 .... ..0. = Not from Distribution System
DLC:                 .... .0.. = Last fragment
DLC:                 .... 0... = Not retry
DLC:                 ...0 .... = Active Mode
DLC:                 ..0  .... = No more data
DLC:                 .0.. .... = Wired Equivalent Privacy is off
DLC:                 0.   .... = Not ordered
DLC: Duration                  = 213 (in microseconds)
DLC: Destination Address       = Station Airont502F3F
DLC: Source Address            = Station 00097CAC4391
DLC: Basic Service Set ID      = 00097CAC4391
DLC: Sequence Control          = 0x2C30
DLC:  .. Sequence Number       = 0x2C3 (707)
DLC:  .. Fragment Number       = 0x0   (0)
DLC: Timestamp                 = 72298844
DLC: Beacon Interval           = 100
DLC: Capability information field #1 = 21
DLC:                         ..  . 1 = Extended Service Set is on
DLC:                         .... ..0. = Independent Basic Service Set is off
DLC:                         ..  00  .  = No point coordinator at Access Point
DLC:                         .. 0 . .. = No privacy
DLC:                         ..1. .... = Short Preamble option is allowed
DLC:                         .0.. .... = Packet Binary Convolutional Coding Modulation mode option is not allowed
DLC:                         0... .... = Channel agility is not in use
DLC: Capability information field #2 = 00
DLC:                         0000 0000 = Reserved
DLC:
DLC: Element ID                = 0 (Service Set Identifier)
DLC:  .. Length                = 9 octet(s)
DLC:  .. Service Set Identity  = 'marketing'
DLC:
DLC: Element ID                = 1 (Supported Rates)
DLC:  .. Length                = 4 octet(s)
DLC:  .. Supported Rates information field = 82
DLC:                         1... .... = Basic Service Set Basic Rate
DLC:                         .000 0010 =  1.0 Megabits per second
DLC:  .. Supported Rates information field = 84
DLC:                         1... .... = Basic Service Set Basic Rate
DLC:                          000 0100 =  2.0 Megabits per second
DLC:  .. Supported Rates information field = 8B
DLC:                         1... .... = Basic Service Set Basic Rate
DLC:                         .000 1011 =  5.5 Megabits per second
DLC:  .. Supported Rates information field = 96
DLC:                         1... .... = Basic Service Set Basic Rate
DLC:                         .001 0110 = 11.0 Megabits per second
DLC:
DLC: Element ID                = 3 (Direct Sequence Parameter set)
DLC:  .. Length                = 1 octet(s)
DLC:  .. dot11CurrentChannelNumber = 1
```

Рис. 2.64. Расшифровка протокола фрейма ответа на зондирование

Контроль фрейма	Продолжительность	Адрес назначения	Адрес источника	BSSID	Управление очередностью	Номер алгоритма аутентификации	Номер транзакции в последовательности аутентификации	Поле кода состояния	IE с изменяющимся текстом (опционально)

Рис. 2.65. Формат фрейма аутентификации

```
DLC: Frame Control Field #1 = B0
DLC:                 .... ..00 = 0x0 Protocol Version
DLC:                 .... 00.. = 0x0 Management Frame
DLC:                 1011 .... = 0xB Authentication (Subtype)
DLC: Frame Control Field #2 = 00
DLC:                 .... ...0 = Not to Distribution System
DLC:                 .... ..0. = Not from Distribution System
DLC:                 .... .0.. = Last fragment
DLC:                 .... 0... = Not retry
DLC:                 ...0 .... = Active Mode
DLC:                 ..0. .... = No more data
DLC:                 .0.. .... = Wired Equivalent Privacy is off
DLC:                 0.   .... = Not ordered
DLC: Duration                  = 213 (in microseconds)
DLC: Destination Address       = Station 0006D7063845
DLC: Source Address            = Station Airont482745
DLC: Basic Service Set ID      = Airont482745
DLC: Sequence Control          = 0x00B0
DLC:  .. Sequence Number       = 0x00B (11)
DLC:  .. Fragment Number       = 0x0   (0)
DLC: Authentication algorithm number = 0 (Open System)
DLC: Authentication transaction sequence number = 2
DLC: Status code               = 0 (Successful)
```

Рис. 2.66. Расшифровка протокола фрейма аутентификации

Фрейм деаутентификации

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

Контроль фрейма	Продолжительность	Адрес назначения	Адрес источника	BSSID	Управление очередностью	Код причины

Рис. 2.67. Формат фрейма деаутентификации

```
DLC: Frame Control Field #1 = C0
DLC:                  . . . . ..00 = 0x0 Protocol Version
DLC:                  .... 00.. = 0x0 Management Frame
DLC:                  1100 .... = 0xC Deauthentication (Subtype)
DLC: Frame Control Field #2 = 00
DLC:                  .... ...0 = Not to Distribution System
DLC:                  .... ..0. = Not from Distribution System
DLC:                  .... .0.. = Last fragment
DLC:                  .... 0... = Not retry
DLC:                  ...0 .... = Active Mode
DLC:                  ..0. .... = No more data
DLC:                  .0.. .... = Wired Equivalent Privacy is off
DLC:                  0... .... = Not ordered
DLC: Duration                   = 213 (in microseconds)
DLC: Destination Address        = Station Aironet502F3F
DLC: Source Address             = Station 00D97CAC4391
DLC: Basic Service Set ID       = 00097CAC4391
DLC: Sequence Control           = 0x2530
DLC:  ...Sequence Number        = 0x253 (595)
DLC:  ...Fragment Number        = 0x0   (0)
DLC: Reason code                = 1 (Unspecified reason)
```

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.

Контроль фрейма	Продолжительность	Адрес назначения	Адрес источника	BSSID	Управление очередностью	Поле информационной способности	Интервал прослушивания	SSID IE	IE поддерживаемых скоростей

Рис. 2.69. Формат фрейма запроса на ассоциирование

```
DLC: Frame Control Field #1 = C0
DLC:                  . . . . ..00 = 0x0 Protocol Version
DLC:                  .... 00.. = 0x0 Management Frame
DLC:                  1100 .... = 0xC Deauthentication (Subtype)
DLC  Frame Control Field #2 = 00
DLC:                  .... ...0 = Not to Distribution System
DLC:                  .... ..0. = Not from Distribution System
DLC:                  .... .0.. = Last fragment
DLC:                  .... 0... = Not retry
DLC:                  ...0 .... = Active Mode
DLC:                  ..0. .... = No more data
DLC:                  .0.. .... = Wired Equivalent Privacy is off
DLC:                  0... .... = Not ordered
DLC: Duration                   = 213 (in microseconds)
DLC: Destination Address        = Station Aironet502F3F
DLC: Source Address             = Station 00097CAC4391
DLC: Basic Service Set ID       = 00097CAC4391
DLC: Sequence Control           = 0x2530
DLC:  ...Sequence Number        = 0x253 (595)
DLC:  ...Fragment Number        = 0x0   (0)
DLC: Reason code                = 1 (Unspecified reason)
```

Рис. 2.70. Расшифровка протокола фрейма запроса на ассоциирование

Фрейм ответа на ассоциирование

На рис. 2.71 показан формат фрейма ответа на ассоциирование, а на рис. 2.72 представлена расшифровка протокола фрейма ответа на ассоциирование.

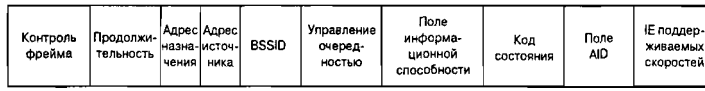


Рис. 2.71. Формат фрейма ответа на ассоциирование

```
DLC: Frame Control Field #1 = 10
DLC:                ......00 = 0x0 Protocol Version
DLC:                ....00.. = 0x0 Management Frame
DLC:                0001.... = 0x1 Association response (Subtype)
DLC: Frame Control Field #2 = 00
DLC:                .... ...0 = Not to Distribution System
DLC:                .... ..0. = Not from Distribution System
DLC:                .... .0.. = Last fragment
DLC:                .... 0... = Not retry
DLC:                ...0 .... = Active Mode
DLC:                ..0  .... = No more data
DLC:                .0.. .... = Wired Equivalent Privacy is off
DLC:                0... .... = Not ordered
DLC: Duration                      = 117 (in microseconds)
DLC: Destination Address           = Station Aironet502F3F
DLC: Source Address                = Station 00097CAC4391
DLC: Basic Service Set ID          = 00097CAC4391
DLC: Sequence Control              = 0x1150
DLC:  .. Sequence Number           = 0x115 (277)
DLC:  ...Fragment Number           = 0x0   (0)
DLC: Capability information field #1 = 21
DLC:                         .... ...1 = Extended Service Set is on
DLC:                         .... ..0. = Independent Basic Service Set is off
DLC:                         .... 00..   = No point coordinator at Access Point
DLC:                         ...0 .... = No privacy
DLC:                         ..1. .... = Short Preamble option is allowed
DLC:                         .0.. .... = Packet Binary Convolutional Coding Modulation mode option is not allowed
DLC:                         0... .... = Channel agility is not in use
DLC: Capability information field #2 = 00
DLC:                         0000 0000 = Reserved
DLC: Status code                   = 0 (Successful)
DLC: Association ID                = 29
DLC:
DLC: Element ID                    = 1 (Supported Rates)
DLC:  ...Length                    = 4 octet(s)
DLC:  .. Supported Rates information field = 82
DLC:                               1... .... = Basic Service Set Basic Rate
DLC:                               .000 0010 =  1.0 Megabits per second
DLC:  ...Supported Rates information field = 84
DLC                                1... .... = Basic Service Set Basic Rate
DLC:                               .000 0100 =  2.0 Megabits per second
DLC:  ...Supported Rates information field = 8B
DLC:                               1... .... = Basic Service Set Basic Rate
DLC:                               .000 1011 =  5.5 Megabits per second
DLC:  .. Supported Rates information field = 96
DLC:                               1... .... = Basic Service Set Basic Rate
DLC:                               .001 0110 = 11.0 Megabits per second
DLC:
```

Рис. 2.72. Расшифровка протокола фрейма ответа на ассоциирование

Фрейм запроса на реассоциирование

На рис. 2.73 показан формат фрейма запроса на реассоциирование, а на рис. 2.74 представлена расшифровка протокола фрейма запроса на реассоциирование.

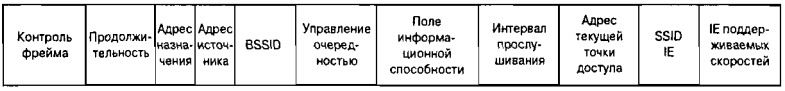


Рис. 2.73. Формат фрейма запроса на реассоциирование

Фрейм запроса на реассоциирование почти идентичен фрейму запроса на ассоциирование, но имеет дополнительное поле, содержащее текущий адрес точки доступа. Главная цель этого фрейма — известить точку доступа о том, что станция, ассоциирующаяся с нею в данный момент, уже имела ассоциацию ранее. Новая точка

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

```
DLC: Frame Control Field #1 = 20
DLC:                  .. .. 00 = 0x0 Protocol Version
DLC:                  .. 00 .. = 0x0 Management Frame
DLC:                  0010 .. .. = 0x2 Reassociation request (Subtype)
DLC: Frame Control Field #2 = 00
DLC:                  .... ..0 = Not to Distribution System
DLC:                  .... .0.. = Not from Distribution System
DLC:                  .... .0... = Last fragment
DLC:                  .... 0 ... = Not retry
DLC:                  ...0 .... = Active Mode
DLC:                  ..0 ..... = No more data
DLC:                  .0.. .... = Wired Equivalent Privacy is off
DLC:                  0... .... = Not ordered
DLC: Duration                    = 314 (in microseconds)
DLC: Destination Address         = Station 00097CAC4391
DLC: Source Address              = Station Aironet502F3F
DLC: Basic Service Set ID        = 00097CAC4391
DLC: Sequence Control            = 0x1FB0
DLC:  .. Sequence Number         = 0x1FB (507)
DLC:  .. Fragment Number         = 0x0   (0)
DLC: Capability information field #1 = 21
DLC:                        .... ...1 = Extended Service Set is on
DLC:                        .... ..0. = Independent Basic Service Set is off
DLC:                        .... 00.. = STA is not Contention Free-Pollable
DLC:                        .. 0 .... = No privacy
DLC:                        . 1. .... = Short Preamble option is implemented
DLC:                        .0.. .... = Packet Binary Convolutional Coding Modulation mode option is not implemented
DLC:                        0... .... = Channel agility is not in use
DLC: Capability information field #2 = 00
DLC:                   0000 0000 = Reserved
DLC: Listen interval             = 200
DLC: Current Access Point address = Station 00097CAC4391
DLC:
DLC: Element ID                  = 0 (Service Set Identifier)
DLC:  Length                     = 9 octet(s)
DLC:  Service Set Identity       = "marketing"
DLC:
DLC: Element ID                  = 1 (Supported Rates)
DLC:  Length                     = 4 octet(s)
DLC:  Supported Rates information field = 02
DLC:                          0  .  .  . = Not Basic Service Set Basic Rate
DLC:                          .000 0010 =  1.0 Megabits per second
DLC:  Supported Rates information field = 04
DLC:                          0... .... = Not Basic Service Set Basic Rate
DLC:                           000 0100 =  2.0 Megabits per second
DLC:  Supported Rates information field = 0B
DLC:                          0. . . . . = Not Basic Service Set Basic Rate
DLC:                          .000 1011 =  5.5 Megabits per second
DLC:  Supported Rates information field = 16
DLC:                          0. . . . . = Not Basic Service Set Basic Rate
DLC:                          .001 0110 = 11.0 Megabits per second
```

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 представлена расшифровка протокола фрейма ответа на реассоциирование.

Фрейм ответа на реассоциирование идентичен фрейму ответа на ассоциирование.

Контроль фрейма	Продолжительность	Адрес назначения	Адрес источника	BSSID	Управление очередностью	Поле информационной способности	Код состояния	Поле AID	IE поддерживаемых скоростей

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 ATIM

Фрейм ATIM не имеет фиксированных полей или информационных элементов.

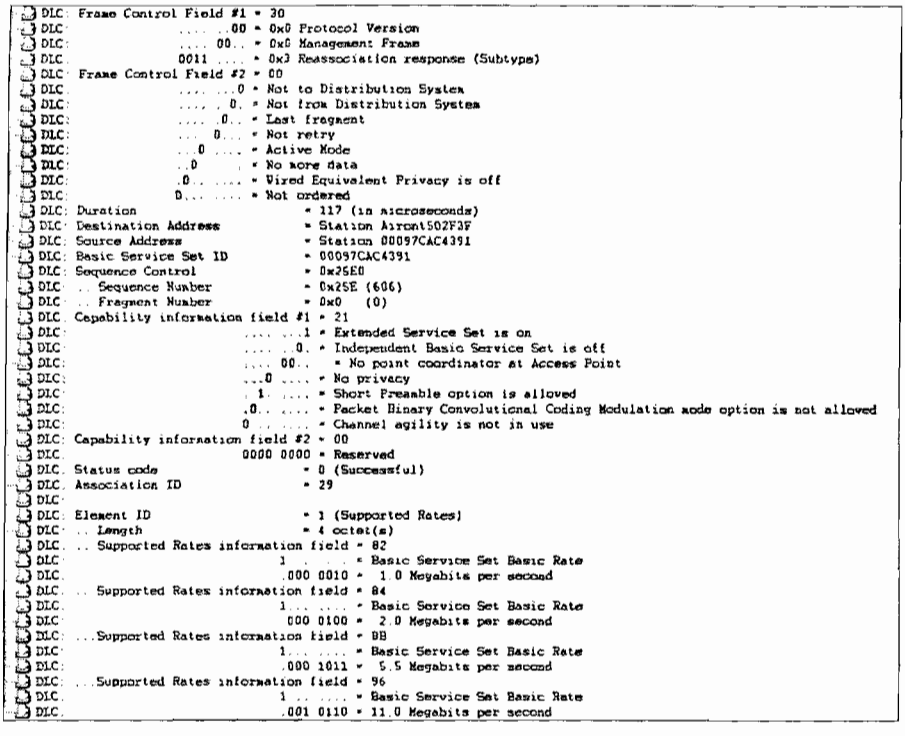


Рис. 2.76. Расшифровка протокола фрейма ответа на реассоциирование

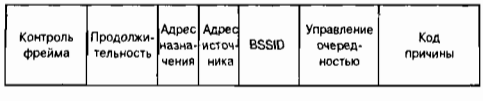


Рис. 2.77. Формат фрейма диссоциирования

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.

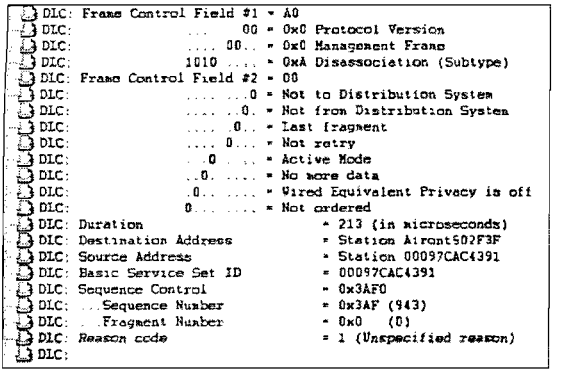


Рис. 2.78. Расшифровка протокола фрейма диссоциирования

Контроль фрейма	Продолжительность	Адрес назначения	BSSID	Адрес источника	Управление очередностью	Полезная нагрузка	FCS
2 байт	2 байт	6 байт	6 байт	6 байт	2 байт	0-2312 байт	4 байт

Рис. 2.79. Формат фрейма данных

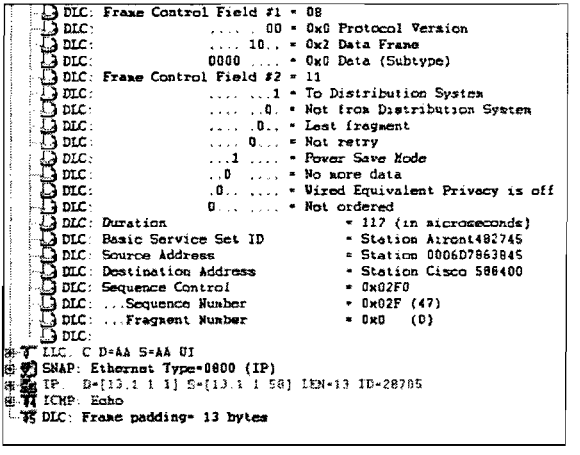


Рис. 2.80. Расшифровка протокола фрейма данных

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

Эти фреймы данных имеют такое же тело фрейма, как и стандартный фрейм данных. Значения подтипов отличаются в обеспечении реализации функциональных возможностей CF-Ack 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 назван так потому, что он не имеет "поля полезной нагрузки". Его задача — указать на изменение бита режима энергосбережения в контрольном поле фрейма.

Контроль фрейма	Продолжительность	Адрес назначения	BSSID	Адрес источника	Управление очередностью	FCS
2 байт	2 байт	6 байт	6 байт	6 байт	2 байт	4 байт

Рис. 2.81. Формат фрейма нулевых данных

```
DLC: Frame Control Field #1 = 48
DLC:                  .... ..00 = 0x0 Protocol Version
DLC:                  .... 10.. = 0x2 Data Frame
DLC:                  0100 .... = 0x4 Null function (no data) (Subtype)
DLC: Frame Control Field #2 = 02
DLC:                  .... ...0 = Not to Distribution System
DLC:                  .... ..1. = From Distribution System
DLC:                  .... .0.. = Last fragment
DLC:                  .... 0... = Not retry
DLC:                  ...0 .... = Active Mode
DLC:                  ..0. .... = No more data
DLC:                  .0.. .... = Wired Equivalent Privacy is off
DLC:                  0... .... = Not ordered
DLC: Duration                   = 117 (in microseconds)
DLC: Destination Address        = Station 0006D7863845
DLC: Basic Service Set ID       = Station Aironet402745
DLC: Source address             = Station Aironet402745
DLC: Sequence Control           = 0x00E0
DLC:  .. Sequence Number        = 0x00E (14)
DLC:  ....Fragment Number       = 0x0   (0)
```

Рис. 2.82. Расшифровка протокола фрейма нулевых данных

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

Эти фреймы имеют такое же тело, как и стандартный фрейм нулевых данных. Значение подтипа различно в обеспечении 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. Беспроводная среда создает новые проблемы по части доступа к ней, в результате вам необходим более надежно работающий уровень MAC. Прочитав эту главу, вы должны иметь отчетливое 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.

Глава 3

Технологии физического уровня стандарта 802.11

Благодаря утверждению в 1999 году стандартов 802.11a и 802.11b технология беспроводных локальных сетей (WLAN) перешла из ниши решений для сканеров штрих-кодов в универсальное решение для доступа к мобильным, дешевым, 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 ключевым был вопрос стандартизации, использование частот, на право пользования 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 подуровнем 802.11 MAC. В этой главе рассматривается каждый 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 по ортогональным частотам (orthogonal frequency division multiplexion, OFDM) в диапазоне 5 ГГц.
- Расширенный физический уровень (extended rate physical (ERP) layer) стандарта 802.11g в диапазоне 2,4 ГГц.

Ethernet стандарта 802.3 эволюционировал долгие годы, прежде чем в него вошли Fast Ethernet стандарта 802.3u и Gigabit Ethernet стандартов 802.3z/802.3ab. Аналогичным образом эволюционировал беспроводной Ethernet стандарта 802.11, и теперь в него входят стандарт 802.11b на высокоскоростную передачу с расширением спектра методом прямой последовательности (high-rate direct sequence spread spectrum, HR-DSSS), стандарт 802.11a OFDM и недавнее дополнение, стандарт 802.11g (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. Подготавливая эти механизмы передачи независимо 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 позволила 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.

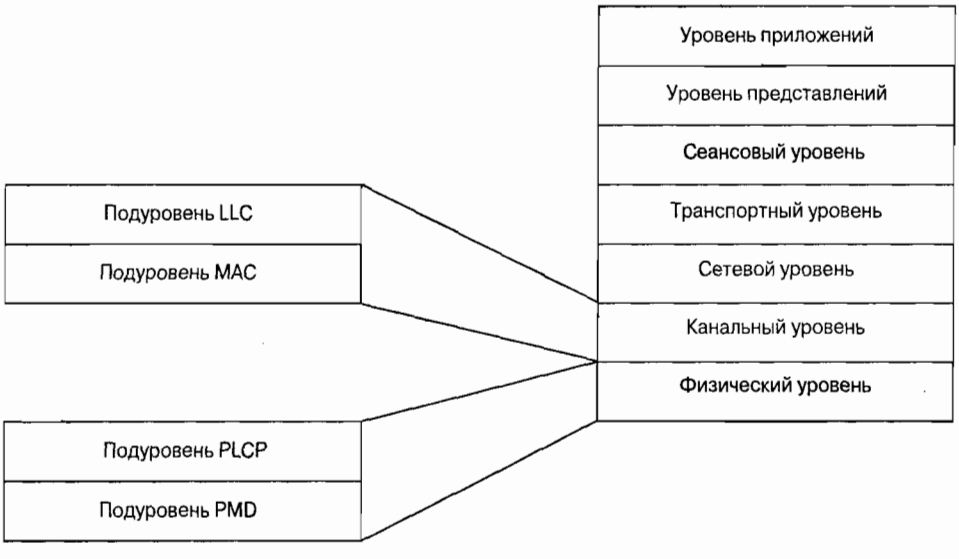


Рис. 3.1. Подуровни уровня PHY модели взаимодействия открытых систем (Open System Interconnection, OSI)

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 и приема данных 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 отличаются 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 сообщить 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 незанятости канала (clear channel assessment (CCA) function) все PLCP обеспечивают для подуровня MAC механизм, посредством которого он может возвратить в исходное состояние CCA-машину (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 незанятости канала (carrier sense/clear channel assessment, CS/CCA). Эта процедура обнаруживает начало передачи сигнала от другой станции и выясняет, свободен ли канал для передачи. Получая 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). Потом 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 PMD, которые обеспечивает каждый уровень PHY стандарта 802.11, нужно вначале рассмотреть следующие основные концепции и "строительные блоки" PHY.

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

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 нереализованными. 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 *отбеливание* (whitening) потока данных. Дескремблер (descrambler) приемника затем выполняет обратное преобразование этой случайной последовательности с целью получения исходной структурированной последовательности. Большинство из способов скремблирования относится к числу самосинхронизирующихся; 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 зашумленным 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 зашумленную среду передачи. Это можно сделать путем замены последовательностей битов более длинными последовательностями, которые позволят распознать и исправить искаженные биты. Например, если вы хотите передать своему 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 ваш друг получит некоторые биты с ошибками (например, примет последовательность 100111111000101), он все равно сможет восстановить исходную последовательность по схеме "большинства голосов". Хотя подобный кодер слишком прост 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 линий задержки (delay) и сумматоров. 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 предшествующих битов. Длина кодового ограничения (constraint length of a code) показывает, как много выходных элементов выходит из системы в пересчете на один входной. Коды часто характеризуются их эффективной степенью (или коэффициентом) кодирования (code rate). Вам может встретиться сверточный код с коэффициентом кодирования 1/2. Этот коэффициент указывает, что на каждый входной бит приходятся два выходных. При сравнении кодов обращайте внимание на то, что, хотя коды с более высокой эффективной степенью 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 предыдущем примере во время передачи первой части вашей беседы с другом под его окном проезжал самосвал, оказывая воздействие на его слух наряду с вашими сигналами. Последовательность, которую принял ваш друг, может в результате оказаться такой: 011001111000111 (рис. 3.4). Он ошибочно может заключить, что исходной последовательностью была 10101.

По этим причинам стали использовать *чередование* для разброса битов блочных ошибок, которые могли бы произойти, таким образом делая ошибки более похожими на независимые. Чередование может быть выполнено на аппаратном или программном уровне; независимо от этого, основная его цель — 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. Коррелирующие события возникновения ошибок

Рис. 3.5. Кодирование с блочным чередованием

Преобразование символов и модуляция

Процесс модуляции может быть осуществлен потоком битов по отношению к носителю в рабочей полосе частот. Если носителем является простая синусоидальная волна, промодулирована 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 *квадратурная* (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 представляют в декартовой системе координат таким образом: синфазные компоненты откладываются по оси x, квадратурные — по оси y, в результате получается *сигнальное созвездие* (constellation). Иногда это также представляют в виде *комплексной плоскости* с мнимой единицей, j, которая равна корню квадратному из единицы, на квадратурной оси, или оси ординат, и действительной компонентой, откладываемой по синфазной оси, или оси x.

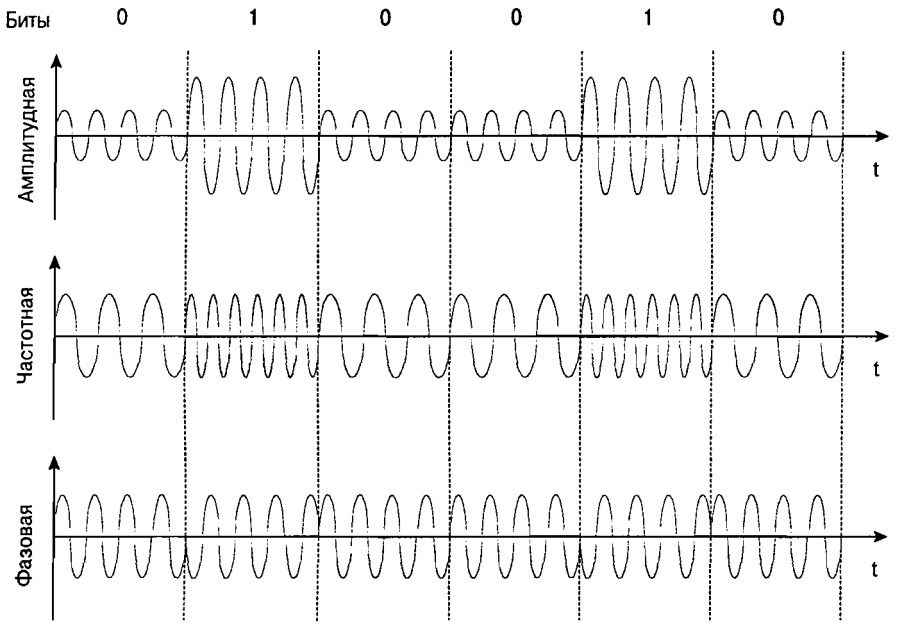


Рис. 3.6. Примеры модуляции

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.[1] 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 созвездия сплошной линией, квадратурные — пунктирной. Этот процесс приводит к появлению в комплексной временной области модулирующего сигнала, который затем сдвигается в частотную область с целью получения реального сигнала в заданной полосе пропускания.

[1] В оригинале — 5,5 Мбит/с. — *Прим. ред.*

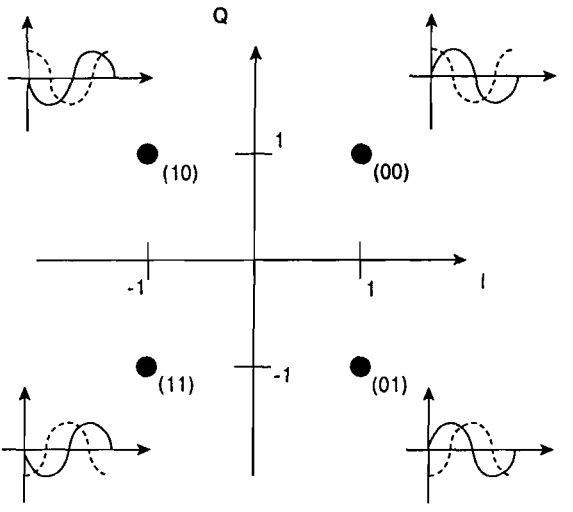


Рис. 3.7. Созвездие QPSK и результирующие синфазная и квадратурная волны

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 Федеральной комиссией 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 предопределенной схеме, как показано на рис. 3.8. Устройства FHSS делят 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.

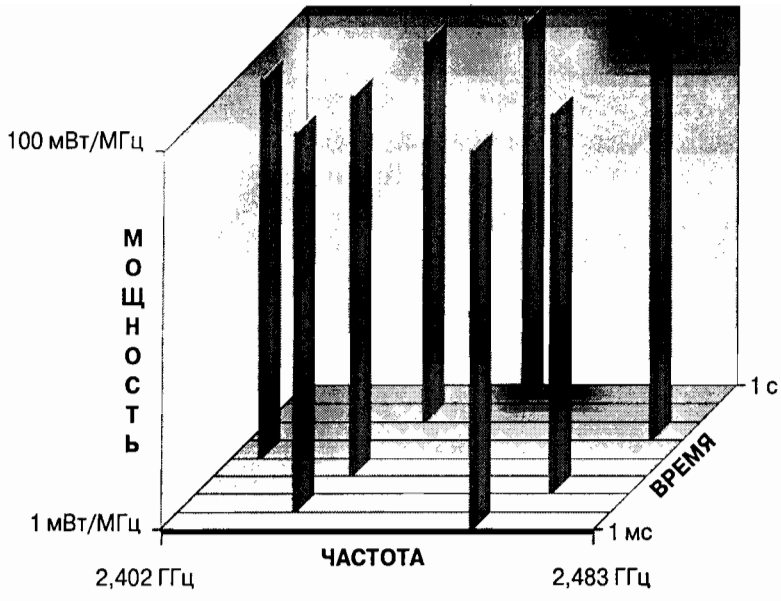


Рис. 3.8. Пример скачкообразной перестройки частоты

Последовательность перестройки частоты должна иметь следующие параметры: частота перескоков не менее 2,5 раз в секунду как минимум между 6-ю (6 МГц) каналами. Чтобы минимизировать число коллизий между перекрывающимися зонами покрытия, возможные последовательности перескоков 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 перекрытие 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}

По сути, схема скачкообразной перестройки частоты обеспечивает неторопливый переход с одного возможного канала на другой таким образом, что после каждого скачка покрывается полоса частот, равная как минимум 6 МГц, благодаря чему в многосотовых сетях минимизируется возможность возникновения коллизий. Уменьшенная длина набора для таких стран, как Япония, Испания и Франция, обусловлена меньшей полосой частот, выделенной ими для промышленного, научного 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 *служебный 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 (напомним, PPDU — это элемент данных протокола PLCP). На рис. 3.9 представлен формат фрейма FHSS подуровня PLCP.

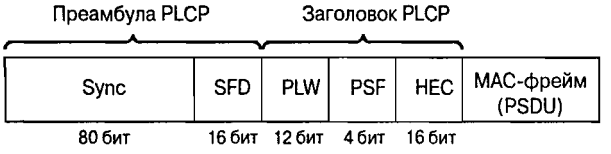


Рис. 3.9. Формат фрейма FHSS подуровня PLCP

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 обеспечение 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 бит. 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 операцию скремблирования с целью отбеливания (рандомизации) последовательности входных битов (см. выше раздел "Составляющие физического уровня"). Получившийся в результате PSDU представлен на рис. 3.10. Заполняющие символы (stuff symbols) вставляются между всеми 32-символьными 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.

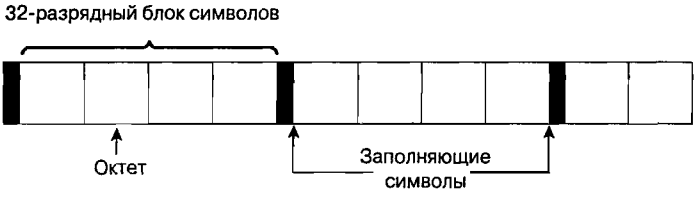


Рис. 3.10. Скремблированный на подуровне PSDU в технологии FHSS

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, вы должны вначале 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 вы хотите передать двоичное значение 0, вы передаете синусоидальный сигнал с частотой f_1, а чтобы переслать 1, передаете сигнал с частотой f_2. Вы договариваетесь о периоде передачи одного символа с вашим другом на другом конце линии связи, и это обусловит 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 представлена частотная область сигналов с магнитудой, представленной в виде высоты векторов $f_1 = f_c - f_d$ и $f_2 = f_c + f_d$.

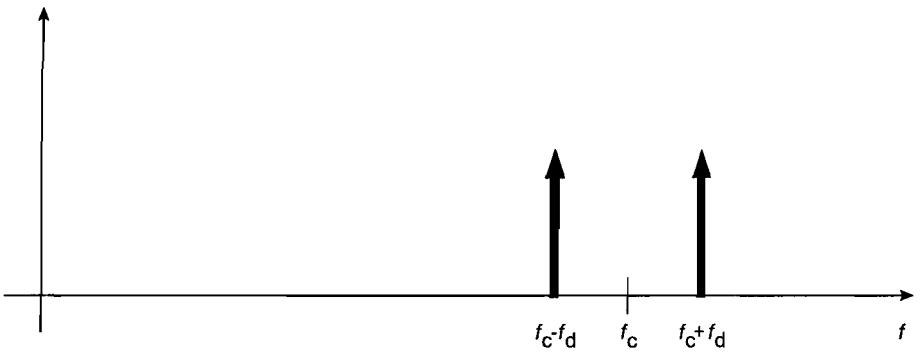


Рис. 3.11. Пример отображения сигналов в частотной области при модуляции FSK

Одним из преимуществ частотной манипуляции является легкость реализации соответствующих передатчика и приемника. FSK функционирует по тем же принципам, что и FM-радиоприемник в вашем автомобиле. Как вы узнаете в главе 8, при использовании FSK значительно упрощается радиочастотный тракт, поскольку модуль сигнала остается постоянным; это означает, что никакая информация не переносится 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 "квант 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 решать 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 позволяет сгладить переходы с 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-

боте на скорости 2 Мбит/с используется модуляция 4GFSK; в этом случае два бита модулируют сигнал одновременно с использованием двух девиаций частоты. В табл. 3.6 представлена информация, которая поможет вам понять, как это делается; f_{d1} примерно в 3 раза больше, чем f_{d2}.

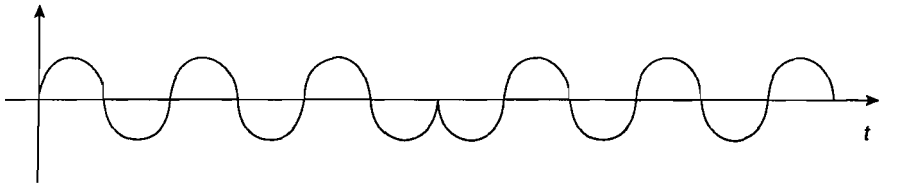


Рис. 3.12. Переход частоты при FSK

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

Символ	Частота
10	$f_c + f_{d2}$
11	$f_c + f_{d1}$
01	$f_c - f_{d1}$
00	$f_c - f_{d2}$

Хотя технология FHSS широко применялась в таких приложениях, как складское хранение и производство на начальном периоде развития локальных беспроводных сетей, она имела ряд недостатков. Первый и основной заключается в том, что эта технология не обеспечивала то качество высокоскоростной передачи данных, которое было характерно для проводных локальных сетей и которое предполагали новые стандарты сетей беспроводных. Второй и менее очевидный состоял в том, что, хотя для использования в последовательности перестройки частот были доступны 79 каналов и три стандартные схемы перестройки частоты, о чем мы говорили в начале данного раздела, сигнал мог "скакать" по всему диапазону ISM, независимо от того, имеются ли поблизости другие устройства (например, медицинские приборы), работающие в этом диапазоне. В главе 8, "Развертывание 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 происходят на половине частот диапазона и вы работаете на скорости 1 Мбит/с, половину времени передача 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 полосе пропускания 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 другого физического уровня — на основе технологии широкополосной модуляции с расширением спектра 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 технологии DSSS стандарта 802.11b такой же, как и для стандарта 802.11, лишь с дополнительными опциональными короткими преамбулой и заголовком.

Беспроводные локальные сети DSSS используют каналы шириной 22 МГц, благодаря чему многие 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 подробно рассматриваться они будут в главе 8, "Развертывание беспроводных LAN".

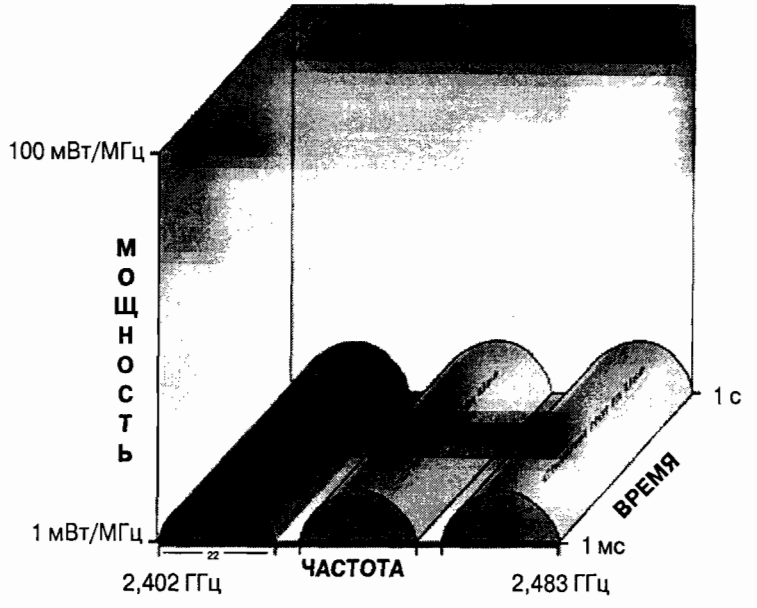


Рис. 3.13. Каналы, используемые в технологии DSSS

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.

