**Протокол 802.11. MAC**

После того как базовая станция ассоциирована с точкой доступа, она может наладить отправку и прием кадров данных базовой станции. Одна­ко, так как несколько станций могут одновременно попытаться отправить кадры данных по одному каналу, чтобы упорядочить передачу данных, по­требуется использование протокола множественного доступа. В данном контексте под **станцией** понимается либо беспроводная станция, либо точка доступа. Как мы уже обсуждали ранее, если говорить в общем, то существует три класса протоколов множественно­го доступа, предполагающие либо разделение каналов связи (в том числе, CDMA), произвольный доступ, либо очередность. Вдохновленные огром­ным успехом технологии Ethernet, использующей протокол произвольно­го доступа, разработчики технологии 802.11 решили также использовать протокол произвольного доступа для беспроводных локальных сетей 802.11. Протокол произвольного доступа часто называют **CSMA с исклю­чением столкновений,** или более кратко, **CSMA/CA.** Как и в случае с про­токолом CSMA/CD, использующемся в технологии Ethernet, аббревиату­ра CSMA расшифровывается как «carrier sense multiple access», по-русски это звучит как «множественный доступ с контролем несущей» — то есть каждая станция анализирует состояние канала перед началом передачи данных, если канал занят, то станция воздерживается от передачи данных. Несмотря на то, что в обеих технологиях, Ethernet и 802.11, используется произвольный доступ с контролем несущей, у двух протоколов MAC есть существенные различия.

Во-первых, вместо обнаружения столкновений (collision detection), в технологии 802.11 применяется исключение столкновений (collision avoidance). Во-вторых, из-за относительно большего количества битовых ошибок в беспроводных каналах связи, в технологии 802.11 (в отличие от Ethernet) используется схема подтверждения/повторной передачи (ARQ) канального уровня. Далее мы опишем исключение столкнове­ний и схемы подтверждения канального уровня технологии 802.11.

Давайте вспомним из разделов 5.3.2 и 5.4.2, что при использовании технологии Ethernet и алгоритма обнаружения столкновений станция Ethernet анализирует параметры передачи канала связи. Если в ходе передачи данных такая станция обнаружит, что в тот же самый момент другая станция отправляет данные, то наша станция прервет передачу и попробует произвести ее вновь через некоторый случайный проме­жуток времени. В отличие от протокола Ethernet 802.3, протокол MAC 802.11 *не* использует алгоритмы обнаружения столкновений. И на это есть две важные причины:

• Способность обнаруживать столкновения требует возможности од­новременно посылать (собственные сигналы станции) и принимать (с целью определения того, передает ли другая станция сигналы). Так как принимаемый сигнал, как правило, значительно слабее пе­редаваемого, создание аппаратного обеспечения, которое могло бы обнаруживать столкновения, слишком затратно.

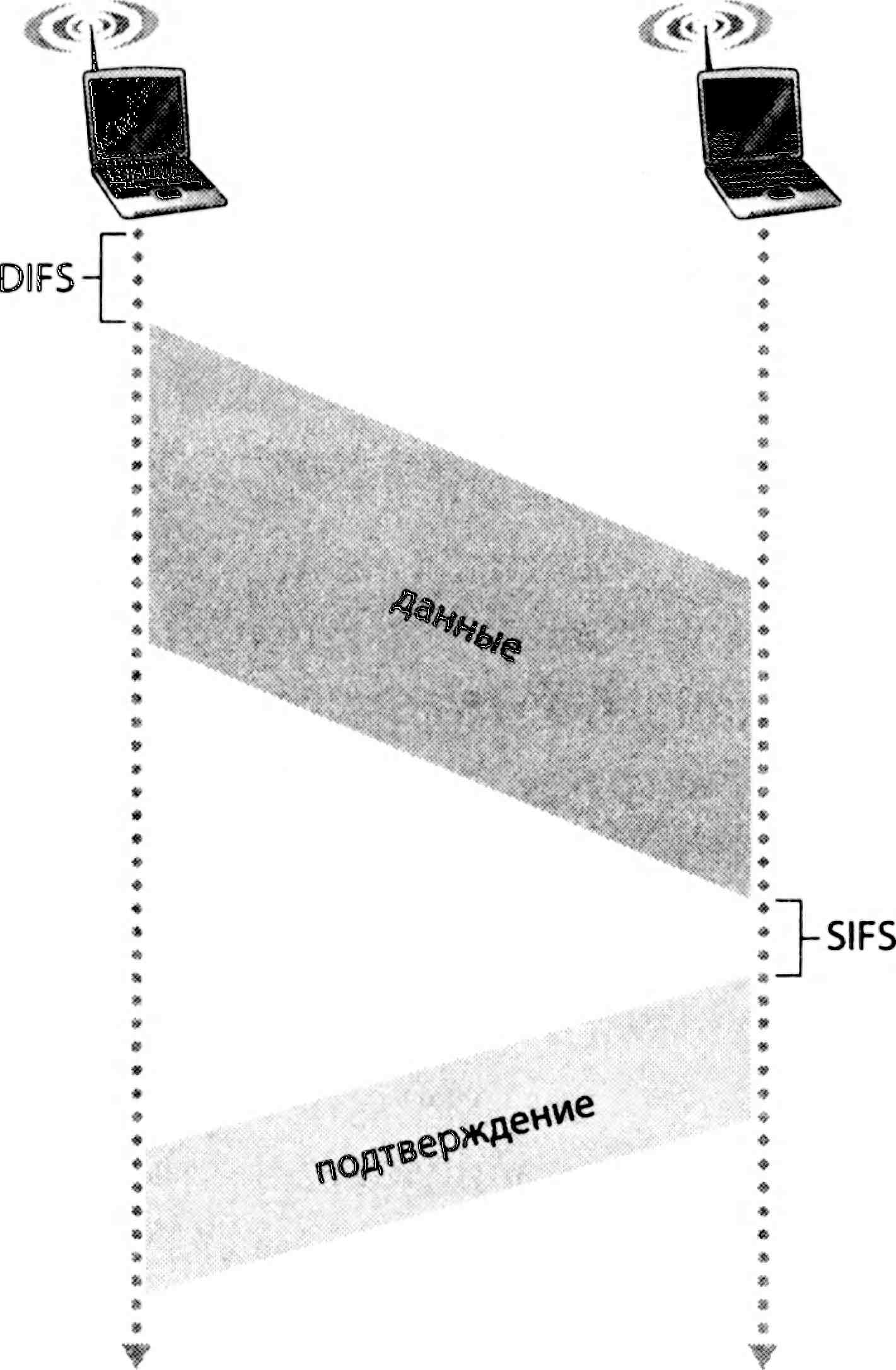
• Однако более важным является то, что даже если бы адаптер мог одно­временно передавать сигналы и прослушивать канал связи (и, соот­ветственно, отменять передачу данных, если прослушиваемый канал оказывался бы занятым), то такой адаптер все равно не смог бы обнару­жить все столкновения из-за проблемы скрытых передатчиков данных и эффекта ослабления сигнала, которые мы обсуждали ранее.

Так как в беспроводных локальных сетях 802.11 не используется технология обнаружения столкновений, станция всегда *передает кадр данных полностью.* Иными словами, после запуска станции обратно­го пути уже нет. Как многие могут подумать, передача кадров данных целиком (в особенности, длинных кадров) при большой вероятности возникновения столкновений может значительно ухудшить производи­тельность протокола множественного доступа. Для уменьшения вероят­ности столкновения, в сетях 802.11 используется несколько технологий, которые мы обсудим в ближайшее время.

Однако прежде чем обсуждать избежание столкновений, мы изучим **схему подтверждения канального уровня** сетей 802.11. Давайте вспом­ним, что, когда станция, подключенная к бес­проводной локальной сети, посылает кадр данных, этот кадр может не достичь места назначения по нескольким причинам. Для того чтобы справиться с неуменьшащейся вероятностью неудачной отправки кадра данных, протокол MAC 802.11 использует подтверждение канального уровня. Как показано на рис. 6.10, когда станция назначения принима­ет сигнал, проходящий контроль с использованием кода циклического контроля (CRC), она ожидает небольшой период времени, известный как **короткий межкадровый промежуток** (Short Inter-Frame Spacing, **SIFS),** после чего посылает обратно кадр данных с подтверждением. Если передающая станция не получает подтверждение в течение опре­деленного времени, делается предположение, что произошла какая-то ошибка, и станция повторно посылает кадр данных, используя для до­ступа к каналу связи протокол CSMA/CA. Если после нескольких по­пыток повторной отправки данных станция не получает подтверждения, то попытки прекращаются и кадр данных уничтожается.

Обсудив, как в сетях 802.11 используется подтверждение канально­го уровня, мы теперь готовы к описанию протокола 802.11 CSMA/CA. Предположим, что станции (беспроводной станции или точке доступа) требуется передать кадр данных.

Отправитель Получатель



**Рис. 6.10.** Использование подтверждения канального уровня в сетях 802.11

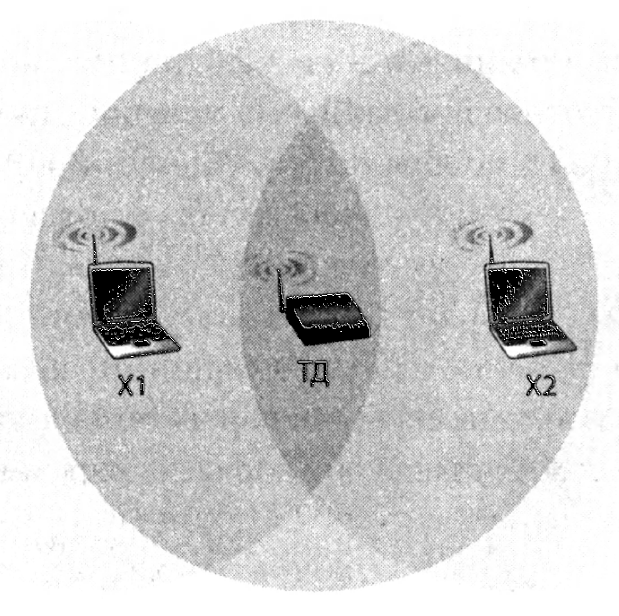
1. Если в результате первоначального прослушивания канала станция определит, что он является свободным, то отправка кадра данных осуществляется через короткий промежуток времени, известный как **распределенный межкадровый промежуток** (Distributed Inter-frame Space, **DIFS).**
2. В противном случае станция случайным образом устанавливает вре­менной интервал для отсрочки передачи кадра данных, используя бинарный экспоненциальный алгоритм, и начинает отсчитывать полученное значение, когда канал определяется свободным. Пока канал остается занятым, отсчет не ведется.
3. Когда отсчет достигает нуля (обратите внимание, что это может случиться, только если канал будет определяться как свободный), станция передает кадр данных целиком — и переходит в режим ожи­дания подтверждения.

