# Развитие технологии беспроводных сетей: стандарт IEEE 802.11

Реферат Кунегина С.В., kunegin.narod.ru

Комитет по стандартам IEEE 802 сформировал рабочую группу по стандартам для беспроводных локальных сетей 802.11 в 1990 году. Эта группа занялась разработкой всеобщего стандарта для радиооборудования и сетей, работающих на частоте 2,4 ГГц, со скоростями доступа 1 и 2 Mbps (Megabits-per-second). Работы по созданию стандарта были завершены через 7 лет, и в июне 1997 года была ратифицирована первая спецификация 802.11. Стандарт IEEE 802.11 являлся первым стандартом для продуктов WLAN от независимой международной организации, разрабатывающей большинство стандартов для проводных сетей. Однако к тому времени заложенная первоначально скорость передачи данных в беспроводной сети уже не удовлетворяла потребностям пользователей. Для того, чтобы сделать технологию Wireless LAN популярной, дешёвой, а главное, удовлетворяющей современным жёстким требованиям бизнес-приложений, разработчики были вынуждены создать новый стандарт.

В сентябре 1999 года IEEE ратифицировал расширение предыдущего стандарта. Названное IEEE 802.11b (также известное, как 802.11 High rate), оно определяет стандарт для продуктов беспроводных сетей, которые работают на скорости 11 Mbps (подобно Ethernet), что позволяет успешно применять эти устройства в крупных организациях. Совместимость продуктов различных производителей гарантируется независимой организацией, которая называется Wireless Ethernet Compatibility Alliance (WECA). Эта организация была создана лидерами индустрии беспроводной связи в 1999 году. В настоящее время членами WECA являются более 80 компаний, в том числе такие известные производители, как Cisco, Lucent,IBM, Apple, Dell, Siemens, AMD и пр. С продуктами, удовлетворяющими требованиям Wi-Fi (термин WECA для IEEE 802.11b), можно ознакомиться на сайте WECA.

Потребность в беспроводном доступе к локальным сетям растёт по мере увеличения числа мобильных устройств, таких как ноутбуки и PDA, а так же с ростом желания пользователей быть подключенными к сети без необходимости "втыкать" сетевой провод в свой компьютер. По прогнозам, к 2003 году в мире будет насчитываться более миллиарда мобильных устройств, а стоимость рынка продукции WLAN к 2002 году прогнозируется более чем в 2 миллиарда долларов.

## Стандарт IEEE 802.11 и его расширение 802.11b

Как и все стандарты IEEE 802, 802.11 работает на нижних двух уровнях модели ISO/OSI, физическом уровне и канальном уровне (рис. 1). Любое сетевое приложение, сетевая операционная система, или протокол (например, TCP/IP), будут так же хорошо работать в сети 802.11, как и в сети Ethernet.


*Рис. 1. Уровни модели ISO/OSI и их соответствие стандарту 802.11.*

Основная архитектура, особенности и службы 802.11b определяются в первоначальном стандарте 802.11. Спецификация 802.11b затрагивает только физический уровень, добавляя лишь более высокие скорости доступа.

**Режимы работы 802.11**

802.11 определяет два типа оборудования – клиент, который обычно представляет собой компьютер, укомплектованный беспроводной сетевой интерфейсной картой (Network Interface Card, NIC), и точку доступа (Access point, AP), которая выполняет роль моста между беспроводной и проводной сетями. Точка доступа обычно содержит в себе приёмопередатчик, интерфейс проводной сети (802.3), а также программное обеспечение, занимающееся обработкой данных. В качестве беспроводной станции может выступать ISA, PCI или PC Card сетевая карта в стандарте 802.11, либо встроенные решения, например, телефонная гарнитура 802.11.

Стандарт IEEE 802.11 определяет два режима работы сети – режим "Ad-hoc" и клиент/сервер (или режим инфраструктуры – infrastructure mode). В режиме клиент/сервер (рис. 2) беспроводная сеть состоит из как минимум одной точки доступа, подключенной к проводной сети, и некоторого набора беспроводных оконечных станций. Такая конфигурация носит название базового набора служб (Basic Service Set, BSS). Два или более BSS, образующих единую подсеть, формируют расширенный набор служб (Extended Service Set, ESS). Так как большинству беспроводных станций требуется получать доступ к файловым серверам, принтерам, Интернет, доступным в проводной локальной сети, они будут работать в режиме клиент/сервер.

