

5. СЕТИ WiFi

Введение

WI-FI - это современная беспроводная технология, благодаря которой Internet становится мобильным и дает пользователю свободу перемещения.

Wi-Fi был создан в 1991 году в лаборатории радиоастрономии CSIRO (Commonwealth Scientific and Industrial Research Organisation) в Канберре, Австралия. Создателем беспроводного протокола обмена данными является инженер Джон О'Салливан (John O'Sullivan).

Под аббревиатурой "Wi-Fi" (от английского словосочетания "Wireless Fidelity", которое можно дословно перевести как "**высокая точность беспроводной передачи данных**"), на данный момент от такой формулировки отказались, и термин «Wi-Fi» никак не расшифровывается. Под аббревиатурой "Wi-Fi", в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам.

С увеличением числа мобильных пользователей возникает острая необходимость в оперативном создании коммуникаций между ними, в обмене данными, в быстром получении информации. Поэтому естественным образом происходит интенсивное развитие технологий беспроводных коммуникаций. Особенно это актуально в отношении беспроводных сетей, или так называемых WLAN-сетей (*Wireless Local Area Network*). Сети WLAN - это беспроводные сети (вместо обычных проводов в них используются радиоволны). Установка таких сетей рекомендуется там, где *развертывание* кабельной системы невозможно или экономически нецелесообразно.

Беспроводные сети особенно эффективны на предприятиях, где сотрудники активно перемещаются по территории во время рабочего дня с целью обслуживания клиентов или сбора информации (крупные склады, агентства, офисы продаж, учреждения здравоохранения и др.).

Благодаря функции роуминга между точками доступа пользователи могут перемещаться по территории покрытия сети Wi-Fi без разрыва соединения.

WLAN-сети имеют ряд преимуществ перед обычными кабельными сетями:

- WLAN-сеть можно очень быстро развернуть, что очень удобно при проведении презентаций или в условиях работы вне офиса;
- пользователи мобильных устройств при подключении к локальным беспроводным сетям могут легко перемещаться в рамках действующих зон сети;
- скорость современных сетей довольно высока, что позволяет использовать их для решения очень широкого спектра задач;
- WLAN-сеть может оказаться единственным выходом, если невозможна прокладка кабеля для обычной сети.

Ограничения беспроводных сетей: меньшая скорость, подверженность влиянию помех и более сложная схема обеспечения безопасности передаваемой информации.

Сегмент Wi-Fi сети может использоваться как самостоятельная сеть, либо в составе более сложной сети, содержащей как беспроводные, так и обычные проводные сегменты. Wi-Fi сеть может использоваться:

- для беспроводного подключения пользователей к сети;
- для объединения пространственно разнесенных подсетей в одну общую сеть там, где кабельное соединение подсетей невозможно или нежелательно;
- для подключения к сетям провайдера Internet-услуги вместо использования выделенной проводной линии или обычного модемного соединения.

Преимущества Wi-Fi

• Позволяет развернуть сеть без прокладки кабеля, что может уменьшить стоимость развертывания и/или расширения сети. Места, где нельзя проложить кабель, например, вне помещений и в зданиях, имеющих историческую ценность, могут обслуживаться беспроводными сетями.

- Позволяет иметь доступ к сети мобильным устройствам.
- Wi-Fi устройства широко распространены на рынке. Гарантируется совместимость оборудования благодаря обязательной сертификации оборудования с логотипом Wi-Fi.
- Мобильность.
- В пределах Wi-Fi зоны в сеть Internet могут выходить несколько пользователей с компьютеров, ноутбуков, телефонов и т. д.
- Излучение от Wi-Fi устройств в момент передачи данных на порядок (в 10 раз) меньше, чем у сотового телефона.

Недостатки Wi-Fi:

- в диапазоне 2,4 ГГц работает множество устройств, таких как устройства, поддерживающие Bluetooth, и др., и даже микроволновые печи, что ухудшает электромагнитную совместимость;
- производителями оборудования указывается скорость на L1 (OSI). Реальная скорость всегда ниже и зависит от доли служебного трафика, которая зависит уже от наличия между устройствами физических преград (мебель, стены), наличия помех от других беспроводных устройств или электронной аппаратуры, расположения устройств относительно друг друга и т. п.;
- частотный диапазон и эксплуатационные ограничения в различных странах не одинаковы. Некоторые страны, например Россия, Беларусь и Италия, требуют регистрации всех сетей Wi-Fi, работающих вне помещений, или требуют регистрации Wi-Fi-оператора;
- как было упомянуто выше — в России точки беспроводного доступа, а также адаптеры Wi-Fi с ЭИИМ, превышающей 100 мВт (20 дБм), подлежат обязательной регистрации;
- стандарт шифрования WEP может быть относительно легко взломан даже при правильной конфигурации (из-за слабой стойкости алгоритма). Новые устройства поддерживают более совершенные протоколы шифрования данных WPA и WPA2. Обе схемы требуют более стойкий пароль, чем те, которые обычно назначаются пользователями. Многие организации используют дополнительное шифрование (например, VPN) для защиты от вторжения. На данный момент основным методом взлома WPA2 является подбор пароля, поэтому рекомендуется использовать сложные цифровые пароли для того, чтобы максимально усложнить задачу подбора пароля;

в режиме точка-точка (Ad-hoc) стандарт предписывает лишь реализовать скорость 11 Мбит/с (802.11b). Шифрование WPA2 недоступно, применяется легко взламываемый WEP.

Модуляция

Существуют три основные технологии кодирования или модуляции, выполняющие преобразование цифровых данных в аналоговый сигнал:

- амплитудная модуляция (Amplitude-Shift Keying - ASK);
- частотная модуляция (Frequency-Shift Keying - FSK);
- фазовая модуляция (Phase-Shift Keying - PSK).

Многочастотная (MFSK)

Более эффективной, но и более подверженной ошибкам, является схема *многочастотной* модуляции (*Multiple FSK - MFSK*), в которой используется более двух частот. В этом случае каждая сигнальная посылка представляет более одного бита. Переданный сигнал MFSK (для одного периода передачи сигнальной посылки) можно определить следующим образом:

$$s_i = A \cos(2\pi f_i t), \quad 1 < i < M. \quad (1)$$

Здесь $f_i = f_c + (2i - 1 - M)f_d$,

где f_c - несущая частота; f_d - разностная частота; $M = 2^L$ - число различных сигнальных посылок; L - количество битов на одну сигнальную посылку.

На **рис. 5.1** представлен пример схемы MFSK с $M=4$. Входной поток битов кодируется по два бита, после чего передается одна из четырех возможных двухбитовых комбинаций.

Для уменьшения занимаемой полосы частот в модуляторах сигналов с фазовой модуляцией применяют сглаживающие фильтры. Применение сглаживающих фильтров приводит к увеличению эффективности использования полосы, но в то же время из-за сглаживания уменьшается расстояние между соседними сигналами, что приводит к снижению помехоустойчивости.