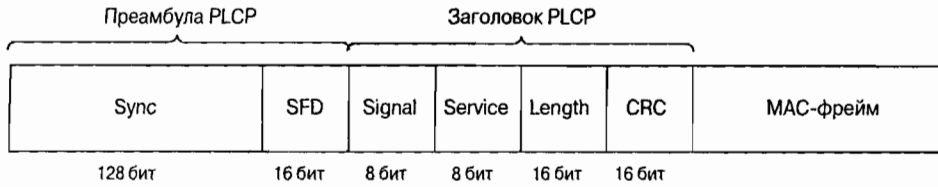


Рис. 3.14. Формат фрейма DSSS PPDU стандарта 802.11

Преамбула 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 и скоростью передачи.
- Подполе Service шириной 8 бит, зарезервировано. Это означает, что во время разработки спецификации стандарта оно осталось неопределенным; предполагается, что оно пригодится в будущих модификациях стандарта.
- Подполе Length шириной 16 бит, указывающее количество микросекунд (из диапазона $16–2^{16} - 1$), 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 преамбула 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

Технологии 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 (поскольку информация заменяется намного большим числом информационных битов) эта технология позволяет передавать информацию при малом соотношении сигнал/шум, обусловленным или помехами, или недостаточной мощностью передатчика. При использовании DSSS переданный сигнал, по сути, усиливается за счет применения расширяющей последовательности, совместно 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-мегагерцевый поток элементарных сигналов, или чипов (chip). Расширяющая спектр последовательность (ее еще называют расщепляющей (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 11111111111, а двоичный 0 — до значения 00000000000). "Расширенные" биты данных затем подаются на схему "ИЛИ" либо "исключающее ИЛИ" одновременно с расширяющей последовательностью, получившиеся в результате чипы преобразуются в символы и модулируются. Этот процесс представлен схематически на рис. 3.15 и 3.16.

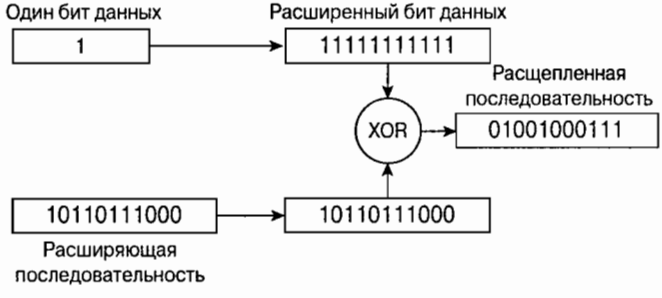


Рис. 3.15. Расширение битов данных с использованием значения 1

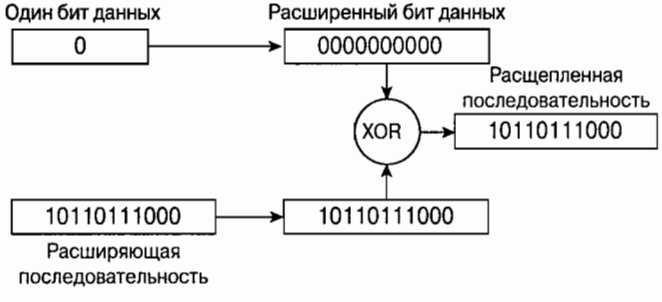


Рис. 3.16. Расширение битов данных с использованием значения 0

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

беспроводную среду. В ходе передачи в нескольких частотных каналах на сигнал накладываются помехи. Поскольку передатчик расширил спектр передаваемого сигнала до 22 МГц, только несколько чипов последовательности окажутся подверженными их влиянию. Приемник сможет восстановить исходную последовательность по полученным чипам. В качестве противоположного данному процессу можно рассматривать таковой получения необработанных данных; в этом случае часть данных из-за помех будет потеряна, и потребуется повторная 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 синфазной компонентой, обе точки сигнального созвездия BPSK располагаются на действительной (Re) оси (рис. 3.17).

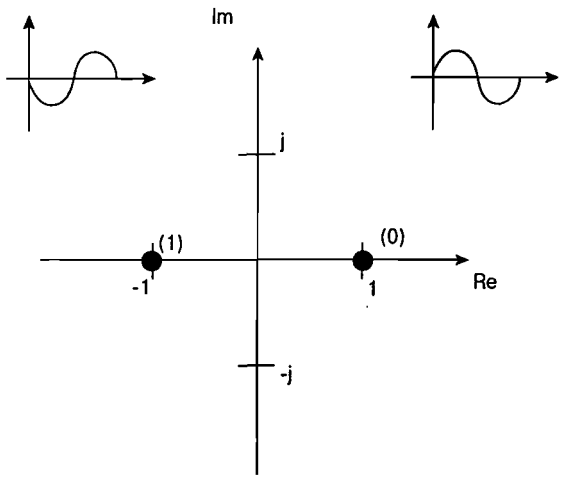


Рис. 3.17. Сигнальное созвездие BPSK

Чтобы приемнику не приходилось удалять фазовую составляющую, возникающую при уходе частоты, используется относительное (иногда его 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 изменяет фазу на 180 градусов, или на π радиан. При модуляции BPSK модуль сигнала также остается неизменным, что упрощает конструкцию радиотракта.

Квадратурная относительная фазовая модуляция (DQPSK)

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

ное кодирование; символы этих двух чипов 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 DBPSK, так и DQPSK приводит к необходимости передавать 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 свойствен тот же недостаток, 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 двоичного пакетного сверточного кодирования (packet binary convolutional coding, PBCC). В технологии HR-DSSS используется та же схема организации каналов, что и в технологии DSSS, — полоса частот 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 значение в подполе Length округляется до ближайшего целого. Например, если необходимо передать 517 октетов, для этого понадобится время длительностью 376 мкс (округленное сверху произведение 517*8/11). Но для передачи 516 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 Extention bit) со значением, равным 1. Благодаря ему приемник будет знать, что нужно вычесть 1 из числа октетов Rx, 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 умножать на 8/11 для получения значения времени в микросекундах.

Таблица 3.9. Значения дополнительного подполя Signal

Signal	Скорость передачи данных
0x37	5,5 Мбит/с
0x6E	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 = CCK, 1 = PBCC
B7	Увеличение длины (length extension)	Используется подполем длины

Короткий фрейм PLCP PPDU 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-

ловков. В случае коротких заголовков 16 бит передается в порядке, обратном по отношению к длинным заголовкам, поэтому они используют значение `0x05CF` вместо `0xF3A0`.

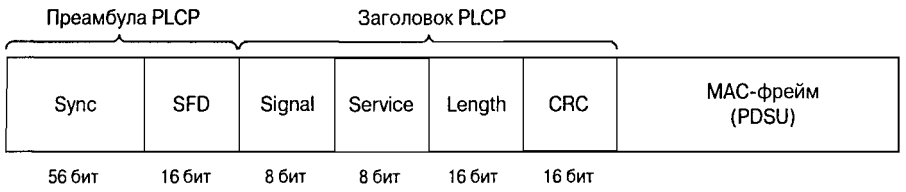


Рис. 3.18. Короткий PPDU технологии HR-DSSS

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 подходящей 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 скоростей 5,5 и 11 Мбит/с с применением CCK, относится к методам, которые применяются для скоростей 1 и 2 Мбит/с, он по-своему уникален. В обоих случаях применяется метод расширения, но при использовании модуляции CCK расширяющий 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 8 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 передавать данные со скоростью 5,5 Мбит/с, нужно сгруппировать 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} представляют чипы последовательности. В табл. 3.11 j представляет мнимое 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	j	1	j	–1	j	1	–1	1
01	–j	–1	–j	1	j	1	–j	1
10	–j	1	–j	–1	–j	1	j	1
11	j	–1	j	1	–j	1	j	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 модуляция CCK

(b0, b1)	Изменение фазы четных символов	Изменение фазы нечетных символов
00	0 (0 градусов)	π (180 градусов)
01	π/2 (90 градусов)	–π/2 (–90 градусов)
11	π (180 градусов)	0 (0 градусов)
10	–π/2 (–90 градусов)	π/2 (90 градусов)

Это вращение фазы применяется по отношению к 8 комплексным чипам 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 последовательность, состоящую из 8 комплексных чипов, 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 опциональный 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 на двоичный сверточный кодер, работающий с эффективной степенью кодирования 1/2, о чем впервые было упомянуто в разделе "Составляющие физического уровня". Особый полускоростной кодер (particular half-rate encoder) имеет шесть линий задержки (delay), или запоминающих ячеек, и выдает 2 бита на каждый входной. Поскольку стандарт 802.11 рассчитан на использование фреймов и сверточные кодеры имеют память, все элементы задержки обнуляются с началом фрейма, а в его конец добавляется один октет нулей, чтобы обеспечить одинаковую помехоустойчивость для всех битов. Этот заключительный октет объясняет, почему вычисления длины, рассмотренные в разделе "Подуровень PLCP технологии HR-DSSS стандарта 802.11b", слегка отличаются для CCK и PLCC. Затем закодированный поток битов пропускается 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, s, поступающего от 256-битовой псевдо-

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.

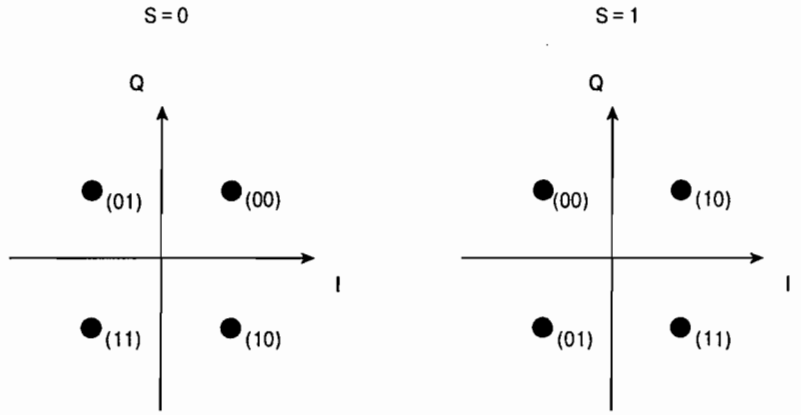


Рис. 3.19. Преобразование символов PBCC QPSK

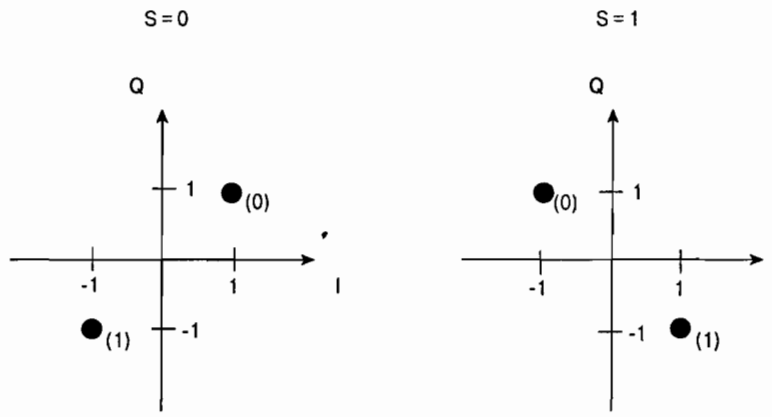


Рис. 3.20. Преобразование символов PBCC BPSK

Беспроводные локальные сети стандарта 802.11a

В то же самое время, когда в проекте стандарта 802.11b в 1999 году был описан физический канал с технологией HR-DSSS, в проекте стандарта 802.11a было предложено использовать физический канал, в котором используется технология мультиплексирования с разделением по ортогональным частотам (orthogonal frequency division multiplexing, OFDM) в диапазоне 5 ГГц. Он узаконивал скорости передачи до 24 Мбит/с и опционально — до 54 Мбит/с в безлицензионных диапазонах национальной информационной инфраструктуры США U-NII (unlicensed national information infrastructure) 5,15–5,25 ГГц, 5,25–5,35 ГГц и 5,725–5,825 ГГц. Стандарт 802.11a регламентирует использование каналов шириной 20 МГц и определяет по четыре канала для каждого из трех диапазонов (о них подробно

рассказывается в главе 8, "Развертывание 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 по 255, 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.

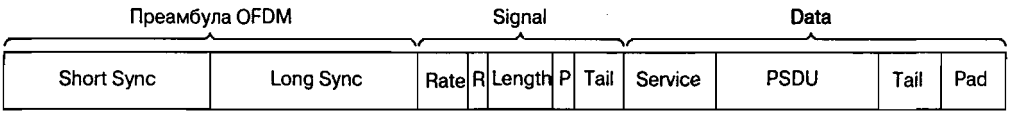


Рис. 3.21. Формат фрейма PPDU стандарта 802.11a

Фрейм PPDU состоит из трех основных частей: преамбулы OFDM, полей 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 (АРУ), 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 псевдослучайных последовательностей).

- Подполе PSDU, содержащее полезные данные, подлежащие передаче.
- Подполе Tail, заменяющее 6 заключительных скремблированных нулей нескремблированными нулями для реинициализации (повторной установки в начальное состояние) сверточного кодера с конечной памятью.
- Подполе Pad 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

R1–R4	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 (intersymbol interference, ISI). Рассмотрим процесс передачи символа по технологии QPSK (напомним, QPSK — это фазовая манипуляция 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[2], первый символ (как правило, его "хвост") может наложиться на второй (точнее, на начало второго символа). Такое наложение 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 количество 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-

[2] Существенные задержки могут быть вызваны многолучевым распространением сигнала. — *Прим. ред.*

вого 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 способов с применением схем выравнивания параметров каналов (channel-equalization scheems), для максимального использования полосы пропускания канала. Схемы многоканальной модуляции (multichannel modulation scheems) 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 осуществляется модуляция сигнала при скачкообразной перестройке частоты (FHSS), весь канал передачи разбивается на N независимых подканалов. При заданной полосе 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.

Полезным 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 4-QAM символов (от англ. quadrature amplitude modulation — квадратурная амплитудная модуляция), которые затем преобразуются во временную область посредством обратного БПФ. Следует также сказать о том, что принятие 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 вдаваясь в дебри 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 приемной стороне, принятый сигнал должен быть подвергнут циклической свертке (circular convolution) входа с каналом (of the input with the channel)[3], что противоположно только свертке. *Свертка* — это математическая операция, применяемая для описания прохождения сигнала через канал и вычисления получающегося выходного сигнала. Чтобы быть уверенным в качестве принятого сигнала, вы должны взять временное представление символа OFTM и создать циклический префикс путем повторения окончания v символа в его начале. Этот процесс проиллюстрирован на рис. 3.22, где v — длина циклического префикса и N — используемый размер входных данных БПФ.

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

[3] Видимо, имеется в виду свертка входного сигнала с импульсной характеристикой канала. — *Прим. ред.*

тервал позволяет последовательно обрабатывать символы, и если описывать данный процесс в частотной области, это означает последовательную обработку подканалов.

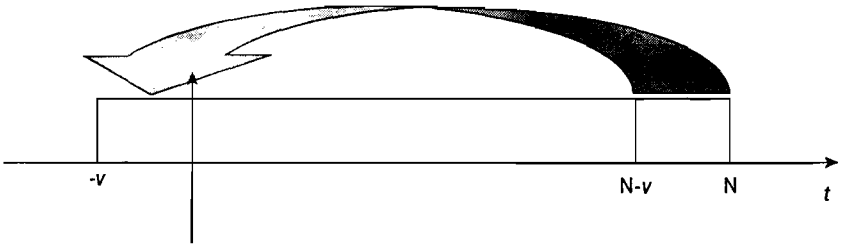


Рис. 3.22. Формирование циклического префикса в технологии OFDM.

Для того чтобы приемник мог определить импульсную характеристику канала (to estimate the channel), часто или вставляют известные настроечные символы на некоторых из N поднесущих частот, или передают отдельный OFDM-символ, который приемник может использовать для определения импульсной характеристики канала. Зачастую также подканалы, расположенные на краях общей полосы пропускания, наполняют 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 небеспроводных приложениях, таких как асимметричная цифровая абонентская линия (asymmetric digital subscriber line, ADSL), где параметры каналов не изменяются со временем, передатчик использует знание о канале и передает больше битов, или информации, по тем абонентским линиям, которые меньше искажают сигнал или имеют меньшее затухание.

Настройка OFDM

Как уже упоминалось ранее, поле Sync состоит из длинных и коротких символов (рис. 3.23). Существует 10 коротких настроечных символов, и каждый из них представляет собой короткий OFDM-символ, который наполняет 12 из 52 используемых подканалов специальным QPSK-символом, умноженным на 4. Это приводит к появлению во временной области периодической последовательности, которую можно использовать для обнаружения начала фрейма, выполнения автоматической регулировки усиления, выбора подходящей антенны, если имеется такая возможность, грубой оценки ухода частоты и синхронизации тайминга.

Рис. 3.23. Поле Sync

Два длинных настроечных символа идентичны и модулируют поднесущую частоту специальной последовательностью. Длинная настроечная последовательность позволяет выполнить оценку параметров канала и точно оценить уход частоты. Поскольку оба длинных настроечных символа предназначены для совместного использования, для них необходим только один охранный 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[4]. Скорость 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 символов с количеством бит на символ, зависящим от скорости передачи данных. Они помещаются на 48 поднесущих OFDM-символа, а на 4 поднесущих передаются пилот-сигналы. Выполняется обратное быстрое преобразование Фурье, после чего формируется циклический префикс. Результирующая последовательность модулирует подходящую несущую.

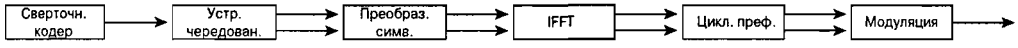


Рис. 3.24. Обобщенная схема передатчика OFDM стандарта 802.11a

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

Таблица 3.14. Параметры передатчика стандарта 802.11a

Скорость передачи данных (Мбит/с)	Сигнальное 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	3/4	6	288	216

Описанное нами 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 подполя 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 заполняющих 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 применяемая опционально в PBCC 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 такая замена приводит к повышению степени кодирования, поскольку на каждый входной бит передается меньше битов кода. Опускание битов производится оговоренным 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 добиваются того, чтобы соседние канальные биты передавались несоседними несущими, на втором — чтобы соседние канальные биты преобразовывались попеременно в менее и более старшие разряды сигнального созвездия отображения символов. Этот процесс является важным, потому что в созвездиях высшего порядка самые младшие биты (LSB) часто передаются с меньшей надежностью. Эта проблема станет для вас более очевидной, если вы рассмотрите сигнальные созвездия; их точки, которые близки и более подвержены искажениям и ошибкам, имеют тенденцию отличаться 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 используются 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	$\frac{1}{\sqrt{42}}$

[4] Их также называют канальные символы или биты кода (coded bits). — *Прим. ред.*

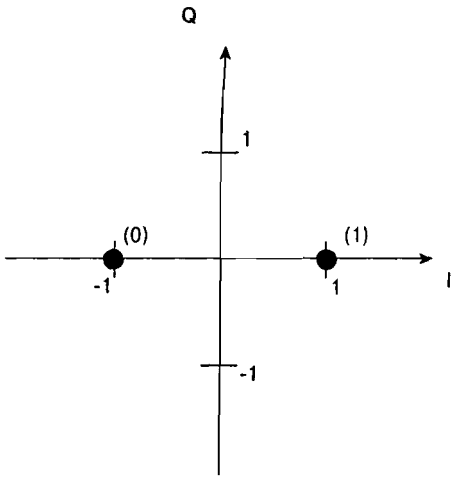


Рис. 3.25. Созвездие стандарта 802.11a для модуляции типа BPSK

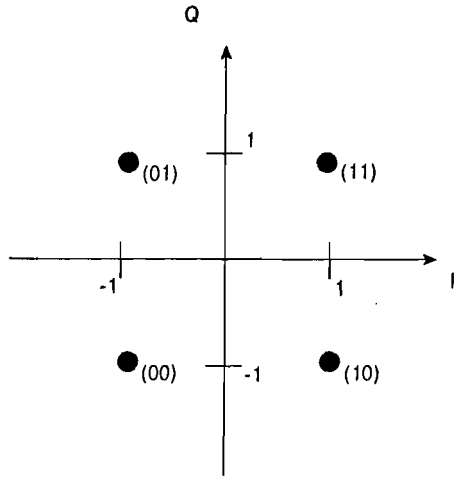


Рис. 3.26. Созвездие стандарта 802.11a для модуляции типа QPSK

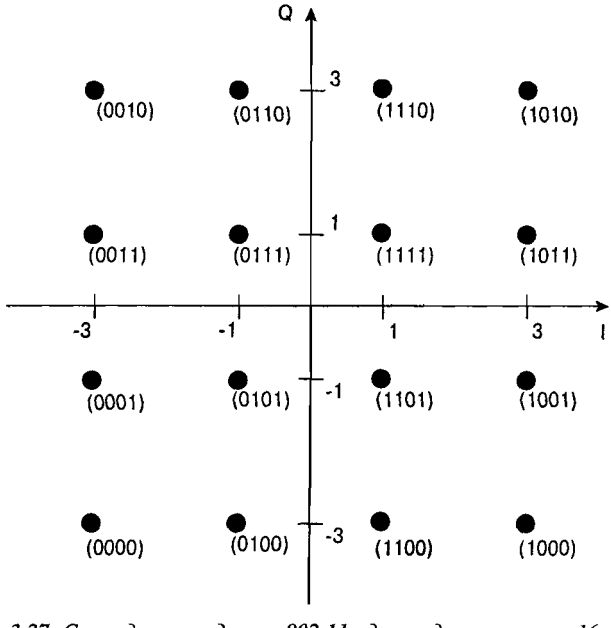


Рис. 3.27. Созвездие стандарта 802.11a для модуляции типа 16-QAM

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

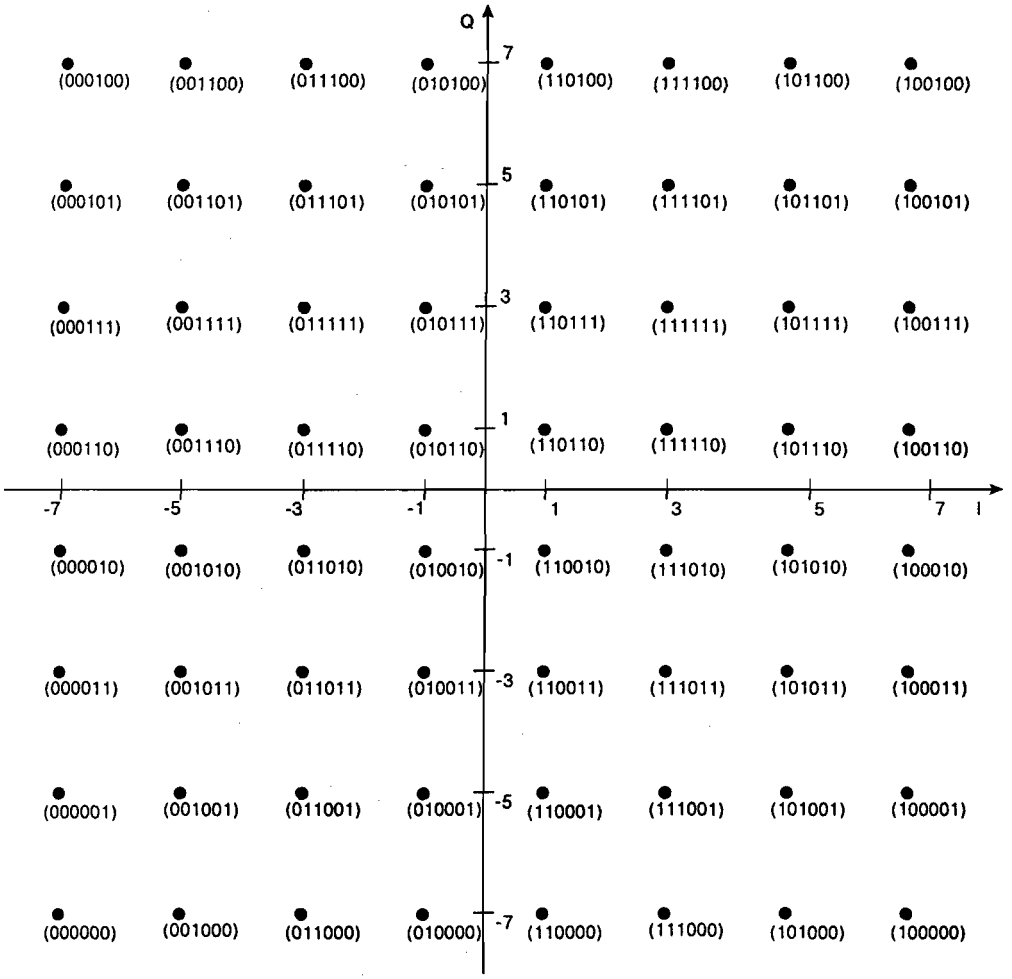


Рис. 3.28. Созвездие стандарта 802.11a для модуляции типа 64-QAM

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-ORFM, ERP-PBCC и DSSS-OFDM. При использовании ERP-ORFM 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-

дачи данных 1, 2, 5,5 и 11 Мбит/с. Стандарт также позволяет опционально использовать режимы PBCC 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-ORFM, ERP-PBCC и DSSS-OFDM.

Подуровень PLCP стандарта 802.11g

Стандарт 802.11g определяет пять подуровней PLCP: с длинной преамбулой, короткой преамбулой, преамбулой ERP-ORFM, длинной преамбулой DSSS-OFDM и короткой преамбулой DSSS-OFDM. Поддержка первых трех обязательна, двух последних — 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 поддерживают/взаимодействуют
Длинная	1, 2, 5,5 и 11 Мбит/с DSSS-OFDM на всех скоростях OFDM ERP-PBCC на всех скоростях ERP-PBCC
Короткая	2, 5,5 и 11 Мбит/с DSSS-OFDM на всех скоростях OFDM ERP-PBCC на всех скоростях ERP-PBCC
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 (locked clocks)	0 — не заблокированы; 1 — генераторы тактовой частоты передатчика и символов заблокированы
b3	Выбор модуляции	0 — не ERP-PBCC; 1 — ERP-PBCC
b4	Зарезервирован	0
b5	Расширение длины	Для ERP-PBCC
b6	Расширение длины	Для ERP-PBCC
b7	Расширение длины	Для PBCC

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

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

Преамбула ERP-OFDM использует таковую стандарта 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. 3.29. В подполе Rate поля Signal устанавливается скорость 3 Мбит/с. Благодаря такой установке обеспечивается совместимость со станциями, не поддерживающими EPR, потому что они по-прежнему считывают значение поля Length и откладывают передачу, несмотря на то что не способны демодулировать полезную нагрузку. Заголовок PLCP соответствует таковому предварительно определенной длинной 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.

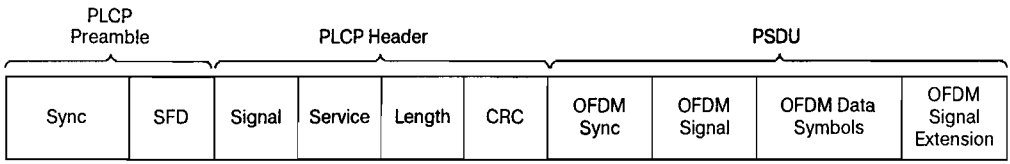


Рис. 3.29. Формат длинной преамбулы PPDU технологии CCK-OFDM

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 диапазона 2,4 ГГц ERP-OFDM также устанавливает, что центральная частота передачи и тактовая частота символов определяются тем же генератором, который был опциональным для DSSS. Он использует канальный интервал длительностью 20 мкс, но она может быть уменьшена до 9 мкс, если выяснится, что в BSS находятся только устройства ERP.

ERP-PBCC

Для передачи данных с более высокими скоростями, 22 и 33 Мбит/с, технология двоичного пакетного сверточного кодирования (PBCC) использует тот же механизм, что и на меньших скоростях, 5,5 и 11 Мбит/с PBCC, но с использованием 8-PCK вместо QPCK и BPCK 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.

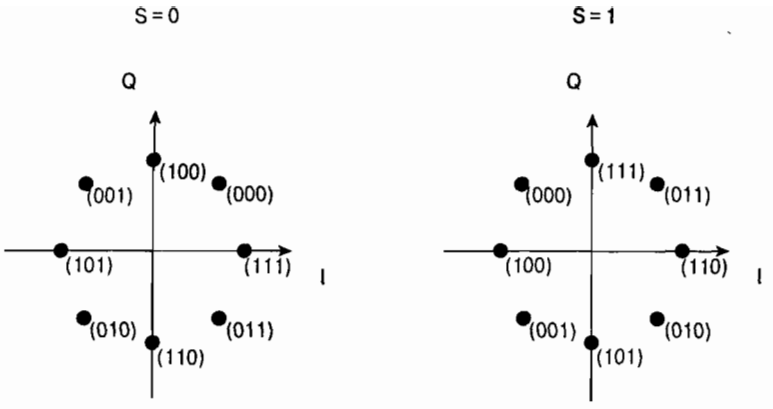


Рис. 3.30. Сигнальное созвездие ERP-PBCC стандарта 802.11g

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 способом, обеспечивающим обратную совместимость со старыми устройствами, соответствующими стандарту 802.11b. Если в локальной сети используются только устройства стандарта 802.11g, передача осуществляется с наивысшей возможной скоростью. Однако, если в нее вводятся устройства стандарта 802.11b, информация заголовков должна передаваться со скоростями стандарта 802.11b, чтобы их могли "понимать" эти старые устройства. Такое снижение скорости должно 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 незанятости основывается на выявлении в канале энергии, превосходящей некоторое пороговое значение.
- Решение о незанятости основывается на обнаружении сигнала несущей, соответствующей стандарту 802.11.
- Обнаружение несущей и выявление энергии (комбинация способов 1 и 2).
- Обнаружение несущей с сообщениями таймера о том, что среда не занята, если никакой сигнал не обнаружен в течение 3,65 мс.
- Выявление 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 технология 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.

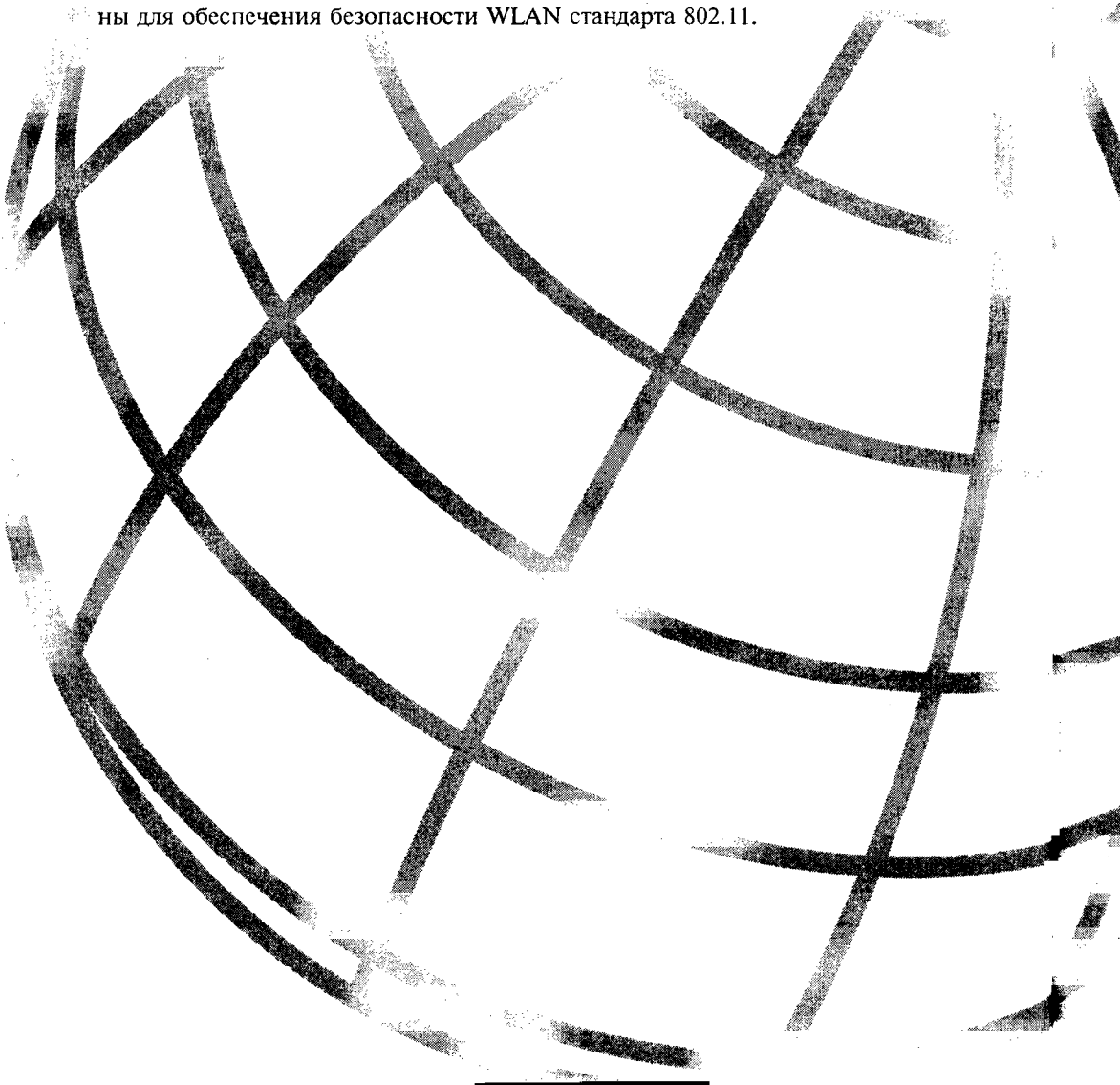
Таблица 3.18. Стандарты PHY 802.11

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	CCK	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 алгоритмов 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 средств аутентификации.
- **Усовершенствования, которые будут внесены в систему защиты беспроводных LAN (WLAN) следующего поколения.** Новые технологии, которые будут использованы для обеспечения безопасности WLAN стандарта 802.11.



Глава 4

Безопасность беспроводных LAN

Разработчикам, которые уже применяли или применяют сейчас беспроводные локальные сети стандарта 802.11, множество аббревиатур, которые описывают повышенную защищенность беспроводных LAN стандарта 802.11, напоминает суп с макаронами в виде 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. Сетевого администратора, привыкшего иметь дело с IP-протоколами и ориентированными на установление соединения технологиями, эти новые, ориентированные на соблюдение безопасности протоколы могут сбить с толку.

Безопасность беспроводных сетей

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

Устройства стандарта 802.11 связываются друг с другом, используя в качестве переносчика данных сигналы, передаваемые 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 необходимы 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.

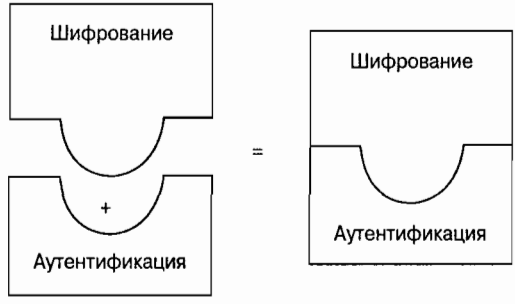


Рис. 4.1. Защита в беспроводных сетях обеспечивается за счет аутентификации и шифрования

В спецификации стандарта 802.11 регламентировано применение механизма аутентификации устройств с открытым и с совместно используемым ключом и механизма WEP, обеспечивающего защищенность данных на уровне проводных 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 (групповой) 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 закодированный 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 дополняется 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 вызывают повышенную, по

сравнению с поточным шифрованием, нагрузку на центральный процессор. В результате производительность устройств, применяющих блочное шифрование, снижается.

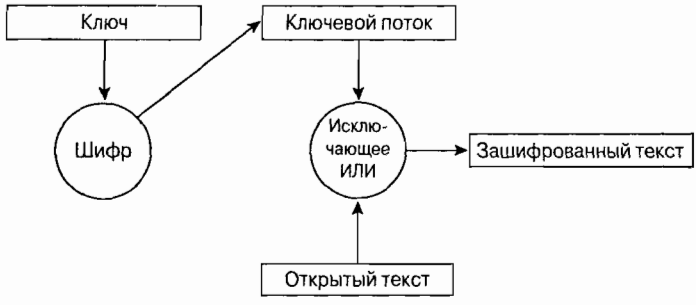


Рис. 4.2. Так осуществляется поточное шифрование

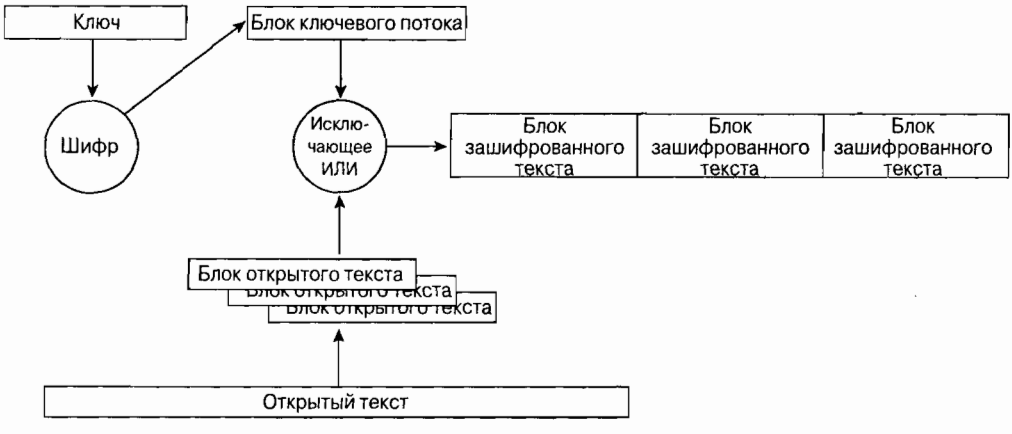


Рис. 4.2. Так осуществляется блочное шифрование

Процесс шифрования, описанный нами для поточных и блочных шифров, называется *режим шифрования с помощью книги электронных кодов* (Electronic 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 получать образцы зашифрованного текста и выдвигать какие-то предположения об исходном тексте.

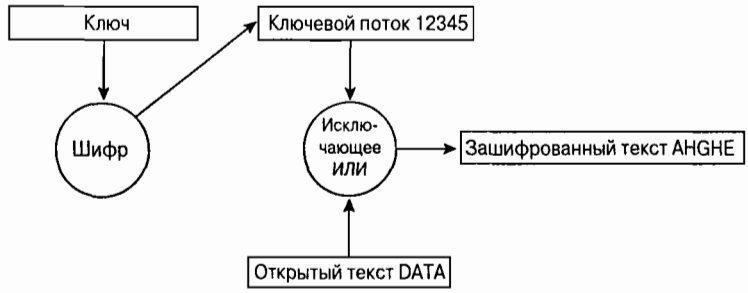
Некоторые методы шифрования позволяют решить эту проблему.