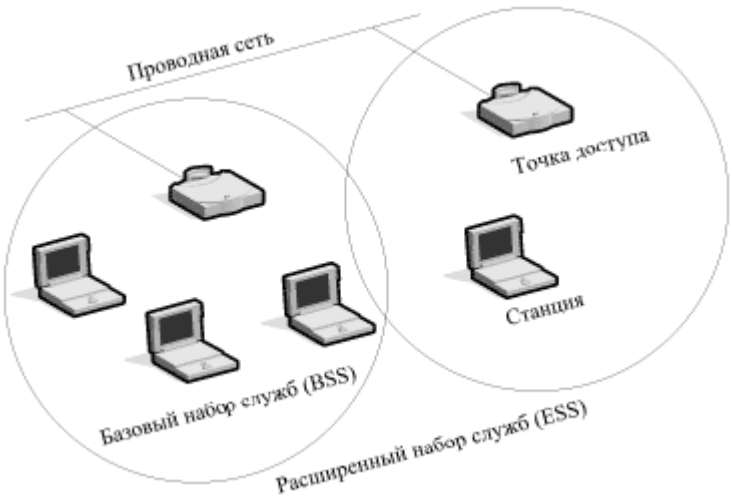


*Рис. 2. Архитектура сети "клиент/сервер".*

Режим "Ad-hoc" (также называемый точка-точка, или независимый базовый набор служб, IBSS) – это простая сеть, в которой связь между многочисленными станциями устанавливается напрямую, без использования специальной точки доступа (рис. 3). Такой режим полезен в том случае, если инфраструктура беспроводной сети не сформирована (например, отель, выставочный зал, аэропорт), либо по каким-то причинам не может быть сформирована.


*Рис. 3. Архитектура сети "Ad-hoc".*

**Физический уровень 802.11**

На физическом уровне определены два широкополосных радиочастотных метода передачи и один – в инфракрасном диапазоне. Радиочастотные методы работают в ISM диапазоне 2,4 ГГц и обычно используют полосу 83 МГц от 2,400 ГГц до 2,483 ГГц. Технологии широкополосного сигнала, используемые в радиочастотных методах, увеличивают надёжность, пропускную способность, позволяют многим несвязанным друг с другом устройствам разделять одну полосу частот с минимальными помехами друг для друга.

Стандарт 802.11 использует метод прямой последовательности (Direct Sequence Spread Spectrum, DSSS) и метод частотных скачков (Frequency Hopping Spread Spectrum, FHSS). Эти методы кардинально отличаются, и несовместимы друг с другом.

Для модуляции сигнала FHSS использует технологию Frequency Shift Keying (FSK). При работе на скорости 1 Mbps используется FSK модуляция по Гауссу второго уровня, а при работе на скорости 2 Mbps – четвёртого уровня.

Метод DSSS использует технологию модуляции Phase Shift Keying (PSK). При этом на скорости 1 Mbps используется дифференциальная двоичная PSK, а на скорости 2 Mbps – дифференциальная квадратичная PSK модуляция.

Заголовки физического уровня всегда передаются на скорости 1 Mbps, в то время как данные могут передаваться со скоростями 1 и 2 Mbps.

**Метод передачи в инфракрасном диапазоне (IR)**

Реализация этого метода в стандарте 802.11 основана на излучении ИК передатчиком ненаправленного (diffuse IR) сигнала. Вместо направленной передачи, требующей соответствующей ориентации излучателя и приёмника, передаваемый ИК сигнал излучается в потолок. Затем происходит отражение сигнала и его приём. Такой метод имеет очевидные преимущества по сравнению с использованием направленных излучателей, однако есть и существенные недостатки – требуется потолок, отражающий ИК излучение в заданном диапазоне длин волн (850 – 950 нм); радиус действия всей системы ограничен 10 метрами. Кроме того, ИК лучи чувствительны к погодным условиям, поэтому метод рекомендуется применять только внутри помещений.