4. Если подтверждение получено, то передающая станция «знает», что переданный ею кадр данных был корректно получен станцией-получателем. Если нужно послать еще один кадр данных, то его от­правка осуществляется при помощи протокола CSMA/CA, начиная с шага 2. Если подтверждение получено не было, то станция возвра­щается в режим отсрочки передачи данных (шаг 2) и вновь выбира­ет случайное значение временного промежутка, но уже из большего интервала.

Вспомним, что при использовании протокола множественного до­ступа CSMA/CD технологии Ethernet станция начинает передачу сигнала, как только канал будет найден свободным. Однако при использовании протокола CSMA/CA станция воздерживается от отправки данных, пока таймер отсчета не достигнет нуля, даже если ка­нал был определен как свободный. Почему в данном случае в протоко­лах CSMA/CD и CMSA/CA используются такие разные подходы?

Для того чтобы ответить на данный вопрос, давайте представим си­туацию, когда две станции должны передать кадр данных, но ни одна не приступает к передаче, так как они определяют, что ее уже осуществляет третья станция. При использовании протокола CSMA/CD технологии Ethernet обе станции начали бы передачу данных сразу же после того, как обнаружили бы, что третья ее завершила. Это привело бы к столк­новению, что для протокола CSMA/CD не является серьезной пробле­мой, так как обе станции во избежание бесполезных усилий по передаче остатков кадров данных тут же прервали бы отправку. Однако в случае с сетями 802.11 ситуация несколько отличается. Так как технология 802.11 не предполагает обнаружение столкновений и прекращение от­правки данных, кадр данных, пострадавший от столкновения, переда­ется полностью. Поэтому целью технологии 802.11 является избежание столкновений во всех случаях, когда это является возможным. Если обе станции, работающие в сети 802.11, обнаруживают, что канал свя­зи занят, они входят в режим отсрочки отправки данных, выбирая при этом в идеале разные значения временного интервала. Если значения на самом деле различаются, то одна из станций начнет передачу дан­ных в освободившийся канал раньше другой. Кроме того, если станции не скрыты друг от друга, то «проигравшая» поймает сигнал «станции-победительницы», заморозит счетчик и будет воздерживаться от пере­дачи данных до тех пор, пока ее не завершит станция-победительница. Таким образом удается избежать дорогостоящих столкновений. Однако столкновения в сетях 802.11 все же иногда происходят. Так, две станции могут быть скрыты друг от друга, либо обе станции могут выбрать слу­чайные значения временного интервала отправки данных, которые на­ходятся слишком близко, и сигнал первой станции не успевает достичь места назначения. Вспомните, что ранее, при обсуждении алгоритмов случайного доступа, мы уже сталкивались с этой проблемой в контексте рис. 5.12.

**Работа со скрытыми передатчиками: RTS и CTS**

Протокол MAC сетей 802.11 также включает изящную (хотя и необя­зательную) схему резервирования, позволяющую избежать столкнове­ний даже при наличии в сети скрытых передатчиков. Давайте исследуем эту схему в контексте рис. 6.11, изображающего две беспроводные стан­ции и одну точку доступа. Обе беспроводные станции находятся в зоне покрытия (обозначена на рис. более темным кругом) точки доступа, обе станции также ассоциированы с данной точкой доступа. Однако из-за эффекта ослабления сигнала, территория покрытия беспроводных стан­ций ограничена площадью более светлых кругов на рис. 6.11, вследствие чего обе станции остаются скрытыми друг от друга, несмотря на то, что не скрыты для точки доступа.

**Рис. 6.11. Пример скрытых передатчиков: станция Х1 скрыта отХ2 и наоборот**

Теперь попытаемся понять, почему скрытые передатчики могут пред­ставлять собой проблему. Представьте, что станция X1 передает кадр данных, но в это же самое время станция Х2 также готова начать передачу кадра данных точке доступа ТД. Станция Х2, не улавливая сигналов станции X1, сначала выждет промежуток времени DIFS, а затем начнет передачу кадра данных, что приведет к столкновению. В результате при­менение канала связи окажется бесполезным на протяжении передачи кадров данных, как от станции X1, так и от Х2.

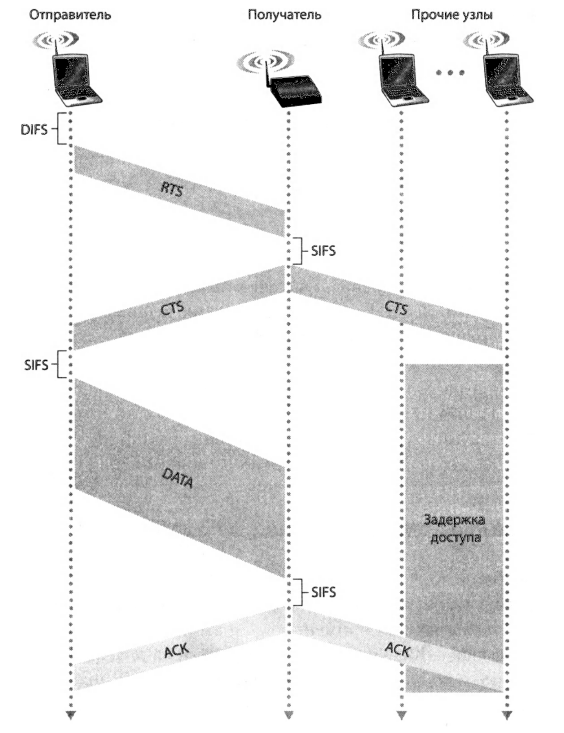
Во избежание возникновения этой проблемы протокол IEEE 802.11 позволяет станциям воспользоваться коротким управляющим кадром **запроса отправки (RTS)** и коротким управляющим кадром **разре­шения на отправку (CTS)** для *резервирования* доступа к каналу свя­зи. Когда передатчик хочет отправить кадр DATA, он сначала должен переслать точке доступа кадр RTS, обозначающий общее количество времени, необходимое для отправки кадра DATA и кадра подтвержде­ния (АСК). Точка доступа, получив кадр RTS, отвечает передачей ка­дра CTS. Кадры CTS имеют две цели: они дают отправителю исклю­чительное разрешение на отправку данных, а также запрещают другим базовым станциям начинать передачу в течение зарезервированного промежутка времени.

Поэтому, как показано на рис. 6.12, перед передачей кадра DATA, станция X1 пересылает кадр RTS, который улавливается всеми станци­ями, находящимися в круге, в том числе точкой доступа ТД. Поле чего точка доступа отвечает отправкой кадра CTS, который также улавлива­ется всеми базовыми станциями, находящимися в зоне покрытия точки доступа, в том числе станциями X1 и Х2. Станция Х2, поймав кадр CTS, воздерживается от отправки данных в течение промежутка времени, указанного в кадре CTS. Кадры RTS, CTS, АСК и DATA изображены на рис. 6.12.

Использование кадров RTS и CTS позволяет улучшить производи­тельность двумя путями:

* Сглаживание проблемы скрытых передатчиков, так как длинные ка­дры DATA передаются только после резервирования канала связи.
* Так как кадры RTS и CTS являются короткими, их столкновение продлится только на протяжении промежутка времени, занимаемо­го этими короткими кадрами. После успешной передачи кадров RTS и CTS проблем с передачей кадров DATA и АСК не возникает.

Мы рекомендуем вам протестировать апплеты на веб-сайтах **tinyurl. com/25nyjp9** и [**tinyurl.com/48mkj**](http://tinyurl.com/48mkj)**.** Эти апплеты иллюстрируют работу протокола CSMA/CA, в том числе порядок обмена кадрами RTS/CTS.

****

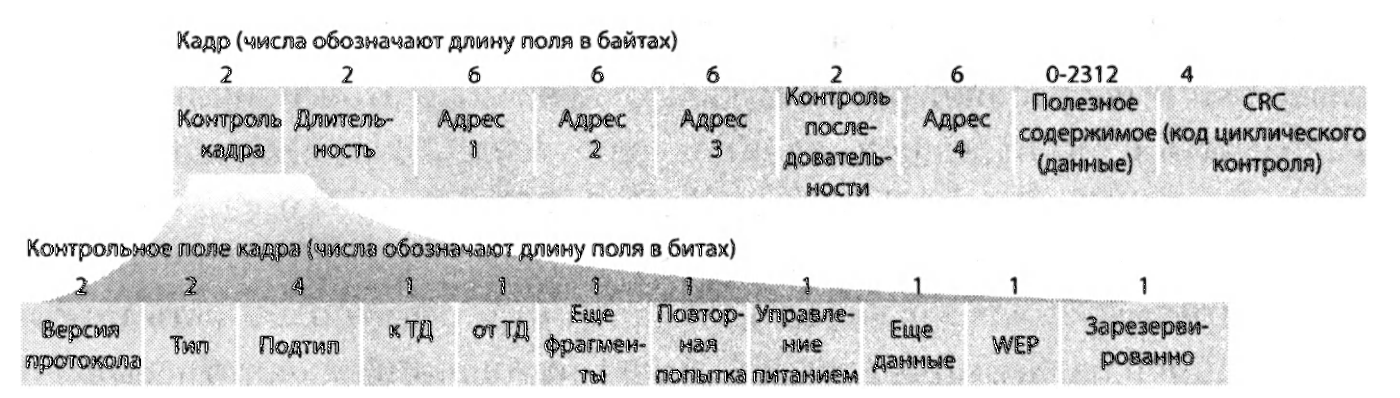
**Рис. 6.12. Избежание столкновений с помощью кадров RTS и CTS**

Несмотря на то что обмен кадрами RTS/CTS позволяет уменьшить количество столкновений, этот обмен также привносит определенные задержки и потребляет ресурсы канала связи. По этой причине обмен кадрами RTS/CTS используется (если используется), только что­бы зарезервировать канал связи для передачи длинного кадра DATA. На практике беспроводные станции часто устанавливают лимиты дли­тельности (пороговые значения) RTS, с тем чтобы использовать техно­логию обмена кадрами RTS/CTS, только если длина кадра превышает установленный лимит. В настройках большого числа беспроводных станций значение RTS по умолчанию превышает максимальную длину кадра, таким образом, обмен кадрами RTS/CTS пропускается для всех отправляемых кадров **DATA.**

**Использование сетей 802.11 для организации двухточечной связи**

До настоящего момента мы сосредоточились на обсуждении исполь­зования сети 802.11 для множественного доступа. Следует отметить, что если два узла оборудованы направленными антеннами, то эти антенны можно использовать для работы с протоколом **802.11** чтобы создать, по сути, двухточечное соединение. Учитывая низкую стоимость аппаратно­го обеспечения сетей 802.11 общего назначения, использование направ­ленных антенн и увеличенная мощность передачи позволяют использо­вать сети 802.11 в качестве недорогого способа обеспечить двухточечное соединение на расстоянии в десятки километров. В работе Раманаописывается такая многопереходная беспроводная сеть, использующая­ся на сельскохозяйственных равнинах бассейна реки Ганг в Индии и со­стоящая из двухточечных соединений по технологии 802.11.