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

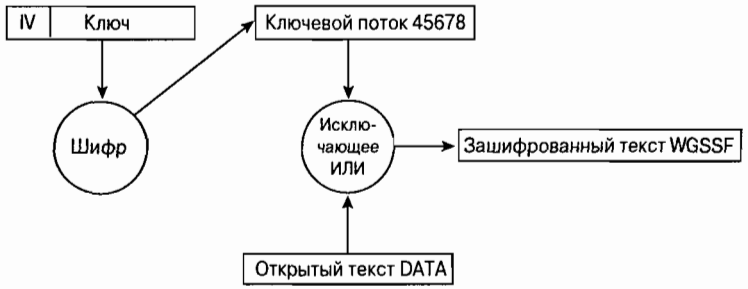
Векторы инициализации

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 поточного 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 сценарий 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 изменять вектор инициализации пофреймово (on a per-frame basis). Это означает, что если один и тот же фрейм будет передан дважды, весьма высокой окажется вероятность того, что зашифрованный текст будет разным.



1. Шифрование с использованием поточного шифра *без применения вектора инициализации*



2. Шифрование с использованием поточного шифра и вектора инициализации

Рис. 4.4. Шифрование и векторы инициализации

Режимы с обратной связью

Режимы с обратной связью представляют собой модификации процесса шифрования, выполненные 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-

ного поточного шифра RC4. Симметричность RC4 означает, что согласованные WEP-ключи размером 40 или 104 бит статично конфигурируются на клиентских устройствах и в точках доступа. Алгоритм WEP был выбран главным образом потому, что он не требует объемных вычислений. 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 слабенькими процессорами. WEP — простой в применении алгоритм, для записи которого в некоторых случаях достаточно 30 строк кода. Малые непроизводительные расходы, возникающие при применении этого алгоритма, делают его идеальным алгоритмом шифрования для специализированных устройств.

Чтобы избежать шифрования 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.

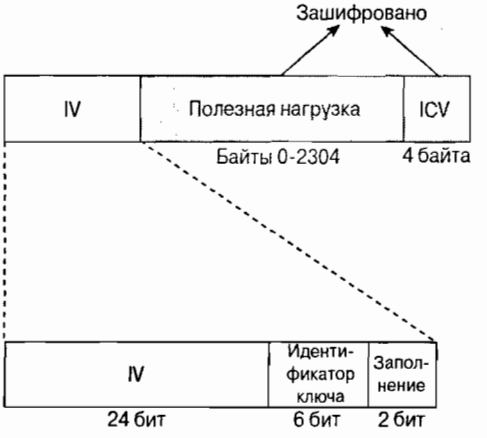


Рис. 4.5. Фрейм, зашифрованный по алгоритму WEP

Вектор инициализации должен изменяться пофреймово во избежание IV-коллизий. 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 предоставляет злоумышленникам большие возможности по разгадыванию данных открытого текста путем сопоставления подобных элементов. При использовании вектора инициализации важно предотвратить подобный сценарий, 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.

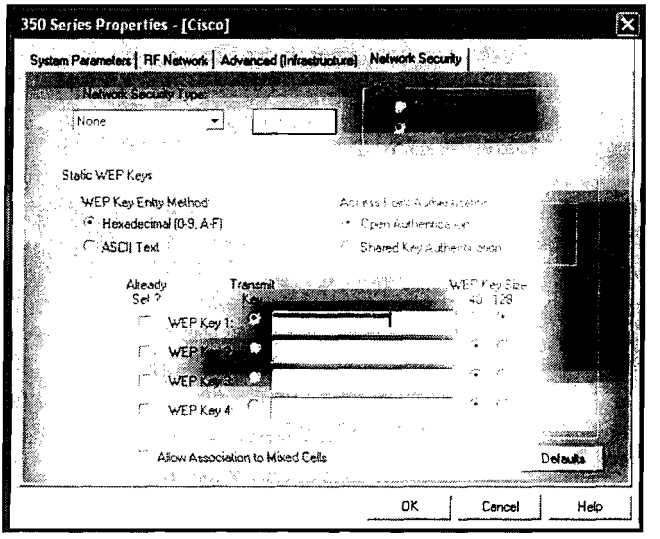


Рис. 4.6. Конфигурирование WEP

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.

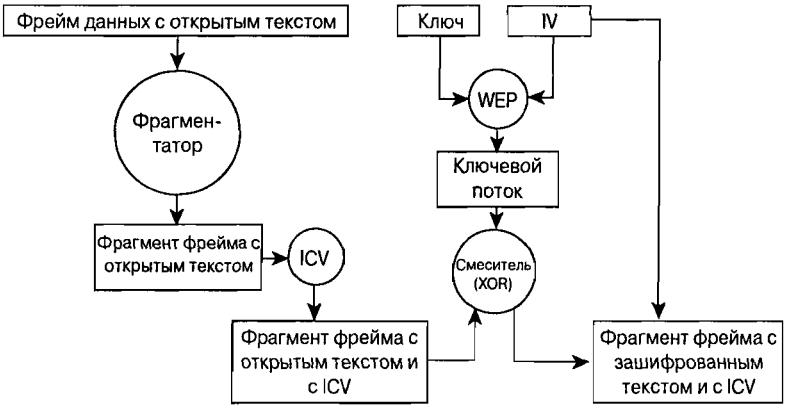
- Данные или полезная нагрузка (payload).
- Контрольный признак целостности (integrity check value, ICV).

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 циклического 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

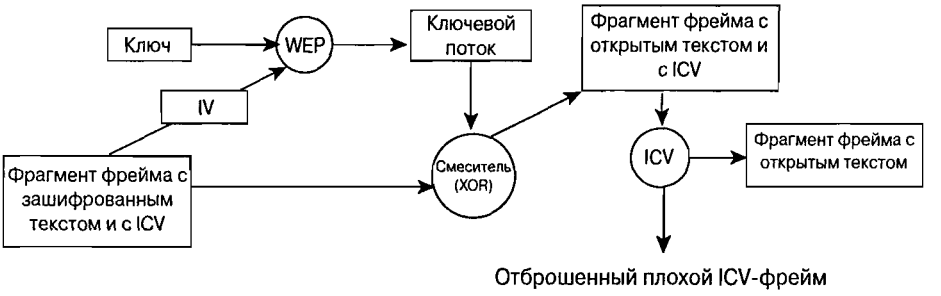


Рис. 4.7. Процесс шифрования и дешифрования

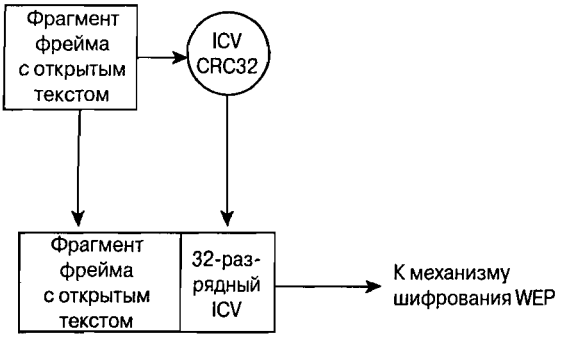


Рис. 4.8. Диаграмма функционирования механизма ICV

Механизмы аутентификации стандарта 802.11

Спецификация 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 нулевой аутентификацией (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 зашифровывать и расшифровывать фреймы, и такие фреймы будут отброшены как точкой доступа, так и клиентской станцией. Этот процесс предоставляет собой довольно-таки эффективное средство контроля доступа к BSS (рис. 4.9).

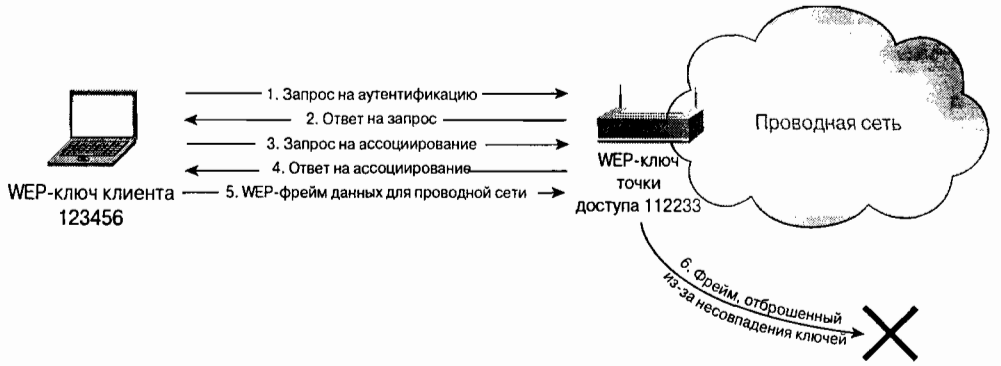


Рис. 4.9. Процесс открытой аутентификации при различии WEP-ключей

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 вызов, 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.

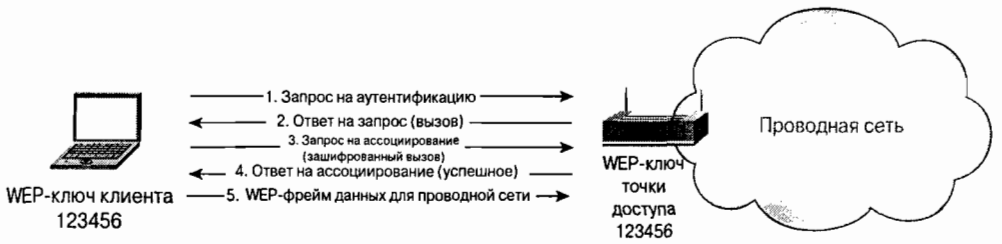


Рис. 4.10. Процесс аутентификации с совместно используемым ключом

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 внешнем аутентификационном сервере (рис. 4.11). Аутентификация с использованием MAC-адресов усиливает действие открытой аутентификации и аутентификации с совместно используемым ключом, обеспечиваемыми стандартом 802.11, потенциально снижая тем самым вероятность того, что неавторизованные устройства получат доступ к сети. Например, администратор сети может пожелать 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.

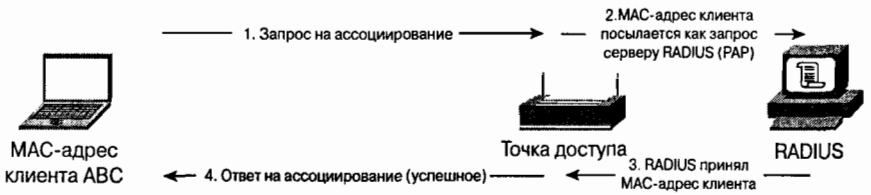


Рис. 4.11. Процесс аутентификации с использованием MAC-адресов

Уязвимость системы защиты стандарта 802.11

В предыдущем разделе рассказывалось о том, как осуществляются 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 статичного 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 шифровал текст вызова, полученного от точки доступа. Точка доступа аутентифицирует клиента путем расшифровки зашифрованного с помощью совместно используемого ключа ответа и проверки того, что полученный текст вызова полностью соответствует отправленному.

Процесс обмена текстом вызова осуществляется по беспроводному каналу связи и является уязвимым для атаки, возможной при знании 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 состоит в перемешивании открытого текста с ключевым потоком и получении в результате зашифрованного текста. Процесс перемешивания представляет собой выполнение двоичной математической операции, которая называется "исключающее ИЛИ" (XOR). Если открытый текст перемешать 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).

Злоумышленник может захватить как открытый, так и зашифрованный текст ответа. Выполнив над этими значениями операцию "исключающее ИЛИ", он может получить действующий ключевой поток. Затем злоумышленник 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-

кующий сеть злоумышленник может проследить процесс аутентификации с совместно используемым ключом и заполучить ключевой поток.

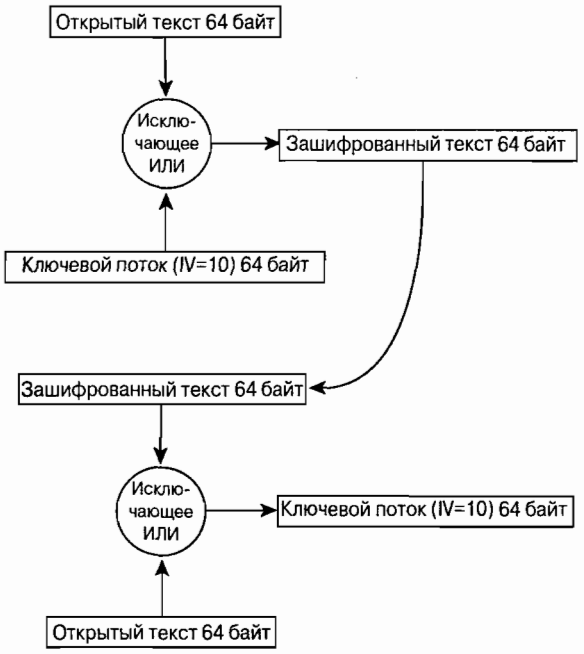


Рис. 4.12. Извлечение ключевого потока

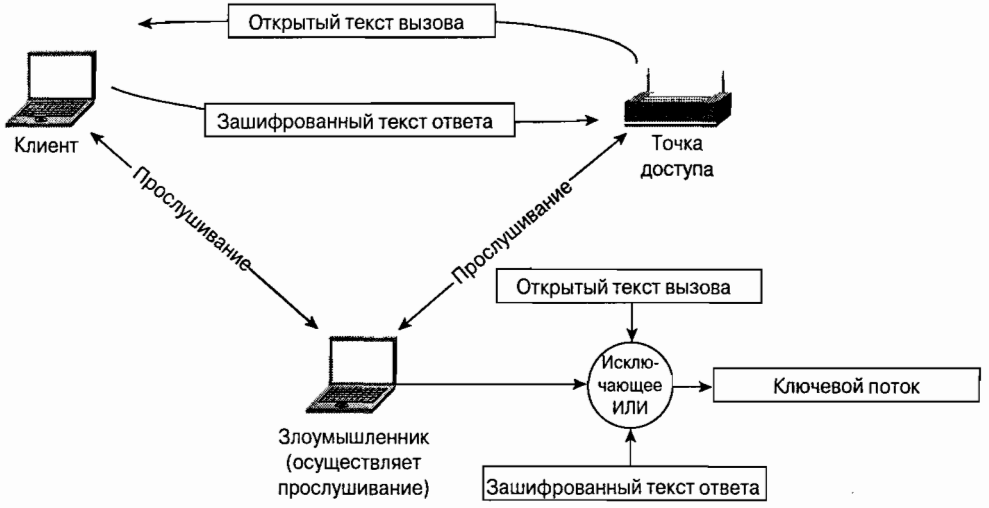


Рис. 4.13. Уязвимость механизма аутентификации с совместно используемым ключом

Уязвимость аутентификации с использованием MAC-адресов

MAC-адреса пересылаются с помощью незашифрованных 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. Атакующий может использовать анализатор протокола для определения разрешенного в BSS MAC-адреса и сетевую карту, допускающую локальное назначение адреса, для имитации разрешенного MAC-адреса.

Уязвимость WEP-шифрования

Наиболее серьезные и непреодолимые проблемы защиты сетей стандарта 802.11 были выявлены криптоаналитиками Флурером (Fluhrer), Мантином (Mantin) и Шамиром (Shamir). В своей статье они показали, что WEP-ключ может быть получен путем пассивного накопления 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 слабые IV — weak IV) могут раскрыть биты ключа в результате проведения статистического анализа. Исследователи компании AT&T и университета Rice, а также разработчики приложения AirSnort воспользовались этой уязвимостью и выяснили, что можно заполучить WEP-ключи длиной 40 или 104 бит 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 переданные фреймы. В отличие от уязвимости аутентификации с совместно используемым ключом, атакующий, как показали Флурер, Мантин и Шамир, может заполучить действующий WEP-ключ, а не только ключевой поток. Эта информация позволит атакующему получить доступ к BSS в качестве аутентифицированного устройства без ведома администратора сети.

Если атаки такого типа окажется недостаточно, можно, как показывает теория, провести на механизм WEP и другую (правда, на практике атаки такого рода не проводились). 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 определенной длины. Умозрительно можно предположить, что атакующий будет прослушивать сеть с целью накопления как можно большего числа таких ключевых потоков, чтобы создать

базу данных ключ–поток, взломать сеть и получить возможность расшифровывать фреймы. В беспроводной LAN, в которой не используется аутентификация с совместно используемым ключом, атака с применением побитовой обработки фрейма позволяет злоумышленнику вывести большое количество ключевых потоков за короткое время.

Атаки с использованием побитовой обработки (или "жонглирования битами", bit flipping) основаны на уязвимости контрольного 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 random 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 устройство более высокого уровня (повторитель или хост-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 находится в зашифрованной с помощью WEP части фрейма; как атакующий может изменить ее, чтобы согласовать изменения, вызванные жонглированием битами, 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.

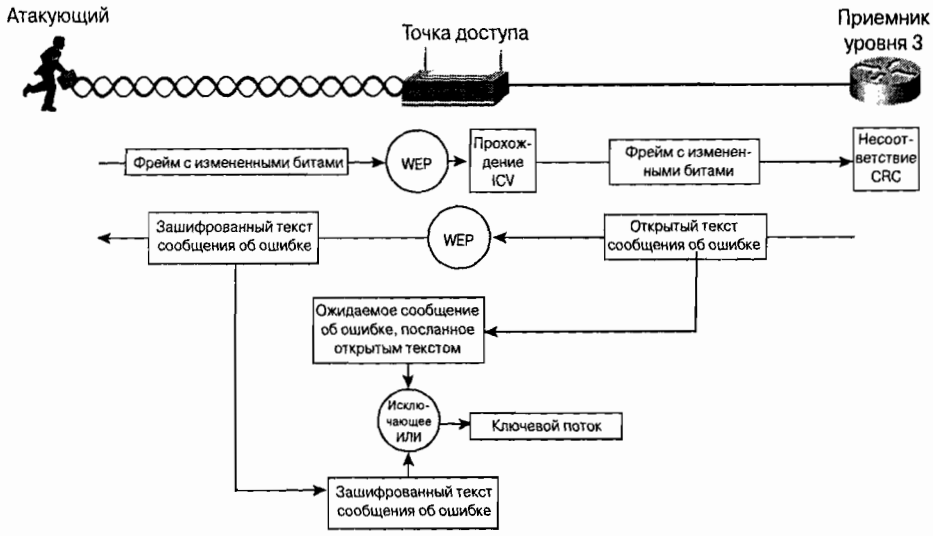


Рис. 4.14. Атака с использованием побитовой обработки

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

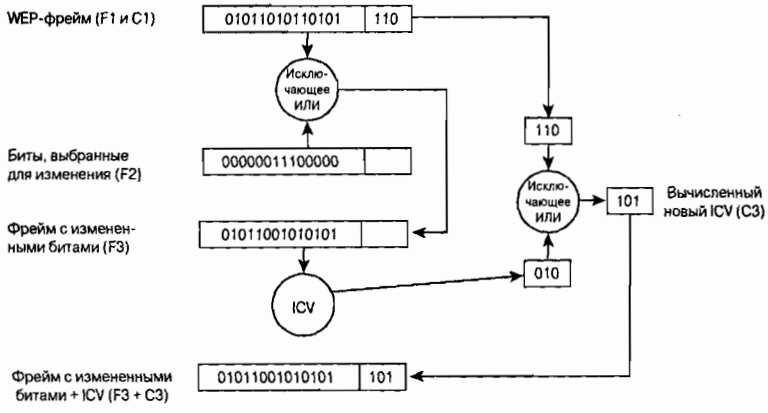


Рис. 4.15. Модифицирование ICV за счет побитовой обработки

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 возник-

новению проблемы, связанной с защитой сети. Для ее решения администратору сети придется долго вручную изменять ключи всех беспроводных устройств сети, если имеющийся ключ "скомпрометирован" 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, когда счет беспроводных пользовательских устройств идет на тысячи. Без механизма распределения или генерации ключей администратору придется дневать и ночевать там, где развернута беспроводная сеть.

Защищенные LAN стандарта 802.11

Промышленность преодолела слабые места в механизмах аутентификации и защиты сетей стандарта 802.11. Чтобы предоставить пользователям решения, обеспечивающие защищенность, масштабируемость и управляемость сетей, IEEE повысил защищенность сетей стандарта 802.11, разработав улучшенный 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 поднабор 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 вопросы защиты сетей стандарта 802.11, а также совместного использования WEP-шифрования и аутентификации — открытой либо с совместно используемым ключом, — многие ошибочно 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 усиливает действие алгоритма аутентификации путем организации защищенного обмена сообщениями между клиентом, точкой доступа и сервером аутентификации.
- **Алгоритм аутентификации**. Представляет собой алгоритм, посредством которого подтверждаются полномочия пользователя.
- **Алгоритм защиты данных**. Обеспечивает защиту при передаче через беспроводную среду фреймов 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 подменены.

Названные четыре составляющие показаны на рис. 4.16.

Первая составляющая: базовая аутентификация

Основой аутентификации стандарта 802.11 является служебный фрейм аутентификации стандарта 802.11. Этот служебный фрейм помогает реализовать алгоритмы открытой аутентификации и аутентификации с совместно используемым ключом, хотя сам по себе фрейм не обладает способностью аутентифицировать клиента. Поскольку о недостатках 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 устройства, подобная открытой аутентификации и аутентификации с совместно используемым ключом, не способна воспрепятствовать неавторизованным пользователям воспользоваться авторизованным устройством. Из этого следует, что при потере или краже такого устройства или по окончании работы по найму администратор сети будет вынужден вручную изменять 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. Разновидности 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 назначаются 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-

зуемым ключом точка доступа или сеть аутентифицирует клиента. Последний не знает наверняка, что подключился именно 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 станция может выдать себя за "законную" точку доступа и повредить данные на клиентской машине. На рис. 4.17 представлены диаграммы, иллюстрирующие процессы односторонней и взаимной аутентификации.

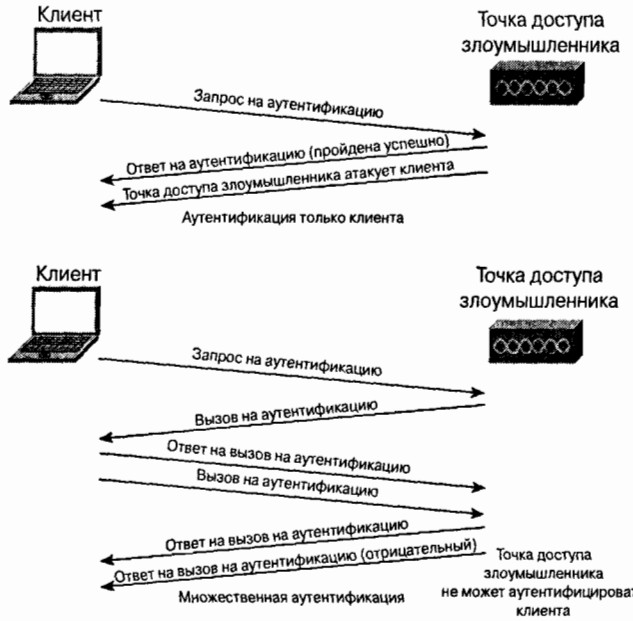


Рис. 4.17. Односторонняя и взаимная аутентификация

Поставщики сетей стандарта 802.11 и IEEE осознают необходимость усиления и замены существующих механизмов обеспечения защиты — и аутентификации, и шифрования. Исследовательская группа I рабочей группы стандарта 802.11 сейчас работает над этим, и после 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 принятия 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 наращивать его механизмы аутентификации до таковых, 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 *расширяемый протокол аутентификации* (Extensible Authentication Protocol, EAP). Попросту говоря, стандарт 802.1X инкапсулирует сообщения для использования их на уровне 2. Стандарт 802.11i включает базовую аутентификацию стандарта 802.1X, требуя, чтобы она применялась для аутентификации пользователей. На рис. 4.18 представлен стандарт 802.1X в части алгоритма аутентификации и топологий канального уровня серии стандартов 802.

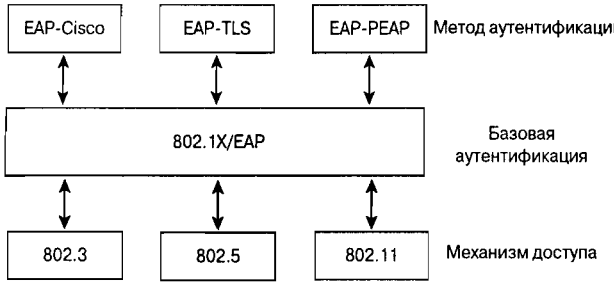


Рис. 4.18. Стандарт 802.1X и топологии канального уровня

Протокол EAP (RFC 2284) и стандарт 802.1X не регламентируют использование особого алгоритма аутентификации. Администратор сети может применять соответствующую протоколу EAP разновидность аутентификации — или 802.1X, или EAP. Единственное требование — чтобы как клиент стандарта 802.11 (здесь он называется *просителем* (supplicant)), так и сервер аутентификации поддерживали алгоритм EAP-аутентификации. Такая открытая и расширяемая архитектура позволяет использовать базовую аутентификацию в различных условиях, и в каждой ситуации можно применять 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-Cisco**. EAP-аутентификация типа EAP-Cisco, которую называют также LEAP, была первой, определенной для применения специально в беспроводных LAN. EAP-Cisco — это алгоритм взаимной аутентификации с использованием пароля.

Аутентификация по стандарту 802.1X требует наличия трех составляющих.

- **Проситель**. 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-проситель становится активным и ассоциируется с аутентификатором точки доступа.
2. Аутентификатор обнаруживает ассоциацию клиента и предоставляет порт просителя. Он переводит порт в неавторизованное 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 диаграммы обмена сообщениями по стандарту 802.1X.
4. Аутентификатор отвечает сообщением с EAP-запросом на идентификацию (EAP-Request Identity) просителю, чтобы удостовериться в идентичности клиента.
5. На сервер аутентификации отправляется пакет EAP-ответа (EAP-Response), содержащий идентификационные данные клиента. Объем ответа на идентификацию изменяется в зависимости от типа EAP, но в общем случае посылается только имя пользователя или его эквивалент, а не какая-либо форма совместно 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 особого алгоритма.
7. В зависимости от регламентированного результата обмена, зависящего от алгоритма аутентификации EAP, последним оговоренным 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.

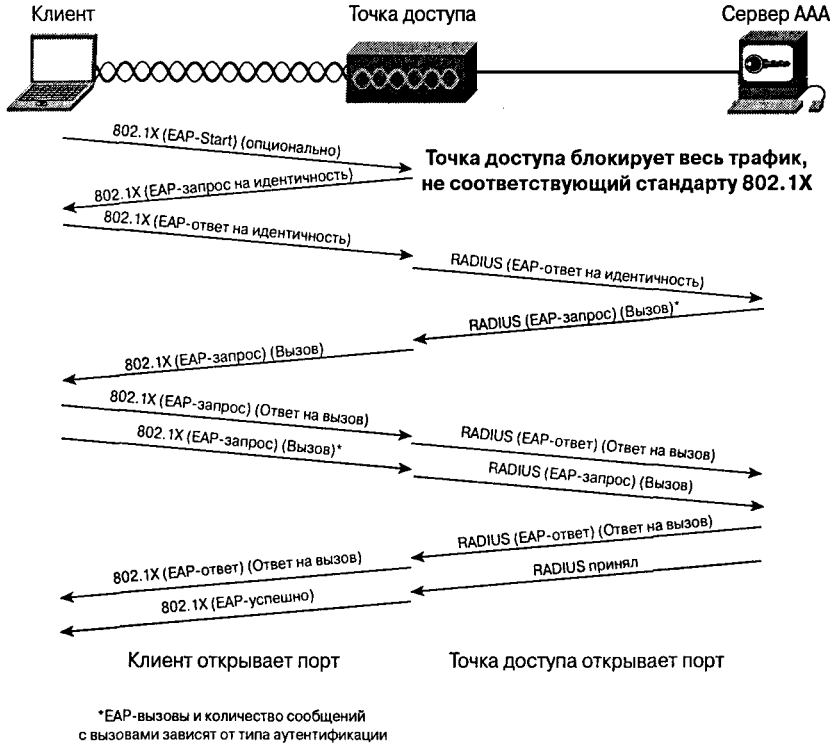


Рис. 4.20. Обмен сообщениями в соответствии со стандартом 802.1X

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 базовой аутентификации стандарта 802.1X. Ни стандарт 802.11i, ни WPA не регламентируют применение особого алгоритма аутентификации, но оба рекомендуют использовать алгоритм, который поддерживал бы взаимную аутентификацию, генерацию динамических ключей шифрования и аутентификацию пользователя. На рис. 4.21 представлены сообщения, которыми обмениваются клиент, точка доступа и AAA-сервер, но быстрее разобраться в этом процессе поможет конкретный пример. В данном разделе рассматривается работа алгоритма EAP-Cisco. 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-Cisco. В нижеследующей последовательности выполняемых действий подробно описывается каждая транзакция.

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

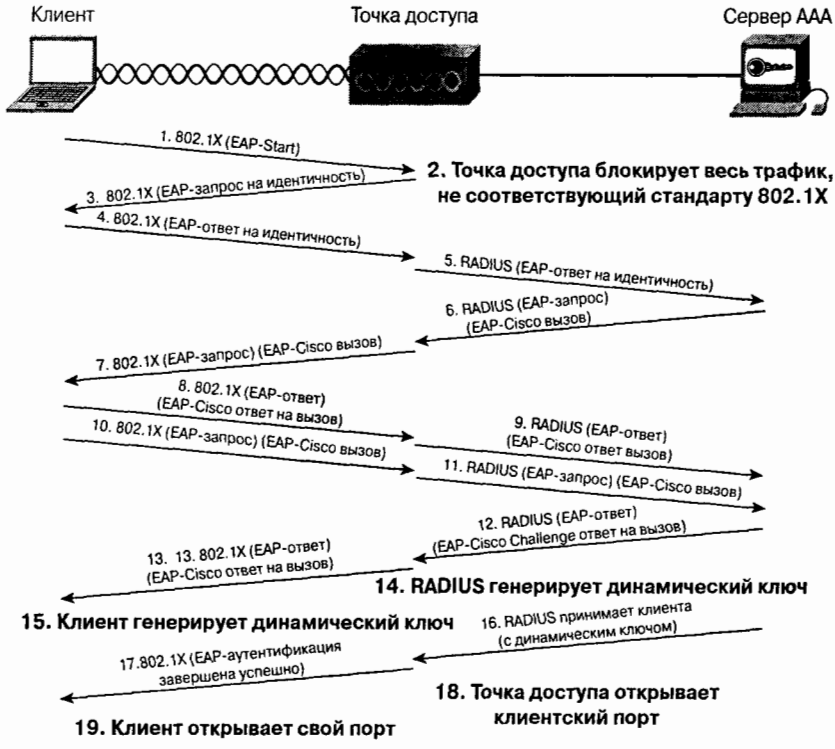


Рис. 4.21. Процесс аутентификации в соответствии с алгоритмом EAP-Cisco

3. Точка доступа посылает клиенту сообщение с EAP-запросом на идентификацию (EAP-Request Identity), инкапсулированным по стандарту 802.1X.
4. Клиент отвечает EAP-ответом (EAP-Response), инкапсулированным по стандарту 802.1X и содержащим пользовательское имя клиента.
5. Точка доступа переправляет это пользовательское имя, инкапсулированное в пакет запроса к серверу RADIUS на доступ (RADIUS ACCESS-REQUEST), на сервер аутентификации
6. Сервер RADIUS создает соответствующее алгоритму EAP-Cisco сообщение с вызовом (challenge message) и посылает его, инкапсулированное в пакет ответа сервера RADIUS на просьбу доступа (RADIUS ACCESS-RESPONSE), клиенту (через точку доступа).
7. Точка доступа перенаправляет вызов EAP-Cisco клиенту, инкапсулированный во фрейм стандарта 802.1X.
8. Клиент обрабатывает вызов в соответствии с алгоритмом EAP-Cisco и посылает ответ на вызов обратно серверу RADIUS через точку доступа.
9. Точка доступа инкапсулирует ответ на вызов в пакет запроса к серверу RADIUS на доступ (RADIUS ACCESS-REQUEST) и перенаправляет его на сервер RADIUS.
10. Клиент посылает вызов в соответствии с алгоритмом EAP-Cisco 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 информации.
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 перевыполняет 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 правильный динамический ключ шифрования.

Третья составляющая: алгоритм защиты данных

Уязвимость шифрования в WEP поставила производителей сетей стандарта 802.11 и исследователей 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 фреймов данных. Основные усовершенствования, внесенные протоколом TKIP, таковы.

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

В статье Флурера, Мантина 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 *пофреймовое изменение ключа* (per-frame keying). (Ее также называют *изменение ключа для каждого пакета* (per-packet keying) и *частое изменение ключа пакета* (fast packet keying).) Основной принцип, на котором основано пофреймовое 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 104-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 такое расширение IV. На рис. 4.22 представлен образец 48-разрядного IV и показано, как этот IV разбивается на части для использования при пофреймовом изменении ключа.

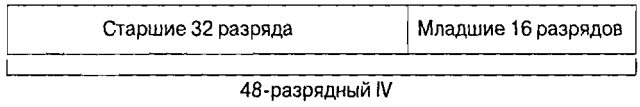


Рис. 4.22. Разбиение на части IV для использования при пофреймовом изменении ключа

Процесс пофреймового изменения ключа можно разбить на следующие этапы.

1. Базовый WEP-ключ (полученный в процессе аутентификации по стандарту 802.1X) 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 занести 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 пофреймового 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 отбрасывается и 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.

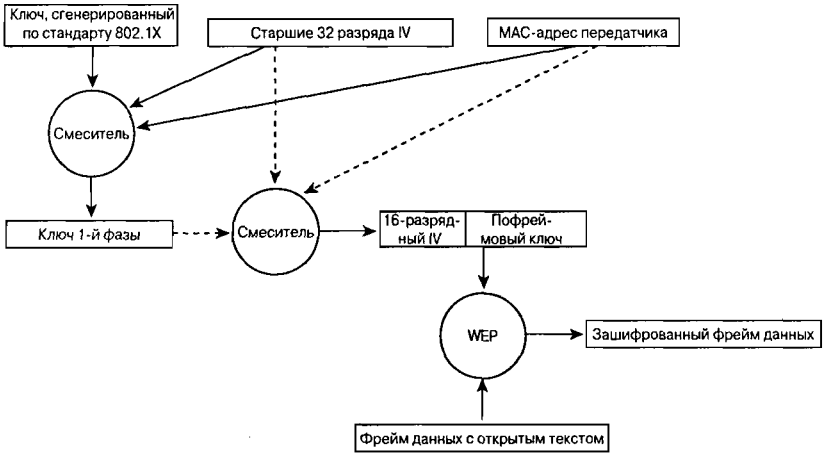


Рис. 4.23. Процесс пофреймового изменения ключа

Пофреймово изменяемый ключ имеет силу только тогда, когда 16-разрядные значения 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 вычисления 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 00000000000000000000000000000000000000000000000000000000.

Первые (старшие) 32 разряда IV (в рассматриваемом случае — первые 32 нуля) перемешиваются с выведенным по стандарту 802.1X ключом (имеющим 128-разрядное значение) и MAC-адресом передатчика (имеющим 48-разрядное значение) для получения значения ключа 1-й фазы (80-разрядное значение).

Ключ 1-й фазы вновь перемешивается 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, следующий из 15 и т.д., пока все 16 разрядов не примут значение, равное 1).

После того как пофреймовые возможности IV будут исчерпаны, IV 1-й фазы (32 бита) увеличивается на 1 (он теперь будет состоять из 31 нуля и одной единицы, 00000000000000000000000000000001).

Следующий логично возникающий вопрос таков: "Может ли подобный механизм привести к возникновению коллизий IV?" Правильный ответ "да", но важно знать, когда это может произойти. Предположим, что максимальная скорость перенаправления для устройств 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^{32} возможных вектора инициализации 1-й фазы (первые 32 разряда 48-разрядного IV), что дает 4 294 967 296 значений. Каждое из этих значений увеличивается после того, 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 * 4 294 967 296 с, что составляет примерно 8852 года. Если администратор не потребует повторной аутентификации, повторное назначение ключей вряд ли понадобится проводить 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 проведению атак с использованием поддельных фреймов и жонглированием битами, рассмотренные ранее в этой главе. IEEE предложила 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 шифровании 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 пофреймового назначения ключей генерируется пофреймовый ключ (рис. 4.25).
2. Алгоритм MIC генерирует MIC для фрейма в целом.
3. Фрейм фрагментируется в соответствии с установками MAC относительно фрагментации.
4. Фрагменты фрейма шифруются с помощью пофреймового ключа.
5. Осуществляется передача зашифрованных фрагментов.

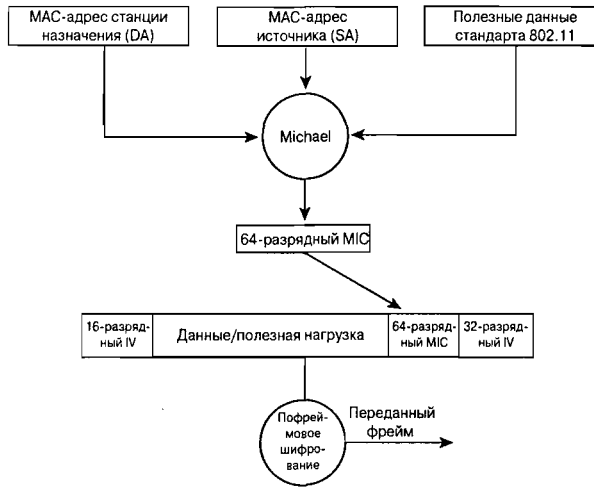


Рис. 4.24. Алгоритм Michael MIC

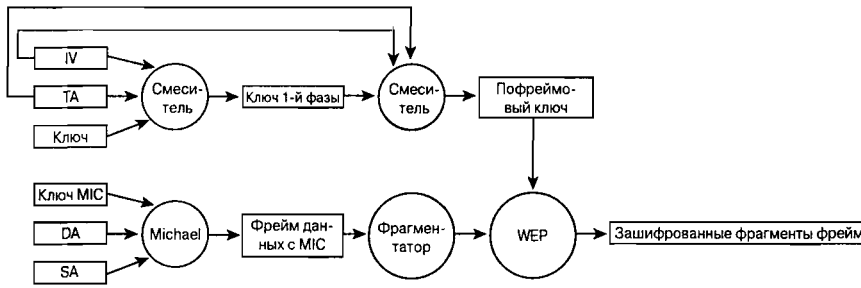


Рис. 4.25. Процесс шифрования по алгоритму TKIP

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 входящего фрагмента фрейма WEP, вычисляется пофреймовый ключ 2-й фазы.
3. Если полученный IV не тот, какой нужно, такой фрейм отбрасывается.
4. Фрагмент фрейма расшифровывается и осуществляется проверка признака целостности (ICV).
5. Если контроль признака целостности дает отрицательный результат, такой фрейм отбрасывается.
6. Расшифрованные 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 обрабатывается приемником.
9. Если эти значения не совпадают, значит, фрейм имеет ошибку MIC и приемник принимает меры противодействия MIC.