Поддерживаются две скорости передачи данных – 1 и 2 Mbps. На скорости 1 Mbps поток данных разбивается на квартеты, каждый из которых затем во время модуляции кодируется в один из 16-ти импульсов. На скорости 2 Mbps метод модуляции немного отличается – поток данных делится на битовые пары, каждая из которых модулируется в один из четырёх импульсов. Пиковая мощность передаваемого сигнала составляет 2 Вт.

**Метод FHSS**

При использовании метода частотных скачков полоса 2,4 ГГц делится на 79 каналов по 1 МГц. Отправитель и получатель согласовывают схему переключения каналов (на выбор имеется 22 таких схемы), и данные посылаются последовательно по различным каналам с использованием этой схемы. Каждая передача данных в сети 802.11 происходит по разным схемам переключения, а сами схемы разработаны таким образом, чтобы минимизировать шансы того, что два отправителя будут использовать один и тот же канал одновременно.

Метод FHSS позволяет использовать очень простую схему приёмопередатчика, однако ограничен максимальной скоростью 2 Mbps. Это ограничение вызвано тем, что под один канал выделяется ровно 1 МГц, что вынуждает FHSS системы использовать весь диапазон 2,4 ГГц. Это означает, что должно происходить частое переключение каналов (например, в США установлена минимальная скорость 2,5 переключения в секунду), что, в свою очередь, приводит к увеличению накладных расходов.

**Метод DSSS**

Метод DSSS делит диапазон 2,4 ГГц на 14 частично перекрывающихся каналов (в США доступно только 11 каналов). Для того, чтобы несколько каналов могли использоваться одновременно в одном и том же месте, необходимо, чтобы они отстояли друг от друга на 25 МГц (не перекрывались), для исключения взаимных помех. Таким образом, в одном месте может одновременно использоваться максимум 3 канала. Данные пересылаются с использованием одного из этих каналов без переключения на другие каналы. Чтобы компенсировать посторонние шумы, используется 11-ти битная последовательность Баркера, когда каждый бит данных пользователя преобразуется в 11 бит передаваемых

данных. Такая высокая избыточность для каждого бита позволяет существенно повысить надёжность передачи, при этом значительно снизив мощность передаваемого сигнала. Даже если часть сигнала будет утеряна, он в большинстве случаев всё равно будет восстановлен. Тем самым минимизируется число повторных передач данных.

**Изменения, внесённые 802.11b**

Основное дополнение, внесённое 802.11b в основной стандарт – это поддержка двух новых скоростей передачи данных – 5,5 и 11 Mbps. Для достижения этих скоростей был выбран метод DSSS, так как метод частотных скачков в силу ограничений FCC не может поддерживать более высокие скорости. Из этого следует, что системы 802.11b будут совместимы с DSSS системами 802.11, но не будут работать с системами FHSS 802.11.

Для поддержки очень зашумлённых сред, а также работы на больших расстояниях, сети 802.11b используют динамический сдвиг скорости, который позволяет автоматически изменять скорость передачи данных в зависимости от свойств радиоканала. Например, пользователь может подключиться с максимальной скоростью 11 Mbps, но в том случае, если повысится уровень помех, или пользователь удалится на большое расстояние, мобильное устройство начнёт передавать на меньшей скорости – 5,5, 2 или 1 Mbps. В том случае, если возможна устойчивая работа на более высокой скорости, мобильное устройство автоматически начнёт передавать с более высокой скоростью. Сдвиг скорости – механизм физического уровня, и является прозрачным для вышестоящих уровней и пользователя.

**Канальный (Data Link) уровень 802.11**

Канальный уровень 802.11 состоит из двух подуровней: управления логической связью (Logical Link Control, LLC) и управления доступом к носителю (Media Access Control, MAC). 802.11 использует тот же LLC и 48-битовую адресацию, что и другие сети 802, что позволяет легко объединять беспроводные и проводные сети, однако MAC уровень имеет кардинальные отличия.

MAC уровень 802.11 очень похож на реализованный в 802.3, где он поддерживает множество пользователей на общем носителе, когда пользователь проверяет носитель перед доступом к нему. Для Ethernet сетей 802.3 используется протокол Carrier Sence Multiple Access with Collision Detection (CSMA/CD), который определяет, как станции Ethernet получают доступ к проводной линии, и как они обнаруживают и обрабатывают коллизии, возникающие в том случае, если несколько устройств пытаются одновременно установить связь по сети. Чтобы обнаружить коллизию, станция должна обладать способностью и принимать, и передавать одновременно. Стандарт 802.11 предусматривает использование полудуплексных приёмопередатчиков, поэтому в беспроводных сетях 802.11 станция не может обнаружить коллизию во время передачи.