**Кадр IEEE 802.11**

Несмотря на то, что между кадрами сетей **802.11** и Ethernet очень много общего, кадры сетей **802.11** также содержат определенный набор полей, специфичных для применяемых в этой технологии беспровод­ных каналов связи. Кадр сети 802.11 изображен на рис. 6.13. Числа над каждым из полей кадра представляют собой длину этих полей в *байтах,* тогда как числа над каждым подполем контрольного поля кадра пред­ставляют длину соответствующих подполей в *битах.* Давайте теперь перейдем к изучению полей кадра и нескольких наиболее важных под­полей контрольного поля кадра.

**Рис. 6.13. Кадр 802.11**

**Полезное содержимое и код циклического контроля**

Сердцем кадра данных является полезное содержимое, которое, как правило, состоит из дейтаграммы IP или пакета ARP Несмотря на то что максимально допустимая длина поля «Полезное содержимое» со­ставляет 2312 байт, как правило, при передаче дейтаграммы IP или па­кета ARP она не превышает 1500 байт. Как и кадр сетевой технологии Ethernet, кадр сети 802.11 также содержит 32-битный алгоритм провер­ки с использованием кода циклического контроля (CRC), благодаря ко­торому получатель сможет обнаружить битовые ошибки в переданном кадре. Как мы уже убедились, битовые ошибки в беспроводных локаль­ных сетях являются гораздо более частым явлением, чем в проводных сетях, поэтому алгоритм CRC здесь очень полезен.

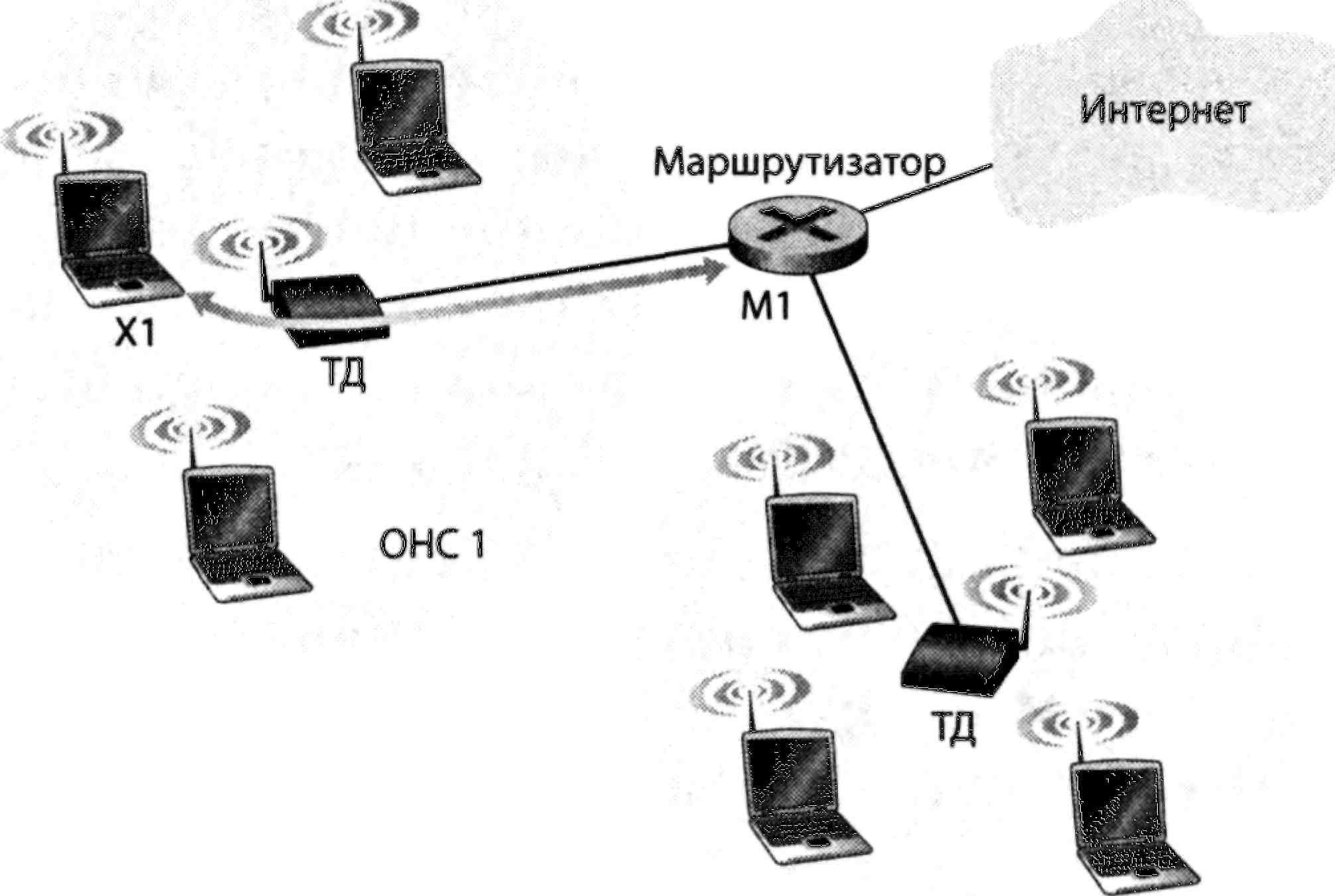
**Поля адреса**

Возможно, самое потрясающее отличие кадра 802.11 заключает­ся в том, что он содержит *четыре* поля адреса, в каждом из которых, в свою очередь, содержатся 6-байтные MAC адреса. Но зачем нужно че­тыре поля адреса? Неужели поля MAC адреса отправителя и поля MAC адреса получателя недостаточно? Ведь при использовании технологии Ethernet этого вполне хватает? Оказывается, что три поля адреса необ­ходимы для целей межсетевой совместимости, а именно для передачи дейтаграммы уровня сети от беспроводной станции через точку доступа на интерфейс маршрутизатора. Четвертое поле необходимо, когда точки доступа пересылают кадры данных в режиме однорангового соединения. Так как мы фокусируем свое внимание только на сетях с инфраструкту­рой, давайте обсудим три первых поля адреса. В стандарте 802.11 они определены следующим образом:

* Адрес 2 — это MAC адрес станции, передающей кадр данных. По­этому, если какая-либо беспроводная станция инициирует переда­чу данных, то ее MAC адрес заносится в поле адреса 2. Аналогично, если точка доступа выступает передатчиком данных, то в поле адре­са 2 записывается MAC адрес этой точки доступа
* Адрес 1 — это MAC адрес станции, которой предназначается переда­ваемый кадр данных. Поэтому, если беспроводная станция передает кадр, то поле адреса 1 будет содержать MAC адрес точки доступа-получателя. Аналогично, если точка доступа выступает передатчи­ком данных, то в поле адреса 1 записывается MAC адрес беспровод­ной станции-получателя.

• Для понимания содержания адреса 3, давайте вспомним такое поня­тие, как основной набор служб (ОНС), состоящий из точек доступа и беспроводных станций и являющийся частью подсети, а также и то, что данная подсеть соединена с другими подсетями посредством не­которого маршрутизатора. В поле адреса 3 содержится MAC адрес этого маршрутизатора.

Чтобы лучше понять, зачем нужно поле адреса 3, давайте изучим пример межсетевого взаимодействия, изображенного на рис. 6.14. На этом рисунке вы можете видеть две точки доступа ТД, каждая из ко­торых отвечает за несколько беспроводных станций. Каждая из точек доступа имеет прямое подключение к маршрутизатору, который, в свою очередь, соединяется с Интернетом. Мы должны понимать, что точка доступа является устройством сетевого уровня, и поэтому не может ни пользоваться IP, ни работать с IP-адресами. Теперь давайте предполо­жим, что нам необходимо переслать дейтаграмму от интерфейса марш­рутизатора Ml к беспроводной станции X1. Маршрутизатору неизвест­но, что между ним и станцией X1 присутствует также Точка доступа ТД. Если смотреть с точки зрения маршрутизатора, X1 — это всего лишь хост в одной из подсетей, подключенный к нему (маршрутизатору).



ОНС 2

**Рис. 6.14. Использование полей адреса в кадрах данных 802.11: пересылка**

**кадров между Х1 и М1**

• Маршрутизатор, которому известен IP-адрес станции X1 (благодаря адресу места назначения дейтаграммы), использует протокол ARP для определения МАС-адреса X1 также, как если бы мы имели дело с обычной локальной сетью Ethernet. После получения МАС-адре­са X1 интерфейс маршрутизатора Ml инкапсулирует дейтаграмму в кадре Ethernet. Поле адреса отправителя данного кадра содержит МАС-адрес интерфейса Ml, а поле адреса получателя — МАС-адрес станции X1.

• Когда кадр данных Ethernet 802.3 поступает на точку доступа ТД, эта точка доступа преобразует его в кадр 802.11 перед передачей по беспроводному каналу связи. Точка доступа заполняет поля адреса 1 и 2 МАС-адресом станции XI и собственным MAC адресом соответственно, как было описано выше. В поле адреса 3 точка доступа записывает адрес интерфейса маршрутизатора Ml. Таким же образом, с помощью поля адреса 3, станция X1 может определить МАС-адрес маршрутизатора, направившего дейтаграмму в подсеть.

Теперь давайте представим, что происходит, когда беспроводная станция X1 отвечает, перемещая дейтаграмму от X1 к интерфейсу Ml.