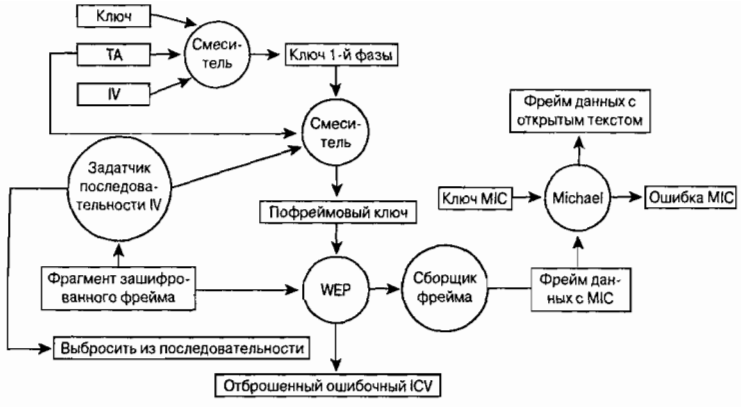


Рис. 4.26. Процесс дешифрования по алгоритму TKIP

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 отбрасывает 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 802.11i WPA для получения всех ключей используется так называемый *мастер-ключ* (master key). На рис. 4.27 представлена иерархия ключей с учетом последовательности их 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 посылает клиенту секретное случайное число, которое называется *временный аутентификатор* (authenticator nonce, ANonce), используя для этого сообщение EAPoL-Key стандарта 802.1X.

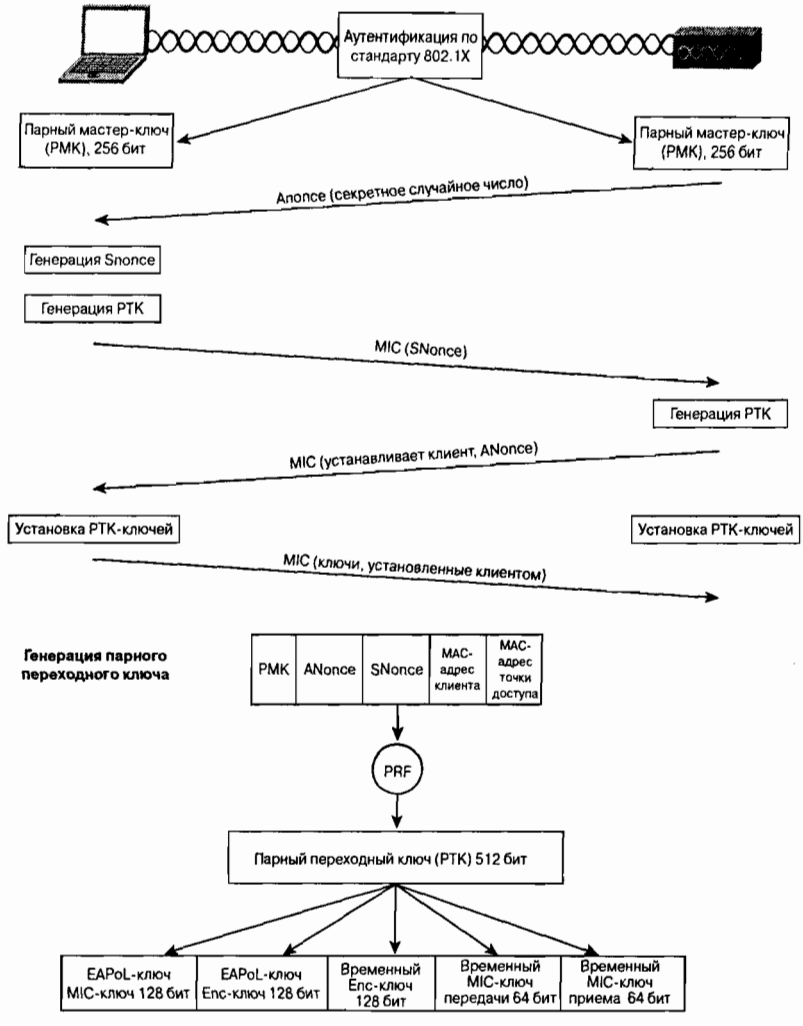


Рис. 4.27. Последовательность создания ключей

3. Этот клиент локально генерирует секретное случайное число, называемое *временный проситель* (supplicant nonce, SNonce).
4. Клиент генерирует парный переходный ключ (pairwise transient key, PTK) путем комбинирования PMK, Snonce, Anonce, MAC-адреса клиента, MAC-адреса точки доступа и строки инициализации. MAC-адреса упорядочены, MAC-адреса низшего порядка предшествуют MAC-адресам высшего порядка. Благодаря этому гарантируется, что клиент и точка доступа "выстроят" MAC-адреса одинаковым образом.
5. Это комбинированное значение пропускается через псевдослучайную функцию (pseudo random function, PRF), чтобы получить 512-разрядный PTK.
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 Snonce для вычисления PTK 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 установить PTK и его Anonce, защищенные ключом EAPoL-Key MIC. Данный этап позволяет клиенту удостовериться в том, что число Anonce, полученное на этапе 2, действительно.
10. Клиент посылает сообщение EAPoL-Key, защищенное ключом EAPoL-Key MIC, указывающее, что ключи установлены.

Парный мастер-ключ (PMK) и парный переходный ключ (PTK) являются одноадресатными по своей природе. Они только шифруют и дешифруют одноадресатные фреймы, и предназначены для единственного пользователя. Широковещательные фреймы требуют отдельной иерархии ключей, потому что использование с этой целью одноадресатных ключей приведет к резкому возрастанию трафика сети. Точке доступа (единственному объекту BSS, имеющему право на рассылку широковещательных или многоадресатных сообщений) пришлось бы посылать один и тот же широковещательный или многоадресатный фрейм, зашифрованный соответствующими пофреймовыми ключами, каждому пользователю.

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

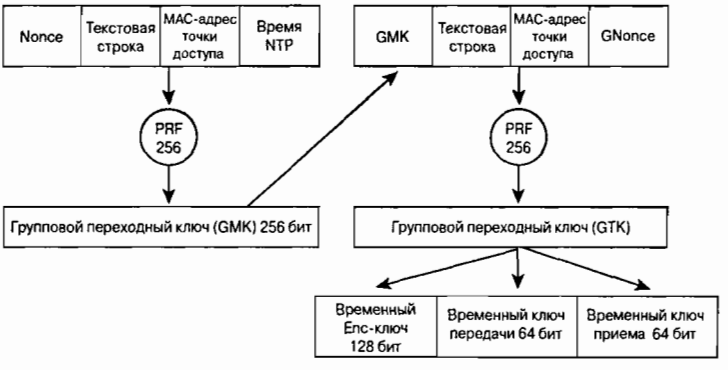


Рис. 4.28. Иерархия групповых ключей

Групповой мастер-ключ, текстовая строка, MAC-адрес точки доступа и Gnonce (значение, которое берется из счетчика ключа точки доступа) объединяются и обрабатываются с помощью PRF, в результате чего получается 256-разрядный групповой переходный ключ (group transient key, GTK). GTK делится на 128-разрядный ключ шифрования широковещательных/многоадресатных фреймов, 64-разрядный ключ передачи MIC (transmit MIC key) и 64-разрядный ключ приема MIC (MIC receive key).

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

Клиент обновляется с помощью групповых ключей шифрования через сообщения EAPoL-Key. Точка доступа посылает такому клиенту сообщение EAPoL, зашифрованное с помощью одноадресатного ключа шифрования. Групповые ключи удаляются и регенерируются каждый раз, когда какая-нибудь станция диссоциируется 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 защищаемых 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 Рийндэла* (Rijndael algorithm). Как и многие другие шифры, AES требует режима обратной связи во избежание риска, связанного с режимом ECB (напомним, это — режим шифрования с помощью книги электронных кодов). IEEE разработал режим AES, предназначенный специально для применения в беспроводных LAN. Этот режим называется *режим счета сцеплений блоков шифра* (Cipher Block Chaining Counter Mode, CBC-CTR) с контролем аутентичности сообщений о сцеплениях блоков шифра (Cipher Block Chaining Message Authenticity 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 решении.

Алгоритм шифрования CBC-CTR работает с использованием счетчика для пополнения 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-байтовые 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 шифрования CBC по отношению ко всему фрейму, к адресу назначения, адресу источника и данным. Результирующий 128-разрядный выход усекается до 64 бит для использования в передаваемом 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 "накладные расходы" шифрования.

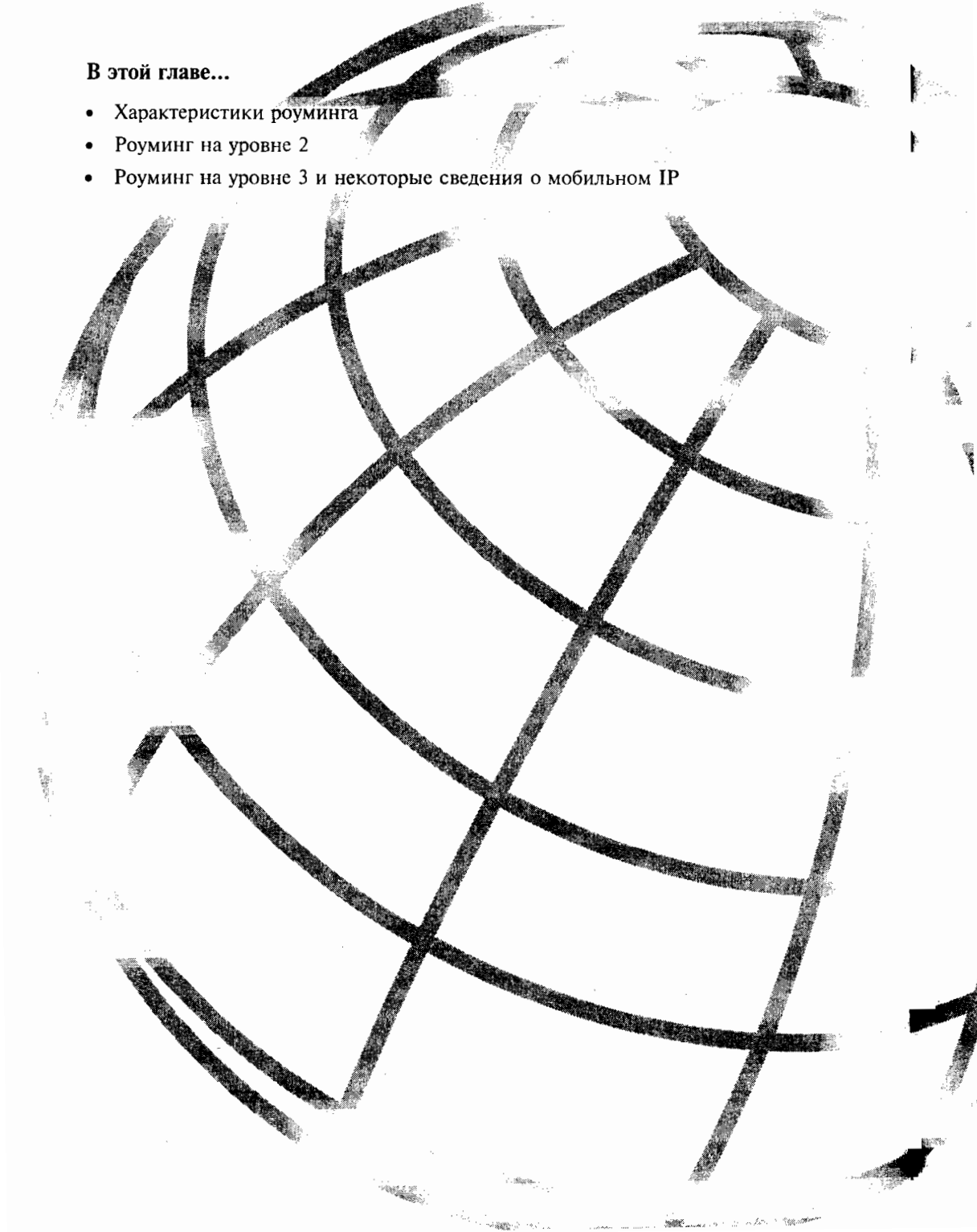
Резюме

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

В этой главе рассказывалось о том, как можно защитить беспроводную локальную сеть, и описывались вопросы 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 мобильном IP



Глава 5

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 нужно 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 станции, осуществляющие роуминг, можно двумя способами.

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

Ближайшей аналогией *бесшовного роуминга* является звонок по сотовому телефону. Например, представьте, что вы говорите по сотовому телефону в то время как ваш автомобиль мчится по автостраде. Типичная базовая станция глобальной системы мобильной связи (GSM) или сота, обеспечивающая множественный доступ с временным разделением (TDMA), действует на площади в несколько квадратных миль, так что с уверенностью можно предположить, что во время вашего телефонного разговора базовые станции осуществляют роуминг. Во время роуминга вы не чувствуете ухудшения качества связи (благодаря чему сотовые 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 сетевое приложение требует постоянного подключения к сети в процессе роуминга.

Кочевой роуминг отличается от бесшовного. *Кочевой 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 кочевым, поскольку пользователь использует службы сети не во время передвижения, а только по 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 создавать ассоциацию с новой. Такой процесс может показаться интуитивно неоправданным, поскольку он оставляет возможность потери данных в ходе роуминга, но благодаря этому упрощаются MAC-протокол и радиотракт.

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 и 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 повышению общей стоимости устройства.

Функционирование и применение

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

надежный и требующий установления соединения протокол. TCP требует позитивных 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 хорошее решение 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 малоизбыточным и требует установления соединения. Пакеты UDP используют такие приложения, как IP-телефония (Voice over IP, VoIP) и приложения, обеспечивающие передачу видеоизображений. Присущая протоколу TCP способность повторной передачи мало поможет 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, "Технологии Ethernet", *широковещательный домен* определялся как сеть, соединяющая устройства, способные получать и отправлять одно другому широковещательные фреймы. Этот домен называют также *сеть уровня 2*. Данная концепция остается справедливой и для сетей стандарта 802.11. О точках доступа, относящихся к одному широковещательному 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), связывающихся 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 A к точке доступа подсети B. Поскольку адрес уровня 3 изменяется, станция прекращает все сеансы связи приложений. Этот сценарий описан ниже, в разделе "Обзор мобильного IP".

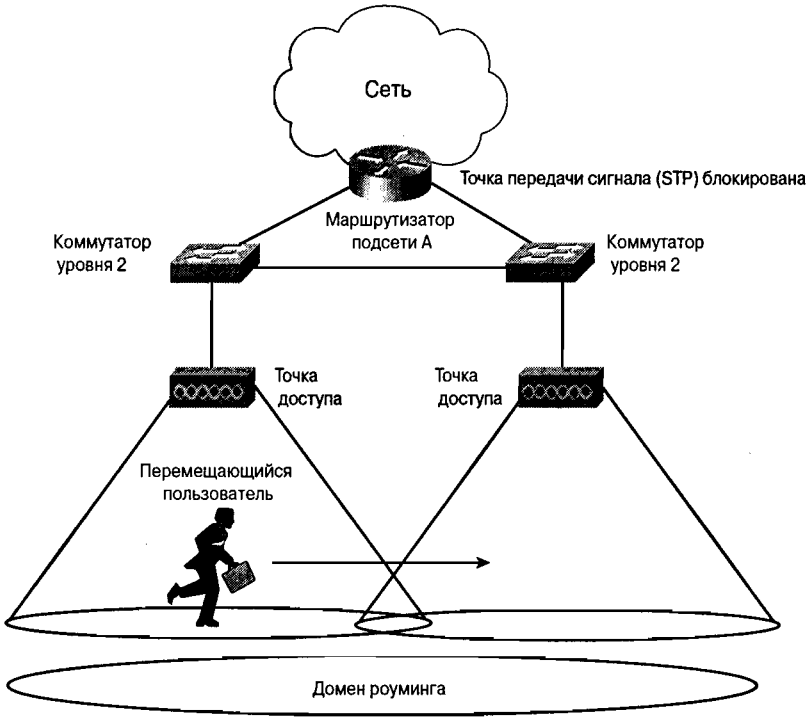


Рис. 5.1. Домен роуминга уровня 2

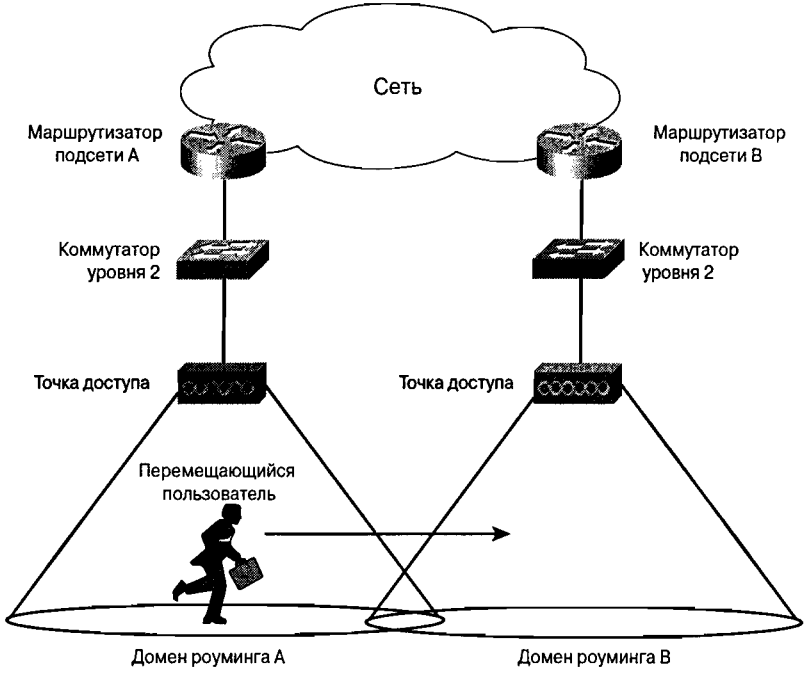


Рис. 5.2. Роуминг между доменами роуминга

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 зондирования.
- 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 осуществиться роуминг, должна произойти следующая последовательность событий.

- **Клиент должен принять решение о перемещении.**[1] Алгоритмы роуминга определяются поставщиком оборудования (и являются его собственностью); они зависят от таких факторов, как уровень сигнала, подтверждение приема фрейма, посланные сигнальный фреймы и т.д.
- **Клиент должен решить, куда он будет перемещаться**. Клиент должен понять, к какой точке доступа он перемещается. 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* (preemptive AP discovery), или после принятия решения о перемещении, этот процесс называется *обнаружение точки доступа во время перемещения* (roam-time 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 поставщиков оборудования. Хотя ранее эта проблема ставила под угрозу возможность взаимодействия первых устройств стандарта 802.11, сейчас поставщики вместе работают над тем, чтобы основы взаимодействия сохранялись. Тот факт, что алгоритмы были оставлены на усмотрение поставщиков, дал последним возможность

[1] Точнее, о том, что владелец начал его перемещать. — *Прим. ред.*

дифференцироваться друг от друга за счет создания новых и лучших алгоритмов, конкурирующих с другими. Алгоритмы роуминга стали "секретным оружием" поставщиков, поэтому их особенности не разглашаются.

Не рискуя ошибиться, можно предположить, что в этих алгоритмах учитываются такие параметры, как уровень сигнала, значения счетчиков числа попыток, посланные сигнальные фреймы и другие концепции, рассмотренные нами в главе 2. Например, вспомним обсуждавшуюся в той же главе работу распределенной функции координации (DCF). Двоичный экспоненциальный возвратный алгоритм (binary exponential backoff algorithm), применявшийся 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 подобные 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 снизится.

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 рассылаются 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 медленнее проходит по каналам, чем при активном, так как прослушивает сигнальные фреймы, посылаемые точками 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 патентованные информационные элементы поставщика, 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 блокировать передачу в сигнальных фреймах имени SSID (в информационном элементе SSID), и тогда клиент не сможет определить, принадлежит ли такая точка доступа к тому же домену роуминга.

Идеального способа 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 переходить к обслуживанию предварительно определенной точкой доступа после того, как клиент примет решение перемещаться. 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 нормальной, 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 потребуется повторная передач их точкой доступа.
- **Приложение клиента может испытать воздействие снижения пропускной способности**. Клиент не может передавать данные во время сканирования каналов (активного либо пассивного), поэтому некоторые приложения, выполняемые клиентом, могут ощутить снижение пропускной способности.

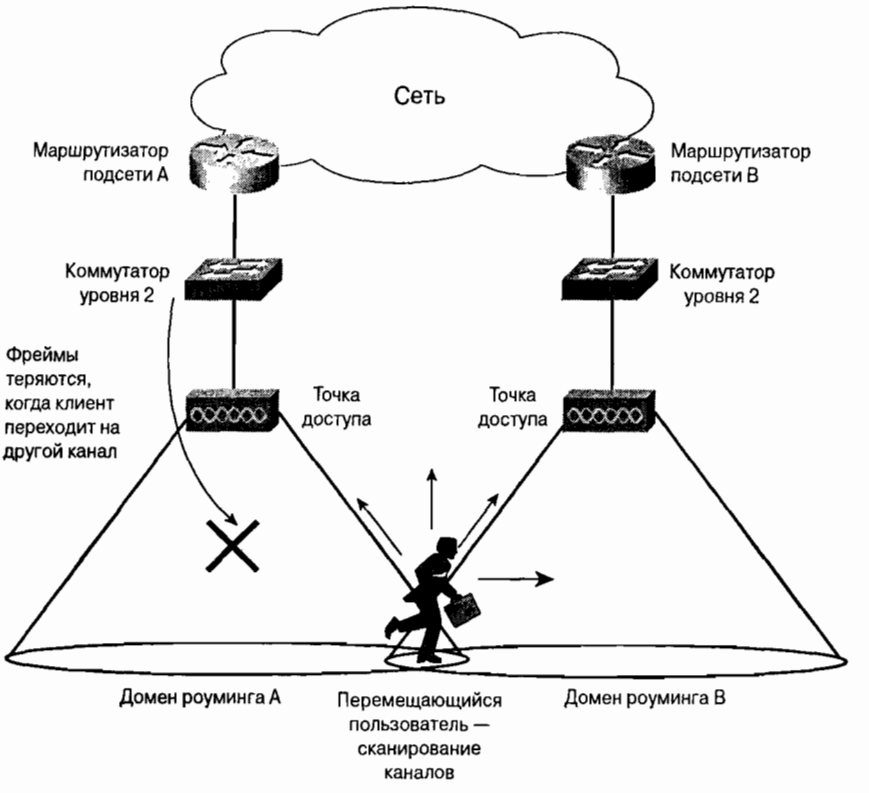


Рис. 5.3. Предварительное обнаружение точки доступа

Для энергосберегающих клиентов существует уникальная возможность практиковать предварительный роуминг и вместе с тем избегать вышеназванных 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 в очередь фреймы, 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 в очередь предназначенные для передачи фреймы, пока не будет завершено сканирование каналов, избегая потери и этих данных.

Такое решение приводит к снижению эффективности энергосберегающего режима, поскольку радиостанция клиента проявляет активность во время сканирования каналов, вместо того чтобы соблюдать режим энергосбережения, а приложения клиента могут выполняться 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 приложений.

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 начальное включение, за исключением того что запрос на ассоциацию, посылаемый клиентом новой точке доступа, является в действительности фреймом запроса на реассоциацию.

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 реассоциироваться, но зато больше времени тратится на сам процесс роуминга. На рис. 5.4 показан процесс обнаружения точки доступа во время перемещения.

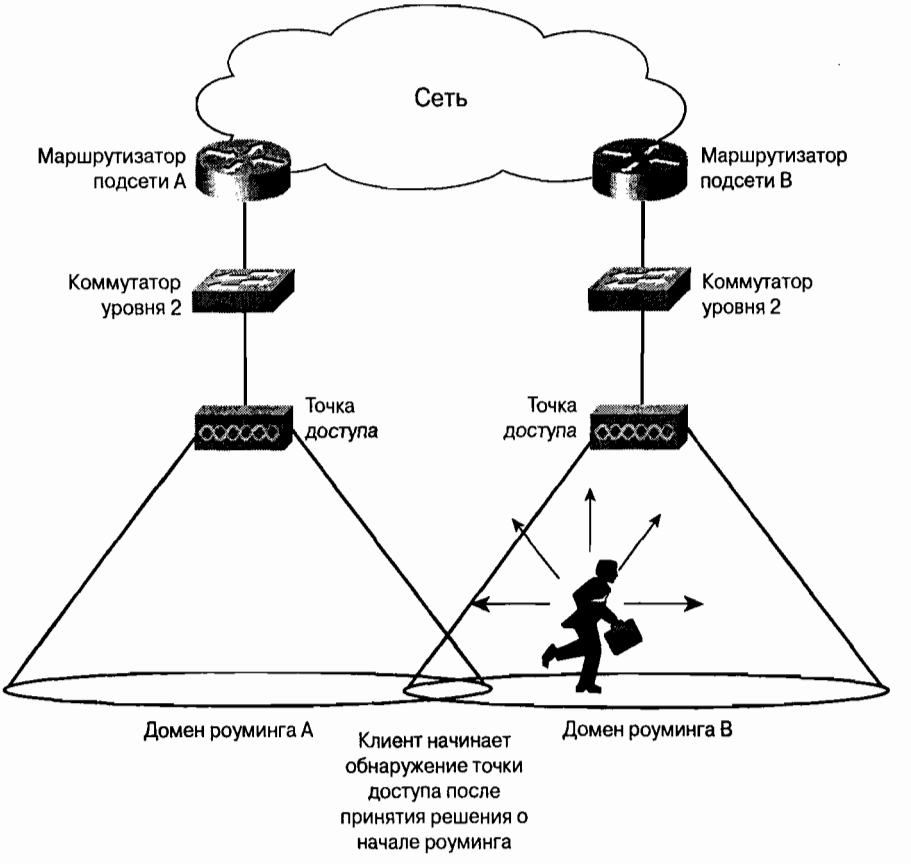


Рис. 5.4. Процесс обнаружения точки доступа во время перемещения

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 уходит из ее области действия.
2. Предыдущая точка доступа должна буферизировать данные, предназначенные для клиента, осуществляющего роуминг[2].
3. Новая точка доступа должна показать предыдущей, что клиент успешно переместился в ее зону. Этот этап обычно выполняется с помощью одно- или многоадресатных 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 потери 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 переместился 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 обстановку, посылая 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 входному 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 направляется 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 и точку доступа 2 (AP2).

---

[2] Эти задачи не регламентированы, потому что они не специфицированы стандартом 802.11. — *Прим. авт.*

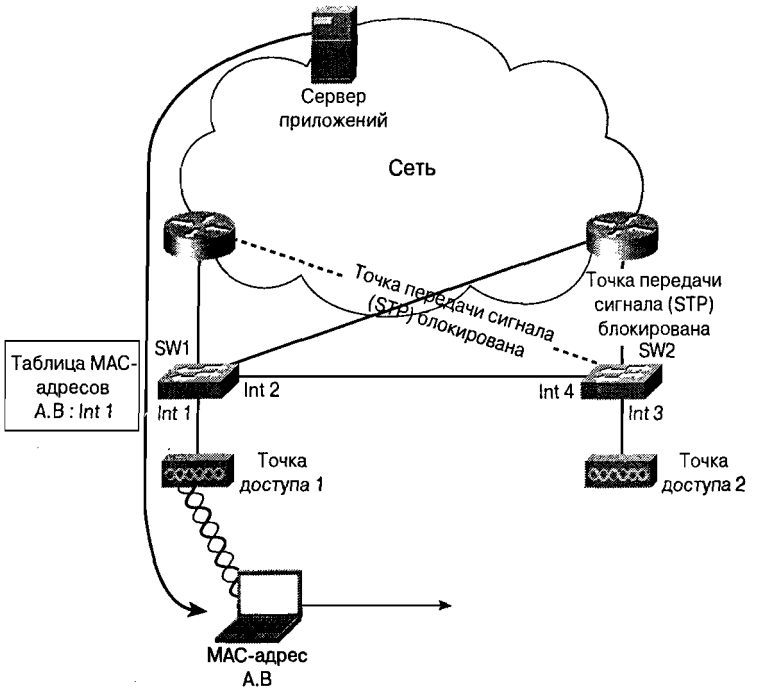


Рис. 5.5. Приложение посылает данные перемещающейся станции

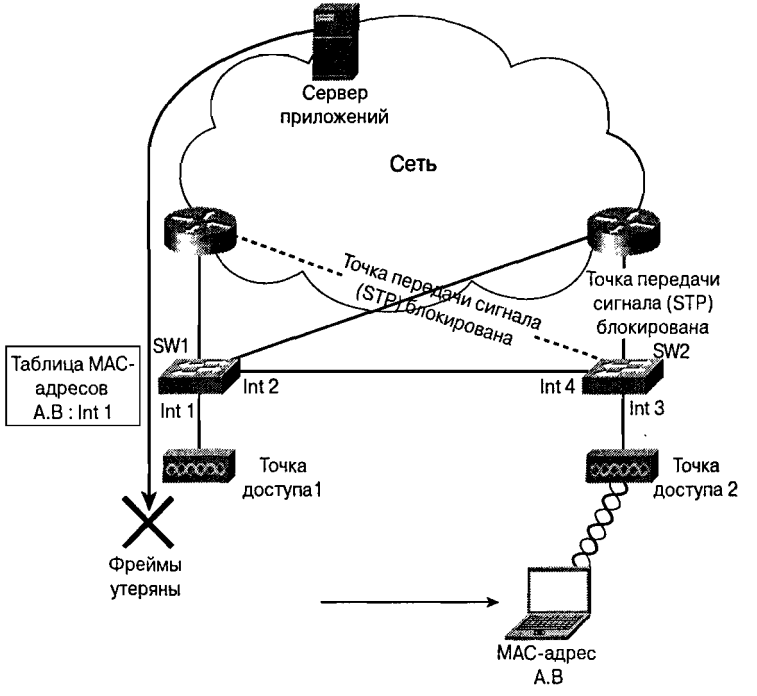


Рис. 5.6. Потеря данных в результате роуминга уровня 2

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 одно- или многоадресатного 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.

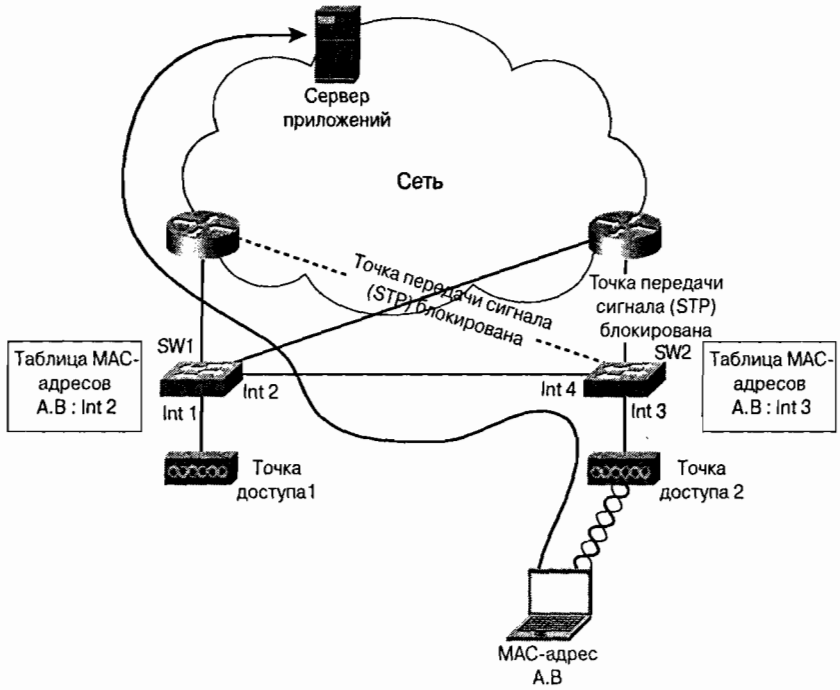


Рис. 5.7. Обновление таблицы MAC-адресов после перемещения клиента

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 выполнять 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 широковещательному домену и сконфигу-

рированы 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, распространяющихся 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 невелики, и беспроводная LAN представляла собой одну подсеть класса С, развернутую в пределах всего здания. Домен роуминга охватывал все четыре этажа здания. Со временем количество пользователей увеличилось настолько, что пропускная способность подсети оказалась исчерпанной и ее характеристики ухудшились из-за увеличившегося 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, а 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, используемых в 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, сеанс связи прерывается, потому что перемещающийся пользователь попадает в другую подсеть.

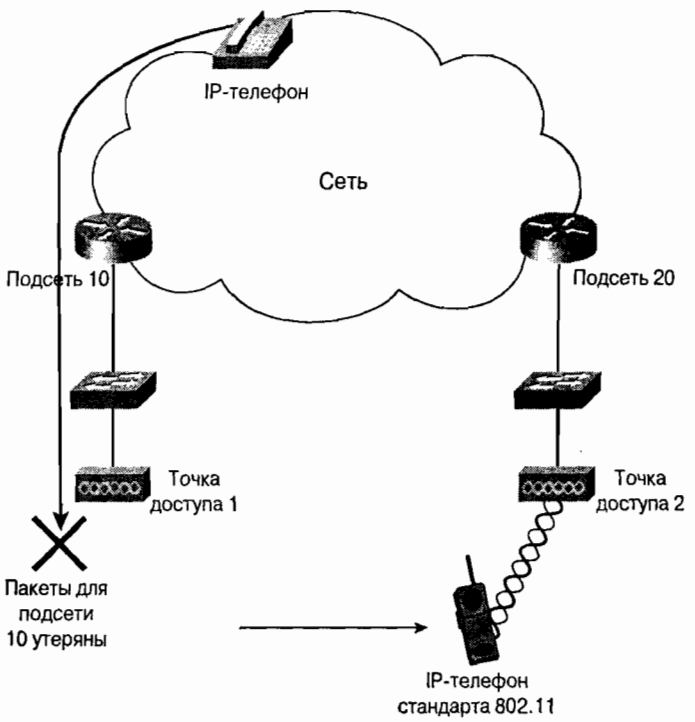


Рис. 5.8. Роуминг между подсетями

Обзор мобильного протокола IP

Сценарий, описанный нами для компании A, относится к числу распространенных. Многие приложения требуют устойчивых соединений и прерывают свои сеансы связи при роуминге между VLAN. Чтобы обеспечить устойчивость сеансов связи, необходим механизм, который позволил бы станции поддерживать один и тот же адрес уровня 3 при роуминге 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, выделенный FA для MN, на который поступают пакеты, посланные HA и предназначенные для MN.
- **Сопряженный 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.

- Обнаружение агента.
- Регистрация.
- Туннелирование.

В следующих разделах каждая из этих фаз рассматривается более подробно.

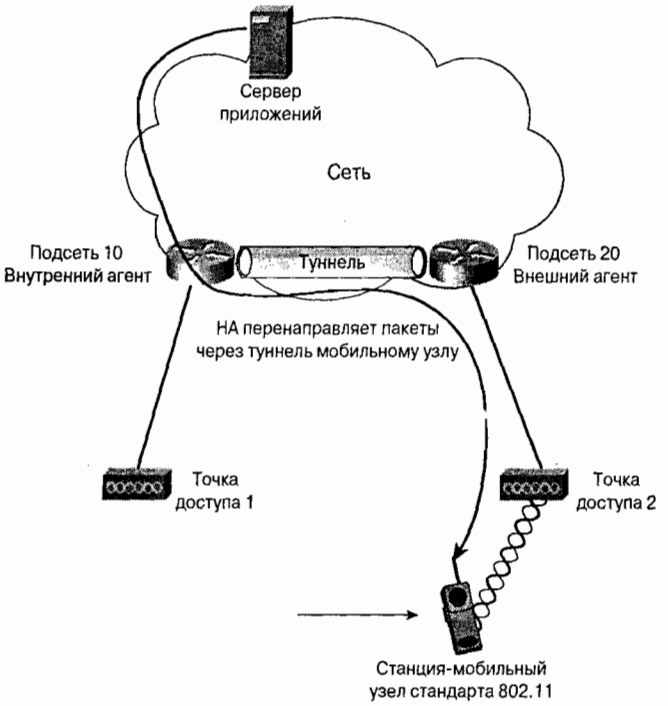


Рис. 5.9. Передача пакетов перемещающемуся MN

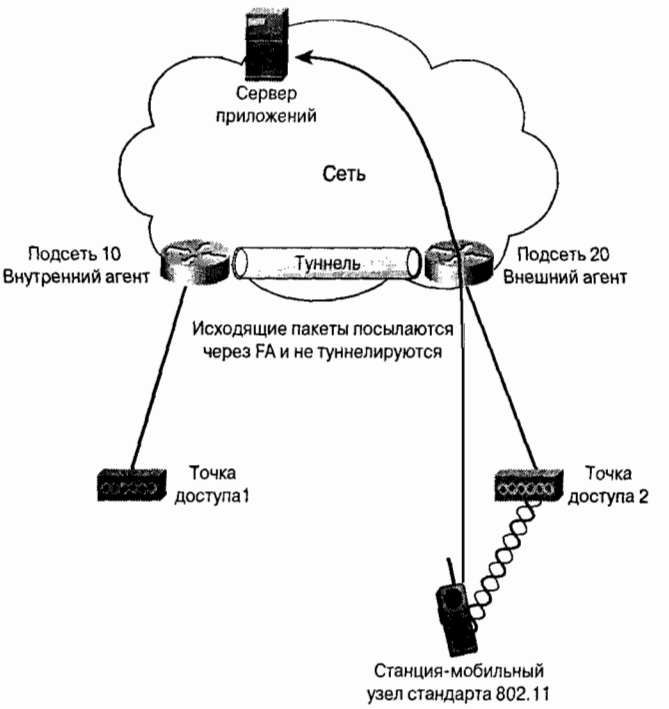


Рис. 5.10. Передача пакетов от перемещающегося MN

Обнаружение агента

Перемещающийся MN должен своевременно обнаружить, что он находится во внешней сети, чтобы минимизировать задержку в выполнении приложений. Внутренние и *внешние* агенты оповещают о своих сервисах, используя сообщения протокола межсетевых управляющих сообщений (Internet control message protocol, ICMP) и протокола обнаружения маршрутизатора (router discovery protocol; вместе эти протоколы называются IRDP) для отправки агенту извещений. Когда MN устанавливает соединение с сетью, в *зону действия которой он перемещается, он получает периодически* рассылаемые IRDP-пакеты. Эти пакеты рассылаются или многоадресатно 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 агента MN может запросить 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 новое извещение не было получено, MN должен повторить процедуру обнаружения нового агента.

Расширение длины префикса указывает на значение адреса сети посылающего извещения 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 CCoA 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 дополнение к обязанностям, связанным 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 облегчить перенаправление пакетов мобильному узлу. Процесс регистрации осуществляется следующим образом (рис. 5.12).

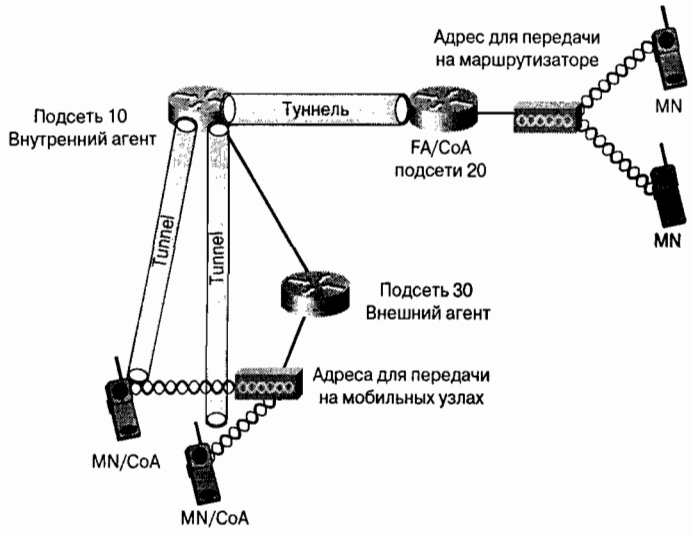


Рис. 5.11. Отличие между MN и CoA

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.