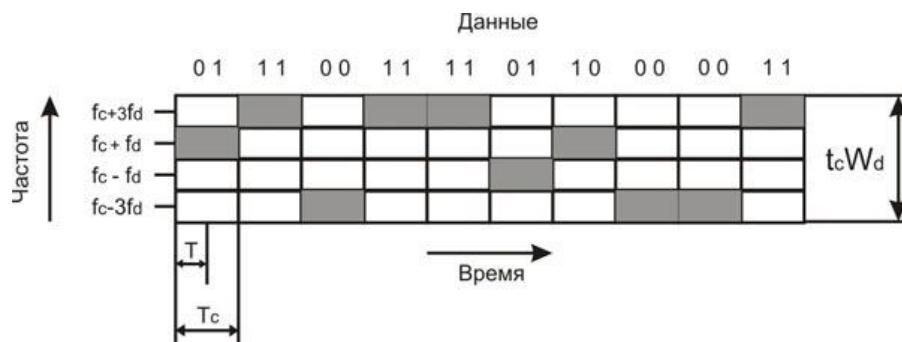


Рис. 5.1. Использование частоты схемой MFSK ($M = 4$)

Квадратурная амплитудная модуляция

Квадратурная амплитудная модуляция (*Quadrature Amplitude Modulation* - **QAM**) является популярным методом аналоговой передачи сигналов, используемым в некоторых беспроводных стандартах.

Данная схема модуляции совмещает в себе амплитудную и фазовую модуляции. В методе QAM использованы преимущества одновременной передачи двух различных сигналов на одной несущей частоте, но при этом задействованы две копии несущей частоты, сдвинутые относительно друг друга на 90 градусов. При квадратурной амплитудной модуляции обе несущие являются амплитудно-модулированными. Итак, два независимых сигнала одновременно передаются через одну среду. В приемнике эти сигналы демодулируются, а результаты объединяются с целью восстановления исходного двоичного сигнала.

При использовании двухуровневой квадратурной амплитудной модуляции (2QAM) каждый из двух потоков может находиться в одном из двух состояний, а объединенный поток - в одном из $2 \times 2 = 4$ состояний. При использовании четырехуровневой модуляции (т.е. четырех различных уровней амплитуды, 4QAM) объединенный поток будет находиться в одном из $4 \times 4 = 16$ состояний. Реализованы системы, имеющие 64 или даже 256 состояний. Чем больше число состояний, тем выше скорость передачи данных, возможная при определенной ширине полосы. Однако, чем больше число состояний, тем выше потенциальная частота возникновения ошибок вследствие помех или поглощения.

Пропускная способность канала

Существует множество факторов, способных искажить или повредить сигнал. Наиболее распространенные из них - помехи или шумы, представляющие собой любой нежелательный сигнал, который смешивается с сигналом, предназначенным для передачи или приема, и искажает его. Для цифровых данных возникает вопрос: насколько эти искажения ограничивают возможную скорость передачи данных? Максимально возможная при определенных условиях скорость, при которой информация может передаваться по конкретному тракту связи, или каналу, называется **пропускной способностью** канала.

Существует четыре важных понятия:

- скорость передачи данных - скорость в битах в секунду (бит/с), с которой могут передаваться данные;
- ширина полосы - ширина полосы передаваемого сигнала (Гц), ограничиваемая передатчиком и природой передающей среды;
- шум - средний уровень шума в канале связи;
- уровень ошибок - частота появления, битовых ошибок.

Чем шире используемая полоса, тем дороже стоят устройства. Все каналы передачи, представляющие практический интерес, имеют ограниченную ширину полосы. Ограничения обусловлены физическими свойствами передающей среды или преднамеренными ограничениями ширины полосы в самом передатчике, сделанными для предотвращения интерференции с другими источниками. Поэтому необходимо максимально эффективно использовать имеющуюся полосу. Для цифровых данных это означает, что для определенной полосы желательно получить максимально возможную при существующем уровне ошибок скорость передачи данных. Главным ограничением при достижении такой эффективности являются помехи.

Методы доступа к среде в беспроводных сетях

Одна из основных проблем построения беспроводных систем - это решение задачи доступа многих пользователей к ограниченному ресурсу среды передачи. Существует несколько базовых методов доступа (их еще называют методами уплотнения или мультиплексирования), основанных на разделении между станциями таких параметров, как пространство, время, частота и код. Задача уплотнения - выделить каждому каналу связи пространство, время, частоту и/или код с минимумом взаимных помех и максимальным использованием характеристик передающей среды.

Уплотнение с частотным разделением (*Frequency Division Multiplexing* - **FDM**)

Каждое устройство работает на определенной частоте, благодаря чему несколько устройств могут вести передачу данных на одной территории (**рис. 5.2**). Это один из наиболее известных методов, так или иначе используемый в самых современных системах беспроводной связи.

Наглядная иллюстрация схемы частотного уплотнения - функционирование в одном городе нескольких радиостанций, работающих на разных частотах. Для надежной отстройки друг от друга их рабочие частоты должны быть разделены защитным частотным интервалом, который позволяет исключить взаимные помехи.

Эта схема, хотя и позволяет использовать множество устройств на определенной территории, сама по себе приводит к неоправданному расточительству обычно скудных частотных ресурсов, поскольку требует выделения своей частоты для каждого беспроводного устройства.

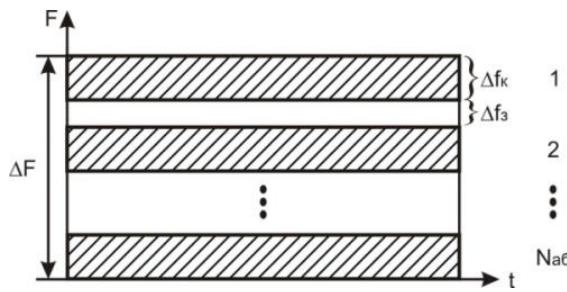


Рис. 5.2. Принцип частотного разделения каналов

Уплотнение с временным разделением (Time Division Multiplexing - TDM)

В данной схеме распределение каналов идет по времени, т. е. каждый передатчик транслирует сигнал на одной и той же частоте f области s , но в различные промежутки времени t_i (как правило, циклически повторяющиеся) при строгих требованиях к синхронизации процесса передачи (рис. 5.3).

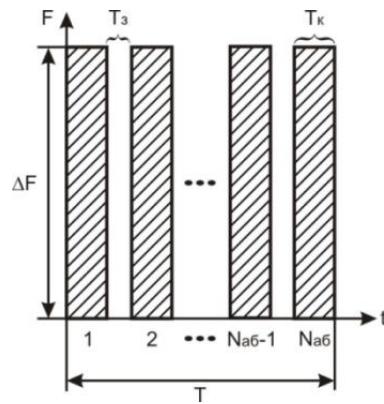


Рис. 5.3. Принцип временного разделения каналов

Подобная схема достаточно удобна, так как временные интервалы могут динамично перераспределяться между устройствами сети. Устройствам с большим трафиком назначаются более длительные интервалы, чем устройствам с меньшим объемом трафика.