* Станция X1 создает кадр 802.11, заполняя поля адреса 1 и 2 MAC адресом точки доступа и собственным MAC адресом соответствен­но, как описано выше. В поле адреса 3 записывается адрес интерфей­са маршрутизатора Ml.
* Когда точка доступа получает кадр 802.11, она преобразует его в кадр Ethernet. Поле адреса отправителя содержит MAC адрес станции X1, а поле адреса получателя — MAC адрес интерфейса Ml. Таким обра­зом, поле адреса 3 позволяет точке доступа определить MAC адрес места назначения при создании кадра Ethernet.

В заключение следует сказать, что поле адреса 3 играет очень важ­ную роль в организации межсетевого взаимодействия основного набора служб ОНС и проводной локальной сети.

**Поля порядкового номера, длительности и контроля кадра**

Давайте вспомним, что в случае с технологией 802.11, при успешном получении кадра данных, станция всегда посылает отправителю под­тверждение. Из-за того, что подтверждение способно затеряться, стан­ция может отправить несколько копий кадра подтверждения. Как мы уже наблюдали по ходу обсуждения протокола rdt2.1, использование порядковых номеров позволяет получателю отличить только что переданный кадр данных от повторно отправляемых копий подтверждения. Поле порядкового номера кадра 802.11, таким образом, служит на канальном уровне тем же целям, что на транспортном уровне.

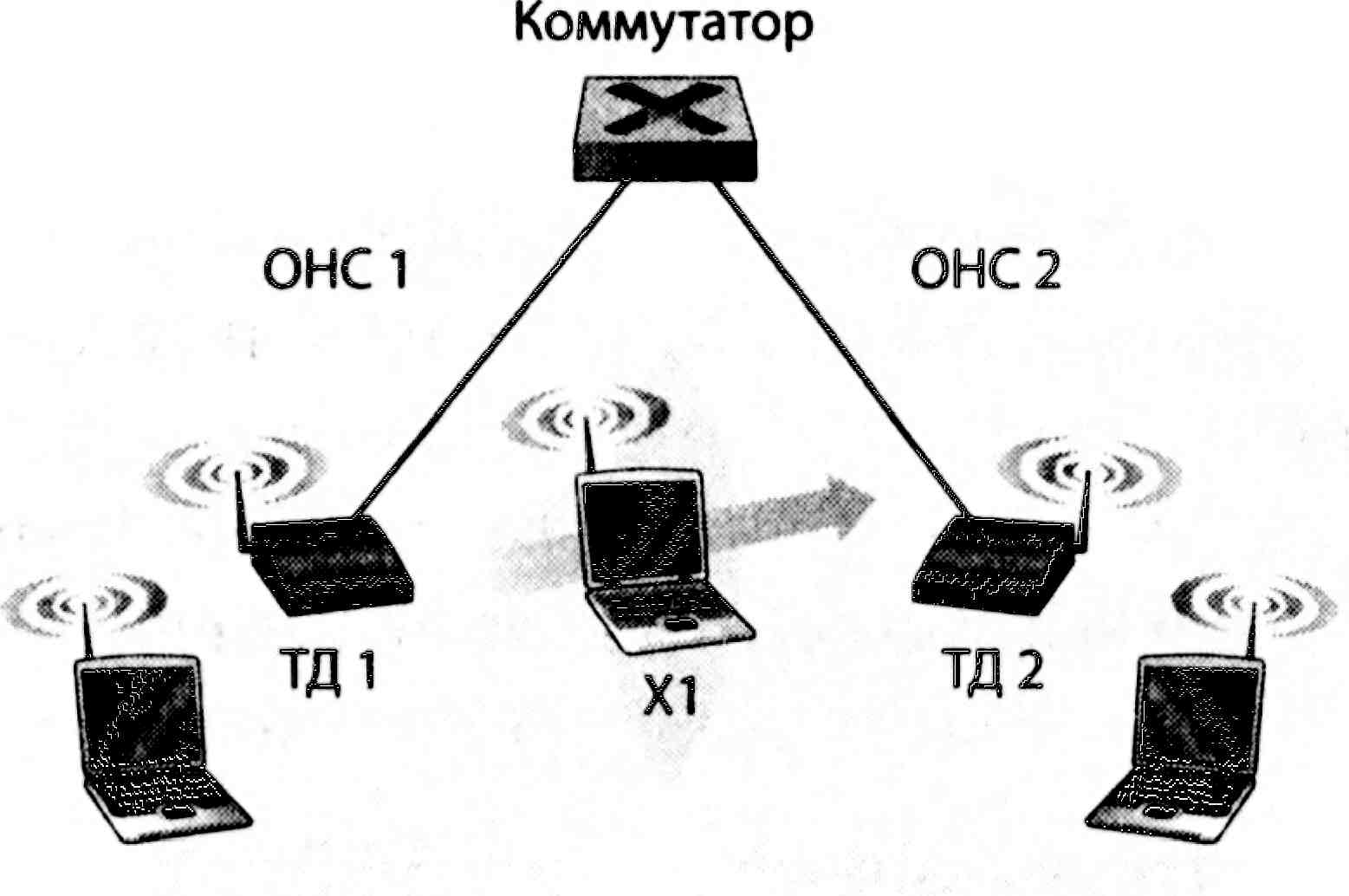
Вспомним также, что протокол 802.11 позволяет передающим стан­циям зарезервировать канал связи на определенный промежуток, вклю­чающий в себя время для передачи кадра данных и время для передачи подтверждения. Значение длительности этого промежутка записывается в соответствующее поле кадра (как данных, так и кадров RTS и CTS).

Как показано на рис. 6.13, поле контроля кадра состоит из большого числа подполей. Мы лишь вкратце обсудим несколько самых важных из них, для получения более подробной информации, мы рекомендуем вам обратиться к спецификации 802.11. Поля *тип* и *подтип* ис­пользуются для различия кадров ассоциации, RTS, CTS, ACK и данных. Поля *к и от* определяют значения различных полей адреса (значения полей изменяются, в зависимости от того, используется ли режим ин­фраструктуры или одноранговой сети, а также в случае с режимом ин­фраструктуры, в зависимости от того, какой элемент сети, беспроводная станция или точка доступа посылает кадр). Наконец, поле WEP служит для указания того, применяется ли шифрование.

**Мобильность в рамках единой IP-подсети**

С целью увеличения физической площади покрытия беспроводной локальной сети, организации и университеты зачастую развертывают несколько основных наборов служб ОНС внутри единой IP-подсети. Из-за чего естественным образом возникает вопрос мобильности между ОНС: каким образом беспроводной станции осуществить переход от одного ОНС к другому, не прекращая текущего сеанса TCP? Как мы увидим в одном из следующих подразделов, вопрос мобильности реша­ется достаточно просто, если ОНС является частью подсети. При пере­мещении станций между подсетями потребуется более сложный прото­кол управления мобильностью.

Сейчас давайте разберем конкретный пример мобильности между ОНС в рамках одной подсети. На рис. 6.15 изображено два соединенных между собой основных набора служб ОНС, а также хост X1, совершаю­щий перемещение от ОНС1 к ОНС2. Так как в данном примере устройство, соединяющее два набора служб, *не является* маршрутизатором, все станции в обоих ОНС принадлежат к единой IP-подсети. Поэтому, когда станция X1 перемещается от ОНС1 к ОНС2, она может сохранять присвоенный ей IP-адрес и, соответственно, все установленные соеди­нения TCP. Если бы соединяющим устройством был маршрутизатор, то станции X1 приходилось бы получать новый IP-адрес всякий раз при перемещении в новую подсеть. Такое изменение адреса нарушит (и, естественно, прекратит) все установленные станцией X1 соединения TCP. Позднее мы увидим, как для избегания подобной проблемы можно воспользоваться протоколом уровня сети, таким как мобильный IP-протокол.



**Рис. 6.15. Мобильность в рамках единой подсети**

Но что же на самом деле происходит, когда станция X1 перемеща­ется от ОНС1 к ОНС2? Как только X1 удаляется от точки доступа ТД1 и определяет ослабление сигнала ТД1, она начинает поиск более силь­ного сигнала. X1 получает сигнальные кадры от ТД2 (которая, в боль­шинстве корпоративных и университетских сетях, будет иметь тот же сетевой идентификатор SSID, что и ТД1). После этого X1 прекращает ассоциацию с ТД1 и ассоциируется с ТД2, при этом сохраняя присвоен­ный ей IP-адрес и установленные подключения TCP.

Вышеописанное позволяет справиться с проблемой перехода, с точ­ки зрения как хоста, так и точки доступа. Но что насчет коммутатора на рис. 6.15? Каким образом он «узнает», что хост переместился от одной точки доступа к другой? Как вы наверняка помните, комму­таторы обладают способностью к самообучению — и самостоятельно­го создания таблиц переадресации. Функция самообучения позволяет справляться со случайными перемещениями (например, если какого-либо работника переводят из одного отдела в другой). Однако коммута­торы не создавались для поддержки высокомобильных пользователей, желающих сохранять подключения TCP, перемещаясь между основны­ми наборами служб ОНС. Для решения этой задачи вспомним, что перед осуществлением перемещения в таблице переадресации коммутатора есть запись, позволяющая соотнести МАС-адрес станции X1 с исходя­щим интерфейсом коммутатора, с помощью которого можно получить доступ к X1. Если станция X1 изначально находилась в ОНС1, то дейта­грамма, предназначенная этой станции, будет направлена ей через точку доступа ТД1. Однако как только станция X1 ассоциируется с основным набором служб ОНС2, все предназначенные ей кадры данных должны направляться через ТД2. Одним из решений (впрочем, оно немного ха-керское) является отправка точкой доступа ТД2 широковещательного кадра Ethernet с адресом станции X1 для коммутатора сразу же по за­вершении ассоциации. Когда коммутатор получает этот кадр, происхо­дит обновление таблицы переадресации, позволяющее получить доступ к станции X1 посредством точки доступа ТД2. Группа по разработке стандартов 802.11f занимается созданием протокола взаимодействия точек доступа для решения вышеописанной и связанной с ней задач.

**Дополнительные функции 802.11**

Мы закончим наше описание технологии 802.11 кратким обсужде­нием двух дополнительных функций сетей типа 802.11. Как мы вско­ре убедимся, обе эти функции *не полностью* описаны в спецификации стандарта 802.11, но существуют благодаря другим механизмам, вклю­ченным в спецификацию. Это позволяет различным производителям реализовывать эти функции, используя собственные (патентованные) подходы, придавая им, в идеале, некоторое конкурентное преимуще­ство.