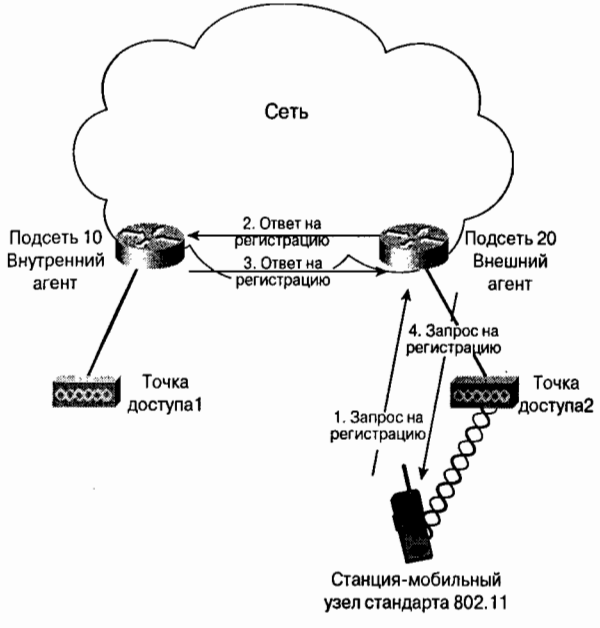


Рис. 5.12. Процесс регистрации в соответствии с мобильным IP

Запрос на регистрацию содержит следующие поля.

- **Синхронные соединения** (simultaneous 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 подсети.
- **Декапсуляция осуществляется мобильным узлом**. MN может запросить, чтобы декапсуляцию туннелированных пакетов осуществлял он сам. Эта опция выбирается 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 выходящие 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 относится MN.
- **CoA**. В этом поле указывается IP-адрес CoA и точки подключения (termination point) туннеля.
- **Идентификация**. Это поле представляет собой 64-разрядное значение текущего времени; оно используется для последующих запросов на регистрацию и ответов на них и препятствует проведению атак на пакеты регистрации.
- **Расширения**. Количество доступных расширений, не требуемых для регистрации.

Ответ на запрос относительно регистрации содержит следующие поля.

- **Код**. 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 основанного на сообщениях механизма аутентификации, используемого для обработки запроса на регистрацию.
- **Расширения**. Количество расширений, которые доступны, 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

Окончание табл. 5.1

Значение поля Code	Источник	Что означает
64	FA	Причина не специфицирована
65	FA	Запрещена административно
66	FA	Недостаточные ресурсы
67	FA	MN не прошел процесс аутентификации
68	FA	HA не прошел процесс аутентификации
69	FA	Затребованное время жизни чересчур длительно
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 недостижима (получено сообщение об ошибке от ICMP)
81	FA	Хост HA недостижим (получено сообщение об ошибке от ICMP)
82	FA	Порт HA недостижим (получено сообщение об ошибке от ICMP)
88	FA	HA недостижим (получено другое сообщение об ошибке от ICMP)
128	HA	Причина не специфицирована
129	HA	Запрещена административно
130	HA	Недостаточные ресурсы
131	HA	MN не прошел процесс аутентификации
132	HA	HA не прошел процесс аутентификации
133	HA	Идентификация регистрации не подходит (Registration identification mismatch)
134	HA	Плохо сформированный запрос
135	HA	Слишком много одновременных мобильных соединений
136	HA	Неизвестный адрес HA

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

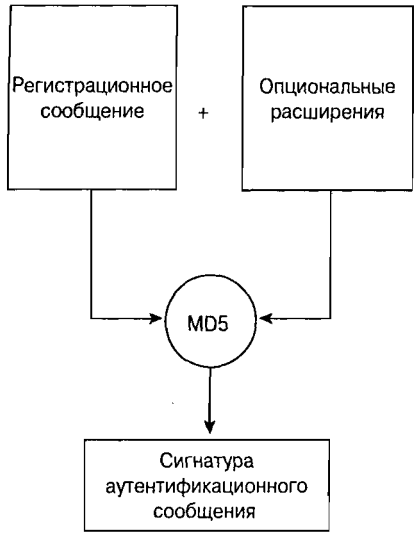


Рис. 5.13. Организация защиты сообщений, посылаемых в ходе регистрации

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 checks, RFC 2827), перенаправление пакетов от MN через FA не может осуществляться. Входной интерфейс FA способен фильтровать только действительные IP-адреса источника, чтобы предотвратить проникновение в сеть неавторизованных 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 разъединены. 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 туннелируемые пакеты, снабжая 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.

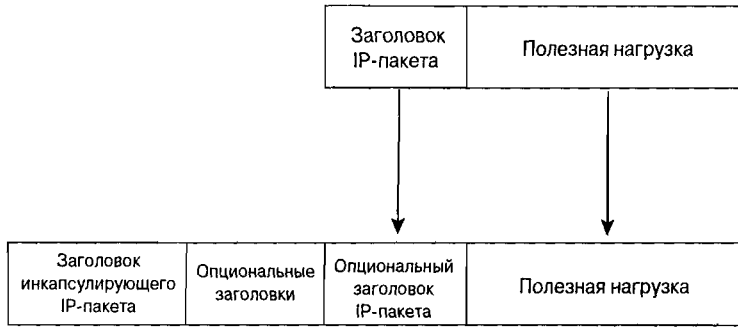


Рис. 5.14. Инкапсуляция IP-пакетов

Мобильный IP поддерживает несколько механизмов туннелирования.

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

Инкапсуляция IP в IP является единственным типом туннелирования, регламентированным спецификацией мобильного IP, но часто используется GRE или минимальная инкапсуляция, потому что каждая из них оказывает несколько другое влияние на сеть, и вы можете использовать их, чтобы определить, какая же лучше удовлетворяет 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 посылать 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 посылать пакеты в данном случае, FA должен перенаправить эти пакеты обратно во внутреннюю подсеть через HA. Этот сценарий показан на рис. 5.15. Реверсное туннелирование ведет к появлению дополнительных пакетов и замедлению работы приложений, но оно облегчает использование фильтрации в соответствии с документом RFC 2827 для обеспечения защиты сети.

Резюме

Беспроводные LAN стандарта 802.11 облегчают реализацию беспроводной мобильности, но для правильного 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 пользователей, 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 большой пропускной способностью (малое отношение число пользователей/число точек доступа, но больше точек доступа в зоне покрытия). Развитие в направлении беспроводных LAN с боль-

шой пропускной способностью требует их развертывания в масштабах предприятия с обеспечением роуминга между доменами роуминга.

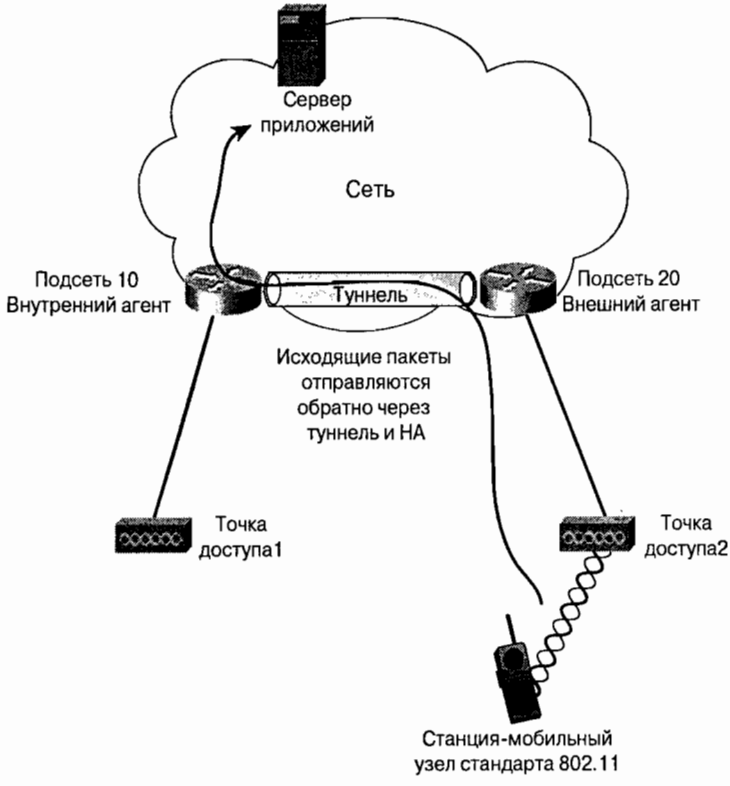


Рис. 5.15. Реверсное туннелирование

Глава 6

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 MAC 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 аналогичные проводные. 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 видеомагнитофоны и пишущие DVD-приводы. Представьте, что все это реализовано в жилом доме, где технология стандарта 802.11 используется в домашней сети, а также для замены проводных устройств, начиная с DVD-проигрывателя 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 видеоданные), по отношению, например, к электронной почте и просмотру Web-страниц. Наверное, прерывание просмотра фильма из-за того, что пришло электронное письмо или кто-то что-то ищет в Internet, 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 пересмотра 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.

Сети стандарта 802.11 хороши для узкополосных, нечувствительных к задержкам приложений. Сканеры штрих-кодов, персональные цифровые помощники (PDA), сервисы Web или электронной почты могут использовать беспроводные сети без физических ограничений, вызванных кабелями сети или возможной существенной потерей информации. Но если предприятие начинает развертывать беспроводную LAN (WLAN), которая будет применяться в условиях вертикального 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 задумаетесь 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 дает администратору сети ощутимую экономию средств, позволяющую повысить коэффициент окупаемости инвестиций (ROI), сделанных в развертывание WLAN.

Высокое качество обслуживания характерно для зрелых технологий, применяемых в проводных сетях, и таких устройств, 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 совмещенному 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 острую конкуренцию за доступ к среде в BSS.

В следующих разделах подробно рассматривается 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, определенные в 1997 году, — с использованием распределенной функции координации (DCF) и точечной функции координации (PCF). Оба механизма позволяют одновременно осуществлять передачу через среду только одной станции, это может быть точка доступа или клиентская станция. Проводная 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 фреймы данных. Такая технология теоретически позволяет Ethernet-среде удваивать свою нормальную полосу пропускания. (Канал Fast Ethernet способен передавать и одновременно принимать данные со скоростью 100 Мбит/с, в сумме это эквивалентно полосе пропускания 200 Мбит/с.) Иначе говоря, станция, которая собирается передавать

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

Этот сценарий противоположен таковому, характерному для сетей стандарта 802.11. За право доступа к среде состязаются не только станция и точка доступа, но и клиенты между собой. Механизм PCF реализует идею последовательного опроса, когда точка доступа может действовать как точка координации и опрашивать каждого клиента на предмет того, нужно ли 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 (DCF). При отсутствии механизмов для координации моментов времени передачи клиентов и установления приоритета между последними поставщики 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 освободить среду и повторить передачу. Вы можете рассмотреть и другой сценарий, называемый *черная дыра широковещания* (broadcast black hole). Если в BSS входит энергосберегающая станция, все широковещательные и многоадресатные фреймы посылаются после сигнального фрейма, содержащего карту маршрутов трафика (DTIM beacon). В большинстве случаев все 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, срабатывают почти одинаково, обе они могут рассылать широковещательный и многоадресатный трафик одновременно, вызывая коллизии фреймов в зоне перекрытия, из-за чего находящийся в этой зоне клиент пропустит эти фреймы. В отличие от одноадресатных фреймов, получение широковещательных и многоадресатных фреймов не подтверждается, поэтому повторно они переданы не будут. Перекрытие по совмещенному каналу может нарушить работу механизмов QoS из-за увеличения конкуренции за среду в сетях стандарта 802.11, вкупе с ситуацией черной дыры это может привести к тому, что клиент не сможет получать потенциально важный для него трафик.

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 готовность к передаче/готовность 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 влияет — на работу чувствительных к задержкам приложений. Устройства, использующие сообщения RTS/CTS при передаче каждого фрейма, также приводят к ухудшению характеристик из-за большого избыточного трафика, сопровождающего каждый фрейм данных.

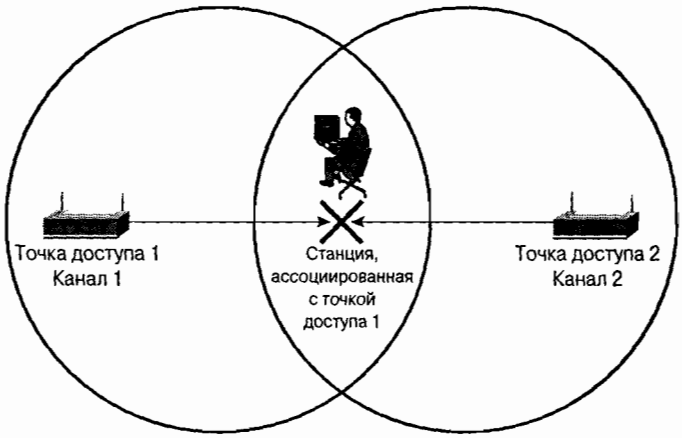


Рис. 6.1. Перекрытие по совмещенному каналу

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 нашей книги. Текущие предложенные группой 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 DSF, EDSF).
- **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), соотношение которых с восемью классами, определенными в стандарте 802.1D, представлено в табл. 6.1. Трафик от обеспечивающих должное качество связи клиентов 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	Видеозондирование (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 приоритезации трафика, основывающийся 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-дейтаграммы или использовать код указателя дифференцированной службы (differentiate services code point, DSCP). Не боясь ошибиться, можно также предположить, что клиентское устройство преобразует эти значения уровня 3 в классы трафика стандарта 802.11e. При наличии классифицированного и снабженного метками трафика стандарт 802.11e обеспечивает механизм дифференциации и приоритезации 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, не связанных непосредственно одно с другим. EDSF берется за решение этой проблемы, вводя несколько новых концепций и реализуя 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 DCF (см. главу 2, "Беспроводные локальные сети стандарта 802.11"), когда каждый фрейм и сопровождающее его подтверждение конкурируют за доступ к среде, механизм TXOP может обеспечить передачу сразу многих фреймов/подтверждений, главное — чтобы они умещались в период TXOP (табл. 6.2).
- **Арбитражный межфреймовый промежуток** (arbitration interframe space, AIFS). AIFS аналогичен межфреймовому промежутку IFS, рассмотренному нами в главе 2,

но размер IFS 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 короче 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 шансы 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_{min}	1	6,0 мс	3,0 мс
3	$((CW_{min} + 1)/4) - 1$	$((CW_{min} +1)/2)-1$	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 DSF-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 длительный TXOP. Чтобы проиллюстрировать влияние менее широкого окна конкуренции, отметим следующее.
  - По умолчанию начальное значение CW_{min} обычно составляет 7 канальных интервалов. DCF-станция случайным образом выбирает значение отсрочки передачи между 0 и CW_{min} (в данном случае 7) и использует 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_{min},

равное 7. В данном случае, после того как станция отказалась от передачи и ее окно конкуренции достигло значения CW_{max}, она будет инкрементировать оставшееся значение счетчика намного быстрее.

- Станция с категорией доступа AC(3) имеет самое 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 коллизию. Станция с менее приоритетной категорией доступа может случайно выбрать короткую отсрочку и вступить в коллизию 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 ограниченны (это напрямую относится к WLAN стандарта 802.11), может оказаться необходимым защищать 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 пользоваться правом первоочередной передачи, без накопления фазовых искажений, и смогут плодотворно общаться.

Пусть теперь в BSS делается седьмой телефонный звонок. Независимая базовая зона обслуживания способна поддерживать только шесть звонков, в то же время механизм приоритезации 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 наличные ресурсы сети и "интеллигентно" разрешает или отклоняет новые сеансы 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. Неиспользуемая доля пропускной способности среды называется *наличный бюджет* (available budget) для дан-

ной категории. О наличном бюджете 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 узлам не приходится увеличивать или расширять TXOP, которые они уже используют. Данный процесс защищает существующие информационные потоки приложений от влияния со стороны новых потоков.

HCF с работой в режиме поочередного доступа

Работа HCF аналогична работе функции точки координации PCF (см. главу 2). Точка доступа содержит логический объект (logical entity), называемый *гибридный координатор* (hybrid coordinator, HC), который отслеживает потоки информации клиентских станций HCF и назначает интервалы опросов. Получение доступа в результате опроса HCF позволяет станции требовать нужный ей TXOP, а не просто определять, какой из них доступен, как в случае использования EDSF. Работа HCF, в сочетании с управлением входом HCF, позволяет гибридному координатору "интеллигентно" определить, какие ресурсы беспроводной среды доступны, и принять либо отклонить информационные потоки трафика приложения. HCF может функционировать в двух режимах, один из них сосуществует с EDSF, а второй использует период, свободный от конкуренции (CFP), аналогично PCF.

Работа HCF в период, свободный от конкуренции

Работа HCF 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 (PCF), в котором определяются момент начала и длительность периода, свободного от конкуренции (CFP).
2. Гибридный координатор (HC) предлагает поддерживающим механизм HCF станциям TXOP, посылая им QoS-фреймы опроса CF-Poll.
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 HC посылает фрейм конца этого периода CF-End или истекает длительность CFP.

Взаимодействие EDCF и HCF

В отличие от работы в режиме PCF, доступ в результате опроса HCF может иметь место в период конкуренции и сосуществовать с режимом работы EDCF, а также с режимом работы DCF. Периоды TXOP опросов "распределяются" между опрашиваемыми станциями HCF и способствуют передаче или приему фреймов с данными при обеспечении QoS. HC получает доступ к среде раньше EDCF-станций, потому что должен выждать только в течение интервала PIFS, прежде чем получить доступ к среде. На рис. 6.3 показано, как сосуществуют оба режима.

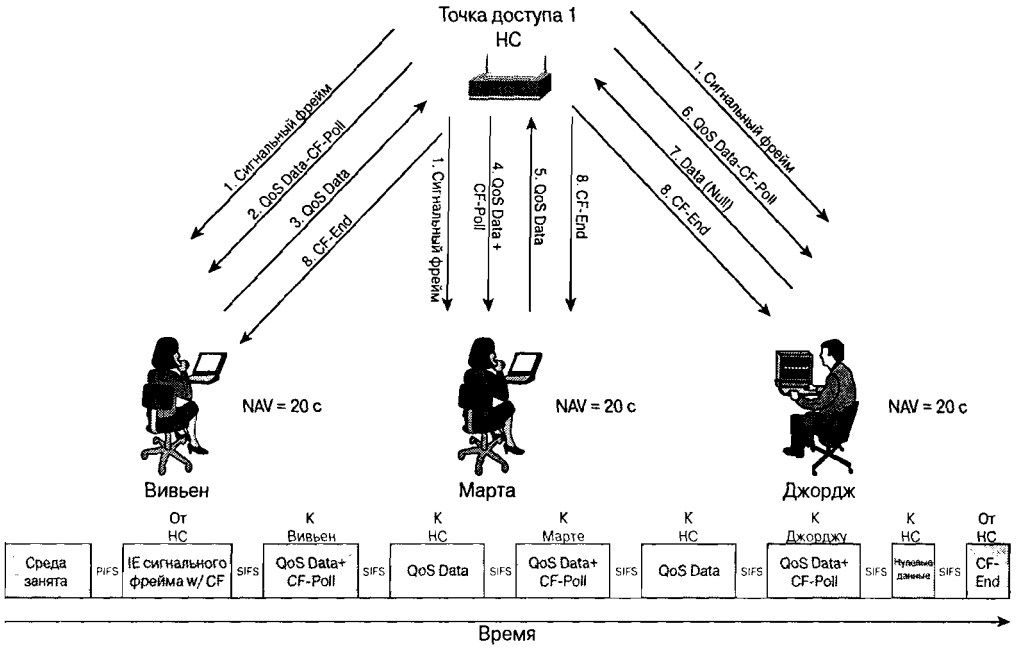


Рис. 6.2. Работа в период, свободный от конкуренции

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 (DAC) основано на том, что станции интерпретируют и соблюдают наличный бюджет для передачи, указываемый в наборе параметров информационного элемента QoS. А вот HCF требует, чтобы станция запрашивала частные параметры резервирования (particular reservation parameters) для информационного потока трафика приложения, такого как VoIP, от HC. Этот гибридный координатор должен оценить и определить, имеет ли беспроводная среда достаточный бюджет для передачи запрошенного информационного потока. Затем HC должен принять, отклонить или даже предложить данной станции альтернативный набор параметров. Как видите, этот механизм намного более выносливый и эффективный, чем DAC. Эта выносливость, однако, не лишена изъянов. Гибридный координатор должен строго соблюдать расписание информационных потоков, и в зависимости от реализации HC (который не стандартизирован 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).

- Скорость передачи данных (например, в бит/с).
- Задержку.

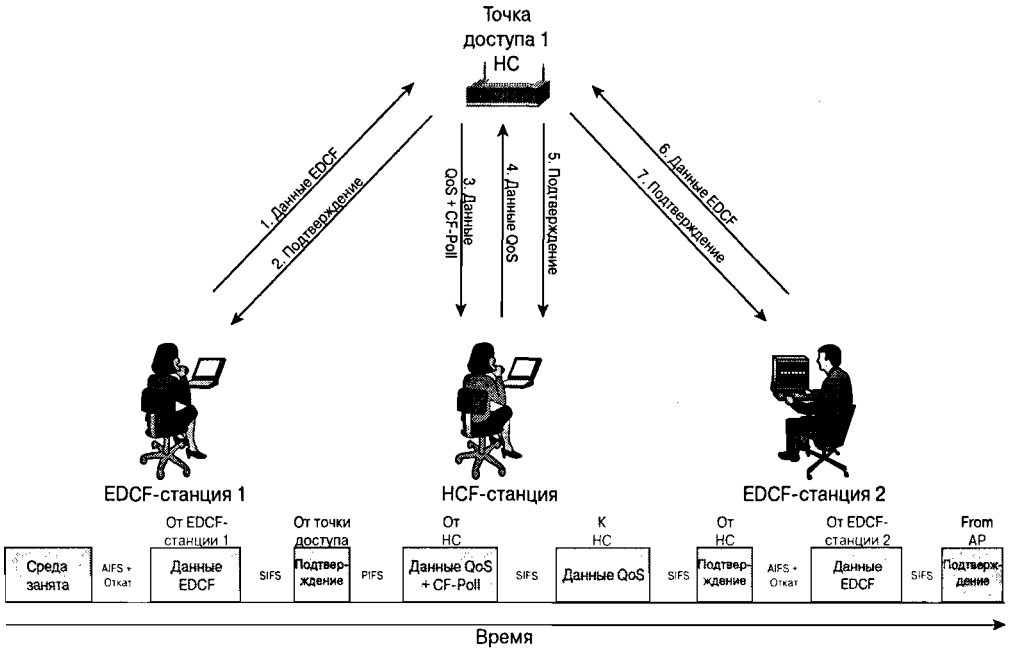


Рис. 6.3. Работа HCF в период конкуренции (совместно с EDCF)

На рис. 6.4 представлен информационный элемент TSPEC в том виде, как он определен в проекте 4.0 стандарта 802.11e.

Эта информация необходима HC для определения, может ли беспроводная среда *поддерживать* существующие информационные потоки и вновь затребованный поток *без ухудшения условий передачи для уже существующих потоков*. Элемент TSPEC показывает также гибридному 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).

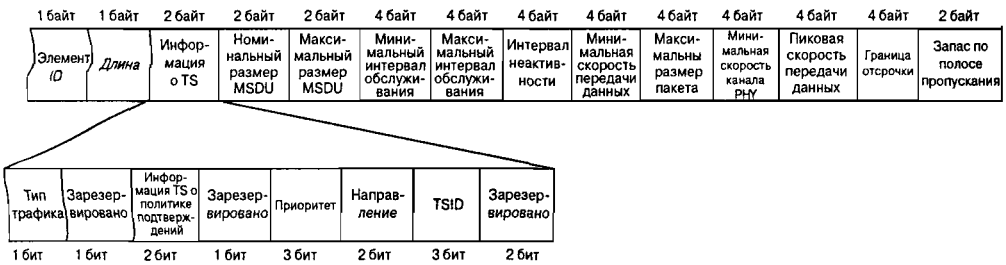


Рис. 6.4. Формат информационного элемента TSPEC

Гибридный координатор может также выполнить 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 состояться 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 опроса 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-станции должны 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 указывать 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 посылает 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 аннулирования TSPEC.

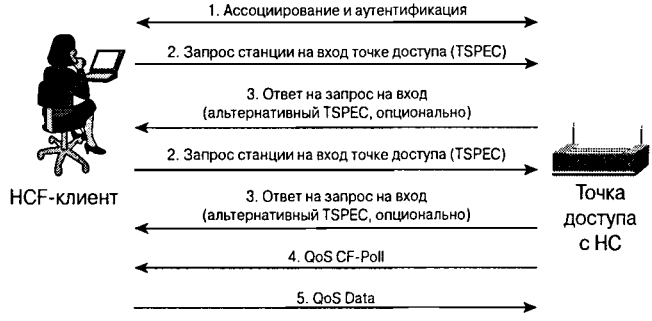


Рис. 6.5. Управляющие сообщения, посылаемые для получения права входа HCF

Если HC не может принять информационный поток, он посылает MA-ответ, отклоняющий 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.

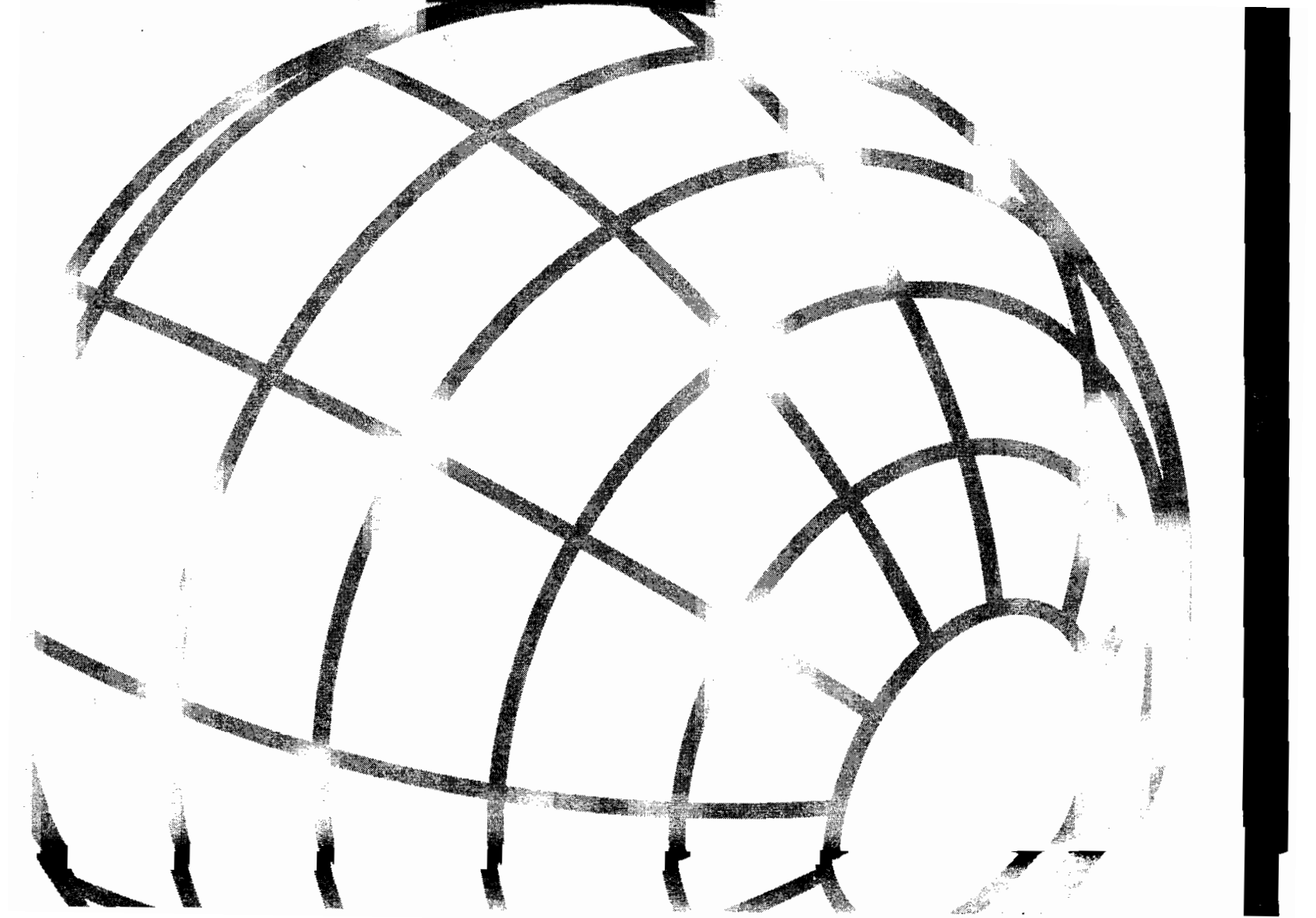
В случае тайм-аута TSPEC после определенного периода тайм-аута для завершения потока HC посылает клиентской станции MA для QoS с целью удаления TSPEC. Этот тайм-аут определяется во время опроса клиентской станции, когда она отвечает нулевыми QoS-фреймами после нескольких опросов в окне (within a set window), определяемом значением тайм-аута, заданным в TSPEC. В случае, когда QoS-станция или HC желает "снести" поток, передается MA-фрейм для уничтожения TSPEC гибридному координатору или 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 операций HCF. Эти вопросы горячо обсуждались представителями различных поставщиков в 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 входами также и для EDCF (использовании TSPEC для приема или отказа в приеме трафика EDCF). HCF имеет свои проблемы. Сторонники превозносят достоинства доступа по опросу как панацею, 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 "головной боли" для пользователей диапазона 2,4 ГГц. 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 практичного и эффективного набора инструментов для развития и распространения WLAN стандарта 802.11.



Глава 7

Радиочастотный тракт

Хотя существует только один предмет, который нужно изучить, чтобы разбираться в основных компонентах физических уровней (PHY) стандарта 802.11, это все же совершенно разные задачи — 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, способствовавших 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 сталкивается разработчик радиотракта. Хотя после прочтения этой главы вы не сможете спроектировать радиостанцию стандарта 802.11, изложенный в ней 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 осознанный выбор среди радиостанций и антенн, предлагаемых поставщиками.

Основы радиотехники

Термин *радио* относится к передаче электромагнитных волн длиной миллиметр и более через свободное пространство (эфир). Область применения радио очень широка — от автомобильных радиоприемников диапазонов AM и FM до радиостанций мобильных телефонов и наземных цифровых микроволновых радиостанций. Иногда это, как в случае радиоприемников диапазонов AM и FM, — однонаправленные или широковещательные радиоустройства. Передача электромагнитных волн осуществляется только в одном направлении, и часто в конфигурации типа "один—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 разница 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 своя частота, и эти две частоты должны быть достаточно различными, чтобы не возникало

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 полосу 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 радиостанций 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 принимающей 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 радиоэфир, или то, что принимает (захватывает) электромагнитные волны для приемника. Обычно приемные и передающие свойства эквивалентны; это означает, что такие параметры антенны, как коэффициент усиления, диаграмма излучения или частота, одинаковы.

Следующий вопрос, который вы могли бы задать, таков: "Как антенна работает?" Согласно учебнику, по которому учатся большинство разработчиков антенн, *Теория и конструирование антенн* авторов Штуцмана и Сили (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 переменного напряжения определенной частоты, который индуцирует в антенне переменный 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 излучения или размеры антенны. Производители антенн, указывая их характеристики, имеют в виду поле в дальней зоне. Помните 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 вообразите 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, диаграмму излучения, направленность, коэффициент усиления, входной импеданс, поляризацию и полосу частот.

Диаграмма излучения антенны описывает "угловое изменение радиоизлучения 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 однородно распределенной мощности излучения. Коэффициент усиления описывает то же самое, но уже с учетом потерь в самой антенне. Вы можете определить коэффициент полезного действия антенны, который используется при градуировке 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, коэффициент усиления в децибелах по отношению к антенне, называемой *полуволновая (симметричная) антенна* (или *вибратор*, иногда — *диполь*). Следует помнить, что при преобразовании одного значения в другое нужно добавить 2,2 к значению коэффициента усиления, выраженного в dBd, чтобы получить значение коэффициента усиления, выраженное в dBi. 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 полюса, которые будут индуцировать переменный ток в пространстве между собой.

Вспомнив, что излучение осуществляется в трехмерном пространстве, вы вскоре выясните, что зачастую антенна имеет *главный лепесток*, или луч, который располагается в направлении максимального коэффициента усиления, и характеризуется также *второстепенными лепестками*, часто называемыми *боковыми* или *задними лепестками* (диаграммы направленности антенны), — в зависимости от направленности второстепенных 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 по уровню 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".

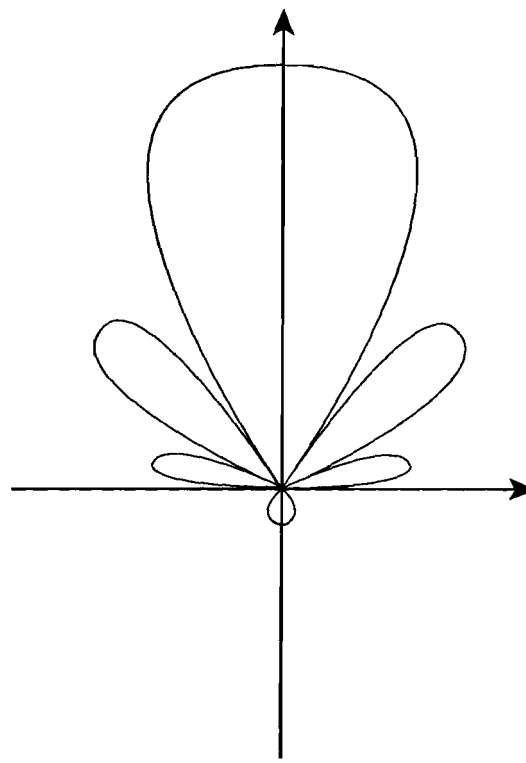


Рис. 7.1. Образец диаграммы излучения

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 вдвое 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 простой диаграммы направленности коэффициент обратного излучения антенны может составлять, допустим, 20 дБ (рис. 7.3). Коэффициент усиления главного лепестка составляет 15 dBi, обратного лепестка –5 dBi. Разница, 15 dBi – (–5) dBi = 20 dBi, и представляет собой коэффициент обратного излучения антенны.

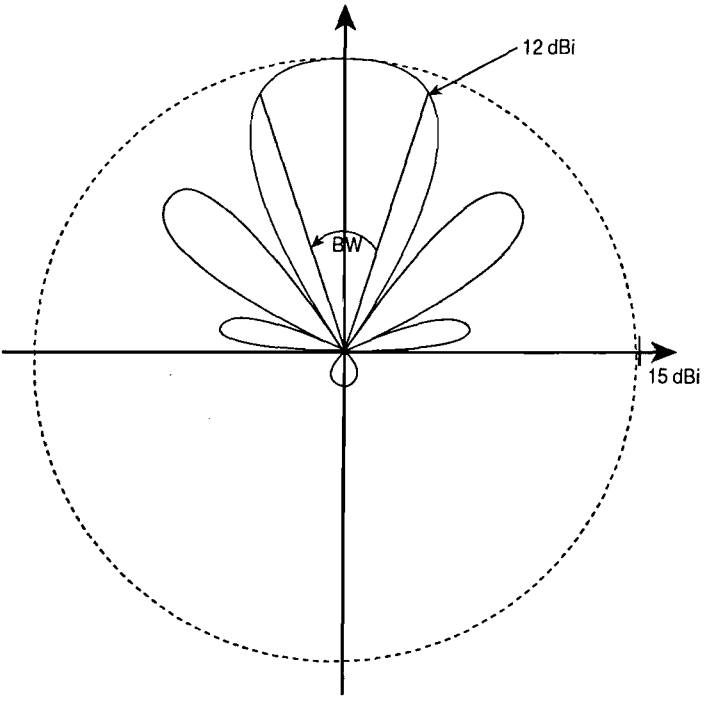


Рис. 7.2. Ширина диаграммы направленности антенны по уровню 0,5

Теперь, когда вы знаете, что такое коэффициент усиления антенны, пришло время рассказать о фактической мощности, передаваемой радиостанцией, к которой подключена антенна. Эквивалентная излучаемая мощность (ЭИМ, ERP) получается после перемножения коэффициента усиления антенны, измеренного в dBd, т.е. по отношению к полуволновому диполю, на полезную мощность, подаваемую передатчиком на антенну. Однако часто подобные математические операции проводятся в логарифмической области, или в децибелах. Это означает, что нужно сложить коэффициент усиления антенны с мощностью передатчика. Поскольку чаще всего коэффициент усиления антенны выражают в dBi, наиболее часто употребляемый термин для излучаемой мощности — эффективная изотропно-излучаемая мощность (EIRP),

это то же самое, что ERP, но с коэффициентом усиления антенны, выраженным относительно изотропного излучателя.

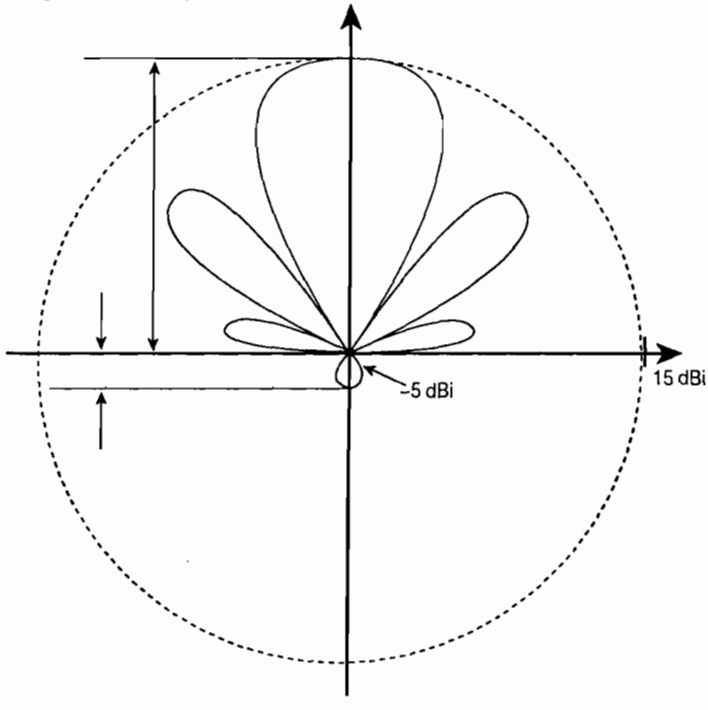


Рис. 7.3. Коэффициент обратного излучения антенны

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 станете применять антенны с круговой поляризацией, при использовании мостов такое вполне 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 он 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 полезности круговой поляризации, потому что она инвариантна по отношению к вращению. При вращении антенны с линейной поляризацией она может изменять ее с вертикальной на горизонтальную.