Чтобы учесть это отличие, 802.11 использует модифицированный протокол, известный как Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), или Distributed Coordination Function (DCF). CSMA/CA пытается избежать коллизий путём использования явного подтверждения пакета (ACK), что означает, что принимающая станция посылает ACK пакет для подтверждения того, что пакет получен неповреждённым.

CSMA/CA работает следующим образом. Станция, желающая передавать, тестирует канал, и если не обнаружено активности, станция ожидает в течение некоторого случайного промежутка времени, а затем передаёт, если среда передачи данных всё ещё свободна.

Если пакет приходит целым, принимающая станция посылает пакет ACK, по приёме которого отправителем завершается процесс передачи. Если передающая станция не получила пакет ACK, в силу того, что не был получен пакет данных, или пришёл повреждённый ACK, делается предположение, что произошла коллизия, и пакет данных передаётся снова через случайный промежуток времени.

Для определения того, является ли канал свободным, используется алгоритм оценки чистоты канала (Channel Clearance Algorithm, CCA). Его суть заключается в измерении энергии сигнала на антенне и определения мощности принятого сигнала (RSSI). Если мощность принятого сигнала ниже определённого порога, то канал объявляется свободным, и MAC уровень получает статус CTS. Если мощность выше порогового значения, передача данных задерживается в соответствии с правилами протокола. Стандарт предоставляет ещё одну возможность определения незанятости канала, которая может использоваться либо отдельно, либо вместе с измерением RSSI – метод проверки несущей. Этот метод является более выборочным, так как с его помощью производится проверка на тот же тип несущей, что и по спецификации 802.11. Наилучший метод для использования зависит от того, каков уровень помех в рабочей области.

Таким образом, CSMA/CA предоставляет способ разделения доступа по радиоканалу. Механизм явного подтверждения эффективно решает проблемы помех. Однако он добавляет некоторые дополнительные накладные расходы, которых нет в 802.3, поэтому сети 802.11 будут всегда работать медленнее, чем эквивалентные им Ethernet локальные сети.

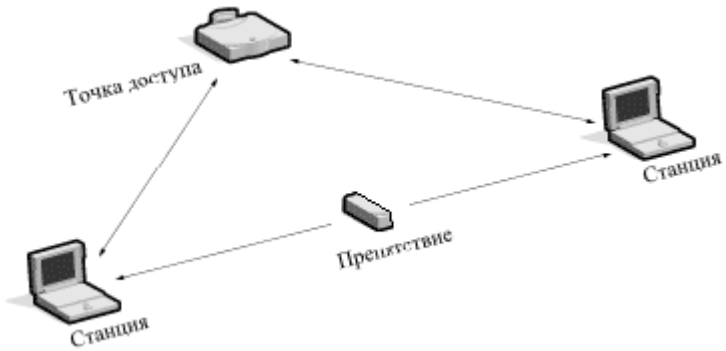


*Рис. 4. Иллюстрация проблемы "скрытой точки".*

Другая специфичная проблема MAC-уровня – это проблема "скрытой точки", когда две станции могут обе "слышать" точку доступа, но не могут "слышать" друг друга, в силу большого расстояния или преград (рис. 4). Для решения этой проблемы в 802.11 на MAC уровне добавлен необязательный протокол Request to Send/Clear to Send (RTS/CTS). Когда используется этот протокол, посылающая станция передаёт RTS и ждёт ответа точки доступа с CTS. Так как все станции в сети могут "слышать" точку доступа, сигнал CTS заставляет их отложить свои передачи, что позволяет передающей станции передать данные и получить ACK пакет без возможности коллизий. Так как RTS/CTS добавляет дополнительные накладные расходы на сеть, временно резервируя носитель, он обычно используется только для пакетов очень большого объёма, для которых повторная передача была бы слишком дорогостоящей.