**Подстройка скорости передачи данных**

Ранее, на рис. 6.3, мы видели, что для различных условий соотношения сигнал-шум (SNR) применяются различные технологии модуляции сиг­нала. Теперь, для примера, давайте представим мобильного пользователя сети 802.11, находящегося в 20 метрах от базовой станции в условиях вы­сокого соотношения сигнал-шум. Учитывая большое значение показате­ля SNR, пользователь может связываться с базовой станцией с помощью технологии модуляции физического уровня, позволяющей сохранить высокие скорости передачи данных при низком показателе количества би­товых ошибок (BER). Счастливчик, не правда ли?! Теперь давайте пред­ставим, что пользователь пришел в движение и начал отходить от базовой станции, при этом по мере увеличения расстояния началось падение зна­чения показателя SNR. В этом случае техника модуляции сигнала в про­токоле 802.11, используемом для связи базовой станции с пользователем, не изменится, количество битовых ошибок станет неприемлемо высоким при снижении соотношения сигнал-шум, в результате чего передаваемые кадры данных будут приниматься некорректно.

По этой причине некоторые решения 802.11 обладают функцией подстройки скорости передачи данных, осуществляющей выбор исполь­зуемой техники модуляции сигнала физического уровня в зависимости от текущих характеристик канала связи. Если узел посылает два кадра подряд и не получает подтверждения (имплицитный индикатор бито­вых ошибок на канале), скорость передачи данных падает до ближайше­го нижнего показателя. Если получение 10 кадров подряд подтвержде­но, либо если время, отсчитываемое таймером с последнего понижения скорости, истекает, то скорость передачи данных увеличивается на по­казатель. Технология адаптации скорости передачи данных основана на той же философии «апробации», что и механизм контроля перегрузки технологии TCP. В некотором роде технология подстройки скорости похожа на ребенка, просящего своих родителей дать ему еще больше и больше сладостей, если ребенок мал, или возможности вернуться до­мой поздней и поздней, если это подросток, до тех пор, пока родители не скажут ему «Хватит!» и ребенок не отступит (чтобы попробовать позже и разузнать, не улучшились ли условия!).

**Управление питанием**

Для мобильных устройств электропитание — это очень ценный ре­сурс. Именно поэтому протокол стандарта 802.11 предлагает возмож­ности по управлению питанием, позволяющие узлам сети 802.11 ми­нимизировать время, необходимое функциям прослушивания канала, передачи и приема данных, а также оставаться включенным другому электрооборудованию. Управление питанием в сетях 802.11 работает следующим образом. Узел может явным образом переходить как в ре­жим сна, так и в рабочее состояние (не то, что сонные студенты в ауди­ториях!). Узел сообщает точке доступа о предстоящем переходе в режим сна, устанавливая значение 1 для соответствующего бита заголовка ка­дра 802.11. После этого таймер узла автоматически настраивается таким образом, чтобы «разбудить» узел прежде, чем точка доступа отправит следующий запланированный сигнальный кадр (вспомним, что, как правило, точка доступа отправляет сигнальные кадры каждые 100 мкс). Так как благодаря установленному значению бита управления питани­ем точка доступа «знает», что узел готовится отойти ко сну, она (точка доступа) не будет направлять ему никаких кадров данных, вместо этого все кадры данных, предназначенные спящему хосту, будут буферизиро-ваны и отправлены позднее.

Узел пробуждается и очень быстро переходит в полноценное рабо­чее состояние (в отличие от сонного студента, всего лишь за 250 мкс!) незадолго до того, как точка доступа пошлет сигнальный кадр. Отправ­ляемый точкой доступа сигнальный кадр содержит список узлов сети, чьи кадры данных были буферизированы в блоке памяти точки доступа. Если для узла нет буферизированных кадров данных, он может вновь вернуться в режим сна. В противном случае узел может явно затребо­вать буферизированные кадры данных с помощью отправки точке до­ступа специального опросного сообщения (polling message). Учитывая время между отправкой сигнальных кадров, равное 100 мкс, время на пробуждение — 250 мкс, и столь же незначительное время, требующееся на получение сигнального кадра и проверку на наличие буферизирован­ных кадров, узел, не отправляющий или не получающий кадров данных, может оставаться в режиме сна до 99% рабочего времени, что позволяет существенно сократить энергозатраты.

**Персональные сети: Bluetooth и Zigbee**

Как показано на рис. 6.2, стандарт IEEE 802.11 WI-FI предназначен для соединения по беспроводной сети устройств, находящихся до 100 м друг от друга (за исключением случаев, когда сеть 802.11 применяет­ся для двухточечной связи с использованием направительных антенн). Два других протокола IEEE 802.11 — Bluetooth и Zigbee (определяемые в стандартах IEEE 802.15.1 и IEEE 802.15.4) и WiMAX (определяемый в стандарте IEEE 802.1 б) — являются стандартами для связи на бо­лее коротких длинных расстояниях соответственно. Мы еще вкратце поговорим о стандарте WiMAX, когда будем обсуждать мобильные сети для передачи данных, сейчас же обратим свое внимание на сети с более короткой дистанцией.

**Bluetooth**

Сеть IEEE 802.15.1 имеет небольшую зону покрытия, потребляет не­большое количество энергии и требует небольших финансовых затрат. По сути это энергосберегающая, низкоскоростная технология, «замеща­ющая кабель» и работающая на коротких дистанциях, используемая для связи между собой ноутбуков, периферийных устройств, сотовых теле­фонов и смартфонов. В то время как 802.11 — это более энергозатратная, скоростная технология «доступа» в Интернет, работающая на средних дистанциях. Именно поэтому сети 802.15.1 часто называют беспровод­ными персональными сетями WPAN (от англ. Wireless Personal Area Networks). Физический и канальный уровни сетей 802.15.1 базируются на более ранних спецификациях технологии **Bluetooth** для персональ­ных сетей. Сети 802.15.1 работают в нелицензируемом радиодиапазо­не 2,4 ГГц по шаблону TDM (Time-Division Multiplexing — мультиплек­сирование с разделением времени). Величина временного промежутка составляет 625 мкс. На протяжении каждого временного промежутка отправитель выполняет передачу на одном из 79 каналов, при этом канал меняется при смене временного промежутка по известной псевдослучай­ной схеме. Таким образом осуществляется переключение каналов, также известное как **расширение спектра со скачкообразной перестройкой частоты FHSS** (Frequency-Hopping Spread Spectrum), распределяющее передачу по полосам частотного диапазона. Скорость передачи данных в сетях 802.15.1 может достигать 4 Мбит/с.

Все сети 802.15.1 являются одноуровневыми, так как для связи устройств 802.15.1 не требуется никакой сетевой инфраструктуры (на­пример, точек доступа). Поэтому устройства 802.15.1 должны занимать­ся самоорганизацией и упорядочиванием. В первую очередь, устрой­ства 802.15.1 организуются в так называемые **пикосети,** содержащие до восьми активных устройств, как показано на рис. 6.16. Одно из таких устройств называется «ведущим» (master), а остальные устройства — «подчиненными» (slaves). Ведущие устройства воистину являются «хо­зяевами» пикосети — часы такого устройства определяют время сети, оно может осуществлять отправку данных во все нечетные промежутки времени, в то время как подчиненные устройства могут вести передачу только после того, как с ними связалось ведущее устройство (в преды­дущий временной интервал), при этом подчиненное устройство может передавать данные только ведущему устройству. В дополнение к под­чиненным, в сети может также находиться до 255 зарегистрированных устройств. Такие устройства не могут осуществлять связь до тех пор, пока их статус не будет изменен ведущим узлом с «зарегистрирован­ных» на «активные».



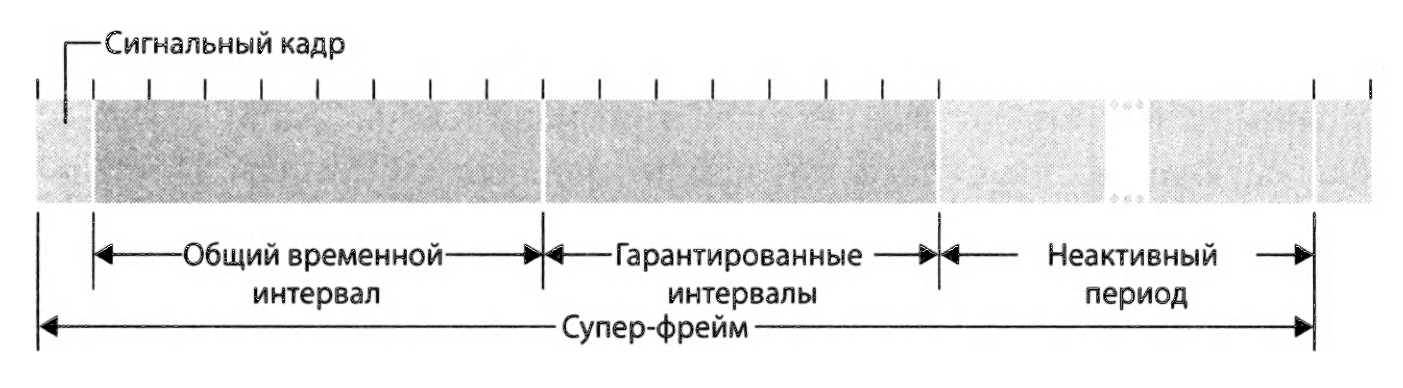
**Рис. 6.16. Пикосеть Bluetooth**

Для получения более подробной информации о сетях WPAN 802.15.1, интересующиеся читатели могут обратиться к справочниками по техно­логии Bluetooth или официальному веб-сайту IEEE 802.15.

**Zigbee**

Следующий вид персональной сети, описываемый в стандар­те IEEE, — это сеть Zigbee стандарта 802.14.5. В то время как сети Bluetooth, являющиеся «кабелезаменителями», предоставляют ско­рость передачи данных более 1 Мбит в секунду, сети Zigbee предназна­чены для работы менее энергоемких, менее требовательных к скорости передачи данных приложений с меньшим циклом активности, нежели сети Bluetooth. Хотя большинство из нас думает, что «больше значит лучше», не для всех сетевых приложений требуются более высокая ско­рость передачи данных и, соответственно, более высокие затраты (как экономические, так и энергетические). Например, домашние датчики температуры и освещенности, устройства обеспечения безопасности, а также настенные переключатели являются очень простыми, не энерго­затратными, дешевыми устройствами с малыми интервалами активно­сти. Таким образом, сеть Zigbee идеально подходит для таких устройств. Скорость передачи данных в каналах сети Zigbee зависит от рабочей ча­стоты канала и может составлять **20,**40,**100** и **250** Кбит/с.