Вообще говоря, для линии связи, работающей в пределах прямой видимости, на обоих ее концах нужно использовать антенны с одинаковой поляризацией. Антенна с вертикальной поляризацией, имеющая коэффициент усиления 21 dBi, может

иметь коэффициент усиления в горизонтальной плоскости от 1 до -4 dBi, это означает, что уровень кроссполяризационной селекции (выделения поперечной поляризации) составляет обычно 20–25 dBi.

Коэффициент полезного действия антенны — это "отношение общей мощности, излучаемой антенной, к полезной мощности, полученной ею от передатчика". Все радиоприборы — радиостанции, линии передачи, антенны — имеют характеристику, получившую название *импеданс*, что означает отношение напряжения и тока на электрических выводах радиоприбора. Если антенна соединяется с передатчиком посредством кабеля и ее импеданс согласован 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 поступать 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 магнитудой. КСВН, равный 2, означает, что отражается 11% мощности.

Высокий КСВН и линия 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 весьма расплывчатому определению, таковыми считаются антенны, у которых отношение максимальной частоты к минимальной превышает 2. Однако, поскольку широкополосные антенны часто имеют низкий коэффициент усиления, а уже развернутые 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 безлицензионные диапазоны в области 5 ГГц национальной информационной инфраструктуры (U-NII) одной антенной.

При выборе антенны помните, что многие ее параметры взаимосвязаны, поэтому, хотя оптимальным вариантом, казалось бы, была максимизация всех "положительных" характеристик антенны или минимизация всех "отрицательных", на практике такое оказывается невозможным. Например, если вы выберете антенну с очень широким главным лепестком, вам придется пожертвовать коэффициентом усиления; выбрав широкополосную антенну, вы можете обнаружить, что ее диаграмма направленности неоднородна. Поэтому важно определить, какие именно характеристики антенны важны для условий конкретного ее применения, и сделать соответствующий выбор.

Типы антенн

Не исключено, что на своем веку 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 полуволнового 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 — одни из самых распространенных направленных антенн, потому что они просты в изготовлении. Направленные антенны, такие как антенны Уда–Яги, обычно обеспечивают покрытие в труднодостижимых зонах или когда необходим больший радиус действия, чем обеспечиваемый ненаправленной антенной.

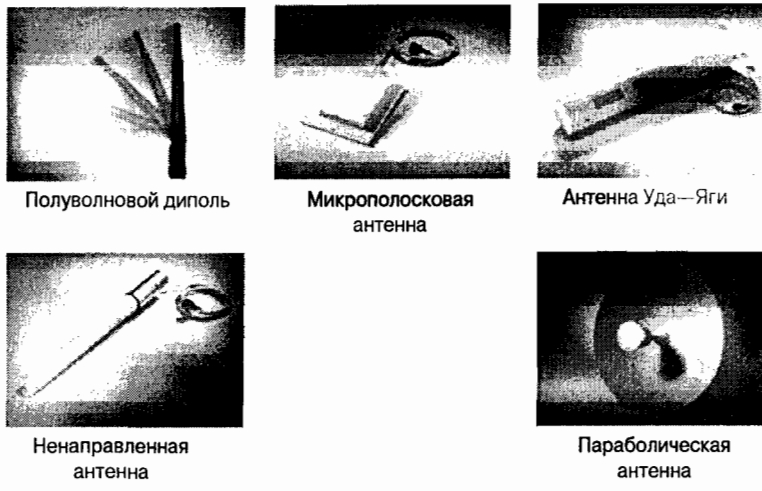


Рис. 7.4. Антенны, применяемые в беспроводных LAN

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 полезными, 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 ratio, FER). Например, стандарт 802.11a указывает, что минимальной приемлемой характеристикой приемника является чувствительность -65 dBm при скорости передачи данных 54 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 должно быть отношение сигнал/шум и, следовательно, тем выше чувствительность приемника. Чувствительность приемника радиостанции зависит также от характера шума приемника. Все приемники имеют некоторый базовый, изначальный уровень шума, определяемый или точностью 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 наглядно представлена на рис. 7.5. Чувствительность приемника — один из важнейших входных параметров для оценки характеристик радиостанции и расчета 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 максимально возможной чувствительностью, если это позволяют средства.

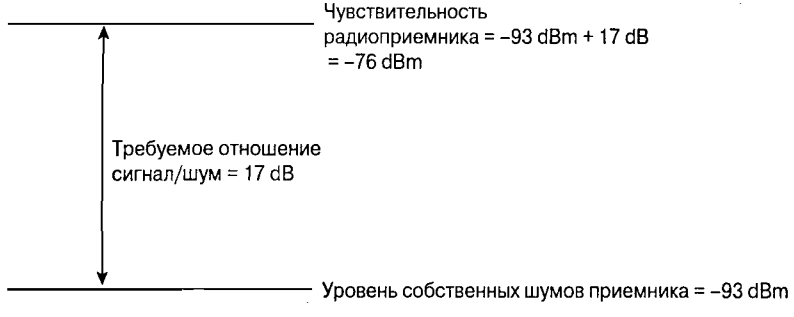


Рис. 7.5. Вычисление чувствительности приемника

Минимальные характеристики радиостанции стандарта 802.11b

Чтобы вы могли выбрать систему с удовлетворяющими вас характеристиками среди оборудования, предлагаемого различными поставщиками, стандарт 802.11b для PHY-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 dBm 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 фильтровать их или быть способным работать при наличии сигнала соседнего канала с поддержанием 0,08 FER. Для тестирования степени подавления помех от соседнего канала уровень нужного сигнала устанавливают таким, чтобы он на 6 дБ превышал уровень чувствительности приемника, а уровень сигнала соседнего канала устанавливают 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 источник 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 перекрестных помех от соседнего канала (alternate adjacent channel rejection) на соединителе антенны для скоростей передачи данных стандарта 802.11a при PER менее 10% и длине PSDU 1000 байт. Что касается характеристик подавления, то уровень полезного сигнала должен на 3 дБ превышать уровень минимальной чувствительности и уровень сигнала помех, задаваемый указанным в таблице отношением.

Таблица 7.2. Минимально допустимые характеристики радиостанции стандарта 802.11a

Скорость передачи данных (Мбит/с)	Минимальная чувствительность (dBm)	Подавление помех от соседнего канала (дБ)	Подавление перекрестных помех от соседнего канала (дБ)
6	–82	16	32
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 dBm. Стандарт 802.11a также регламентирует чувствительность функции оценки незанятости канала (CCA); она должна быть такой, чтобы уступающая среду передачи радиостанция могла определять ее занятость с 90-процентной вероятностью в течение 4 мкс в том случае, если уровень полученного сигнала превышает или равен -82 dBm в течение преамбулы. Если преамбула пропущена, то указанный уровень составляет -62 dBm.

Характеристики системы

Наконец, то, что больше всего интересует вас и пользователей вашей WLAN, — это такие характеристики радиостанции, как зона уверенного приема и пропускная способность. Они напрямую связаны с радиусом действия и скоростью передачи данных. Для определения радиуса действия вы должны знать, как можно перейти от коэффициента усиления системы, которую вы собираетесь приобрести, к ее радиусу действия в условиях развертывания вашей 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 необходимы дополнительные 6 дБ. Однако обычно WLAN развертываются в помещениях, и прохождению сигнала мешают стены, столы, люди и другие объекты, все они уменьшают уровень сигнала и увеличивают потери. В главе 8, "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.

Энергетический потенциал линии 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 поставщиком в спецификации кабеля. В общем случае чем выше частота, тем выше потери в кабеле, поэтому нужно более продуманно использовать 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 коэффициенты усиления антенн и затем поделите результат на потери в кабеле и чувствительность приемника, то получите общий коэффициент усиления системы K_S:

$$K_s = \frac{p_{Tx} * g_{Tx} * g_{Rx}}{l_{Tx} * l_{Rx} * l_{Rx}}.$$

Если проводить эти же вычисления с помощью логарифмов или используя в качестве единицы измерения децибелы, все вычисления сведутся к сложению и вычитанию:

$$K_S = P_{Tx} + G_{Tx} + G_{Rx} - (L_{Tx} + L_{Rx} + S_{Rx}).$$

В табл. 7.3 представлены два примера энергетического потенциала линии связи с неким 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 именно параметры нисходящего канала ограничивают общий радиус действия и скорость 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	–76
Коэффициент усиления системы (дБ)	100,7	106,7	97,7	95,7

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 (замирание сигнала).

Взаимные помехи возникают, когда какой-нибудь посторонний 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-

гое устройство, осуществляющее передачу в той же полосе частот. Чем сильнее этот источник взаимных помех, тем большим 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 многолучевого 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 многолучевого распространения. На рис. 7.7 представлен 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 ноутбуком на коленях и работать через точку доступа, расположенную в коридоре. Если кто-то закроет дверь, ведущую в конференц-зал, потери на трассе возрастут, что приведет к уменьшению уровня принимаемого сигнала. Вот так и получается замирание сигнала.

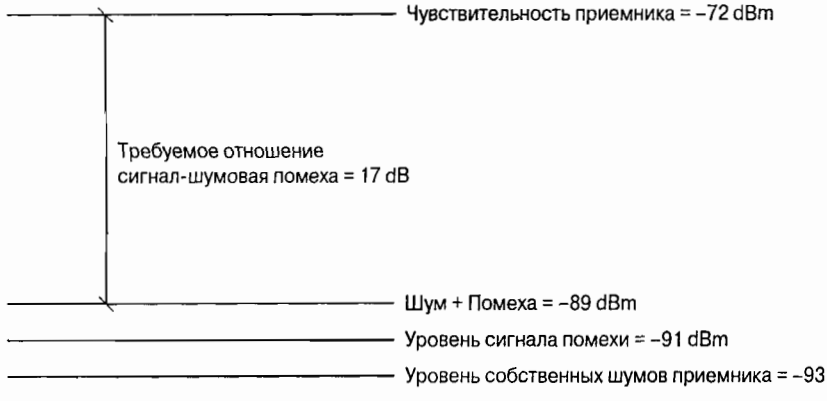


Рис. 7.6. Чувствительность приемника при наличии помех

Равномерное 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 ослабляться 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 потом уже осуществляются кодирование и чередование. Этот процесс обеспечивает определенное преимущество технологии OFDM перед другими методами модуляции, например перед кодированием с использованием комплементарных кодов (CCK), потому что в случае частотно-избирательного замирания может произойти ослабление только нескольких тонов OFDM-сигнала. Следователь-

но, остается возможность восстановления исходного потока битов за счет кодирования и чередования. В случае же CCK целостность потока битов может быть нарушена.

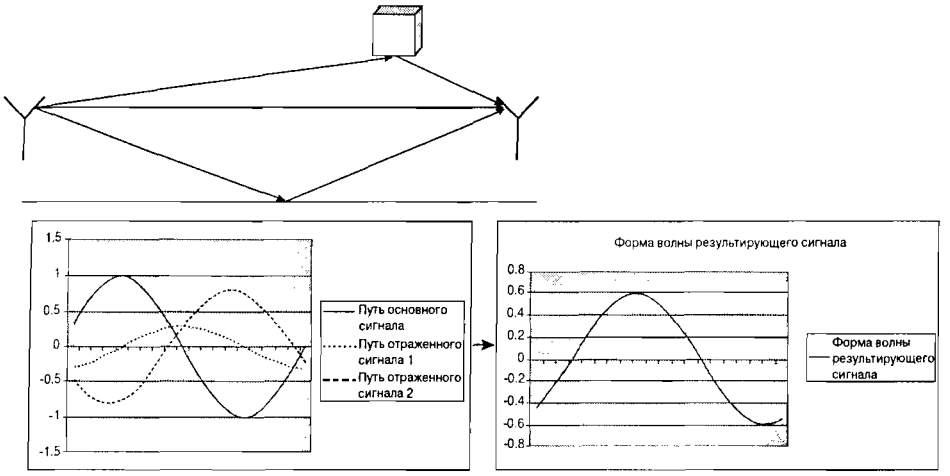


Рис. 7.7. Суммирование сигналов при многолучевом распространении

В зависимости от параметров многолучевого распространения модель потерь на трассе, характерная для свободного пространства, когда они 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 ($10*\log(2^4)=6$), а на 12 дБ ($10*\log(2^2 2)=12$). Другими словами, если вы организовываете связь в условиях прямой видимости между передатчиком и приемником при отсутствии мешающих отраженных сигналов или поглотителей энергии электромагнитных волн, вам нужно увеличивать энергетический потенциал вашего 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 недалеко отстоящих одна от другой точках может наблюдаться существенно различное замирание сигнала (что говорит об изменении характера многолучевого распространения). Вы можете столкнуться с таким явлением в вашей повседневной жизни, когда слушаете радио в своем автомобиле, стоящем перед светофором. Иногда бывает достаточно сместиться 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 используют одновременно несколько антенн или разнообразные передающие и приемные антенны. Если эти антенны отстоят одна от другой хотя бы на расстояние, равное длине волны, принимаемые ими сигналы становятся некоррелированными, 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 поразному 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. Рабочие 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 взаимодействия, 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 помог объединить европейские страны вокруг общего набора документов, регулирующих 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 неизлучающее 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 технологии 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, изданные FCC. Часть 15 CFR47 регулирует использование нелицензированных излучателей, независимо от того, какие они — преднамеренные, непреднамеренные или побочные. Часть 15 правил напрямую регулирует выходную мощность, чтобы вторичный пользователь не создавал помехи для первичного пользователя. В общем случае вторичный пользователь использует частоту (или ряд частот) при уровнях мощности, меньших, чем разрешены для первичного пользователя, такого как оператор радиолюбительской 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 первичному пользователю легко подавлять вторичного, если пути их радиоволн пересекутся.

Частоты диапазона ISM

В диапазоне ISM имеются каналы, предназначенные для использования нелицензионными 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. Относительно пика 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 излучения 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 пиковая мощность до 1 Вт с антенной, имеющей коэффициент усиления 6 dBi. В результате получается эффективная изотропно-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 увеличения 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 1 дБ свыше 6 dBi, таким образом поддерживая ограничение на EIRP значением 36 dBm.

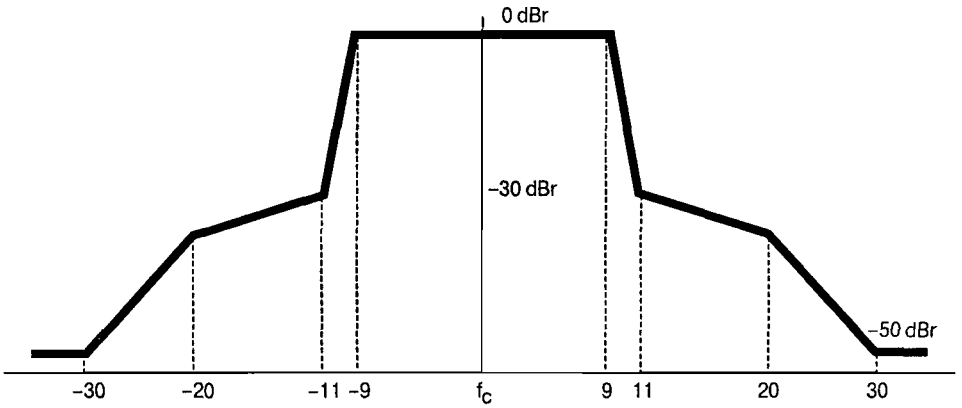


Рис. 7.8. Спектральная маска стандарта 802.11b

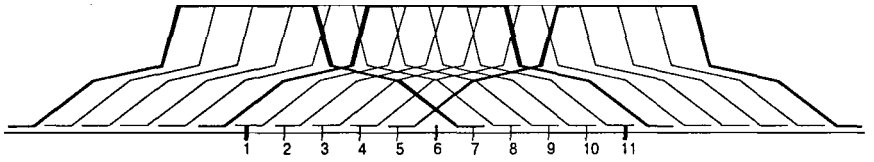


Рис. 7.9. Неперекрывающиеся каналы стандарта 802.11b

Для стран, применяющих правила ETSI, Европейский стандарт на телекоммуникации (European Telecommunications Standard, ETS) инструкцией 300328 ограничивает уровни передаваемой мощности, которые могут быть использованы. Она предусматривает мощность EIRP на уровне 100 мВт, или 30 dBm. В Японии статья 49-20 распоряжения MPT, регулирующего использование радиооборудования, определяет параметры передачи в этом диапазоне. Для сигналов устройств, использующих технологию расширения спектра методом прямой последовательности (DSSS), может использоваться выходная мощность 10 мВт/МГц. Для передачи сигналов, полученных 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

Вообще говоря, частоты диапазона U-NII доступны в основном в США и странах, которые приняли правила использования 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 неперекрывающиеся 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 20 МГц от граничных частот диапазона. Этот факт важно помнить при рассмотрении требований к побочному радиоизлучению и спектральной маске для этого диапазона, потому что выполнять их разработчикам радиотракта сложнее, чем аналогичные требования нижних диапазонов.

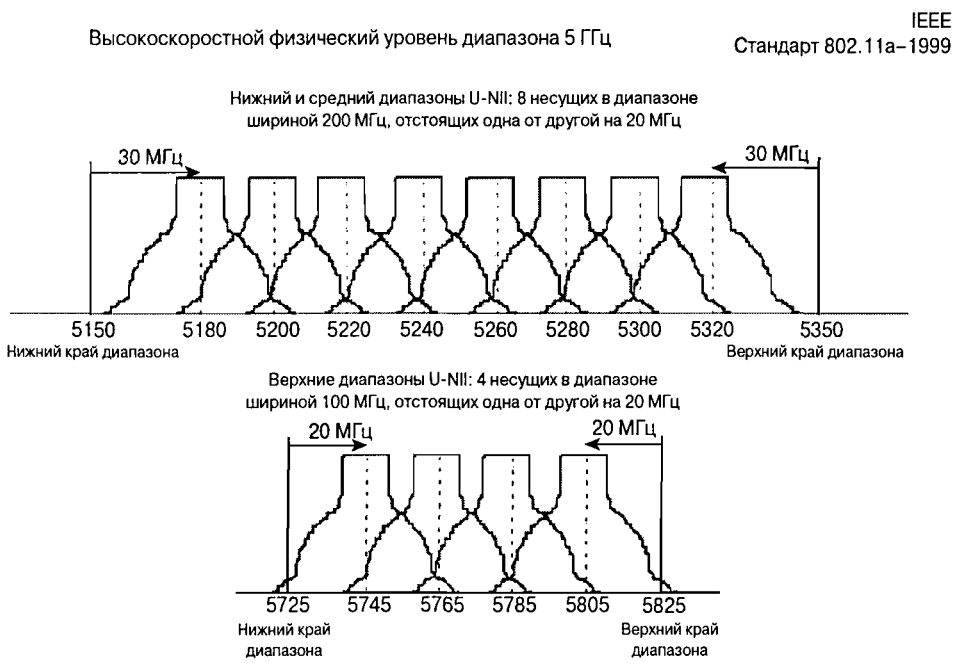


Рис. 7.10. Каналы диапазонов U-NII 1, U-NII 2 и U-NII 3

Побочное радиоизлучение и спектральная маска диапазона U-NII

В части 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 встроенная антенна. Для диапазона U-NII 2 опционально справедливы точно такие же правила, но можно размещать радиостанции и вне помещений; они могут иметь не только встроенные 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 побочное радиоизлучение должно иметь EIRP меньший 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 dBr по отношению к максимуму спектральной плотности сигнала вплоть до максимальной ширины полосы частот 18 МГц, а затем он должен быть меньше -20 dBr "на расстоянии" 11 МГц от центральной частоты, -28 dBr на частотах, отстоящих от центральной на 20 МГц, и -40 dBr для частот, отстоящих от центральной на 30 МГц и более. Эта спектральная маска показана на рис. 7.11.

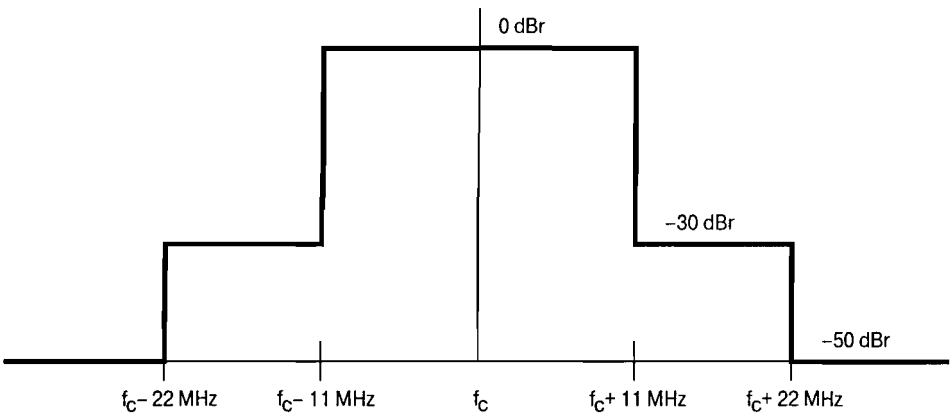


Рис. 7.11. Спектральная маска стандарта 802.11a

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 –14dBr 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 накапливаться.

Вам также необходимо иметь информацию о требованиях, предъявляемых к спектральной маске и побочному радиоизлучению, когда вы применяете удаленные антенны. Когда производители сертифицируют свои радиостанции и антенны на пред-

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 бывает 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.

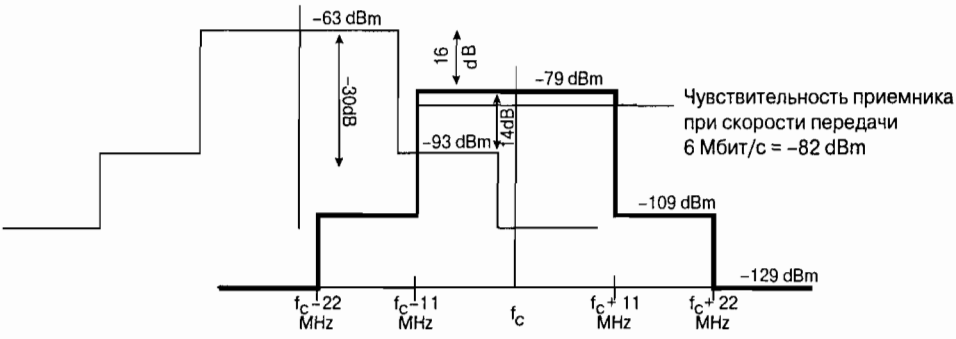


Рис. 7.12. Помеха от соседнего канала

Ограничения на передаваемую мощность диапазона U-NII

Три диапазона U-NII имеют различные ограничения на мощность излучения. U-NII 1 предназначен для использования устройствами, рассчитанными на работу только в помещениях, при наименьших уровнях излучения. Диапазон U-NII 3 имеет наивысшие уровни, потому что он предназначен для устройств, работающих вне помещений и на больших расстояниях.

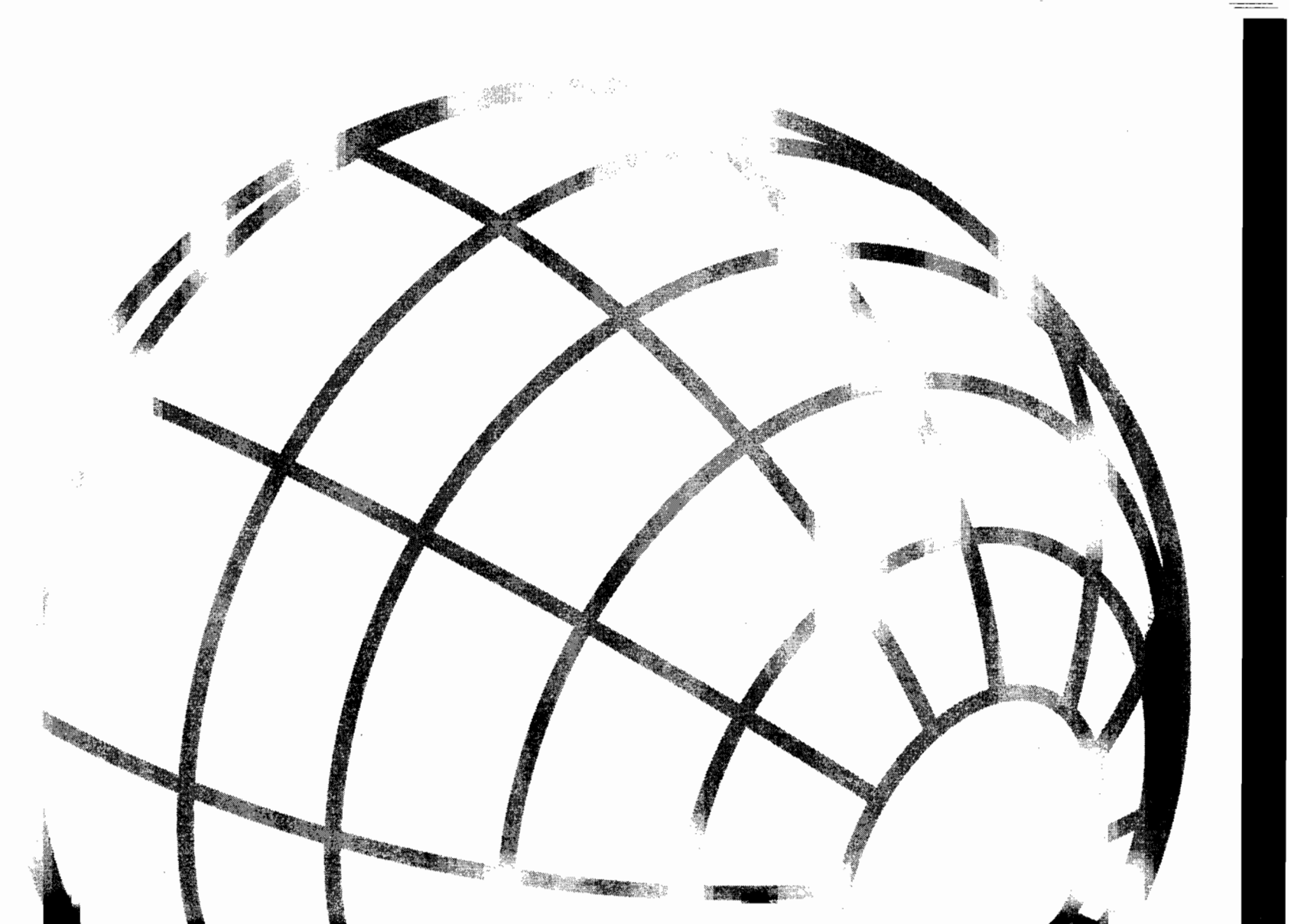
Следующие ограничения на излучаемую мощность установлены стандартом 802.11a для работы в диапазонах U-NII.

- 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, 23 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 800 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 23 dBi без снижения мощности передатчика, но только в фиксированных

каналах типа “точка–точка”. При таких условиях максимум EIRP может составлять 52 dBm.

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 излучаемой мощности ее передатчика. Следует рассматривать 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.



Глава 8

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 потолочный монтаж устройств. Физический аспект выполнения картирования места работ дает возможность администратору понять, какую зону покрытия имеет каждая точка доступа, каково количество точек доступа, необходимое для покрытия заданной области, и установить параметры каждого канала и излучаемую мощность. Администратор сети должен также принять во внимание следующее.

- Схемы роуминга беспроводных клиентов.
- Приложения, используемые беспроводными клиентами.

На основании этого следует принять следующие важные решения: как много точек доступа придется использовать, каково 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 поразному. Вам важно разобраться в этом, прежде чем вы начнете планировать развертывание своей WLAN. Ключевые моменты перечислены ниже.

- Расчетная производительность в пересчете на одного клиента.
- Потоковые и пульсирующие типы приложений.
- Конкуренция за среду передачи и задержка выполнения приложений.

Расчетная производительность каждого клиента уменьшается 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.

Задавая 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 сугубо 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 пульсирующего типа, например использующих протокол HTTP или POP3. Типичный двухсторонний разговор по технологии G.711 требует средней производительности на уровне MAC 240 Кбит/с. Приняв это во внимание, вы можете ошибочно предположить, что одна BSS может поддерживать 25 таких разговоров (25 * 240 Кбит/с приблизительно составляет 5,86 Мбит/с).

Но каждый двухсторонний разговор требует также перенаправления фреймов со скоростью 200 фреймов в секунду (50 фреймов в секунду и 50 подтверждений по стандарту 802.11 для каждого направления, итого 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 этого числа не принимались во внимание никакие другие данные, которые могли бы передаваться через точку доступа, — только телефонные разговоры. Любой трафик данных, предаваемых 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 по необходимости обеспечить для каждого клиента возможность использовать IP-телефонию (VoIP) стандарта 802.11, в то время как при развертывании, ориентированном на производительность, можно обеспечить необходимую плотность "количество клиентов/количество точек доступа".

Приложения пульсирующего 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 правила 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 возникновение коллизий 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. Станции тратят больше времени на получение доступа к среде, чем на передачу и получение фреймов. Этот процесс приводит к возникновению тайма-аутов протокола более высокого уровня и потенциально может привести к прерыванию сеанса связи выполняемого 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 их числа на производительность, имеет смысл сразу же корректно развернуть WLAN, а не выполнять повторно картирование места работ и расширять существующую сеть.

У вас есть возможность должным образом настроить клиентские станции, создающие высокую конкуренцию в BSS.

- **Регулирование порога фрагментации**. Порог фрагментации указывает наибольший размер, который может иметь нефрагментируемый 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 пошлет RTS. Значение RTS позволяет передатчику (клиента либо точки доступа) эффективно резервировать среду на время, необходимое для передачи фрейма и получения ожидаемого подтверждения.

В LAN обычно не применяют ни один из этих механизмов, потому что соответствующие настройки следует выполнять вручную на клиентских устройствах, они не выполняются через точку доступа. Пользователь или администратор сети должен сконфигурировать каждую клиентскую станцию на период перегруженности каналов связи, что не практикуется, особенно в больших WLAN. Кроме того, параметры фрагментации и порога RTS нужно устанавливать очень аккуратно. За улучшение характеристик, обеспечиваемое за их счет, приходится платить ростом конкуренции и увеличением числа непроизводительных 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

соотношение количества пользователей к числу точек доступа 25:1.) Некоторые типовые особенности WLAN, развертываемых в расчете на максимальную зону обслуживания, таковы.

- В них применяются приложения пульсирующего типа с низкой скоростью передачи пакетов, такие как сканеры штрих-кодов, и приложения, формирующие запросы к базам данных.

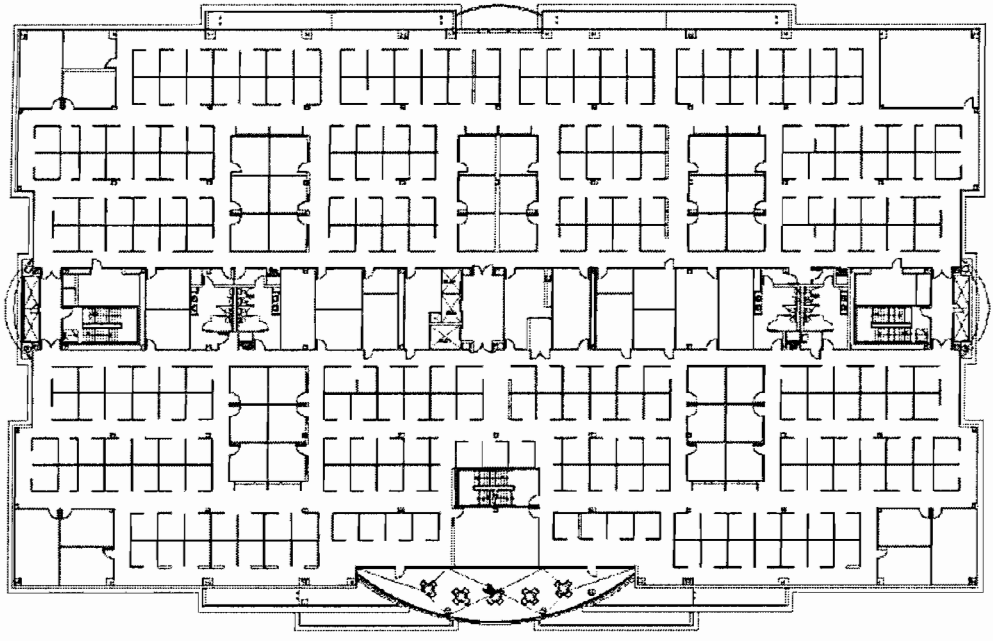


Рис. 8.1. План этажа типичного офиса

- 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 невелик или отсутствует вовсе.

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.

Подобные варианты развертывания типичны для применения внутри строений или в розничной торговле, где WLAN незаменимы при решении вопросов управления запасами и оперативной закупочной деятельности, когда специалисты по информационным 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 филиалов 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 в развертывании WLAN обеспечивают основные соединения в локальной сети, необходимые для совместного использования файлов и принтеров.

На рис. 8.2 показан пример плана этажа, представленного на рис. 8.1, с развернутой на нем WLAN, ориентированной 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 предполагается развертывание 14 точек доступа. Обратите внимание на то, что предполагается покрытие всех помещений, включая туалеты, комнаты отдыха и лестничные колодцы, где в общем случае доступ к WLAN не является обязательным. Разумно предположить, что возможны и другие конфигурации, с меньшим числом точек доступа; но представленной на рис. 8.2 конфигурацией проще всего проиллюстрировать обсуждаемый вариант развертывания.

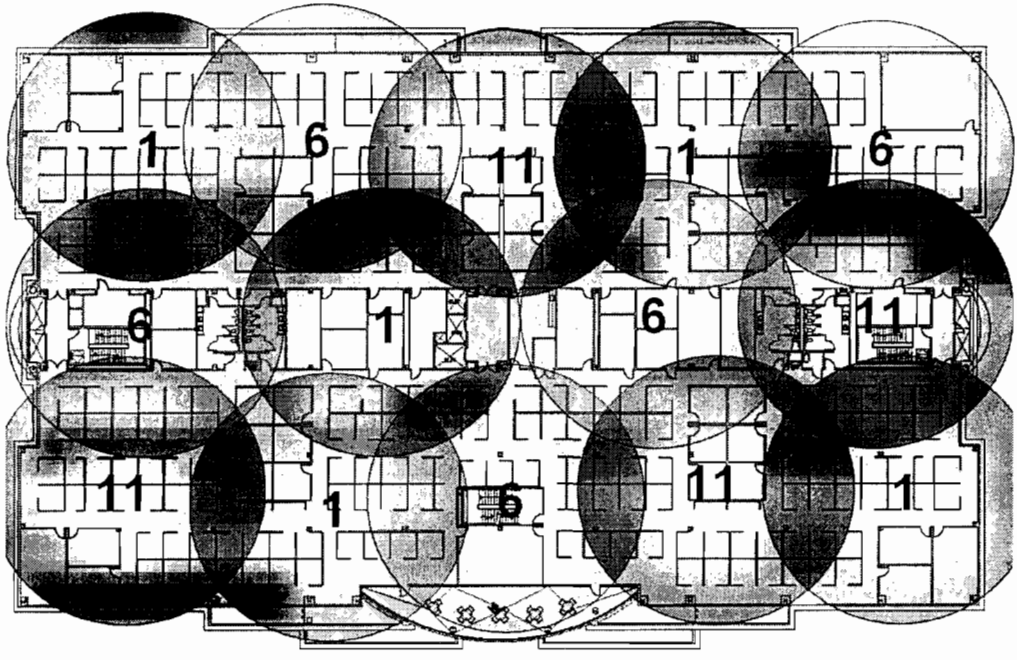


Рис. 8.2. План типичного офиса с беспроводной LAN, ориентированной на максимальную зону обслуживания

Беспроводные LAN с максимальной пропускной способностью

Беспроводные LAN, ориентированные на высокую пропускную способность, должны обеспечивать максимальную производительность и скорость передачи пакетов для каждого клиента BSS. Размеры сот ориентированной на пропускную способность WLAN меньше, чем таковые 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. 8.3 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 более 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.

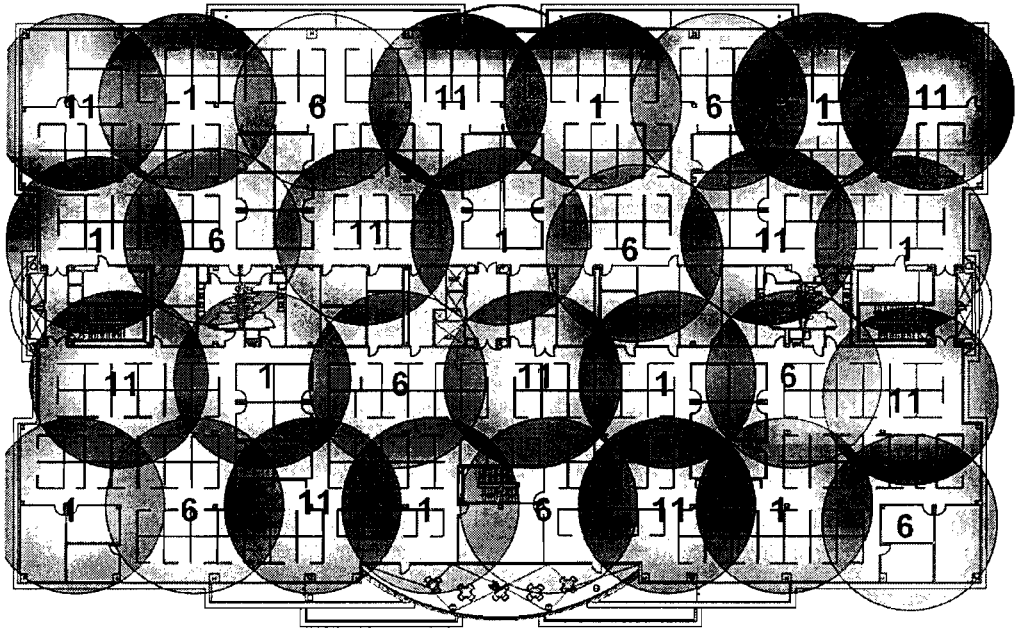


Рис. 8.3. План типичного офиса с WLAN, ориентированной на высокую пропускную способность

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 поблизости 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 готовиться к полномасштабному развертыванию сети, даже если первоначально ее задачей является обслуживание лишь нескольких помещений.

Целесообразно провести первоначальное картирование места работ в расчете сразу же на полномасштабное развертывание сети. На рис. 8.4 показан вариант частичного развертывания сети для офиса, план которого был представлен на рис. 8.2 (с проектом сети, ориентированной на максимальную зону обслуживания). Разворачиваемые точки доступа должны обслуживать конференц-залы и другие помещения, в которых часто бывают многие пользователи. Черными точками обозначены места, где в будущем предполагается разместить точки доступа так, чтобы они не вносили помехи 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.