Основной недостаток систем с временным уплотнением - это мгновенная потеря информации при срыве синхронизации в канале, например из-за сильных помех, случайных или преднамеренных. Однако успешный опыт эксплуатации таких знаменитых TDM-систем, как сотовые телефонные сети стандарта GSM, свидетельствует о достаточной надежности механизма временного уплотнения.

Уплотнение с кодовым разделением (Code Division Multiplexing - CDM)

В данной схеме все передатчики транслируют сигналы на одной и той же частоте f , в области s и во время t , но с разными кодами c_i . Механизм разделения каналов *CDMA* положен в основу стандарта сотовой телефонной связи IS-95a, а также ряда стандартов третьего поколения сотовых систем связи (cdma2000, WCDMA и др.).

В схеме CDM каждый передатчик заменяет каждый бит исходного потока данных на CDM-символ - кодовую последовательность длиной в 11, 16, 32, 64 и т.п. бит (их называют чипами). Кодовая последовательность уникальна для каждого передатчика. Как правило, если для замены "1" в исходном потоке данных используют некий CDM-код, то для замены "0" применяют тот же код, но инвертированный.

В приемнике известен CDM-код передатчика. Приемник постоянно принимает все сигналы и оцифровывает их. Затем в корреляторе производится операция свертки (умножения с накоплением) входного оцифрованного сигнала с известным ему CDM-кодом и его инверсией. В несколько упрощенном виде это выглядит как операция скалярного произведения вектора входного сигнала и вектора с CDM-кодом. Если сигнал на выходе коррелятора превышает некий установленный пороговый уровень, приемник считает, что принимается решение о принятом символе (1 или 0). Для увеличения вероятности приема передатчик может повторять посылку каждого бита несколько раз. При этом сигналы других передатчиков с другими CDM-кодами приемник воспринимает как аддитивный шум. Благодаря большой избыточности (каждый бит заменяется десятками чипов), мощность принимаемого сигнала может быть сопоставима с интегральной мощностью шума. Сходства CDM-сигналов со случайным (гауссовым) шумом добиваются, используя CDM-коды, порожденные генератором псевдослучайных последовательностей. Поэтому данный метод еще называют методом расширения спектра сигнала посредством прямой последовательности (DSSS - Direct Sequence Spread Spectrum).

Преимущество данного уплотнения заключается в повышенной защищенности и *скрытности* передачи данных: не зная кода, невозможно получить сигнал, а в ряде случаев - и обнаружить его присутствие. Кроме того, кодовое пространство несравненно больше по сравнению с частотной схемой уплотнения, что позволяет без особых проблем присваивать каждому передатчику свой индивидуальный код. Основной же проблемой кодового уплотнения до недавнего времени являлась сложность технической реализации приемников и необходимость обеспечения точной синхронизации передатчика и приемника для гарантированного получения пакета.

Механизм мультиплексирования посредством ортогональных несущих частот (*Orthogonal Frequency Division Multiplexing - OFDM*)

Весь доступный частотный диапазон разбивается на большое количество поднесущих (от нескольких сот до тысяч). Одному каналу связи (приемнику и передатчику) назначают для передачи несколько таких несущих, выбранных из множества по определенному закону. Передача ведется одновременно по всем поднесущим, т.е. в каждом передатчике исходящий поток данных разбивается на N субпотоков, где N - число поднесущих, назначенных данному передатчику. Распределение поднесущих в ходе работы может динамически изменяться, что делает данный механизм не менее гибким, чем метод временного уплотнения.

Схема OFDM имеет несколько преимуществ. Во-первых, *селективному* замиранию будут подвержены только некоторые подканалы, а не весь сигнал. Если поток данных защищен кодом прямого исправления ошибок, то с этим замиранием легко бороться. Во-вторых, что более важно, OFDM позволяет подавить межсимвольную интерференцию. Межсимвольная интерференция оказывает значительное влияние при высоких скоростях передачи данных, так как расстояние между битами (или символами) мало. В схеме OFDM скорость передачи данных уменьшается в N раз, что позволяет увеличить время передачи символа в N раз. Таким образом, если время передачи символа для исходного потока составляет T_s , то период сигнала OFDM будет равен NT_s . Это позволяет существенно снизить влияние межсимвольных помех. При проектировании системы N выбирается таким образом, чтобы величина NT_s значительно превышала среднеквадратичный разброс задержек канала.

Технология расширенного спектра

Изначально метод расширенного спектра создавался для разведывательных и военных целей. Основная идея метода состоит в том, чтобы распределить информационный сигнал по широкой полосе радиодиапазона, что в итоге позволит значительно усложнить подавление или перехват сигнала. Первая разработанная схема расширенного спектра известна как метод перестройки частоты. Более современной схемой расширенного спектра является метод прямого последовательного расширения. Оба метода используются в различных стандартах и продуктах беспроводной связи.

Расширение спектра скачкообразной перестройкой частоты (*Frequency Hopping Spread Spectrum - FHSS*)

Чтобы радиообмен нельзя было перехватить или подавить узкополосным шумом, было предложено вести передачу с постоянной сменой несущей в пределах широкого диапазона частот. В результате мощность сигнала распределялась по всему диапазону, и прослушивание какой-то определенной частоты давало только небольшой шум. Последовательность несущих частот была псевдослучайной, известной только в приемном и передающем устройствах. Попытка подавления сигнала в каком-то узком диапазоне также не слишком ухудшала сигнал, так как подавлялась только небольшая часть информации. Идею этого метода иллюстрирует **рис. 5.4**.



Рис. 5.4. Расширение спектра скачкообразной перестройкой частоты

В течение фиксированного интервала времени передача ведется на неизменной несущей частоте. На каждой несущей частоте для передачи дискретной информации применяются стандартные методы модуляции,

такие как FSK или PSK. Для того чтобы приемник синхронизировался с передатчиком, для обозначения начала каждого периода передачи в течение некоторого времени передаются синхробиты. Так что полезная скорость этого метода кодирования оказывается меньше из-за постоянных потерь времени на синхронизацию.

Несущая частота меняется в соответствии с номерами частотных подканалов, вырабатываемых алгоритмом псевдослучайных чисел. Псевдослучайная последовательность зависит от некоторого параметра, который называют начальным числом. Используя алгоритм и значение начального числа, то в передатчике и приемнике частоты изменяются в одинаковой последовательности, называемой последовательностью псевдослучайной перестройки частоты.

Если частота смены подканалов ниже, чем скорость передачи данных в канале, то такой режим называют *медленным расширением спектра* (рис. 5.5а); в противном случае - *быстрым расширением спектра* (рис. 5.5б).



Рис. 5.5. Соотношение между скоростью передачи данных и частотой смены подканалов

Метод быстрого расширения спектра более устойчив к помехам, поскольку узкополосная помеха, которая подавляет сигнал в определенном подканале, не приводит к потере бита, так как его значение повторяется несколько раз в различных частотных подканалах. В этом режиме не проявляется эффект межсимвольной интерференции, потому что ко времени прихода задержанного вдоль одного из путей сигнала система успевает перейти на другую частоту.

Метод медленного расширения спектра таким свойством не обладает, но зато он проще в реализации и сопряжен с меньшими накладными расходами.