Наконец, MAC уровень 802.11 предоставляет возможность расчёта CRC и фрагментации пакетов. Каждый пакет имеет свою контрольную сумму CRC, которая рассчитывается и прикрепляется к пакету. Здесь наблюдается отличие от сетей Ethernet, в которых обработкой ошибок занимаются протоколы более высокого уровня (например, TCP).

Фрагментация пакетов позволяет разбивать большие пакеты на более маленькие при передаче по радиоканалу, что полезно в очень "заселённых" средах или в тех случаях, когда существуют значительные помехи, так как у меньших пакетов меньше шансы быть повреждёнными. Этот метод в большинстве случаев уменьшает необходимость повторной передачи и, таким образом, увеличивает производительность всей беспроводной сети. MAC уровень ответственен за сборку полученных фрагментов, делая этот процесс "прозрачным" для протоколов более высокого уровня.

**Подключение к сети**

MAC уровень 802.11 несёт ответственность за то, каким образом клиент подключается к точке доступа. Когда клиент 802.11 попадает в зону действия одной или нескольких точек доступа, он на основе мощности сигнала и наблюдаемого значения количества ошибок выбирает одну из них и подключается к ней. Как только клиент получает подтверждение того, что он принят точкой доступа, он настраивается на радиоканал, в котором она работает. Время от времени он проверяет все каналы 802.11, чтобы посмотреть, не предоставляет ли другая точка доступа службы более высокого качества. Если такая точка доступа находится, то станция подключается к ней, перенастраиваясь на её частоту (рис. 5).

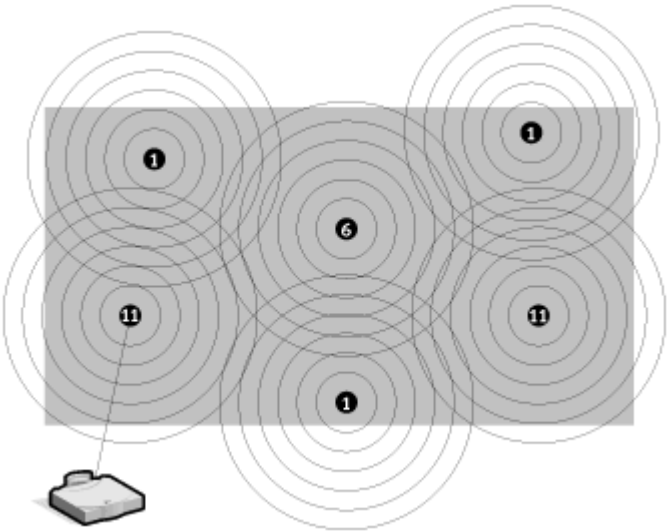


*Рис. 5. Подключение к сети и иллюстрация правильного назначения каналов для точек доступа.*

Переподключение обычно происходит в том случае, если станция была физически перемещена вдаль от точки доступа, что вызвало ослабление сигнала. В других случаях повторное подключение происходит из-за изменения радиочастотных характеристик здания, или просто из-за большого сетевого трафика через первоначальную точку доступа. В последнем случае эта функция протокола известна как "балансировка нагрузки", так как её главное назначение – распределение общей нагрузки на беспроводную сеть наиболее эффективно по всей доступной инфраструктуре сети.

Процесс динамического подключения и переподключения позволяет сетевым администраторам устанавливать беспроводные сети с очень широким покрытием, создавая частично перекрывающиеся "соты". Идеальным вариантом является такой, при котором соседние перекрывающиеся точки доступа будут использовать разные DSSS каналы, чтобы не создавать помех в работе друг другу (Рис. 5).

**Поддержка потоковых данных**

Потоковые данные, такие как видео или голос, поддерживаются в спецификации 802.11 на MAC уровне посредством Point Coordination Function (PCF). В противоположность Distributed Coordination Function (DCF), где управление распределено между всеми станциями, в режиме PCF только точка доступа управляет доступом к каналу. В том случае, если установлен BSS с включенной PCF, время равномерно распределяется промежутками для работы в режиме PCF и в режиме CSMA/CA. Во время периодов, когда система находится в режиме PCF, точка доступа опрашивает все станции на предмет получения данных. На каждую станцию выделяется фиксированный промежуток времени, по истечении которого производится опрос следующей станции. Ни одна из станций не может передавать в это время, за исключением той, которая опрашивается. Так как PCF даёт возможность каждой станции передавать в определённое время, то гарантируется максимальная латентность. Недостатком такой схемы является то, что точка доступа должна производить опрос всех станций, что становится чрезвычайно неэффективным в больших сетях.