Узлы сетей Zigbee делятся на два вида. Так называемые ограничен­но-функциональные устройства работают под контролем единствен­ного «полнофункционального устройства», что напоминает ведомые устройства сетей Bluetooth. Полнофункциональное устройство может играть роль, аналогичную роли «ведущего» устройства сети Bluetooth, заключающуюся в управлении множеством подчиненных устройств. Кроме того, несколько полнофункциональных устройств могут быть ор­ганизованы в смешанную сеть, в которой они занимаются маршрутиза­цией кадров данных между собой. В технологии Zigbee также применя­ется большое количество механизмов, с которыми мы уже сталкивались при рассмотрении других протоколов канального уровня: сигнальные кадры и подтверждения канального уровня (аналогичны сетям 802.11), протоколы множественного случайного доступа с анализом состояния канала и двоичной экспоненциальной задержкой (как в сетях 802.11 и Ethernet), а также фиксированное, гарантированное резервирование временных интервалов (как в технологии DOCSIS).

**Рис. 6.17. Структура супер-фрейма сетей Zigbee 802.14.4**

Существует множество вариантов конфигурации сетей Zigbee. Да­вайте рассмотрим вариант с единым полнофункциональным устрой­ством, управляющим множеством ограниченно-функциональных устройств с использованием механизма разделения по временным ин­тервалам и сигнальных кадров. На рис. 6.17 изображен случай, когда сеть Zigbee делит время на рекуррентные суперфреймы, каждый из ко­торых начинается с сигнального кадра. Каждый сигнальный кадр под­разделяет суперфрейм на активный период (на протяжении которого устройства могут осуществлять передачу данных) и неактивный период (на протяжении которого все устройства, в том числе, контроллер, могут переходить в режим сна и экономить тем самым электроэнергию). Ак­тивный период состоит из 16 временных интервалов, некоторые из них используются устройствами для осуществления случайного доступа на манер технологии CDMA/CA. Некоторые из временных интервалов резервируются контроллером для каких-либо конкретных устройств, что, таким образом, гарантирует этим устройствам доступ к каналу связи. Более подробную информацию о сетях Zigbee вы можете найти в публи­кациях Баронти и спецификации IEEE 802.15.4 2012.

**Доступ в Интернет посредством сетей сотовой радиосвязи**

В предыдущем разделе мы рассмотрели механизмы, с помощью которых хосты, подключенные к точке Wi-Fi — иными словами, точке доступа типа 802.11, — могут получить доступ в Интернет. Однако пло­щадь покрытия большинства точек доступа Wi-Fi сравнительно мала: от 10 до 100 м в диаметре. Что же мы делаем, когда нам срочно необ­ходимо получить доступ в Интернет, но мы не можем подключиться к точке Wi-Fi?

Принимая во внимание тот факт, что сотовая телефония очень широ­ко распространена во всех уголках мира, вполне естественным является желание дополнить сотовые сети так, чтобы они обеспечивали не только голосовую телефонную связь, но также и беспроводной доступ к Интерне­ту. В идеале, такой вариант доступа в Интернет будет достаточно высоко­скоростным и предоставит пользователям безусловную мобильность, по­зволяя им сохранять активные TCP-подключения во время перемещений в пространстве, например, поездки на автобусе. Обладая высокой скоро­стью передачи данных в восходящем и нисходящем направлениях, такие сети могут даже поддерживать видеоконференцию при постоянном пере­мещении пользователей. Сценарий тут не такой уж и изысканный. По дан­ным на 2012 год, большое количество операторов сотовой связи в США предоставляли своим абонентам услугу доступа в Интернет посредством сотовой сети на скорости в несколько сотен килобит в секунду по цене около 50 долларов или даже ниже. В сотовых сетях с услугами широкопо­лосного доступа в Интернет, которые мы рассмотрим в этом разделе, ста­новится возможным достижение скоростей в несколько мегабит в секунду, кроме того, такие сети становятся все более и более распространенными.

В этом разделе мы вкратце рассмотрим уже используемые и только зарождающиеся технологии доступа в Интернет посредством сотовой связи. Мы обратим внимание не только на первичный, беспроводной, транзитный участок сети, но также и на сеть, соединяющую беспровод­ной транзитный участок в большую телефонную сеть и/или подключающую его к Интернету. Мы порассуждаем над вопросами маршрутизации телефонных вызовов в условиях перемещения поль­зователя от одной базовой станции к другой. Наше краткое обсужде­ние будет обязательно включать только упрощенное высокоуровневое описание технологий сотовой связи. Конечно же, современная сотовая связь имеет большую ширину и глубину, при этом во многих универси­тетах она изучается в рамках сразу нескольких дисциплин. Читателям, желающим более детально разобраться в вопросе, мы бы порекомендо­вали обратиться к работам Гудмена, Кааранена, Лина, Корхоне-на, Шиллера, Скауриаса, Тернера и Акилдиза. Книга Моулиособенно замечательна и заслуживает наших отдельных рекомендаций.

**Обзор архитектуры сотовых сетей**

При описании архитектуры сетей сотовой связи мы будем пользо­ваться терминологией, употребляемой в стандартах *глобальной систе­мы мобильной связи* (Global System for Mobile Communication, **GSM).** В целях исторической справедливости следует отметить, что аббреви­атура GSM изначально расшифровывалась как Groupe Special Mobile, прежде чем в западном мире стали применять более англофицирован-ный термин, позволивший сохранить буквы изначальной аббревиату­ры. В 1980-х годах европейцы осознали потребность в создании единой общеевропейской системы цифровой сотовой связи, которая заменила бы большое количество несовместимых друг с другом аналоговых си­стем, что, собственно и привело к появлению стандарта GSM. В на­чале 1990-х годов европейцам удалось успешно развернуть первые сети GSM, и с тех пор этот стандарт уже превратился в огромного многотон­ного Кинг-Конга мира сотовой связи: ему принадлежит более 80% всех абонентов сотовой связи мира.

Когда говорят о технологиях сотовой связи, их зачастую распределя­ют по принадлежности к тому или иному «поколению». Первые поколе­ния систем сотовой связи создавались в основном для обеспечения голо­сового трафика. Системами первого поколения (1G) были сети FDMA, разработанные только для голосовой связи. Такие системы поколения 1G сейчас практически не встречаются: их заменяют цифровые системы по­коления 2G. Первоначально системы сотовой связи второго поколения также создавались только для голосовой связи, однако позже они были расширены (2,5G) для предоставления услуг обмена данными (например, доступа в Интернет) при сохранении доступа к услугам передачи голоса. В настоящее время в мире развертываются сети поколения 3G, они пре­доставляют пользователям услуги по передаче голоса и данных, однако роль передачи данных в таких сетях постоянно растет, при этом каналы радиосвязи предоставляют все большие и большие скорости.

**ИСТОРИЯ**

**Мобильные сети поколения 3G против беспроводных локальных сетей**

Большое количество операторов сотовой связи разворачивают сети поколения 3G, предоставляющие скорости передачи данных до 2 Мбит/с в помещении и до 384 кбит/с или выше на улице. Сети тре­тьего поколения работают в лицензируемых радиочастотных диа­пазонах, при этом некоторые операторы сотовой связи вынуждены платить правительствам стран огромные суммы денег за лицензии на использование частотного диапазона. Сети третьего поколения позволяют пользователям, находясь на улице, в достаточно удален­ной точке, получить доступ в Интернет, при этом не прекращая дви­жения, наподобие современных возможностей доступа к мобильной сети. Например, сеть 3G позволяет абоненту получить доступ к до­рожной карте, находясь в движущемся автомобиле, или к афише кино и театров, когда абонент загорает на пляже. Однако у кого-то могут появиться сомнения по поводу того, до какой степени будут расти такие сети, принимая во внимание их себестоимость, а также тот факт, что зачастую абоненты могут одновременно иметь доступ и к 3G и к беспроводной локальной сети.

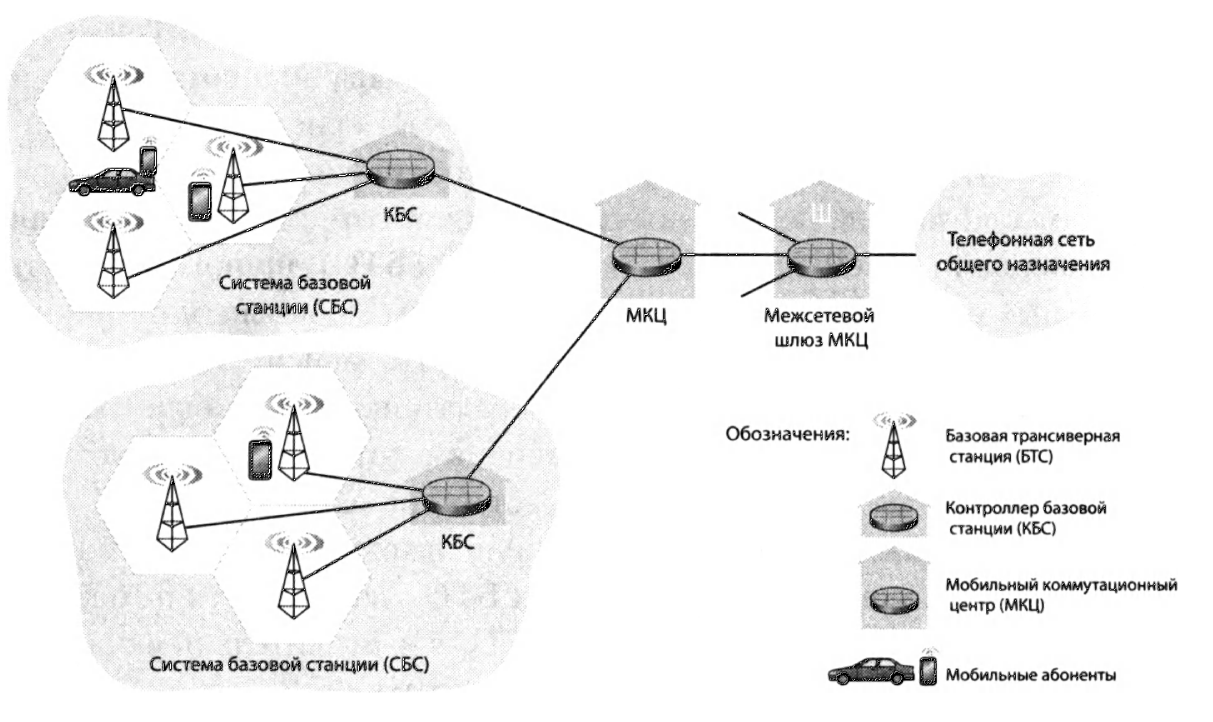
* Зарождающаяся инфраструктура беспроводных локальных сетей в скором времени может разрастись до очень больших размеров и стать всеобъемлющей. Беспроводные локальные сети 802.11, работающие на скорости 54 Мбит/с, получают очень широкое при­менение. Практически все портативные компьютеры и смартфо­ны оснащены интерфейсами для подключения к локальным сетям 802.11. Более того, только появляющиеся Интернет-устройства, такие как беспроводные камеры и цифровые фоторамки, также комплектуются экономичными интерфейсами для подключения к беспроводным локальным сетям.
* Базовые станции беспроводных локальных сетей также могут взять на себя выполнение задач мобильной телефонии. Большое коли­чество мобильных телефонов уже в наши дни могут подключаться не только к сотовым сетям, но и к сетям IP-телефонии благодаря встроенному программному обеспечению или сервисам VoIP, на­подобие Skype. Таким образом обеспечивается «обход» сервисов оператора сотовой связи 3G по передаче голоса и данных.