Методы FHSS используются в беспроводных технологиях IEEE 802.11 и Bluetooth.

В FHSS подход к использованию частотного диапазона не такой, как в других методах кодирования - вместо экономного расхождения узкой полосы делается попытка занять весь доступный диапазон. На первый взгляд это кажется не очень эффективным - ведь в каждый момент времени в диапазоне работает только один канал. Однако последнее утверждение не всегда справедливо - коды расширенного спектра можно использовать и для мультиплексирования нескольких каналов в широком диапазоне. В частности, методы FHSS позволяют организовать одновременную работу нескольких каналов путем выбора для каждого канала таких псевдослучайных последовательностей, чтобы в каждый момент времени каждый канал работал на своей частоте (конечно, это можно сделать, только если число каналов не превышает числа частотных подканалов).

Прямое последовательное расширение спектра (Direct Sequence Spread Spectrum - DSSS)

В методе прямого последовательного расширения спектра также используется весь частотный диапазон, выделенный для одной беспроводной линии связи. В отличие от метода FHSS, весь частотный диапазон занимается не за счет постоянных переключений с частоты на частоту, а за счет того, что каждый бит информации заменяется N -битами, так что тактовая скорость передачи сигналов увеличивается в N раз. Это означает, что спектр сигнала также расширяется в N раз. Достаточно соответствующим образом выбрать скорость передачи данных и значение N , чтобы спектр сигнала заполнил весь диапазон.

Цель кодирования методом DSSS та же, что и методом FHSS, - повышение устойчивости к помехам. Узкополосная помеха будет искажать только определенные частоты спектра сигнала, так что приемник с большой степенью вероятности сможет правильно распознать передаваемую информацию.

Код, которым заменяется двоичная единица исходной информации, называется расширяющей последовательностью, а каждый бит такой последовательности - чипом. Соответственно, скорость передачи результирующего кода называют **чиповой скоростью**. Двоичный нуль кодируется инверсным значением расширяющей последовательности. Приемники должны знать расширяющую последовательность, которую использует передатчик, чтобы понять передаваемую информацию.

Количество битов в расширяющей последовательности определяет коэффициент расширения исходного кода. Как и в случае FHSS, для кодирования битов результирующего кода может использоваться любой вид модуляции, например BFSK. Чем больше коэффициент расширения, тем шире спектр результирующего сигнала и выше степень подавления помех. Но при этом растет занимаемый каналом диапазон спектра. Обычно коэффициент расширения имеет значение от 10 до 100.

Пример 1

Очень часто в качестве значения расширяющей последовательности берут последовательность Баркера (*Barker*), которая состоит из 11 бит: 10110111000. Если передатчик использует эту последовательность, то передача трех битов 110 ведет к передаче следующих битов: 10110111000 10110111000 01001000111.

Последовательность Баркера позволяет приемнику быстро синхронизироваться с передатчиком, то есть надежно выявлять начало последовательности. Приемник определяет такое событие, поочередно сравнивая получаемые биты с образцом последовательности. Действительно, если сравнить последовательность Баркера с такой же последовательностью, но сдвинутой на один бит влево или вправо, мы получим меньше половины совпадений значений битов. Значит, даже при искажении нескольких битов с большой долей вероятности приемник правильно определит начало последовательности, а значит, сможет правильно интерпретировать получаемую информацию.

Метод DSSS в меньшей степени защищен от помех, чем метод быстрого расширения спектра, так как мощная узкополосная помеха влияет на часть спектра, а значит, и на результат распознавания единиц или нулей.

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, в том числе и в России, каналы шириной 22 МГц позволяют создать в диапазоне 2,4- 2,473 ГГц три неперекрывающихся канала передачи. Эти каналы показаны на **рис. 5.6**.

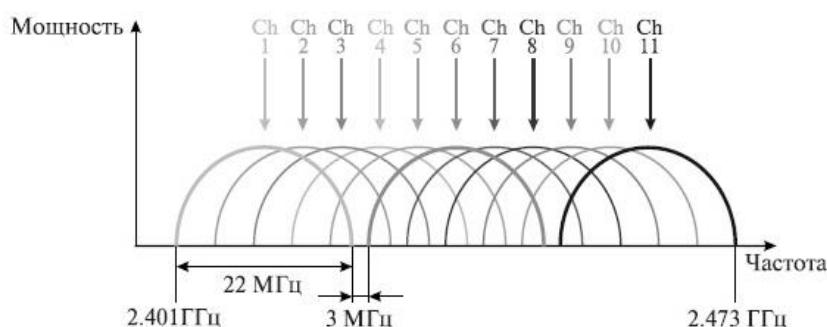


Рис. 5.6. Каналы, используемые в технологии DSSS

Кодирование и защита от ошибок

Существует три наиболее распространенных орудия борьбы с ошибками в процессе передачи данных:

- коды обнаружения ошибок;
- коды с коррекцией ошибок, называемые также схемами прямой коррекции ошибок (*Forward Error Correction - FEC*);
- протоколы с автоматическим запросом повторной передачи (*Automatic Repeat Request - ARQ*).

Код обнаружения ошибок позволяет довольно легко установить наличие ошибки. Как правило, подобные коды используются совместно с определенными протоколами канального или транспортного уровней, имеющими схему ARQ. В схеме ARQ приемник попросту отклоняет блок данных, в котором была обнаружена ошибка, после чего передатчик передает этот блок повторно. Коды с прямой коррекцией ошибок позволяют не только обнаружить ошибки, но и исправить их, не прибегая к повторной передаче. Схемы FEC часто используются в беспроводной передаче, где повторная передача крайне неэффективна, а уровень ошибок довольно высок.

1) методы обнаружения ошибок

Методы обнаружения ошибок основаны на передаче в составе блока данных избыточной служебной информации, по которой можно судить с некоторой степенью вероятности о достоверности принятых данных.

Избыточную служебную информацию принято называть контрольной суммой, или контрольной последовательностью кадра (*Frame Check Sequence, FCS*). Контрольная сумма вычисляется как функция от основной информации, причем не обязательно путем суммирования. Принимающая сторона повторно вычисляет контрольную сумму кадра по известному алгоритму и в случае ее совпадения с контрольной суммой, вычисленной передающей стороной, делает вывод о том, что данные были переданы через сеть корректно. Рассмотрим наиболее распространенные алгоритмы вычисления контрольной суммы, отличающиеся вычислительной сложностью и способностью обнаруживать ошибки в данных.

Контроль по паритету представляет собой наиболее простой метод контроля данных. В то же время это наименее мощный алгоритм контроля, так как с его помощью можно обнаружить только одиночные ошибки в проверяемых данных. Метод заключается в суммировании по модулю 2 всех битов контролируемой информации. Нетрудно заметить, что для информации, состоящей из нечетного числа единиц, контрольная сумма всегда равна 1, а при четном числе единиц - 0. Например, для данных 100101011 результатом контрольного суммирования будет значение 1. Результат суммирования также представляет собой один дополнительный бит данных, который пересыпается вместе с контролируемой информацией. При искажении в процессе пересылки любого бита исходных данных (или контрольного разряда) результат суммирования будет отличаться от принятого контрольного разряда, что говорит об ошибке. Однако двойная ошибка, например 110101010, будет неверно принята за корректные данные. Поэтому контроль по паритету применяется к небольшим порциям данных, как правило, к каждому байту, что дает коэффициент избыточности для этого метода 1/8. Метод редко применяется в компьютерных сетях из-за значительной избыточности и невысоких диагностических способностей.