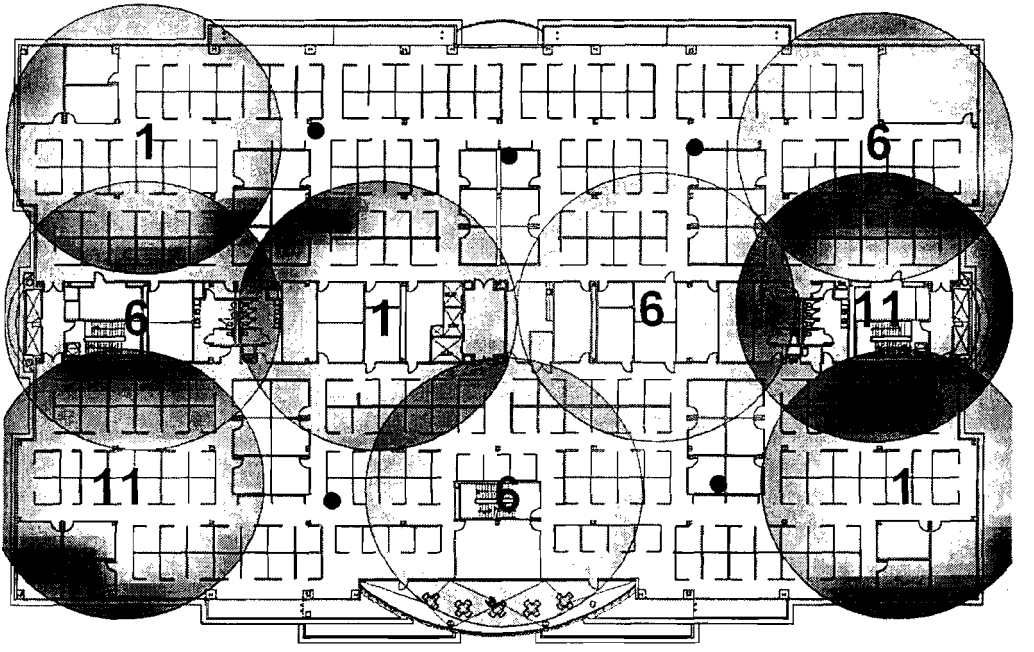


Рис. 8.4. План частичного развертывания сети для офиса

Картирование места развертывания сети

Все, что вы как системный администратор или картировщик места работ должны знать, — это число, расположение и необходимую конфигурацию точек доступа в зданиях компании. Чтобы получить эту информацию, как уже говорилось, важно вначале определить, какой будет развертываемая 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 передатчики какой мощности следует использовать и какого типа или с каким коэффициентом усиления должны быть

антенны. Зная все это, администратор может определить 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 в пересчете на одного пользователя, а также выяснить плотность размещения пользователей, чтобы определить отношение число пользователей/число точек доступа. Кроме того, вам необходимо учесть и другие факторы, такие как ограничения, накладываемые проводной инфраструктурой и возможностью 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 должны отчетливо осознавать их наличие еще до того, как приступите к изучению места развертывания сети. Например, если вы не знаете, какова инфраструктура помещения, то можете обнаружить, что разместили свои точки доступа на расстояниях, 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 понять: все нужно начинать сначала. Многие из препятствий, которые вам придется преодолевать, могут оказаться специфичными для отрасли промышленности, в которой вы работаете, как в предыдущем рассмотренном нами примере, когда из-за большого количества помещений могут потребоваться уникальные решения. В данном разделе мы рассматриваем проблемы, с которыми вы можете встретиться и которые должны выявить; 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 многолучевое распространение (см. главу 7, "Радиочастотный тракт"), или на объекты, которые могут поглощать радиоволны, мешая их распространению в принципе. Например, полки, заполненные поглощающими энергию бумажными продуктами, вообще препятствуют распространению радиоволн, иногда создавая "тени", в которых прием крайне затруднен, точно так же, как непрозрачные объекты мешают распространению света. Возможен и противоположный случай, когда пустые металлические полки способствуют вредному многолучевому 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, захочется 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 вы должны минимизировать количество энергии, которая просачивается в другие зоны, когда полки пусты, или уменьшая мощность передатчика, или за счет применения направленных антенн. В любом случае вам придется тщательно промерить 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 ночной инвентаризации с использованием сканеров штрих-кодов. Эти сканеры могут потребовать передачи очень большого числа пакетов транзакций, которые должны достигнуть мест своего назначения в ограниченный период времени. И наоборот, дисплеи камер наблюдения могут потребовать очень высокой пропускной способности сети. В первом случае важно, чтобы на 100% покрывались все участки, где могут применяться сканеры. Поскольку совместно используются немногие данные, в некоторых зонах достаточно обеспечить низкую скорость передачи данных. Для передачи видеосигналов потребуется, по-видимому, 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 определенные источники помех, например некоторые беспроводные телефоны, микроволновые печи и даже другие WLAN. Беспроводные телефоны, не соответствующие стандарту 802.11, — наиболее часто встречающийся 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 бытовые телефоны диапазона 2,4 ГГц могут загромождать всю полосу пропускания, другие используют спектр в щадящем 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 телефонами общий уровень 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 ваших 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 медаппаратуры, и вам следовало бы использовать в сети те каналы, которые не используются медицинскими приборами, или при уровнях мощности, не вносящих помех в работу медаппаратуры. Первое и главное — вы должны выяснить, где расположены медицинские приборы и каковы их характеристики. Оборудование WLAN, параметры которого не выходят за рамки требований 601-1.2 Международной электротехнической комиссии (МЭК), удовлетворяет индустриальным стандартам. Это не означает, что помехи не могут возникнуть, но шансы их появления

снижаются. Если в зданиях размещается ответственное 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 вашему оборудованию 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 зоны покрытия вне помещений и не хотите тянуть длинный радиочастотный кабель от расположенной внутри помещения точки доступа к месту расположения внешней антенны, вы можете расположить точку доступа в правильно выбранном стандартном корпусе NEMA[1], 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 вносить помехи в работу сети второго этажа, и наоборот, в зависимости от особенностей конструкции здания. Потенциально это может привести к затягиванию процесса картирования места работ, потому что нужно будет измерять интенсивность сигнала не только на "своем" этаже, но и на этажах одним выше и одним ниже.

В случае развертывания сети на предприятии розничной торговли 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 пазухах подвесного 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 должна поддерживать сеть, какой именно персонал применяет эти клиентские устройства, и типы приложений, которые он выполняет с использованием WLAN. В случае стационарных ПК, размещенных в офисе, объем роуминга будет невелик, так что основное внимание можно будет уделить уменьшению степени перекрытия каналов. Если даже используются ноутбуки, не обязательно бывает необходимым обеспечивать высокую скорость передачи данных вдали от рабочих столов 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. уменьшить 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 охвата с бесшовным роумингом и обеспечением возможности связи во всех возможных точках. Помимо телефонных разговоров, такая сеть может быть наполнена множеством мелких пакетов данных, поэтому придется выяснять, насколько устройства инфраструктуры WLAN

[1] NEMA — Национальная ассоциация электротехнической промышленности. — *Прим. ред.*

приспособлены к поддержанию телефонных разговоров. В таких случаях обычно требуется, чтобы в зоне покрытия сети не было "дыр". 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 перенаправлению 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 ваши точки доступа, так и клиентские устройства должны иметь такой логотип — это императив. Альянс Wi-Fi выполняет тестирование на совместимость (см. главу 7, "Радиочастотный тракт"), так что проверенные им устройства можно использовать, не опасаясь возникновения проблем, связанных с несовместимостью.

Как уже говорилось выше, недостаточно изучить только требования, предъявляемые к беспроводным устройствам. Необходимо также исследовать 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 выяснить, 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 100BASE-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 пазухах подвесного потолка и можно ли там разместить устройства инфраструктуры WLAN. Во многих строениях имеются противопожарные перегородки, процедуры прокладки кабелей через них регламентируются Национальным сводом правил по эксплуатации электроустановок (National Electric Code). Вы должны отмерить нужные отрезки кабеля, состоящие из прямых сегментов и изгибных участков, когда кабель меняет свое направление на 90 градусов, обеспечив запас для подрядчика по прокладке кабеля на случай возникновения непредвиденных проблем. Если используется антенный кабель, следует минимизировать его длину и не забывать о потерях, которые он вносит для сигнала на рабочей частоте.

Инструменты, используемые при картировании места работ

После рассказа о проблемах, характеристиках и целях развертывания вашей WLAN пришла пора познакомить вас с инструментарием, посредством которого вы будете проводить картирование места работ.

- Клиентское устройство, радиостанция и антенна, которые вы будете обслуживать в своей сети.
- Точки доступа с портативными батарейными источниками питания, способными поддерживать их работоспособность по 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 скрещивания (brackets), изоляционная 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 удаленных антенн.
- Радиоприборы, которые обеспечат необходимые уровень и качество принятого сигнала, уровни шума и помех, а также характеристики передачи пакетов.

Проведение картирования места работ

После того как будет подготовлен весь необходимый инструментарий, настанет 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 расположены точки доступа?
- Каким 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 многоэтажном здании, не забывайте о краевых зонах — этаже над и этаже под рассматриваемым; на них тоже нужно провести все измерения. Проводите все измерения на канале, который вы собираетесь использовать, в противном случае вы можете столкнуться с помехами неизвестного происхождения. Если соты 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 применить 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 края сот и предусмотреть приемлемый уровень их перекрытия. На рис. 8.5 представлен подход "от краев к середине", а на рис. 8.6 — подход "от одной точки доступа к другой". На каждом из рисунков используемый канал показан в центре каждой окружности ряда. Бледные точки доступа указывают их начальные 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.

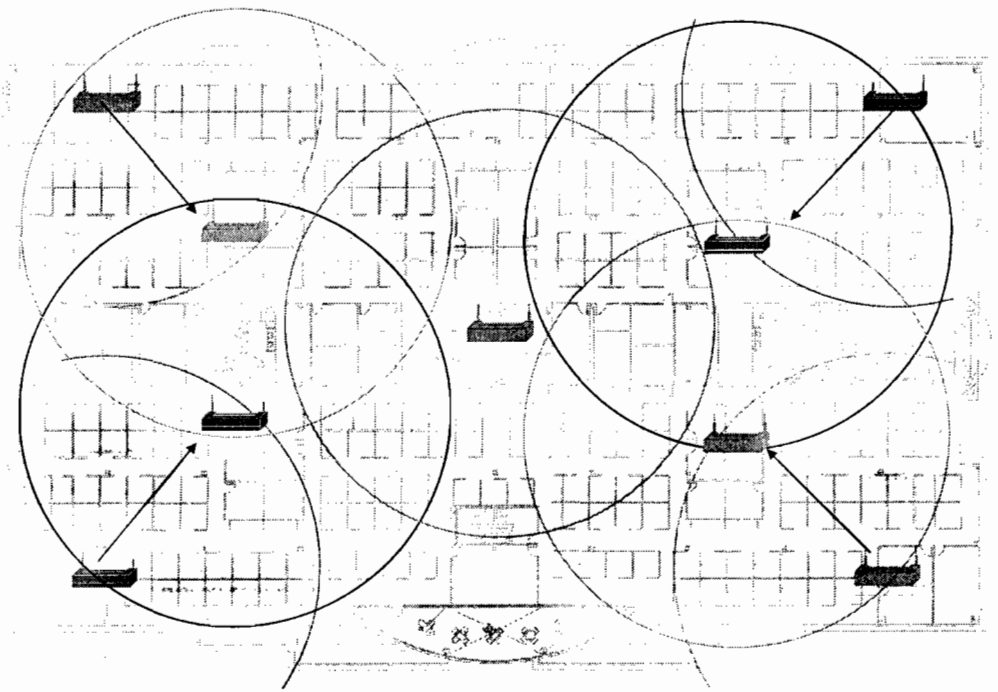


Рис. 8.5. Картирование ориентированной на максимальное покрытие LAN методом "от краев к середине" с последующим заполнением "дыр"

При подходе, ориентированном на достижение максимальной производительности, 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 до тех пор, пока не достигнете желаемых размеров сот. Вероятнее всего, вам придется использовать подход "от краев к середине", если пользователи размещаются до некоторой степени изолированными группами, но возможны и другие подходы, 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 "паззла".

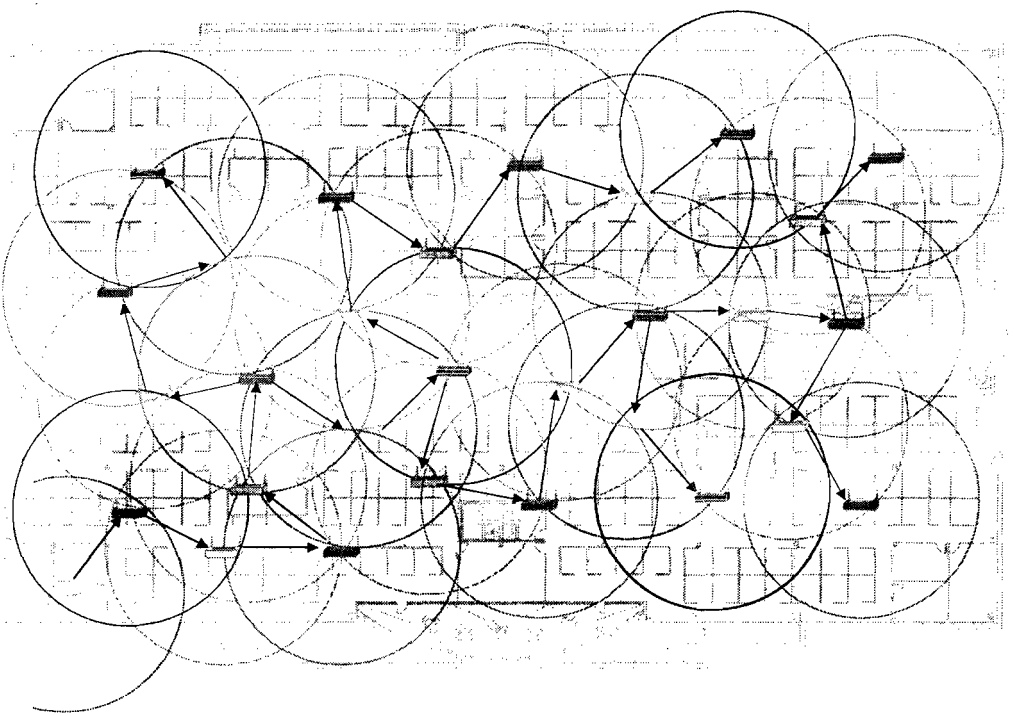


Рис. 8.6. Картирование ориентированной на максимальное покрытие LAN методом "от одной точки доступа к другой"

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 введения 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-

званному обеспечить безопасность WLAN. Решение, обеспечивающее защиту, требует применения AAA-сервера для проведения ориентированной на пользователя аутентификации. Возможно, AAA-сервер будет размещен в защищенном информационном центре, "на расстоянии" в несколько маршрутизаторов от края сети. С помощью механизмов уровня 3 можно измерить задержку в сети (network latency) между краем сети и информационным центром, которая может составлять несколько миллисекунд, если не микросекунд.

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 первые могут оказаться перегруженными. Перегрузка может оказать существенное влияние на процесс аутентификации, если он базируется 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 роуминг (рис. 8.7).

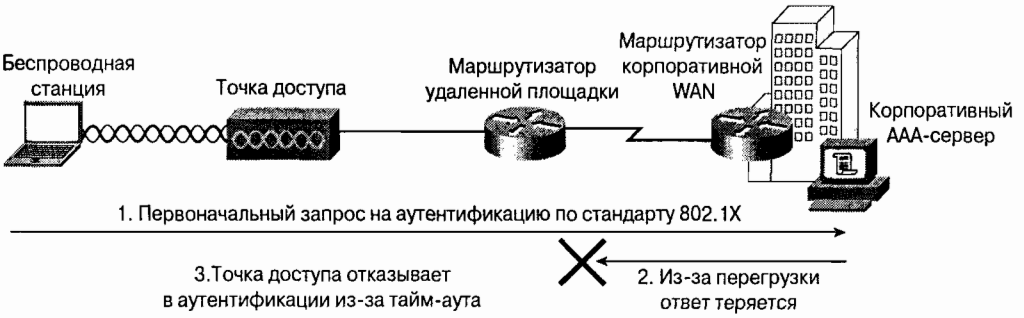


Рис. 8.7. Влияние перегрузки канала WAN на процесс аутентификации по стандарту 802.1x на удаленных площадках

Эту проблему можно сгладить двумя путями.

- Использовать механизмы QoS для задания приоритетов в отправке 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 несложно. 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). Видеосигналы 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-разговором 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 приоритезации 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 терминал со сверхмалой апертурой луча, VSAT) могут также негативно повлиять на процесс аутентификации, потому что точка доступа или клиент 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 площадок может быть много.
- **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 своих точек доступа, дабы клиенты могли избежать излишних затрат и справиться с узкими местами, появившимися в результате использование 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.

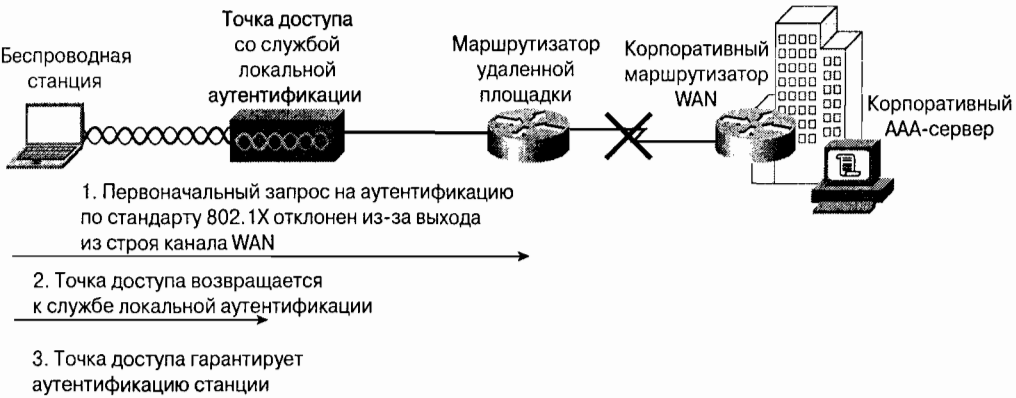


Рис. 8.8. Служба локальной аутентификации в точке доступа

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 справедливо следующее высказывание.

Нельзя управлять тем, что 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. Локальные LAN могут оказывать большое влияние на то, как вы управляете своей сетью, а также изменять используемый вами инструментарий. Чтобы добиться от WLAN такой же надежности, какую обеспечивают проводные LAN, и понизить сложность управления, вам необходимо решение для механизма управления, обеспечивающее одновременно и управление беспроводной LAN.

Многие первые энтузиасты WLAN с трудом несли бремя 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: опрос 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 местоположение внешних источников помех, таких как микроволновые печи, могут оказывать влияние на характеристики WLAN, а влияние устройств, использующих технологию Bluetooth, неплановых клиентов (ad-hoc clients) и соседей, также использующих WLAN, могут ухудшить характеристики WLAN до уровня, когда она станет вообще бесполезной.

Система управления радиотрактом дает администратору возможность четко видеть все эти проблемы и, в зависимости от применяемого решения, может помочь автоматизировать контроль таких параметров радиостанций, как выбор частоты/канала и излучаемой мощности клиента/точки доступа для адаптации сети к суровой окружающей радиосреде.

Ищите 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, выявления источников помех и мест возможного размещения служб, определенно имеет смысл.

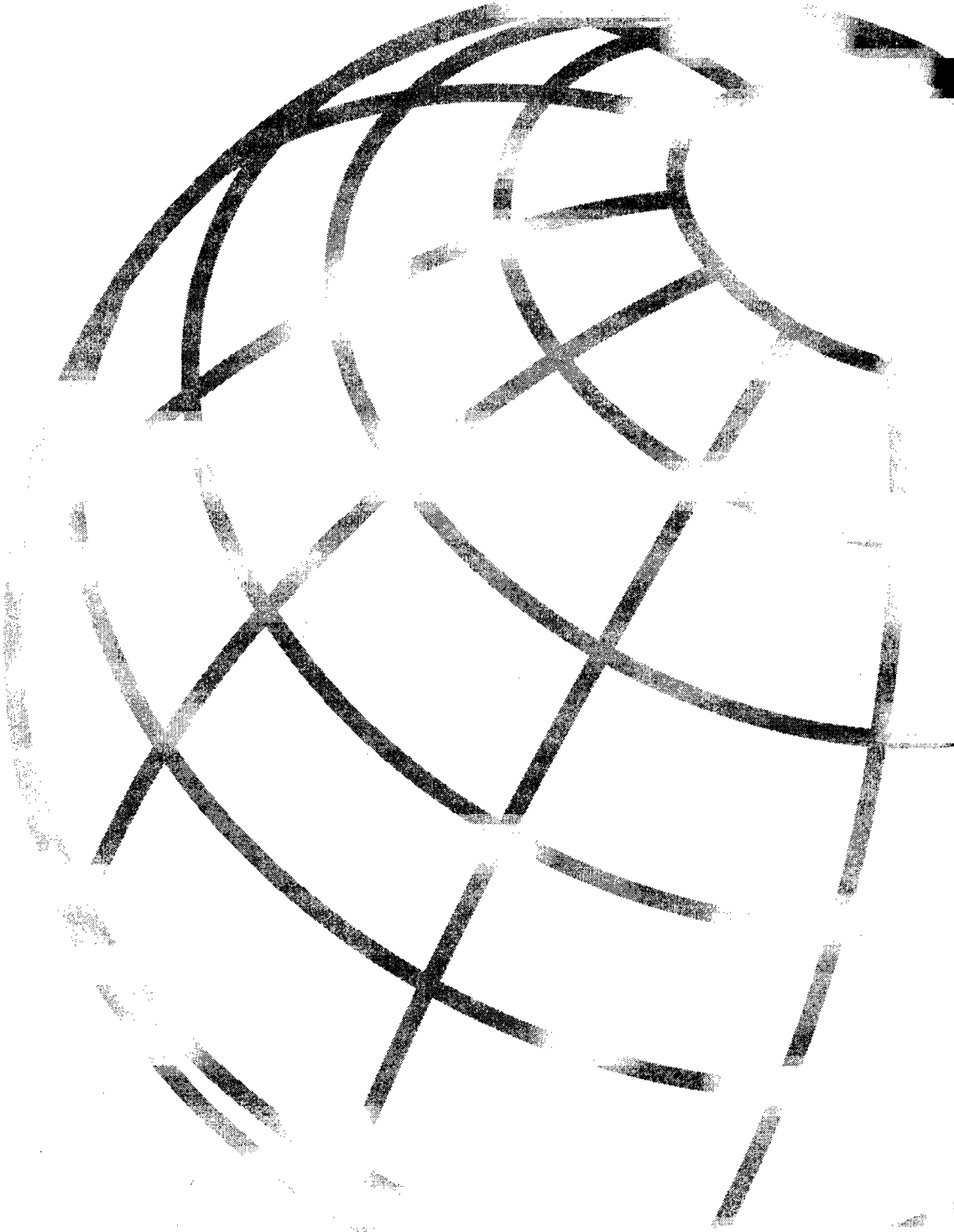
Резюме

Решения, которые вы принимаете при развертывании WLAN, весьма важны для достижения ее оптимальных характеристик.

- Какие пользователи будут использовать WLAN (чрезвычайно мобильные или кочующие)?
- Приложения какого типа будут выполнять эти пользователи с помощью LAN?

Хотя эти два вопроса являются основными и почти самоочевидными, им обычно не придают значения во время развертывания. Однако они являются основными для сбережения средств за время жизни развернутой сети, а именно при выборе сценария развертывания, т.е. при выборе между сетью, ориентированной на максимальную зону обслуживания или максимальную производительность.

Решив, как будет развертываться сеть, выясните, какой инструментарий следует использовать для проведения картирования места работ; лучший метод организации таких работ позволит сберечь время и средства, необходимые для решения этих утомительных и отнимающих много времени задач. На сегодняшний день исследование места развертывания является задачей, подлежащей решению вручную. Это означает, что все вычисления 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.



Глава 9

Будущее беспроводных LAN

Предсказывать будущее какой-либо технологии — непростая задача, однако в данной главе мы расскажем о некоторых уже имеющихся 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 хорошими дополняющими решениями.

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 *технологию 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 расположиться 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 находятся 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 говорилось, 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 отомрут.

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, находящегося

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.

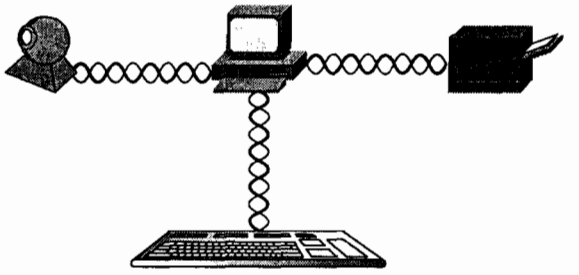


Рис. 9.1. Замена кабелей каналами связи Bluetooth

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 вызывали помех для лицензированных пользователей, и устанавливают, что они не имеют защиты от помех со стороны других пользователей, как лицензированных, так и нелицензированных. Этот момент важен потому, что в будущем такие устройства станут главным источником помех для WLAN, и наоборот, если производители ноутбуков начнут встраивать те и другие устройства в свои изделия. Подобно WLAN, они также будут подвержены влиянию помех со стороны микроволновых печей и беспроводных телефонов.

Каждое устройство сети Bluetooth (или *пикосети* (piconetwork) — крохотной 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.

Большинство устройств Bluetooth имеет уровень эффективной изотропно-излучаемой мощности 0 дБ относительно 1 мВт (dBm), хотя в спецификации оговорены три класса устройств Bluetooth.

- Передатчики 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.
- Передатчики класса 2 должны иметь максимальную излучаемую мощность 4 dBm (2,5 мВт).
- Передатчики 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. Схемы модуляции, применяемые в технологии Bluetooth, — это модуляция, основанная на гауссовом переключении частот (Gaussian frequency shift keying, GFSK), похожая на применяемую в WLAN модуляцию с расширением спектра путем скачкообразного переключения частоты (FHSS), со скоростью передачи символов 1 миллион в секунду, что дает в результате базовую скорость передачи данных 1 Мбит/с.

Аналогично старым WLAN стандарта 802.11, в технологии Bluetooth применяется механизм доступа на основе дуплексной связи с временным разделением каналов (time division duplex, TDD), использующий FHSS. Диапазон 2,4 ГГц ISM делится на 79 каналов шириной 1 МГц каждый, и каждая пикосеть скачкообразно переходит с канала на канал псевдослучайным образом. Устройства Bluetooth передают каждый пакет на новом канале. Для соединения "точка–точка" или создания пикосети с одним ведомым создаются и нумеруются временные интервалы длительностью 625 мкс, каждый для нового канала; ведущий передает в четные интервалы времени, ведомый — в нечетные. В течение каждого интервала можно передать 366 бит. В случае многоточечной пикосети ведущий тоже осуществляет передачу в четные интервалы, но каждый ведомый может передавать данные только в том случае, если в течение предшествующего 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 бит, накладные расходы протокола могут оказаться достаточно большими, поэтому в спецификации Bluetooth предусмотрена передача "многоинтервальных" (multislot) пакетов длительностью три и пять интервалов. Они передаются на одном и том же канале, и когда передача заканчивается, следующая осуществляется на канале, который использовался 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 последовательности передачи в многоточечной сети с двумя ведомыми, когда ведущий осуществляет передачу многоинтервального пакета одному из ведомых.

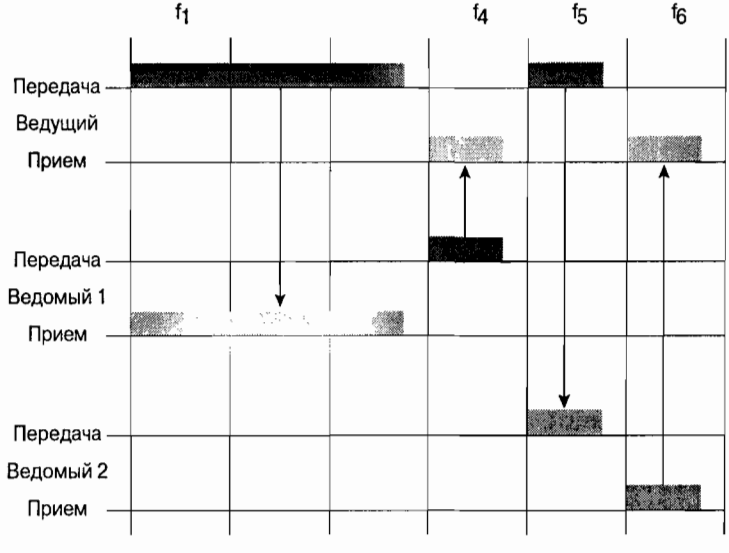


Рис. 9.2. Образец последовательности передачи по технологии Bluetooth

В технологии Bluetooth используются физические каналы двух разных типов.

- Асинхронные каналы без установления соединения (asynchronous connectionless links, ACLs) чаще всего используются для передачи данных в 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 уникальный 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 широковещательные пакеты, в которых ведущий использует адрес припаркованного участника сети для того, чтобы распарковать его. Ведущий также назначает им адрес запроса 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, в то время как ведомый — это устройство, которое включается в пикосеть по запросу ведущего. Ведущий может инициировать переход в энергосберегающий режим, отказ (sniff), удержание (hold) и парковку — для сбережения энергии, для обеспечения работы в пикосети, включающей более семи ведомых, для предоставления ведущему 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 (limitless store-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 протоколы более высоких уровней сталкиваются с проблемами маршрутизации и устранения ошибок. В случае трафика ACL участник распределенной сети может использовать режимы sniff, hold и park для управления двумя пикосетями, но в случае трафика SCO каждый член распределенной сети должен выбирать 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 устанавливать два Bluetooth-устройства на одном хосте.

Специальная группа Bluetooth (Bluetooth Special Interest Group, SIG), которая разрабатывает спецификацию Bluetooth и, помимо всего прочего, управляет действую-

щими рабочими группами, сейчас определяет несколько моделей использования специфических приложений, применяя устройства от различных поставщиков. В модели использования входят (но не ограничиваются ими) следующие.

- Обеспечение работы сотовых и беспроводных телефонов в дополнение к выполнению функций переносной рации (walkie-talkie) по принципу "три в одном".
- Наушники, обеспечивающие аудиоинтерфейс к другим устройствам, таким как телефоны, компьютеры и стереосистемы.
- Мост Internet, позволяющий через сотовый телефон создавать мост для доступа в Internet через сеть сотовой связи и компьютер с интерфейсом Bluetooth.
- Модели использования проталкивания объектов (object push) и преобразования файлов (file transfer), позволяющие осуществлять базовые преобразования данных между пригодными 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 умышленно 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 излучаемые 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 пока что руководящие принципы использования экстремально широкополосных сигналов, генерируемых при передаче коротких импульсов малой мощности; считается, что они позволят создать широкополосные и помехоустойчивые системы связи. FCC определяет UWB как сигнал, который имеет относительную ширину полосы частот, т.е. отношение полосы частот сигнала к частоте несущей, превышающую 25%. Принципы использования, разработанные FCC, регламентируют передачу UWB-сигналов в широком диапазоне, используемом многими другими технологиями, но применяющими более узкие полосы частот, чем характерные для UWB-сигналов. Это становится возможным потому, что пределы на излучаемую мощность столь низки, 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 импульсов, 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 подповерхностного 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 активизации пневмоподушек (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/МГц)					
		< 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	–53,3	–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 помещения	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 излучаемые мощности для этих систем.

Таблица 9.2. Предельные излучаемые мощности для мобильных радарных систем

Классификация	Диапазон частот в соответствии с частью 15	Предельная излучаемая мощность в соответствии с частью 15 (dBm/МГц)					
		< 0,960 ГГц	0,960–1,61 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 период следования 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 композитного сигнала, который мог бы являться одной из отдельных копий. Если длительность импульсов сигналов Bluetooth очень коротка по отношению к временны*м* интервалам между импульсами, RAKE-приемникам удобнее разделять копии.

Основные проблемы, стоящие пред 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 радиотракта, то антенны 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 беспроводную революцию, похожую на ту, которую совершает ныне технология 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 расстоянии прямой видимости, на физическом уровне типа "точка–точка" для передачи инфракрасных (ИК) сигналов непосредственно через воздух. Ожидается, что будет реализована беспроводная передача многогигабитовых сигналов, но с некоторыми серьезными ограничениями, которые до сих пор препятствуют ее широкому распространению и применению. Однако, в зависимости от специфических условий применения, такая технология может обеспечить решения, которые станут хорошей альтернативой беспроводному мосту стандарта 802.11.

Основные технические проблемы, стоящие перед технологией FSO, описаны ниже.

- Туман, состоящий из мельчайших капелек 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 вывести канал 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, атмосферной дымки или загрязняющие вещества. При увеличении длины канала потери на рассеяние возрастают.
- Физические объекты, такие как птицы, могут временно нарушить работу канала FSO.
- Покачивания высотных зданий могут нарушить юстировку передатчика и приемника и нарушить работу канала.
- Турбулентность, возникающая, когда нагретые объекты создают перемещающиеся воздушные ямы различной температуры, вызывает изменяющиеся во времени изменения показателя преломления на границах этих воздушных ям. Луч может отклонятся из-за случайных отражений при прохождении воздуш-

ных ям, это может привести к мерцаниям в виде флуктуаций интенсивности и расширению луча.

К счастью для сообщества FSO, две наиболее часто используемые в волоконной оптике длины волны, 850 и 1550 нм, совпадают с окнами прозрачности атмосферы.

Простой FSO-передатчик состоит из светоизлучающего диода (СИД, LED) или лазерного источника света и телескопа, сформированного из линз и зеркал. 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 лазеров. Поскольку полупроводниковые лазеры весьма малы по размерам, имеют большую мощность и широко используются в волоконной оптике, большинство производителей FSO создают свои системы на основе именно этих компонентов. Оптическая подсистема, состоящая из зеркал и линз, 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 больших радиусов действия необходимо использовать лучи с очень малой расходимостью, порядка миллирадиан (мрад)[1].

Если приемник находится далеко от передатчика, диаметр луча увеличивается и становится больше диаметра телескопа приемника, в результате часть переданной энергии не собирается последним, что приводит к возникновению дополнительных, "геометрических" потерь на трассе (geometrical 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 получен только 1% переданной энергии, что означает потери 20 дБ для энергетического потенциала линии связи. В чистом воздухе потери возрастают на 3 дБ при каждом удвоении длины канала.

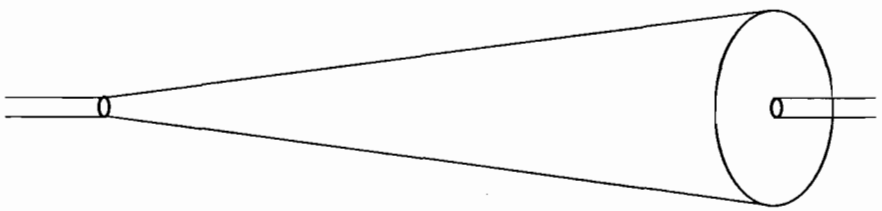


Рис. 9.3. Пример возникновения потерь на трассе, обусловленных геометрией луча

При уменьшении расходимости луча возрастают проблемы, связанные с начальной юстировкой, и канал связи становится более восприимчивым к покачиваниям зданий, из-за чего возникают потери наведения луча. Для преодоления этой проблемы при использовании узких лучей приходится использовать системы захвата и 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.

---

[1] В оригинале — milliradiant. — *Прим. ред.*

Процесс развертывания канала связи FSO может оказаться более трудоемким, чем беспроводной мостовой линии (bridging link), в основном из-за проблем, рассмотренных выше. Вы должны тщательно провести картирование места работ, сделав значительный запас на замирание сигнала, вызванное воздействием окружающей среды. Во время установки следует позаботиться о том, чтобы канал находился подальше от источников турбулентности, а сама юстировка должна быть выполнена очень точно. 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.

Вопреки всем этим предостережениям, перспектива создания каналов связи с пропускной способностью порядка несколько гигабит в секунду без необходимости копать траншеи для укладки оптических кабелей делают 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 предосторожностями 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 108 Мбит/с предлагают 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 вдвое шире стандартного. В недалеком будущем мы можем оказаться свидетелями формирования рабочей группы 802.11 по созданию технологии с более высокой производительностью. Ожидается, что она будет заниматься не только вопросами 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 привыкли получать 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, радиуса действия и потребляемой мощности, эта группа должна также рассмотреть вопросы совместного использования и обратной совместимости.

Что касается стимулов для развития WLAN с производительностью 100 Мбит/с, то их два — это эквивалентность таких сетей с проводной Ethernet 100BASE-T и перспективы применения беспроводной мультимедиа-технологии для домашнего использования. Первый будет содействовать делу создания полностью 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 Internet-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.

Глава 10

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 непростого протокола стандарта 802.11. А это значит, что нужно основательно поработать над планом развертывания и конструктивными особенностями сети, необходимыми для того, чтобы предоставить клиентам простой в использовании интерфейс.

В этой главе рассматриваются особенности конструкций WLAN для наиболее часто встречающихся вариантов развертывания: розничная торговля, здравоохранение, филиалы офисов/надомные работники, образование, общественная безопасность и доступ в общественных местах.

Сфера розничной торговли

К счастью для поставщиков WLAN, одним из секторов рынка, для которого WLAN жизненно необходимы, оказалась розничная торговля. В будущий раз, когда вы пойдете в хозяйственный магазин, магазин электроники или универмаг, обратите внимание на его стены и потолки. Вы обязательно обнаружите точки доступа или как минимум антенны, установленные в обеспечение зоны обслуживания клиентских устройств стандарта 802.11.

Бизнес такого рода нуждается в приложениях клиент/сервер, обеспечивающих управление запасами и сетью 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 клиентов стандарта 802.11, способных обеспечивать IP-телефонию (Voice over IP, VoIP), также приветствовалось многими компаниями в качестве замены патентованных узкополосных систем радиодиапазона, систем диапазона 900 МГц или приемо-передающих радиостанций. Эти новые телефонные трубки наряду с VoIP-переговорами способны обеспечивать выполнение функций, недоступных обычным телефонным трубкам, а также поддерживать двустороннюю пейджинговую связь и Web-приложения. Например, служащий

может начать работу, зарегистрировавшись с помощью своей трубки и через нее же получив рабочие задания. Использование в этих VoIP-трубках интерфейсов "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 широковещательное сообщение на все активные трубки с инструкцией одному служащему относительно выполнения какого-то конкретного задания. Все служащие получат это сообщение, один из них подтвердит получение сообщения и отправится выполнять задание.

Магазины розничной торговли начали применять технологии WLAN задолго до ратификации стандарта 802.11 в 1997 году. Многие компании производили патентованные беспроводные системы диапазонов 2,4 ГГц и 900 МГц в 1990-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 создавали пульсирующий трафик в силу своей природы. Поэтому многие из этих ранних сетей были ориентированы на достижение максимальной зоны обслуживания, и это вполне естественно. Картирование места работ проводилось с целью минимизации общего количества точек доступа и обеспечения максимальной зоны обслуживания. В типичном большом хозяйственном магазине сейчас нечасто встретишь 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 "расплодившихся" 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 магазина могут возникнуть новые. Магазин розничной торговли обычно имеет 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 хабах или центральном узле.
- Решения, относящиеся к управлению, должны легко масштабироваться, т.е. обеспечивать поддержку большего числа точек доступа.

Понятно, что магазин должен продолжать работу даже в случае аварийного отключения системы. Поскольку большинство каналов WLAN нерезервированы, базы данных, размещенные на центральном узле, могут оказаться недоступными для служащих магазина в течение всего времени неработоспособности WLAN. По этой причине серверы, обеспечивающие выполнение основных приложений, обычно располагаются в самом магазине.