Впрочем, другие специалисты, наоборот, уверены, что сети поколе­ния 3G не только станут очень успешными, но также совершат ре­волюцию в стиле нашей работы и жизни. Наиболее вероятно, что и 3G и Wi-Fi станут основными стандартами беспроводной связи, при этом перемещающиеся по сети беспроводные устройства будут самостоятельно осуществлять выбор технологии доступа, наиболее подходящей для использования, в зависимости от фактического ме­стонахождения.

**Архитектура сети сотовой связи, 2G: Голосовая связь**

Сам термин «сотовая» означает, что область, покрываемая сетью со­товой связи, разделена еще на несколько зон, называемых **сотами,** — они изображены в виде шестиугольников в левой части рис. 6.18. Как и стан­дарт 802.11 Wi-Fi, у сетей GSM существует собственная, присущая толь­ко сетям такого вида номенклатура. В каждой соте сети есть **базовая трансиверная** (приемопередающая) **станция (БТС),** принимающая от мобильных станций в соте и посылающая этим мобильным станциям собственные сигналы. Площадь покрытия соты зависит от множества факторов, в том числе и от мощности передатчика БТС, мощности пе­редатчиков абонентских устройств, наличия в соте создающих помехи зданий, а также высоты антенн базовой станции. Хотя на рис. 6.11 изо­бражено, что базовая трансиверная станция находится в центре каждой соты, в настоящее время во многих сетях БТС располагается на пересе­чении трех сот таким образом, что одна БТС с направительными антен­нами может обслуживать одновременно три соты.

Стандарт GSM для сетей поколения 2G предполагает сочетание тех­нологий частотного и временного мультиплексирования FDM/TDM (радио) для воздушного интерфейса. Вспомните из текста главы 1, что при использовании только технологии FDM (частотное мультиплекси­рование) канал связи разделяется на сегменты, представляющие собой разные частотные диапазоны, причем для осуществления одного голо­сового вызова выделяется одна частота. Также вспомним из главы 1, что при использовании только технологии TDM (временное мульти­плексирование) время разделяется на фреймы, а каждый из фреймов дополнительно разбит на промежутки (слоты), при этом каждому осу­ществляемому вызову назначается конкретный временной промежуток в цикличном фрейме. При сочетании технологий частотного и времен­ного мультиплексирования канал связи разбивается на несколько ча­стот, при этом время каждой из выделенных частот канала разбивается на отдельные фреймы, а затем промежутки (слоты). Поэтому в случае с системой, сочетающей технологии FDM и TDM, если канал разбит на *F* частот, а время — на *Т* промежутков, то канал связи сможет одно­временно поддерживать количество вызовов, равное *FxT.* Вспомните также, что в кабельных сетях также применяется под­ход сочетания частотного и временного мультиплексирования FDM/ TDM. В системах GSM выделяются частоты по 200 кГц, при этом каж­дая из частот поддерживает восемь вызовов с временным мультиплек­сированием. Речь, передаваемая по сетям GSM, кодируется на скорости 13 и 12,2 кбит/с.

**Рис. 6.18. Компоненты архитектуры сети GSM поколения 2G**

Контроллер базовой станции (КБС) сетей GSM, как правило, обслу­живает сразу несколько десятков базовых трансиверных станций. Роль КБС состоит в том, чтобы выделить мобильным абонентам радиоканал БТС, выполнить пеленг (например, определить, в какой из сот сети на­ходится нужный абонент), а также осуществить передачу мобильного абонента. Множество кон­троллеров базовой станции и управляемых ими базовых трансиверных станций представляет собой систему базовой станции (СБС).

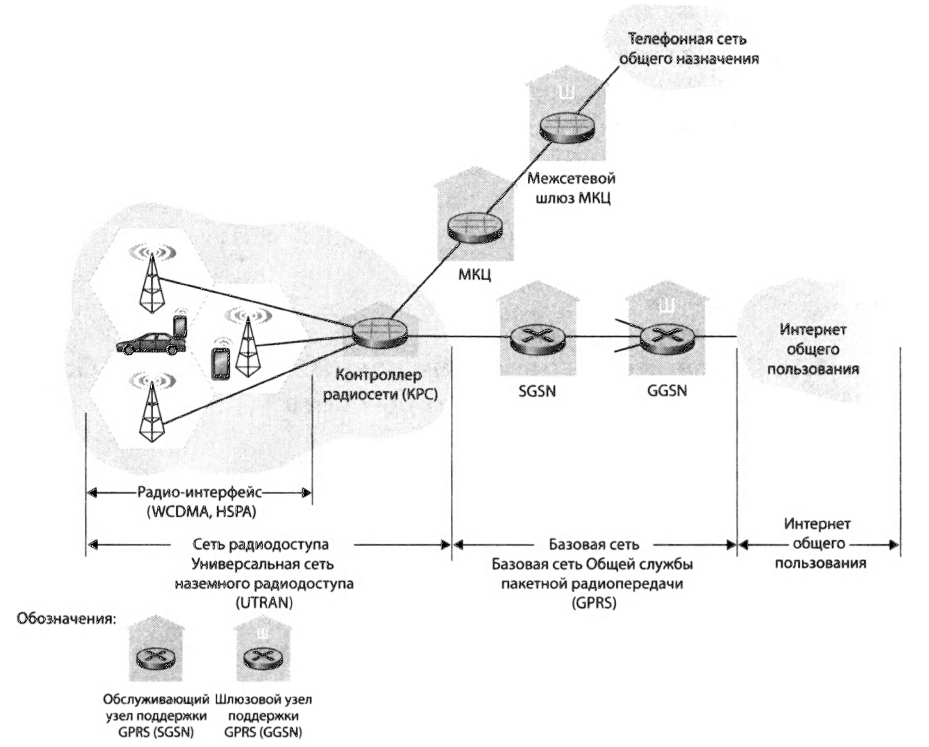
Позднее мы увидим, что мобильный коммуникационный центр

**(МКЦ)** играет важную роль в авторизации пользователя и обслужи­вании его абонентского счета (например, определяет, имеет ли право мобильное устройство подключаться к сети), установлении и прекра­щении вызова, а также передачи абонента. Единый МКЦ может содер­жать до 5 КБС, в результате чего количество абонентов на один МКЦ равняется примерно 200 тысячам. Сеть оператора сотовой связи, как правило, включает несколько МКЦ, в том числе и специальные МКЦ, называемые межсетевыми шлюзами, которые соединяют сотовую сеть оператора связи с более крупной телефонной сетью общего назна­чения.

**Сотовая сеть передачи данных поколения 3G: Интернет для абонентов сотовых сетей**

Главной темой нашей дискуссии было подключение абонентов сотовой сети, осуществляющих голосовой вызов, к телефон­ной сети общего назначения. Однако, конечно, находясь в пути, нам также хотелось бы иметь возможность просмотреть электронную по­чту, подключиться ко Всемирной паутине, воспользоваться сервисами, связанными с местоположением (например, картами или советами по выбору ресторана) и, возможно, даже посмотреть видео в режиме он­лайн. Чтобы осуществить все вышеописанное, нашему смартфону по­требуется запустить полный пакет протокола TCP/IP (в том числе канальный, сетевой, транспортный и прикладной уровни) и подклю­читься к Интернету через сотовую сеть передачи данных. Сама тема сотовых сетей передачи данных представляет собой весьма запутанное собрание конкурирующих и постоянно развивающихся стандартов, появляющихся как только одно поколение (или полу поколение) при­ходит на смену предыдущему и приносит с собой новые технологии с новыми сервисами и аббревиатурами. Однако проблема состоит еще и в том, что на сегодня в мире не существует единой организации, ко­торая бы задавала требования к технологиям поколений 2,5G, 3G, 3,5G и 4G. Это усложняет процесс выявления различий между соревнующи­мися стандартами. В нашем следующем обсуждении мы обратим наше внимание на стандарты третьего поколения UMTS (Universal Mobile Telecommunications Service — Универсальная система мобильной свя­зи), созданные организацией 3GPP (3rd Generation Partnership project — Проект партнерства третьего поколения). Сегодня технология UMTS очень популярна.

Давайте теперь пройдемся сверху вниз по архитектуре сотовой сети передачи данных поколения 3G, представленной на рис. 6.19.

**Рис. 6.19. Архитектура системы 3G**

**Базовая сеть 3G**

Базовая мобильная сеть передачи данных 3G ответственна за под­ключение сетей радиодоступа к Интернету общего пользования. Базо­вая сеть взаимодействует с компонентами имеющейся сотовой сети для передачи голоса (в частности, с МКЦ), с которыми мы уже встречались ранее на рис. 6.18. Принимая во внимание внушительное количество уже имеющихся инфраструктурных компонентов (и выгодных серви­сов!) в существующих мобильных сетях для передачи голоса, подход разработчиков к сервисам передачи данных поколения 3G становится предельно ясен: *оставить без изменений существующие мобильные сети GSM для передачи голоса, добавить возможности по передаче данных в дополнение к уже имеющейся сотовой сети.* Альтернативный подход — попытка интеграции новых сервисов по передаче данных напрямую в уже имеющуюся базовую сеть для передачи голоса — породила бы трудности аналогичные тем, с которыми мы познакомились ранее, когда обсуждали интеграцию новых (IPv6) и старых, доставшихся нам в наследство (IPv4) технологий в Интернете.