Вертикальный и горизонтальный контроль по паритету представляет собой модификацию описанного выше метода. Его отличие состоит в том, что исходные данные рассматриваются в виде матрицы, строки которой составляют байты данных. Контрольный разряд подсчитывается отдельно для каждой строки и для каждого столбца матрицы. Этот метод обнаруживает значительную часть двойных ошибок, однако обладает еще большей избыточностью. Он сейчас также почти не применяется при передаче информации по сети.

Циклический избыточный контроль (*Cyclic Redundancy Check - CRC*) является в настоящее время наиболее популярным методом контроля в вычислительных сетях (и не только в сетях; в частности, этот метод широко применяется при записи данных на гибкие и жесткие диски). Метод основан на рассмотрении исходных данных в виде одного многоразрядного двоичного числа. Например, кадр стандарта Ethernet, состоящий из 1024 байт, будет рассматриваться как одно число, состоящее из 8192 бит. Контрольной информацией считается остаток от деления этого числа на известный делитель R . Обычно в качестве делителя выбирается 17- или 33-разрядное число, чтобы остаток от деления имел длину 16 разрядов (2 байт) или 32 разряда (4 байт). При получении кадра данных снова вычисляется остаток от деления на тот же делитель R , но при этом к данным кадра добавляется и содержащаяся в нем контрольная сумма. Если остаток от деления на R равен нулю, то делается вывод об отсутствии ошибок в полученном кадре, в противном случае кадр считается искаженным.

Этот метод обладает более высокой вычислительной сложностью, но его диагностические возможности гораздо шире, чем у методов контроля по паритету. Метод CRC обнаруживает все одиночные ошибки, двойные ошибки и ошибки в нечетном числе битов. Метод также обладает невысокой степенью избыточности. Например, для кадра Ethernet размером 1024 байта контрольная информация длиной 4 байта составляет только 0,4 %.

2) методы коррекции ошибок

Техника кодирования, которая позволяет приемнику не только понять, что присланные данные содержат ошибки, но и исправить их, называется прямой коррекцией ошибок (*Forward Error Correction - FEC*). Коды, обеспечивающие прямую коррекцию ошибок, требуют введения большей избыточности в передаваемые данные, чем коды, которые только обнаруживают ошибки.

При применении любого избыточного кода не все комбинации кодов являются разрешенными. Например, контроль по паритету делает разрешенными только половину кодов. Если контролируют три информационных бита, то разрешенными 4-битными кодами с дополнением до нечетного количества единиц будут:

000 1, 001 0, 010 0, 011 1, 100 0, 101 1, 110 1, 111 0, то есть всего 8 кодов из 16 возможных.

Для того чтобы оценить количество дополнительных битов, необходимых для исправления ошибок, нужно знать так называемое расстояние Хемминга между разрешенными комбинациями кода. Расстоянием Хемминга называется минимальное число битовых разрядов, в которых отличается любая пара разрешенных кодов. Для схем контроля по паритету расстояние Хемминга равно 2.

Можно доказать, что если построить избыточный код с расстоянием Хемминга, равным n , такой код будет в состоянии распознавать $(n-1)$ -кратные ошибки и исправлять $(n-1)/2$ -кратные ошибки. Так как коды с контролем по паритету имеют расстояние Хемминга, равное 2, они могут только обнаруживать однократные ошибки и не могут исправлять ошибки.

Коды Хемминга эффективно обнаруживают и исправляют изолированные ошибки, то есть отдельные искаженные биты, которые разделены большим количеством корректных битов. Однако при появлении длинной последовательности искаженных битов (пульсации ошибок) коды Хемминга не работают.

Наиболее часто в современных системах связи применяется тип кодирования, реализуемый сверточным кодирующим устройством (*Convolutional coder*), потому что такое кодирование несложно реализовать 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*). Для сверточного кода с коэффициентом кодирования 1/2, коэффициент указывает, что на каждый входной бит приходится два выходных. Можно отметить, что, хотя коды с более высокой эффективной степенью кодирования позволяют передавать данные с более высокой скоростью, они более чувствительны к шуму.

В беспроводных системах с блочными кодами широко используется метод чередования блоков. Преимущество чередования состоит в том, что приемник распределяет пакет ошибок, исказивший некоторую последовательность битов, по большому числу блоков, благодаря чему становится возможным исправление ошибок. Чередование выполняется с помощью чтения и записи данных в различном порядке. Если во время передачи пакет помех воздействует на некоторую последовательность битов, то все эти биты оказываются разнесенными по различным блокам. Следовательно, от любой контрольной последовательности требуется возможность исправить лишь небольшую часть от общего количества инвертированных битов.

3) методы автоматического запроса повторной передачи

В простейшем случае защита от ошибок заключается только в их обнаружении. Система должна предупредить передатчик об обнаружении ошибки и необходимости повторной передачи. Такие процедуры защиты от ошибок известны как методы автоматического запроса повторной передачи (*Automatic Repeat Request - ARQ*). В беспроводных локальных сетях применяется процедура "запрос ARQ с остановками" (*stop-and-wait ARQ*).

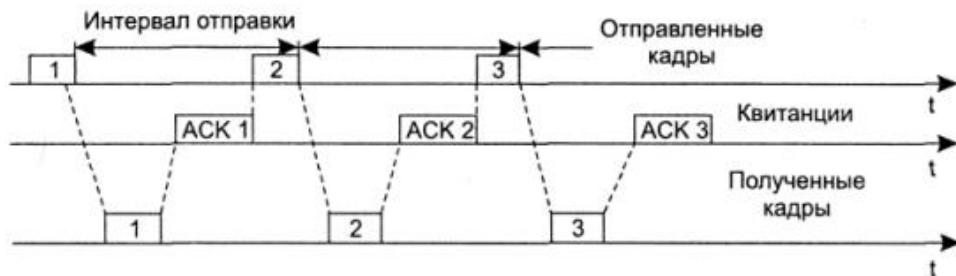


Рис. 5.7. Процедура запрос ARQ с остановками

В этом случае источник, пославший кадр, ожидает получения подтверждения (*Acknowledgement - ACK*), или, как еще его называют, квитанции, от приемника и только после этого посыпает следующий кадр. Если же подтверждение не приходит в течение тайм-аута, то кадр (или подтверждение) считается утерянным и его передача повторяется. На **рис. 5.7** видно, что в этом случае производительность обмена данными ниже

потенциально возможной; хотя передатчик и мог бы послать следующий кадр сразу же после отправки предыдущего, он обязан ждать прихода подтверждения.