**Управление питанием**

Дополнительно по отношению к управлению доступом к носителю, MAC уровень 802.11 поддерживает энергосберегающие режимы для продления срока службы батарей мобильных устройств. Стандарт поддерживает два режима потребления энергии, называемые "режим продолжительной работы" и "сберегающий режим". В первом случае радио всегда находится во включенном состоянии, в то время как во втором случае радио периодически включается через определённые промежутки времени для приёма "маячковых" сигналов, которые постоянно посылает точка доступа. Эти сигналы включают в себя информацию относительно того, какая станция должна принять данные. Таким образом, клиент может принять маячковый сигнал, принять данные, а затем вновь перейти в "спящий" режим.

**Безопасность**

802.11b обеспечивает контроль доступа на MAC уровне (второй уровень в модели ISO/OSI), и механизмы шифрования, известные как Wired Equivalent Privacy (WEP), целью которых является обеспечение беспроводной сети средствами безопасности, эквивалентными средствам безопасности проводных сетей. Когда включен WEP, он защищает только пакет данных, но не защищает заголовки физического уровня, так что другие станции в сети могут просматривать данные, необходимые для управления сетью. Для контроля доступа в каждую точку доступа помещается так называемый ESSID (или WLAN Service Area ID), без знания которого мобильная станция не сможет подключиться к точке доступа. Дополнительно точка доступа может хранить список разрешённых MAC адресов, называемый списком контроля доступа (Access Control List, ACL), разрешая доступ только тем клиентам, чьи MAC адреса находятся в списке.

Для шифрования данных стандарт предоставляет возможности шифрования с использованием алгоритма RC4 с 40-битным разделяемым ключом. После того, как станция подключается к точке доступа, все передаваемые данные могут быть зашифрованы с использованием этого ключа. Когда используется шифрование, точка доступа будет посылать зашифрованный пакет любой станции, пытающейся подключиться к ней. Клиент должен использовать свой ключ для шифрования корректного ответа для того, чтобы аутентифицировать себя и получить доступ в сеть.

Выше второго уровня сети 802.11b поддерживают те же стандарты для контроля доступа и шифрования (например, IPSec), что и другие сети 802.

**Безопасность для здоровья**

Так как мобильные станции и точки доступа являются СВЧ устройствами, у многих возникают вопросы по поводу безопасности использования компонентов Wave LAN. Известно, что чем выше частота радиоизлучения, тем опаснее оно для человека. В частности, известно, что если посмотреть внутрь прямоугольного волновода, передающего сигнал частотой 10 или более ГГц, мощностью около 2 Вт, то неминуемо произойдёт повреждение сетчатки глаза, даже если продолжительность воздействия составит менее секунды. Антенны мобильных устройств и точек доступа являются источниками высокочастотного излучения, и хотя мощность излучаемого сигнала очень невелика, всё же не следует находиться в непосредственной близости от работающей антенны. Как правило, безопасным расстоянием является расстояние порядка десятков сантиметров от приёмо-передающих частей. Более точное значение можно найти в руководстве к конкретному прибору.

**Дальнейшее развитие**

В настоящее время разрабатываются два конкурирующих стандарта на беспроводные сети следующего поколения – стандарт IEEE 802.11a и европейский стандарт HIPERLAN-2. Оба стандарта работают во втором ISM диапазоне, использующем полосу частот в районе 5 ГГц. Заявленная скорость передачи данных в сетях нового поколения составляет 54 Mbps.

**Производители устройств 802.11b**

На сегодняшний день наиболее известными и популярными производителями на рынке WaveLAN решений являются компании Lucent (серия ORiNOCO) и Cisco (серия Aironet). Помимо них существует достаточно большое количество компаний, производящих 802.11b совместимое оборудование. К их числу можно отнести такие компании, как 3Com (серия 3Com AirConnect), Samsung, Compaq, Symbol, Zoom Telephonics и пр. В следующей части статьи мы рассмотрим характеристики серий ORiNOCO компании Lucent и Aironet компании Cisco, а затем произведём тестирование обоих серий.