В базовой сети 3G есть два типа узлов: **обслуживающий** узел **под­держки GPRS (SGSN)** и **шлюзовой узел поддержки GPRS (GGSN).**

Аббревиатура GPRS расшифровывается как «общая служба пакетной радиопередачи (данных)» — ранний вариант услуги передачи данных в сетях 2G. В данном разделе мы обсудим преобразованную версию тех­нологии GPRS, используемую в сетях 3G. Узел SGSN ответственен за доставку дейтаграмм от/на мобильные узлы сети радиодоступа, с кото­рой этот узел связан. Узел SGSN взаимодействует с МКЦ, находящим­ся в нужной зоне сети, предоставляющим возможности по авторизации абонента и его передачи с сохранением информации местоположения (соты) об активных мобильных узлах в сети радиодоступа, и выполняю­щим переадресацию дейтаграмм между мобильными узлами в сети ра­диодоступа и узлом GGSN. Узел GGSN играет роль шлюза, подключаю­щего несколько узлов SGSN к более крупной сети — Интернету. Таким образом, узел GGSN — это последний компонент инфраструктуры сети 3G, с которым встречается дейтаграмма, созданная мобильным узлом перед попаданием в более крупную сеть Интернет. Для внешнего мира узел GGSN выглядит как еще один шлюзовой маршрутизатор, коих много, так как мобильность узлов сети 3G скрыта от внешнего мира за узлом GGSN.

**Сеть радиодоступа поколения 3G: беспроводная периферия**

**Сеть радиодоступа** 3G — это сеть первого скачка, непосредственно с которой мы взаимодействуем как пользователи сервисов 3G. **Контрол­лер радиосети (КРС),** как правило, управляет сразу несколькими базовы­ми трансиверными станциями сот сети, как это делают базовые станции, встречающиеся в системах второго поколения (в словаре сетей 3G UMTS из называют «Узлами Б» — крайне неочевидное название!). Беспровод­ной канал связи каждой соты соединяет мобильные узлы с трансиверной станцией, точно так же, как и в случае с сетью 2G. КРС подключается и к голосовой сотовой сети с коммутацией каналов через МКЦ, а также к Интернету с коммутацией пакетов данных через узел SGSN. Таким об­разом, несмотря на то, что для предоставления услуг по передаче голоса и данных в сетях 3G используются разные базовые сети, эти сети подклю­чены к единой сети радиодоступа первого/последнего скачка.

Существенное отличие технологии 3G UMTS от сетей второго по­коления заключается в том, что вместо схемы FDMA/ стандарта GSM, в сетях UMTS в рамках временных промежутков TDMA использует­ся механизм CDMA под названием Direct Sequence Wideband CDMA (DS-WCDMA — широкополосный множественный доступ с кодовым разделением каналов и прямой последовательностью). Временные промежутки TDMA поочередно становятся доступными для множества частот, что позволяет с еще большей эффективностью использовать все три подхода разделения канала связи, которые мы обозначили ранее. Такой механизм, опять же, аналогичен механизму, использую­щемуся в кабельных сетях. Такое концептуальное из­менение требует создания новой сети беспроводного доступа поколения 3G, работающей параллельно с сетью 2G и ее системами базовых стан­ций, как показано на рис. 6.19. Сервис по передаче данных, связанный с технологией WCDMA, получил название HSPA (High Speed Packet Access — Высокоскоростная пакетная передача данных), заявленная максимальная скорость передачи данных по нисходящему каналу свя­зи может достигать 14 Мбит/с. Более подробную информацию о сетях третьего поколения вы можете найти на официальном сайте Проекта партнерства третьего поколения (3GPP).

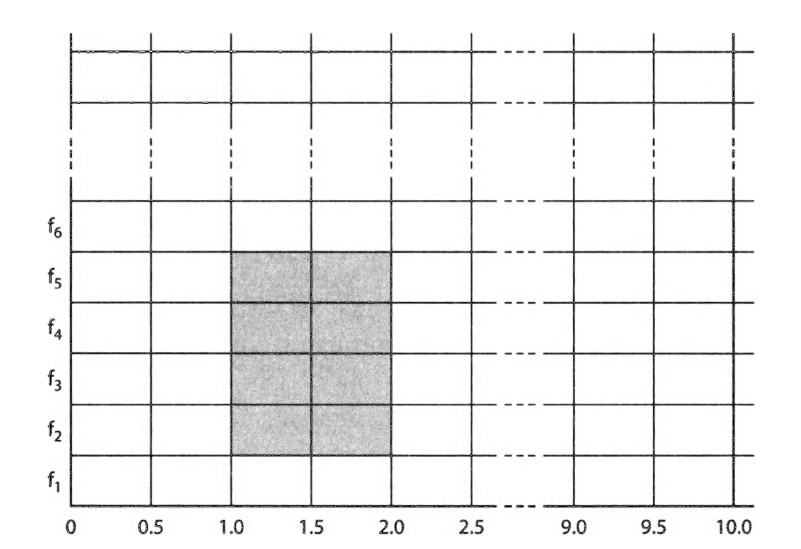
**Переход к 4G: LTE**

Сейчас, когда по всему миру разворачиваются сети поколения 3G, следует ли ожидать, что появление сетей 4G будет очень нескорым? Конечно же нет! Более того, разработка, тестирование и первичное раз­вертывание систем 4G осуществлюется уже сегодня! Стандарт 4G LTE (Long-Term Evolution — Долгосрочное развитие), изданный организа­цией 3GPP несет в себе два инновационных изменения по сравнению с сетями 3G:

• **Усовершенствование пакетное ядро** (Evolved Packet Core, EPC). ЕРС представляет собой упрощенную базовую сеть, полностью по­строенную на IP, которая объединяет прежде раздельные сеть пере­дачи голоса с коммутацией по каналам связи и сеть для передачи дан­ных с коммутацией по пакетам данных, изображенные на рис. 6.19. Таким образом, в сети, полностью построенной на IP (сеть AIPN), голос и данные передаются в виде IP-дейтаграмм. Как мы уже виде­ли ранее и еще обсудим более детально, модель серви­са IP под названием «лучшее из возможного» изначально не очень хорошо отвечает строжайшим требованиям по производительности, выдвигаемым к трафику данных технологии VoIP (Voice-over-IP — Голос по IP), если только сетевые ресурсы не подвергаются тщатель­ному управлению с целью избежать перенасыщения, а не реакции на него. Поэтому ключевая задача ЕРС — управлять ресурсами сети та­ким образом, чтобы сохранялась возможность предоставлять услуги высокого качества. Кроме того, технология ЕРС позволяет отчет­ливо разделять плоскости управления сетью и передачи пользова­тельских данных, поддерживая при этом большое количество функ­ций мобильности, применение которых мы изучим в разделе 6.7 на контрольной плоскости. Технология ЕРС допускает использование сетей радиодоступа разных типов, в том числе Motorola 2007 уста­ревших сетей 2G и сетей радиодоступа поколения 3G, которые могут быть подключены к базовой сети. Мы рекомендуем вам обратиться к двум очень полезным источникам на сайтах **www.motorola.com**и [**lightreading.com**](http://lightreading.com18)**.**

**• Сеть радиодоступа LTE.** В сетях LTE применяется сочетание частот­ного и временного мультиплексирования нисходящего канала, назы­ваемое также мультиплексированием с ортогональным разделением частот (Orthogonal Frequency Division Multiplexing — OFDM). В данном случае термин «ортогональный» подчеркивает то, что сигналы, посылаемые в разные частотные каналы, практически не накладываются один на другой, даже если разрыв между частота­ми каналов очень невелик. В сети LTE каждому мобильному узлу предоставляется один или несколько временных промежутков дли­ной 0,5 мс в одной или нескольких частотах канала. На рис. 6.20 изображено выделение восьми временных промежутков на четырех частотах. Предоставление мобильному узлу значительно больше­го количества временных промежутков (на одной или нескольких частотах) позволяет достичь значительно больших скоростей пере­дачи данных. Выделение и повторное выделение временных проме­жутков для мобильных узлов может производиться, внимание, один раз в миллисекунду! Кроме того, для изменения скорости передачи данных могут использоваться различные схемы модуляции сигна­ла (см. обсуждение рис. 6.3 выше и схем модуляции в сетях Wi-Fi). Еще одной инновацией в сетях радиодоступа LTE является исполь­зование сложных антенн многоканального ввода и многоканального вывода (MIMO). Максимальная скорость передачи данных пользо­вательского устройства в сетях LTE по нисходящему каналу состав­ляет 100 Мбит/с и 1 Мбит/с — по восходящему при полезном исполь­зовании 20 МГц беспроводного спектра.

Стандарт LTE не обязывает к выделению конкретных временных промежутков для мобильных узлов. Вместо этого, решение о том, какие мобильные узлы смогут осуществить передачу данных в заданный вре­менной промежуток на заданной частоте, принимается алгоритмами-планировщиками использования времени производителя оборудования сети LTE и/или оператора данной сети. Планирование «на ходу» (или «оппортунистическое планирование»), подбирающее протокол физического уровня в зависимости от состояния канала связи между отправителем и получателем, а также позволяющее осуществить выбор получателей, которым будут отправлены пакеты данных в зависимо­сти от состояния канала связи, способствует наиболее эффективному использованию беспроводной среды контроллером радиосети. Кроме того, становится возможным применение приоритетов пользователей и договорных уровней обслуживания (например, серебряный, золотой или платиновый) при передаче пакетов данных по нисходящему каналу. В дополнении к вышеописанным возможностям сетей LTE, технология LTE-Advanced (Расширенный LTE) позволяет мобильным узлам раз­вивать скорости передачи данных в несколько сотен мегабит в секунду в нисходящем направлении с помощью выделения таким узлам агреги­рованных каналов связи.

**Рис. 6.20. Двадцать временных промежутков по 0,5 мс организованы в 10 мс фреймы на всех частотах канала. Затенены восемь выделенных временных**

**промежутков**

Еще одна беспроводная технология четвертого поколения — WiMAX (World Interoperability for Microwave Access — Глобальная совместимость для микроволнового доступа) — семейство стандартов IEEE 802.16, значительно отличающихся от LTE. Пока еще не извест­но, в пользу какой из технологий четвертого поколения — LTE или WiMAX — будет сделан выбор, но в момент написания данной книги (весна 2012-го) технология LTE имела значительное превосходство. С подробным описанием технологии WiMAX вы можете познакомить­ся на сайте [www.wimaxforum.org](http://www.wimaxforum.org)