Архитектура IEEE 802.11

IEEE (Institute of Electrical and Electronics Engineers) 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 Мбит/с. 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.

Стек протоколов IEEE 802.11

Стек протоколов стандарта *IEEE 802.11* соответствует общей структуре стандартов комитета 802, то есть состоит из физического уровня и канального уровня с подуровнями управления доступом к среде MAC (*Media Access Control*) и логической передачи данных LLC (*Logical Link Control*). Как и у всех технологий семейства 802, технология 802.11 определяется двумя нижними уровнями, то есть физическим уровнем и уровнем MAC, а уровень LLC выполняет свои стандартные общие для всех технологий LAN функции (рис. 2.1).

На физическом уровне существует несколько вариантов спецификаций, которые отличаются используемым частотным диапазоном, методом кодирования и как следствие - скоростью передачи данных. Все варианты физического уровня работают с одним и тем же алгоритмом уровня MAC, но некоторые временные параметры уровня MAC зависят от используемого физического уровня.

Уровень доступа к среде стандарта 802.11

В сетях 802.11 уровень MAC обеспечивает два режима доступа к *разделяемой среде* (рис. 5.8):

- распределенный режим DCF (Distributed Coordination Function);
- централизованный режим PCF (Point Coordination Function).

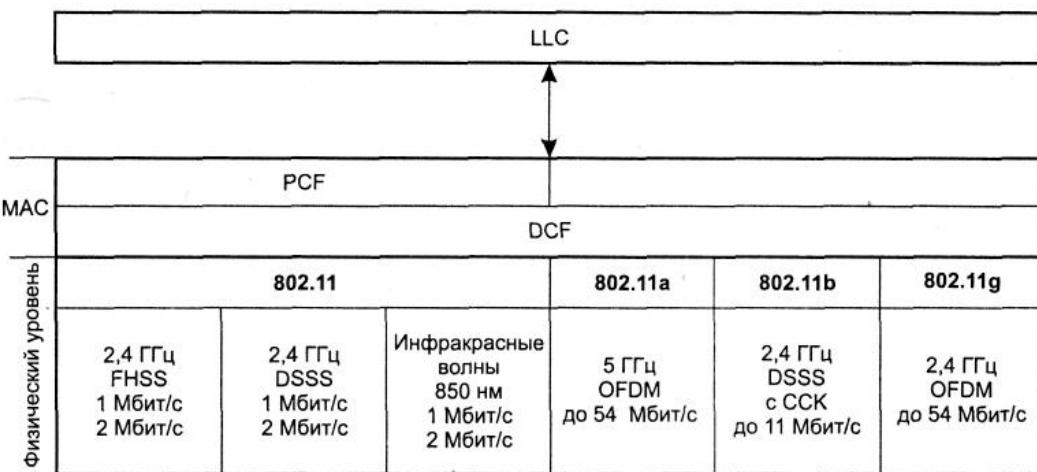


Рис. 5.8. Стек протоколов IEEE 802.11

1) распределенный режим доступа DCF

В этом режиме реализуется метод *множественного доступа с контролем несущей и предотвращением коллизий* (*Carrier Sense Multiple Access with Collision Avoidance* - CSMA/CA). Вместо неэффективного в беспроводных сетях прямого распознавания коллизий по методу CSMA/CD здесь используется их косвенное выявление. Для этого каждый переданный кадр должен подтверждаться кадром положительной квитанции, посыпаемым станцией назначения. Если же по истечении оговоренного тайм-аута квитанция не поступает, станция-отправитель считает, что произошла коллизия.

Режим доступа DCF требует синхронизации станций. В спецификации 802.11 эта проблема решается достаточно элегантно - временные интервалы начинают отсчитываться от момента окончания передачи очередного кадра (рис. 5.9). Это не требует передачи каких-либо специальных синхронизирующих сигналов и не ограничивает размер пакета размером слота, так как слоты принимаются во внимание только при принятии решения о начале передачи кадра.

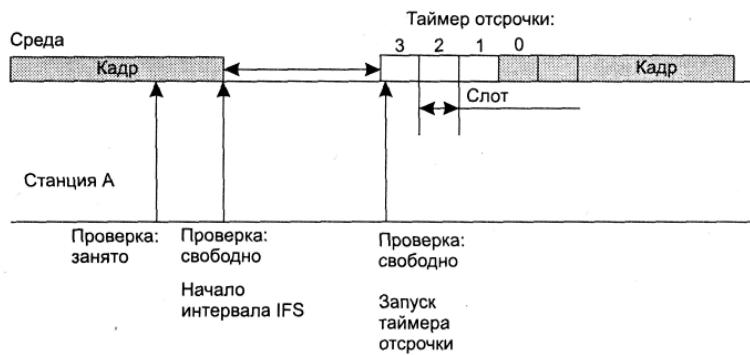


Рис. 5.9. Режим доступа DCF

Станция, которая хочет передать кадр, обязана предварительно прослушать среду. Стандарт IEEE 802.11 предусматривает два механизма контроля активности в канале (обнаружения несущей): *физический* и *виртуальный*. Первый механизм реализован на физическом уровне и сводится к определению уровня сигнала в антенну и сравнению его с пороговой величиной. Виртуальный механизм обнаружения несущей основан на том, что в передаваемых кадрах данных, а также в управляющих кадрах ACK и RTS/CTS содержится информация о времени, необходимом для передачи пакета (или группы пакетов) и получения подтверждения. Все устройства сети получают информацию о текущей передаче и могут определить, сколько времени канал будет занят, т.е. устройство при установлении связи сообщает всем, на какое время оно резервирует канал. Как только станция фиксирует окончание передачи кадра, она обязана отсчитать интервал времени, равный межкадровому интервалу (IFS). Если после истечения IFS среда все еще свободна, начинается отсчет слотов фиксированной длительности. Кадр можно передавать только в начале какого-либо из слотов при условии, что среда свободна. Станция выбирает для передачи слот на основании усеченного экспоненциального двоичного алгоритма отсрочки, аналогичного используемому в методе CSMA/CD. Номер слота выбирается как случайное целое число, равномерно распределенное в интервале $[0, CW]$, где "CW" означает "*Competition Window*" (конкурентное окно).

Рассмотрим этот довольно непростой метод доступа на примере рис. 2.2. Пусть станция A выбрала для передачи на основании усеченного экспоненциального двоичного алгоритма отсрочки слот 3. При этом она присваивает таймеру отсрочки (назначение которого будет ясно из дальнейшего описания) значение 3 и начинает проверять состояние среды в начале каждого слота. Если среда свободна, то из значения таймера отсрочки вычитается 1, и если результат равен нулю, начинается передача кадра. Таким образом, обеспечивается условие незанятости всех слотов, включая выбранный. Это условие является необходимым для начала передачи.

Если же в начале какого-нибудь слота среда оказывается занятой, то вычитания единицы не происходит, и таймер "замораживается". В этом случае станция начинает новый цикл доступа к среде, изменяя только алгоритм выбора слота для передачи. Как и в предыдущем цикле, станция следит за средой и при ее освобождении делает паузу в течение межкадрового интервала. Если среда осталась свободной, то станция использует значение "замороженного" таймера в качестве номера слота и выполняет описанную выше процедуру проверки свободных слотов с вычитанием единиц, начиная с замороженного значения таймера отсрочки.