С целью повышения эффективности использования вложенных средств приложение VoIP обычно выполняется централизованно. Выход из строя WLAN может повлиять на работу VoIP-приложения. Для преодоления этой проблемы многие производители предлагают режимы повышения живучести. Инфраструктура локальной сети может обнаружить утрату соединения с центральным узлом и перейти в режим автономного обеспечения живучести.

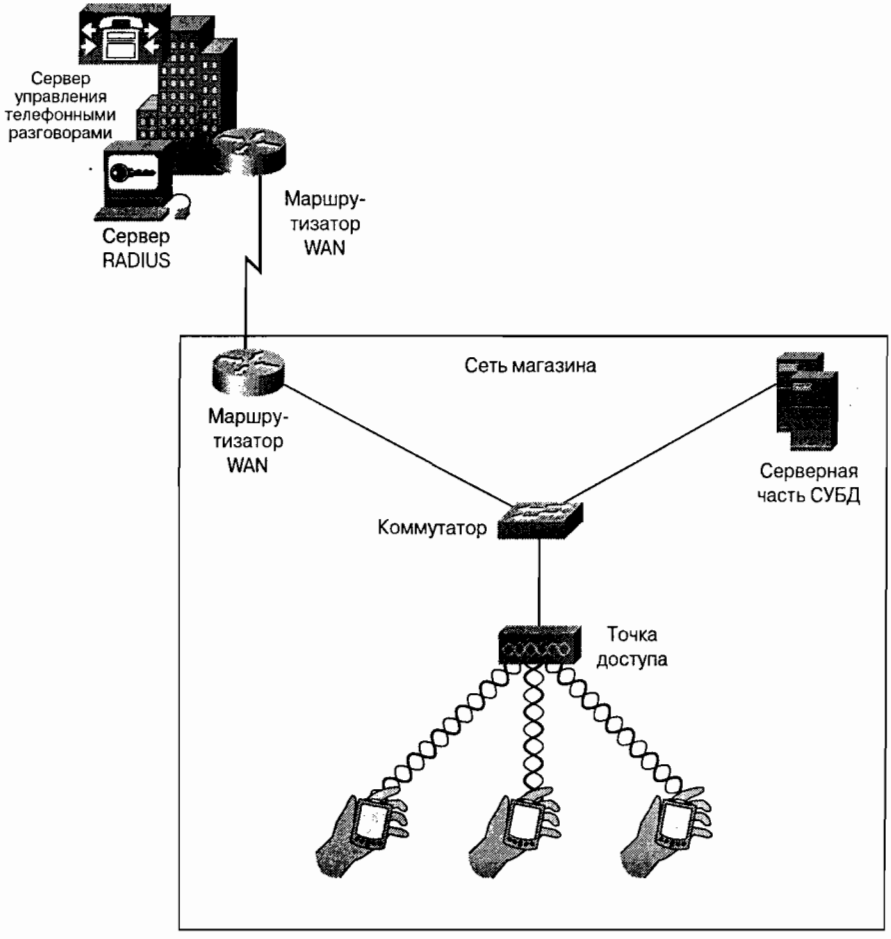


Рис. 10.1. Сеть типичного предприятия розничной торговли

Этот режим позволяет служащему продолжать 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 802.11 рабочей группы I IEEE и спецификация на возможность взаимодействия сетей (Wi-Fi Protected Access, WPA) требуют использования сервера аутентификации, авторизации и учета (AAA) для проведения аутентификации, ориентированной на пользователя. 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 централизовать эту 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 инвентарной 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 *безотказной телефонии для удаленной площадки компании Cisco* (Cisco Survivable Remote Site Telephony, SRST). Устройство SRST обычно применяется в маршрутизаторах филиалов и контролирует трафик служебных сигналов 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 защищенную аутентификацию даже в том случае, если соединение с центральным AAA-сервером неработоспособно. Эти решения обеспечивают максимальную готовность WLAN выполнять свои функции и необходимые пользователям приложения при минимизации влияния на работоспособность сети каналов WAN и расходов на них. На рис. 10.2 показана сеть магазина розничной торговли, усиленная функциями повышения ее живучести.

Масштабирование систем управления сетями для адекватного обслуживания большого количества развернутых точек доступа — давняя и все еще нерешенная проблема для WLAN. Широко распространенные ныне инструменты управления, как правило, разрабатывались для проводных сетей. При широкомасштабном развертывании WLAN на предприятии 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 не могут быть применены по отношению к большинству беспроводных сетей. В результате администраторы сети вынуждены сами создавать инструментарий для эффективного управления сетями магазинов. Многие производители, пользуясь случаем, разрабатывают платформы управления, обеспечивающие возможность масштабирования, и инструментарий, необходимый для управления беспроводными сетями. Этим инструментам недостает интеграции

в платформы управления проводными сетями, необходимой для того, чтобы обеспечить одну точку обзора и управления постоянно изменяющейся сетью. Потребители со стороны розничной торговли в последнее время требуют, чтобы необходимые им инструменты предоставлял их текущий поставщик, иначе они сменят его на другого.

Сфера здравоохранения

Степень использования беспроводных технологий в здравоохранении значительно повысилась в результате распространения устройств стандарта 802.11b и снижения цен на соответствующее этому стандарту 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).

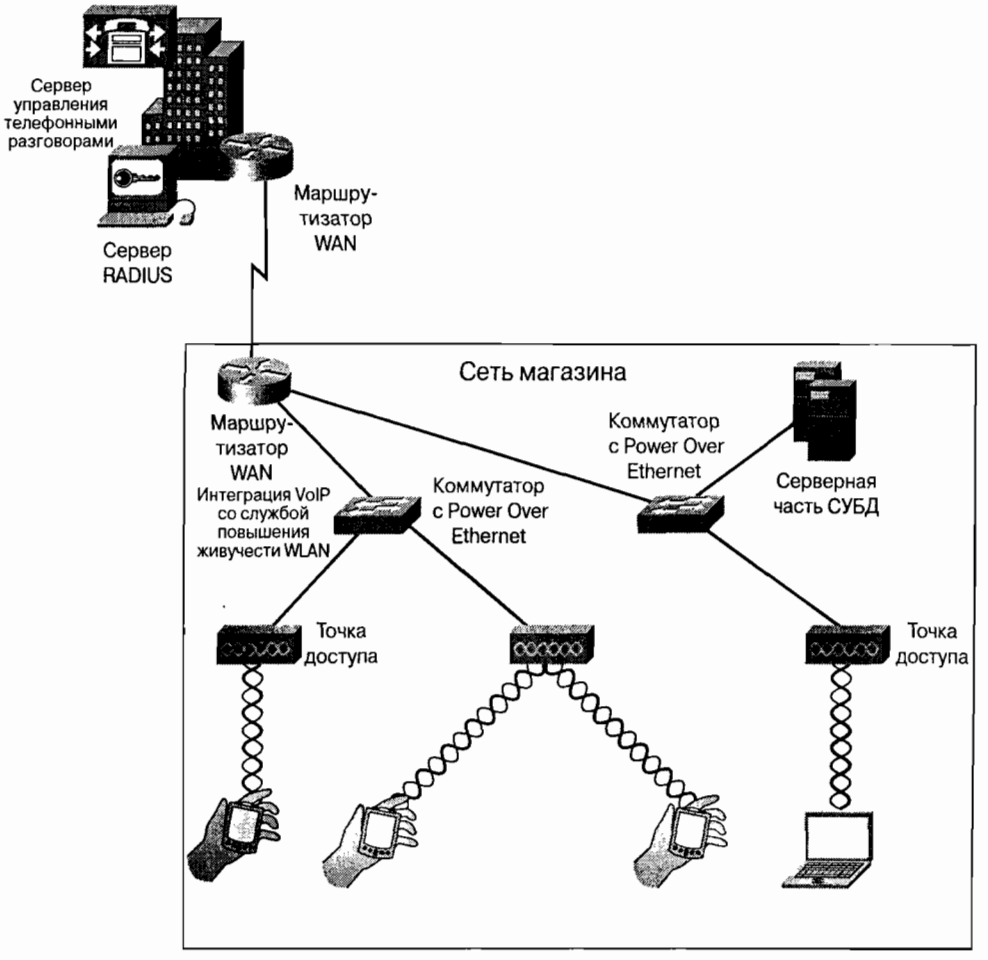


Рис. 10.2. Сеть магазина розничной торговли с механизмами повышения живучести

Многие компании начинают развертывать мобильные приложения на PDA, что позволяет врачам и медсестрам быстро обрабатывать формы требований к страховым 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, в противоположность применению стандартной ненаправленной антенны "волновой канал" на 2,2 dBi.

Многие медицинские учреждения с уже развернутыми сетями сейчас пересматривают отношение к ним, стараясь заставить 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 производительность 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 основано *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 местоположению данные, когда медперсонал будет появляться 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 их популярность, а некоторые их особенности совершенно нехарактерны для сетей крупных предприятий.

Развертывание сетей в филиалах

Как уже говорилось, кризис, поразивший экономику США в конце 2000 года, воздвиг финансовые барьеры на пути развития предприятий. Любые расходы требовали 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 решались. 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 проводятся различного рода реорганизации. Основные затраты при проведении 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 полном 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 сходные 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 хабом 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 ускорения окупаемости инвестиций, сделанных в развертывание WLAN. Помните, что на большинстве предприятий не выполняются ответственные приложения, для которых необходимы WLAN. В таких условиях WLAN полезны тем, что за их счет можно снизить стоимость прокладки кабелей и обеспечить мобильность.

Это — огромное благо для производителей WLAN. Технология WLAN заразительна по своей природе. Многие пользователи "пристрастились" к ее гибкости и обеспечиваемой ею свободе и утверждают, что без этого они теперь не могут эффективно работать. Производители резонно полагают, 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-сервера), надежностью канала WAN и управлением WLAN. Многие из решений, разработанных с целью

удовлетворения потребностей сектора розничной торговли, были применены в офисах предприятий. Важно, однако, отметить, что во многих случаях живучесть WAN обеспечивается за счет его резервирования, а именно за счет резервирования аппаратуры и каналов. В филиалах предприятий обычно используются данные и приложения, размещенные в информационных центрах предприятия на центральном узле. Потеря соединения через WAN-канал может вызвать приостановку выполнения операций на удаленных площадках, из-за чего и делаются инвестиции в повышение надежности WAN.

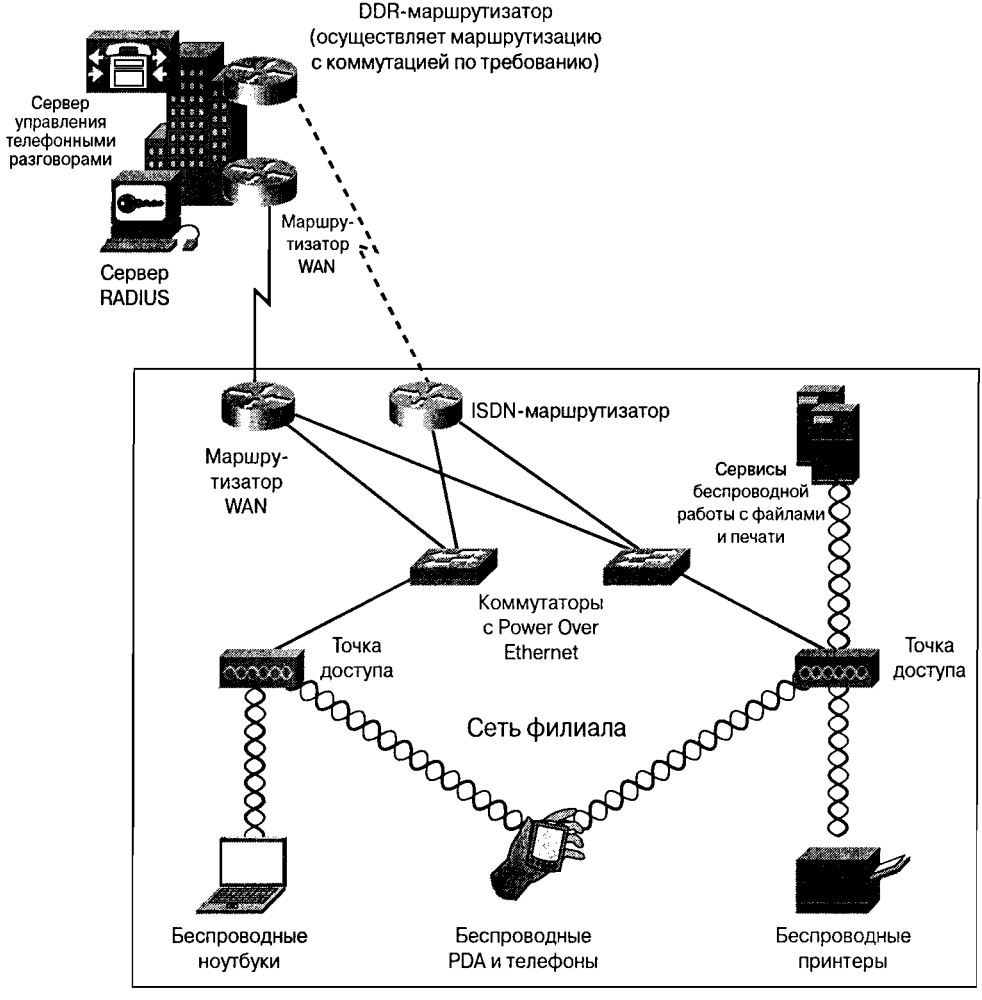


Рис. 10.3. Филиал, оборудованный беспроводной LAN

Надомные работники

Надомные работники предприятий 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 каналов, такие как ISDN, представлявшие собой лишь обеспечивающую высокую пропускную способность надстройки 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.

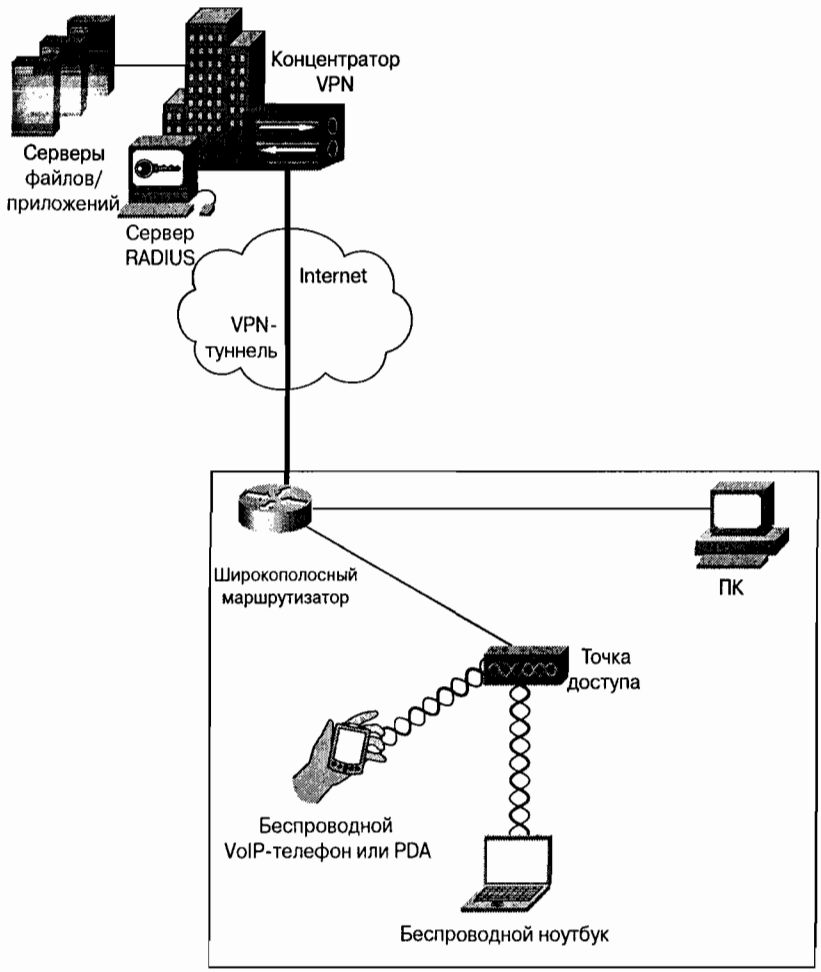


Рис. 10.4. Сеть надомного работника, использующая VPN и высокоскоростное широкополосное Internet-соединение

В некоторых случаях VPN-клиент устанавливается в ноутбуке или ПК пользователя, создавая защищенный туннель от этой машины до концентратора VPN. При такой конфигурации только одно устройство с соответствующим программным обеспечением VPN-клиента имеет доступ к сети предприятия. Можно было бы развернуть такие устройства, как IP-телефоны, в доме служащего. На рис. 10.4 показано, что широкополосный маршрутизатор действует как VPN-клиент и все устройства, расположенные за ним, способны получать доступ к корпоративной сети. Такая конфигурация позволяет администратору сети обеспечивать надомных работников решениями, которые включают все корпоративные объединенные приложения (converged 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, заканчивающийся в конкретной конечной точке, 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 никакой возможности обнаружить такие точки доступа. Рекомендуется, чтобы отделы информационных технологий развертывали на территории корпорации механизмы обнаружения "незаконных" точек доступа и выполняли процедуры "тотального контроля" с целью обнаружения незаконных точек доступа вручную. По отношению к надомным 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 оборудование, которое заранее сконфигурировано и использует центральные AAA-серверы для защищенного доступа. Хотя это и не воспрепятствует подключению пользователями неавторизованных устройств, применение стандарта 802.1X на портах коммутатора на широкополосном маршрутизаторе могло бы удерживать их от поведения такого рода. Следует учесть, что многие пользователи, подключающие незаконные точки доступа к сетям, делают это не по 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 в университетах, так и в учебных заведениях первого-второго уровней, 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 довести сеть

до студентов, вместо того чтобы доставлять студентов к сети. Компьютеры играют все большую роль в учебном процессе; сбережение времени и ресурсов — это главное преимущество, которое дают 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. Сбережение времени и средств, возникающее из-за отсутствия необходимости протягивать провода, часто является компенсацией 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 многих отдельных офисов выступают учебные аудитории. Зачастую зоной обслуживания беспроводной сети должен стать покрытый травой четырехугольный двор, окруженный зданиями и заполненный студентами и кафетериями. Наибольшей проблемой, 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 клиентское оборудование WLAN стоит недорого, используют свои собственные сетевые интерфейсные платы (NIC) беспроводного интерфейса. В учебных заведениях первого-второго уровня нередко случается так, что какая-то группа без ведома группы сетевой инфраструктуры принимает решение по закупке компьютеров. В результате этого создается ситуация, когда студентами используются клиентские устройства с различными (и многочисленными) операционными системами и беспроводными NIC-устройствами, которые должны связываться с общей инфраструктурой.

В то время, когда писались эти строки, одновременное использование устройств многих поставщиков стандарта 802.11b с 40- или 128-разрядным ключом WEP (напомним, WEP — это защищенность, эквивалентная таковой 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. Наибольшей проблемой с этой точки зрения является безопасность, поскольку иногда возникает необходимость ограничить уровень доступа для различных групп пользователей. Например, полный доступ к университетской сети может предоставляться только студентам, преподавателям и персоналу; остальные получают доступ лишь к Internet. Даже среди тех, кто имеет доступ к сети, может осуществляться "разделение на классы", и студенты не получат 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 по-прежнему нерешенной задача поддержки "унаследованных" клиентов, появившихся еще до внедрения WPA. Если инфраструктура ваших точек доступа позволяет использовать 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-

вающими аутентификацию по стандарту 802.11X, будут все же иметь доступ к части сети. Таким образом можно обеспечивать работу устаревших клиентов, не поддерживающих WPA, и операционных систем, не поддерживающих используемый вами механизм аутентификации.

Может также выясниться, что доступ к сети нужно обеспечить во временных учебных аудиториях или в удаленных точках. Вместо того чтобы прокладывать кабель или арендовать линии связи, ведущие к этим точкам, зачастую быстрее и проще можно развернуть беспроводные мосты, чтобы соединить удаленную сеть с сетью учебного заведения (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 публике. Желание обеспечить сервис такого рода растет в отелях, кафе, аэропортах и других местах, где собираются люди. Поскольку, как правило, такие фирмы не собираются предоставлять доступ бесплатно, многие из разработок, обеспечивающих доступ в общественных местах, относились к механизму аутентификации, который должен работать совместно с системой выписки счетов. Что касается разработок, ведущихся в Европе, то применение схем аутентификации, основанных на применении смарт-карт с модулем идентификации подписчика (Subscriber Identity Module, SIM), оказалось ключевым решением, поскольку может быть легко осуществлена интеграция с существующими системами выписки счетов 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 *роуминга*. Под роумингом в данном случае понимается возможность использования услуг многих провайдеров при заключении договора только с одним из них. В то время, когда писались эти строки, в большинстве случаев перемещения беспроводного устройства в другую зону обслуживания приходилось приобретать эфирное время у поставщика, обеспечивающего этот сервис, хотя гораздо удобнее было бы, если бы плата за услугу вносилась в домашний счет. WECA сформировала комитет Internet-провайдеров по беспроводному роумингу (WISPr). Поскольку не существует набора стандартов, в результате работы комитета, наверное, получится несколько большее, чем просто предложения по наилучшей практике. По мере интеграции систем выписки счетов, основанных на применении SIM-карт, в схемы аутентификации стандарта 802.1X ситуация улучшается, и ожидается, что со временем соглашения относительно роуминга между поставщиками услуг станут реальностью.

На рис. 10.5 представлен пример решения для обеспечения доступа в общественных местах со множеством "горячих" зон доступа (access hot spots), подключенных к одной точке присутствия провайдера Internet (point of presence, POP). Интегрированный шлюз выбора служб (Service Selection Gateway, SSG) открывает экран с основным пользовательским интерфейсом, управляет процессом аутентификации и затем направляет трафик (и управляет им), основанный на оплаченных профиле и сервисах. 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 роуминга, 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, предлагающий сервис доступа в общественных местах, использует 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.

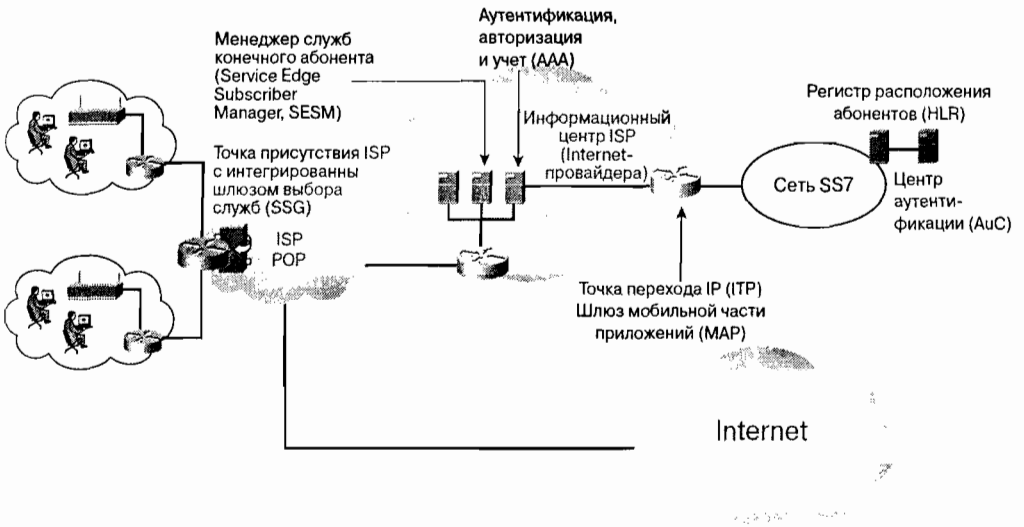


Рис. 10.5. Образец архитектуры, обеспечивающей доступ в местах общественного пользования

Сфера общественной безопасности

Органы государственной безопасности используют технологию мобильных радиостанций уже более 70 лет. Однако чаще всего это всего лишь служба низкоскоростной 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 пилотной программы в сфере общественной безопасности офицерам полиции были выданы PDA с беспроводными источниками сигналов стандарта 802.11, поступающих с беспроводных камер, установленных в автомобилях, патрулирующих криминогенные зоны, а 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 формировались как перекрывающие зоны покрытия для лицензируемых решений с меньшей скоростью передачи. На рис. 10.6 показан пример с зоной обслуживания устройствами стандарта 802.11 в центральном деловом районе города и областью покрытия низко-

скоростными мобильными радиостанциями в остальной части региона. В сельскохозяйственных районах, при кооперативном использовании спектра частот, более приемлемым может оказаться расширение зоны покрытия службами общественной безопасности, деловыми кругами и провайдерами, обеспечивающими доступ в местах общественного пользования за счет виртуальных LAN. В зависимости от того, необходимо ли соединить мостом мобильные сети или просто предоставить клиентский доступ, можно использовать или беспроводные мосты, или точки доступа. Очевидно, главным является то, что будут использованы адекватные меры в виде аутентификации и шифрования для защиты информации, касающейся общественной безопасности, или в виде механизмов защиты последних модификаций стандарта 802.11, или механизмов VPN.

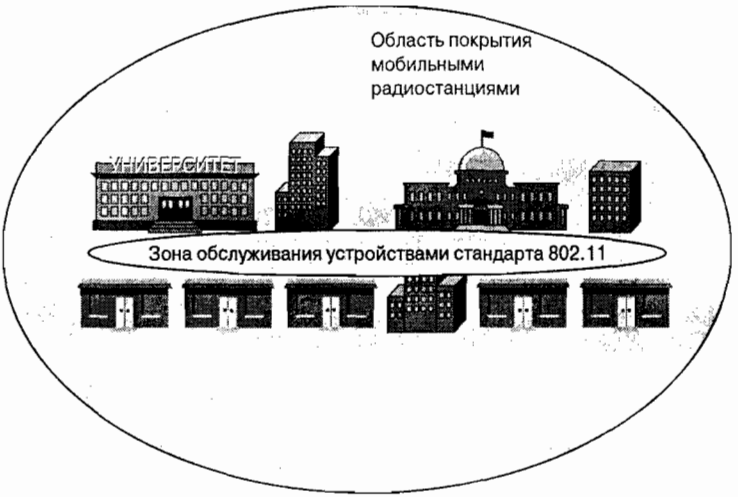


Рис. 10.6. Область покрытия для устройств стандарта 802.11 в сфере общественной безопасности

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).

Короче говоря, устройства стандарта 802.11 могут служить дополнением 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 рассказывалось о применении WLAN в таких различных сферах, как здравоохранение, образование и общественная безопасность. Беспроводные LAN делают доступными пользователю эффективные и новейшие приложения, которые раньше

он выполнять не мог. В данной главе обрисованы 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.

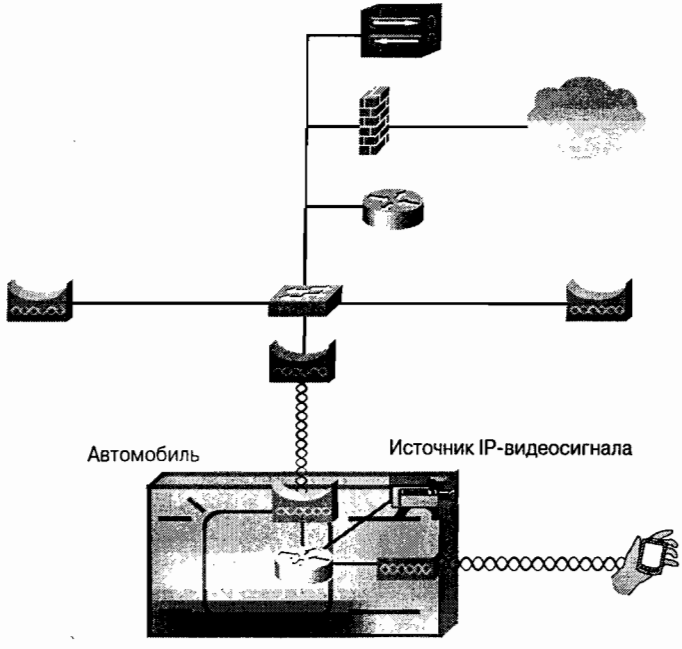


Рис. 10.7. Пример сети в сфере общественной безопасности

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 многомодового волокна. Каждый канал 10BASE-FL может иметь длину до 2 км.

10BASE-T. Разновидность Ethernet, в которой используются кабели категорий 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 1000BASE-CX может иметь длину не более 25 м.

100BASE-FX. Разновидность Fast Ethernet, в которой используется кабель на основе многомодового оптического волокна. Сегмент100BASE-FX может иметь длину до 400 м при работе в полудуплексном режиме и до 2 км — в полнодуплексном.

100BASE-LX. Разновидность Gigabit Ethernet, в которой применяется оптический кабель, выполненный на основе одномодового волокна. Каждый сегмент 1000BASE-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 сети стандарта 802.11 с защитой на канальном уровне.

802.11e. Стандарт IEEE на сети 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 многомодовых волокон. Каждый сегмент 1000BASE-SX может иметь максимальную длину 220 м.

1000BASE-T. Разновидность Gigabit Ethernet, в которой используется кабель категории 5, выполненный на основе неэкранированных 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, посылает пославшей его станции подтверждение этого факта.

Active scanning (активное сканирование). Клиент активно ищет точку доступа (AP). Этот процесс обычно включает отправку клиентом зондирующего запроса по каждому из сконфигурированных на нем каналов и ожидание ответов на зондирующий запрос от точек доступа.

AES (Advanced Encryption Standard, усовершенствованный стандарт шифрования). Новейший стандарт на алгоритм шифрования, предложенный Национальным институтом стандартов и технологий (NIST). AES основан на алгоритме шифрования Рийндэла (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.

B

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 небольшой радиус действия.

Block cipher (блочный шифр). Шифр, который геенерирует ключевой поток (key stream) 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 коллизионных 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.

C

CCK (complementary code keying, последовательность дополнительных кодов). Метод расширения физического уровня, используемый в устройствах стандарта 802.11b для достижения скоростей 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 коллизионном домене.

Collision domain (коллизионный 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 центральный уровень сети. Задача 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 расширенного распределенного управления входом, при использовании которого станции определяют, должны ли они осуществлять передачу, основываясь на объявлениях, передаваемых точкой доступа.

Data link layer (канальный уровень). Второй уровень модели взаимодействия открытых систем (OSI). Состоит из двух поуровней: подуровня канального уровня (data link sublayer) и подуровня логического канала (logical link sublayer).

Data link sublayer (подуровень канального уровня, назвается также MAC-уровень). 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, прошедшего после того, как среда становится доступной, в течение которого станция должна ожидать, прежде чем начнет 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 широковещательные домены уровня 2 с помощью маршрутизаторов или коммутоторов 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 станций 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 подключенными к сети устройствами (*см.* full duplex) или невозможность делать это (*см.* half duplex).

E

EAP (Extensible Authentication Protocol, расширяемый протокол аутентификации). Протокол соединения "точка–точка" (PPP), лежащий в основе механизма аутентификации.

EAP-MD5 (Message Digest 5, дайджест 5 EAP-сообщений). 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 незашифрованного 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, излучаемая 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 порт проводной Ethernet в точке доступа.

Ethernet. Стандарт IEEE 802.3, регламентирующий работу проводной сети со скростью передачи 10 Мбит/с. Другими высокоскоростными вариантами Ethernet являются Fast Ethernet и Gigabit Ethernet.

Ethernet slot time (канальный интервал Ethernet). Время, которое необходимо фрейму Ethernet для преодоления диаметра сети.

Ethertype (тип фрейма Ethernet). Данные, содержащиеся в поле полезной нагрузки MAC-фрейма.

F

FA (foreign agent, внешний агент). Агент на маршрутизаторах или коммутаторах уровня 3, который помогает MN в определении, куда он переместился, и в получении пакетов от внутреннего агента (HA).

Fading (фединг, замирание сигнала). Происходит, 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. Приемная 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 скачкообразного 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.

G

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 многоадресатных 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 многоадресатных фреймов. GTK выводится из группового мастер-ключа (GMK).

H

HA (home agent, внутренний агент). Агент на маршрутизаторах или коммутаторах уровня 3, обеспечивающий получение перемешающимся MN его IP-пакетов.

Half duplex (полудуплексный). Топология сети, при которой станции в каждый из моментов времени могут или передавть, или принимать данные.

HCF (hybrid coordination function, гибридная функция координации). Опциональный механизм доступа к среде по результатам опроса (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 полудуплексного 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). Группа станций стандарта 802.11, напрямую связывающихся между собой. IBSS также называют специальной, или неплановой (ad hoc), сетью, 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.

IRDP (Internet router discovery 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 до 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 стандартным для всех разновидностей сетей семейства 802, этот подуровень содержит простой протокол передачи фреймов, который обеспечивает доставку фреймов без установления соединений.

M

MIC (message integrity check, контроль целостности сообщения). Гарантирует получателю фрейма, что фрейм направлен именно получателем (а не злоумышленником) и не был подменен во время 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 (многоадресатный 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 аутентификации). Аутентификация, в процессе которой не только сеть аутентифицирует клиента, но и клиент аутентифицирует сеть. Проведения именно такой аутентификации требует стандарт 802.11i.

N

NAV (network allocation vector, вектор распределения сети). Виртуальная функция опроса несущей станций (virtual carrier-sense function) стандарта 802.11. NAV — это таймер, имеющийся на каждой станции, значение которого обновляется фреймами данных, передаваемыми через среду. Станция, желающая начать передачу, должна иметь NAV, равный 0, прежде чем она начнет выполнение DCF-операции.

Network diameter (диаметр сети). Расстояние между Ethernet-станциями, находящимися на противоположных концах широковещательного домена.

Nonce (от number once, временное число). Число, которое используется только один раз, в основном в криптографии, например при аутентификации и шифровании.

O

OFDM (orthogonal frequency-division multiplexing, мультиплексирование с разделением по ортогональным частотам). Метод модуляции, используемый для обеспечения очень высоких скоростей 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.

P

Passive scanning (пассивное сканирование). Сканирование, при котором клиент не передает никакие фреймы, а лишь получает сигнальный фреймы по каждому каналу. Клиент продолжает переходить с канала на канал через определенный промежуток времени, но не посылает зондирующие запросы.

PBCC (packet binary convolutional coding, двоичное пакетное сверточное 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 осуществляется аутентификация по стандарту 802.1X другого типа, такая как EAP-MD5.

PIFS (PCF interframe space, преимущественный межфреймовый интервал). Промежуток времени между моментом, 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 волн 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 (домен 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 типа оклик/оклик-отзыв, 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 выжидает, прежде чем пытается 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 диапазона. 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 приведения в соответствие размера незашифрованного текста или незашифрованного фрейма данных.

Supplicant (проситель). 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 коллизионными 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 ICV стандарта 802.11.

Token Ring. Топология типа "кольцо" с предопределенным, 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 обеспечивать 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 (одноадресатный 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 отражений, возникающих при рассогласовании импедансов линий передачи.

W

WEP (wired equivalent privacy, защищенность, эквивалентная таковой проводных сетей). Алгоритм шифрования уровня 2, основанный на алгоритме RC4, обеспечивающий защиту данных в сетях стандарта 802.11.

Предметный указатель

C

D

K

L

M

N

O

P

Q

R

S

T

U

V

W

А

Б

В

Г

Д

З

И

К

Л

М

Н

О

П

P

C

T

У

Ф

Ц

Ч

Ш

Э

Научно-популярное издание

Педжман Рошан, Джонатан Лиэри

Основы построения беспроводных локальных сетей стандарта 802.11

Литературный редактор *И.А. Попова*
Верстка *О.В. Линник*
Художественные редакторы *В.Г. Павлютин, Т.А. Тараброва*
Корректоры *З.В. Александрова, Л.А. Гордиенко*

Издательский дом "Вильямс".
101509, Москва, ул. Лесная, д. 43, стр. 1.
Изд. лиц. ЛР № 090230 от 23.06.99
Госкомитета РФ по печати.

Подписано в печать 14.09.2004. Формат 70×100/16.
Гарнитура Times. Печать офсетная.
Усл. печ. л. 24,51. Уч.-изд. л. 20,9.
Тираж 3000 экз. Заказ № 555.

Отпечатано с диапозитивов в ФГУП "Печатный двор"
Министерства РФ по делам печати,
телерадиовещания и средств массовых коммуникаций.
197110, Санкт-Петербург, Чкаловский пр., 15.

ВИЛЬЯМС

CISCO SYSTEMS

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 радиотракту 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
- Особенности, 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 высокие скорости передачи

По мере повышения скорости передачи данных в беспроводных ЛВС (WLAN) и снижения их стоимости преимущества новой технологии становятся все более ощутимыми. Потребителям больше нет нужды располагать свои рабочие места только там, где есть кабели Ethernet, а развитие их бизнеса не сдерживается какими-либо физическими ограничениями. За счет применения WLAN можно резко увеличить производительность труда сотрудников и сэкономить значительные средства при развертывании сети, охватывающей несколько зданий. Однако, по мере того как все больше и больше компаний, оценив преимущества WLAN, приступают к их развертыванию, возникает все больше вопросов относительно того, как нужно проектировать, развертывать сети стандарта 802.11 и работать с ними. Беспроводные ЛВС предоставляют администраторам сетей, привыкшим иметь дело с проводными технологиями, уникальные возможности. Однако им приходится разбираться во множестве новых для себя вопросов. Это и стандарты беспроводных сетей, и концепции мобильности, и основы радиотехники, и проблемы безопасности, и вопросы обеспечения качества обслуживания, а также проектирования сетей и картирования места их развертывания.

Книга *Основы построения беспроводных локальных сетей стандарта 802.11* дает читателю начальные знания, необходимые для выбора, разработки, развертывания и эксплуатации беспроводной ЛВС, а также предоставляет множество практических сведений. Начинается она с обзора технологий Ethernet, стандартов серии 802.11 и технологий физического уровня (эти сведения необходимы читателю для того, чтобы быстро разобраться в других материалах книги). В последующих главах рассматриваются проблемы и решения, связанные с безопасностью, мобильностью и качеством обслуживания. Даны основные сведения о радиотракте и описаны методики картирования места развертывания сети. Рассмотрен ряд конкретных случаев применения беспроводных ЛВС в различных отраслях, благодаря чему концепции, описанные в книге, наполняются реальным содержанием. Независимо от того, нужен ли вам учебник по основам работы беспроводных ЛВС или практическое руководство по их разработке и использованию, в книге *Основы построения беспроводных локальных сетей стандарта 802.11* вы найдете множество практических советов, которые дают авторы, имеющие большой опыт проектирования сетей; это поможет вам быстро развернуть WLAN и эффективно управлять ею.

"Эта книга поможет вам разобраться в основах построения сетей Wi-Fi и подготовит вас к грядущим переменам".

– Денис Итон, председатель Wi-Fi Alliance

Педжман Рошан — менеджер линейки продуктов 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.

Джонатан Лиэри — менеджер линейки продуктов подразделения беспроводных сетей корпорации Cisco Systems. Джонатан занимается в основном использованием технологии WLAN вне помещений

*Эта книга является частью серии **Networking Technologies Series**, которая ориентирована на профессионалов по работе с сетями и содержит ценную информацию по созданию многофункциональных сетей, а также поможет понять новейшие технологии и ускорить карьерный рост.*

ISBN 5-8459-0701-2

Категория:
Cisco Press — беспроводные сети

Предмет рассмотрения:
Беспроводные ЛВС стандарта 802.11

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