Размер слота зависит от способа кодирования сигнала; так, для метода FHSS размер слота равен 28 мкс, а для метода DSSS - 1 мкс. Размер слота выбирается таким образом, чтобы он превосходил время распространения сигнала между любыми двумя станциями сети плюс время, затрачиваемое станцией на распознавание занятости среды. Если такое условие соблюдается, то каждая станция сети сумеет правильно распознать начало передачи кадра при прослушивании слотов, предшествующих выбранному ею для передачи слоту. Это, в свою очередь, означает следующее.

Коллизия может иметь место только в том случае, когда несколько станций выбирают один и тот же слот для передачи.

В этом случае кадры искажаются, и квитанции от станций назначения не приходят. Не получив в течение определенного времени квитанцию, отправители фиксируют факт коллизии и пытаются передать свои кадры снова. При каждой повторной неудачной попытке передачи кадра интервал $[0, CW]$, из которого выбирается номер слота, удваивается. Если, например, начальный размер окна выбран равным 8 (то есть $CW = 7$), то после первой коллизии размер окна должен быть равен 16 ($CW = 15$), после второй последовательной коллизии - 32 и т. д. Начальное значение CW, в соответствии со стандартом 802.11, должно выбираться в зависимости от типа физического уровня, используемого в беспроводной локальной сети.

Как и в методе CSMA/CD, в данном методе количество неудачных попыток передачи одного кадра ограничено, но стандарт 802.11 не дает точного значения этого верхнего предела. Когда верхний предел в N

попыток достигнут, кадр отбрасывается, а счетчик последовательных коллизий устанавливается в ноль. Этот счетчик также устанавливается в ноль, если кадр после некоторого количества неудачных попыток все же передается успешно.

В беспроводных сетях возможна ситуация, когда два устройства (A и B) удалены и не слышат друг друга, однако оба попадают в зону охвата третьего устройства C (рис. 5.10) - так называемая проблема скрытого терминала. Если оба устройства A и B начнут передачу, то они принципиально не смогут обнаружить конфликтную ситуацию и определить, почему пакеты не проходят.



Рис. 5.10. Проблема скрытого терминала

В режиме доступа DCF применяются меры для устранения эффекта скрытого терминала. Для этого станция, которая хочет захватить среду и в соответствии с описанным алгоритмом начинает передачу кадра в определенном слоте, вместо кадра данных сначала посыпает станции назначения короткий служебный кадр *RTS* (*Request To Send* - запрос на передачу). На этот запрос станция назначения должна ответить служебным кадром *CTS* (*Clear To Send* - свободна для передачи), после чего станция-отправитель посыпает кадр данных. Кадр *CTS* должен оповестить о захвате среды те станции, которые находятся вне зоны сигнала станции-отправителя, но в зоне досягаемости станции-получателя, то есть являются скрытыми терминалами для станции-отправителя.

Максимальная длина кадра данных 802.11 равна 2346 байт, длина *RTS*-кадра - 20 байт, *CTS*-кадра - 14 байт. Так как *RTS*- и *CTS*-кадры гораздо короче, чем кадр данных, потери данных в результате коллизии *RTS*- или *CTS*-кадров гораздо меньше, чем при коллизии кадров данных. Процедура обмена *RTS*- и *CTS*-кадрами не обязательна. От нее можно отказаться при небольшой нагрузке сети, поскольку в такой ситуации коллизии случаются редко, а значит, не стоит тратить дополнительное время на выполнение процедуры обмена *RTS*- и *CTS*-кадрами.

При помехах иногда случается, что теряются большие фреймы данных, поэтому можно уменьшить длину этих фреймов путем *фрагментации*. 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. 5.11).

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, передавать повторно придется только его, а не весь фрейм. Это увеличивает пропускную способность среды.



Рис. 5.11. Фрагментация фрейма

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

Хотя за счет фрагментации можно повысить надежность передачи фреймов в беспроводных локальных сетях, она приводит к увеличению "накладных расходов" MAC-протокола стандарта 802.11. Каждый фрагмент

фрейма включает информацию, 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.

2) централизованный режим доступа PCF

В том случае, когда в сети имеется станция, выполняющая функции точки доступа, может также применяться централизованный *режим доступа PCF*, обеспечивающий приоритетное обслуживание трафика. В этом случае говорят, что точка доступа играет роль арбитра среды.

Режим доступа PCF в сетях 802.11 существует с режимом DCF. Оба режима координируются с помощью трех типов межкадровых интервалов (рис. 5.12).

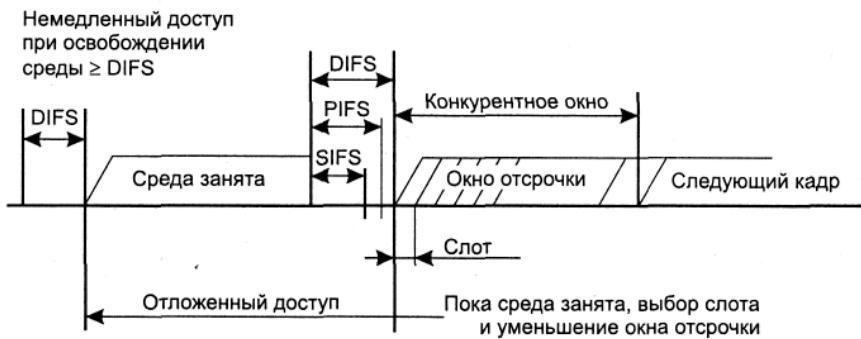


Рис. 5.12. Сосуществование режимов PCF и DCF

После освобождения среды каждая станция отсчитывает время простоя среды, сравнивая его с тремя значениями:

- короткий межкадровый интервал (*Short IFS* - *SIFS*);
- межкадровый интервал режима PCF (*PIFS*);
- межкадровый интервал режима DCF (*DIFS*).

Захват среды с помощью распределенной процедуры *DCF* возможен только в том случае, когда среда свободна в течение времени, равного или большего, чем *DIFS*. То есть в качестве *IFS* в режиме *DCF* нужно использовать интервал *DIFS* - самый длительный период из трех возможных, что дает этому режиму самый низкий приоритет.

Межкадровый интервал *SIFS* имеет наименьшее значение, он служит для первоочередного захвата среды ответными *CTS*-кадрами или квитанциями, которые продолжают или завершают уже начавшуюся передачу кадра.

Значение межкадрового интервала *PIFS* больше, чем *SIFS*, но меньше, чем *DIFS*. Промежутком времени между завершением *PIFS* и *DIFS* пользуется арбитр среды. В этом промежутке он может передать специальный кадр, который говорит всем станциям, что начинается контролируемый период. Получив этот кадр, станции, которые хотели бы воспользоваться алгоритмом *DCF* для захвата среды, уже не могут этого сделать, они должны дожидаться окончания контролируемого периода. Его длительность объявляется в специальном кадре, но этот период может закончиться и раньше, если у станций нет чувствительного к задержкам трафика. В этом случае арбитр передает служебный кадр, после которого по истечении интервала *DIFS* начинает работать режим *DCF*.

На управляемом интервале реализуется *централизованный метод доступа PCF*. Арбитр выполняет процедуру опроса, чтобы по очереди предоставить каждой такой станции право на использование среды, направляя ей специальный кадр. Станция, получив такой кадр, может ответить другим кадром, который подтверждает прием специального кадра и одновременно передает данные (либо по адресу арбитра для транзитной передачи, либо непосредственно станции).

Для того чтобы какая-то доля среды всегда доставалась асинхронному трафику, длительность контролируемого периода ограничена. После его окончания арбитр передает соответствующий кадр и начинается неконтролируемый период.

Каждая станция может работать в режиме PCF, для этого она должна подписать на данную услугу при присоединении к сети.

Кадр MAC-подуровня

На рис. 5.13 изображен формат кадра 802.11. Приведенная общая структура применяется для всех информационных и управляющих кадров, хотя не все поля используются во всех случаях.

2	2	6	6	6	2	6	0-2312	4 октеты
FC	D/I	Адрес	Адрес	Адрес	SC	Адрес	Тело кадра	CRC

FC — управление кадром
 D/I — идентификатор длительности/соединения
 SC — управление очередностью

Рис. 5.13. Формат кадра MAC IEEE 802.11

Перечислим поля общего кадра:

- *Управление кадром.* Указывается тип кадра и предоставляется управляющая информация.
- *Идентификатор длительности/соединения.* Если используется поле длительности, указывается время (в микросекундах), на которое требуется выделить канал для успешной передачи кадра MAC. В некоторых кадрах управления в этом поле указывается идентификатор ассоциации или соединения.
- *Адреса.* Число и значение полей адреса зависит от контекста. Возможны следующие типы адреса: источника, назначения, передающей станции, принимающей станции.
- *Управление очередностью.* Содержит 4-битовое подполе номера фрагмента, используемое для фрагментации и повторной сборки, и 12-битовый порядковый номер, используемый для нумерации кадров, передаваемых между приемником и передатчиком.
- *Тело кадра.* Содержит модуль данных протокола LLC или управляющую информацию MAC.
- *Контрольная последовательность кадра.* 32-битовая проверка четности с избыточностью.

Поле управления кадром, показанное на **рис. 5.14**, состоит из следующих полей:

- *Версия протокола.* Версия 802.11, текущая версия - 0.
- *Тип.* Определим тип кадра: контроль, управление или данные.
- *Подтип.* Дальнейшая идентификация функций кадра. Разрешенные сочетания типов и подтипов перечислены в **таблице 5.1**.

Таблица 5.1. Разрешенные комбинации типа и подтипа

Значение типа	Описание типа	Значение подтипа	Описание подтипа
00	Управление	0000	Запрос ассоциации
00	Управление	0001	Ответ на запрос ассоциации
00	Управление	0010	Запрос повторной ассоциации
00	Управление	0011	Ответ на запрос повторной ассоциации
00	Управление	0100	Пробный запрос
00	Управление	0101	Ответ на пробный запрос
00	Управление	1000	Сигнальный кадр
00	Управление	1001	Объявление наличия трафика
00	Управление	1010	Разрыв ассоциации
00	Управление	1011	Аутентификация
00	Управление	1100	Отмена аутентификации
01	Контроль	1010	PS-опрос
01	Контроль	1011	Запрос передачи
01	Контроль	1100	"Готов к передаче"
01	Контроль	1101	Подтверждение
01	Контроль	1110	Без состязания (CF)-конец
01	Контроль	1111	CF-конец + CF-подтверждение
10	Данные	0000	Данные
10	Данные	0001	Данные + CF-подтверждение
10	Данные	0010	Данные + CF-опрос
10	Данные	0011	Данные + CF-подтверждение + CF-опрос
10	Данные	0100	Нулевая функция (без данных)
10	Данные	0101	Данные + CF-подтверждение
10	Данные	0110	Данные + CF-опрос
10	Данные	0111	Данные + CF-подтверждение + CF-опрос

- *K DS*. Координационная функция MAC присваивает этому биту значение 1, если кадр предназначен распределительной системе.

- *От DS*. Координационная функция MAC присваивает этому биту значение 0, если кадр исходит от распределительной системы.

- *Больше фрагментов*. 1, если за данным фрагментом следует еще несколько.

- *Повтор*. 1, если данный кадр является повторной передачей предыдущего.

- *Управление мощностью*. 1, если передающая станция находится в режиме ожидания.

- *Больше данных*. Указывает, что станция передала не все данные. Каждый блок данных может передаваться как один кадр или как группа фрагментов в нескольких кадрах.

- *WEP*. 1, если реализован алгоритм конфиденциальности проводного эквивалента (*Wired Equivalent Privacy - WEP*). Протокол *WEP* используется для обмена ключами шифрования при безопасном обмене данными.

- *Порядок*. 1, если используется услуга строгого упорядочения, указывающая адресату, что кадры должны обрабатываться строго по порядку.

2	2	4	1	1	1	1	1	1	1	1	октеты
Версия протокола	Тип	Подтип	к DS	от DS	MF	RT	PM	MD	W	О	

DS — система распределения
 MF — больше фрагментов
 RT — повтор
 PM — управление мощностью
 MD — больше данных
 W — бит защиты проводного эквивалента
 0 — порядок

Рис. 5.14. Поле управления кадром

Рассмотрим теперь различные типы кадров MAC.

Контрольные кадры

Контрольные кадры способствуют надежной доставке информационных кадров. Существует шесть подтипов контрольных кадров:

- *Опрос после выхода из экономичного режима (PS-опрос)*. Данный кадр передается любой станцией станции, включающей точку доступа. В кадре запрашивается передача кадра, прибывшего, когда станция находилась в режиме энергосбережения, и в данный момент размещенного в буфере точки доступа.

- *Запрос передачи (RTS)*. Данный кадр является первым из четверки, используемой для обеспечения надежной передачи данных. Станция, пославшая это сообщение, предупреждает адресата и остальные станции, способные принять данное сообщение, о своей попытке передать адресату информационный кадр.

- *"Готов к передаче" (CTS)*. Второй кадр четырехкадровой схемы. Передается станцией-адресатом станции-источнику и предоставляет право отправки информационного кадра.

- *Подтверждение (ACK)*. Подтверждение успешного приема предыдущих данных, кадра управления или кадра "PS-опрос".

- *Без состязания (CF-конец)*. Объявляет конец периода без состязания; часть стратегии использования распределенного режима доступа.

- *CF-конец + CF-подтверждение*. Подтверждает кадр "CF-конец". Данный кадр завершает период без состязания и освобождает станции от ограничений, связанных с этим периодом.

Информационные кадры

Существует восемь подтипов информационных кадров, собранных в две группы. Первые четыре подтипа определяют кадры, переносящие данные высших уровней от исходной станции к станции-адресату. Перечислим эти кадры:

- *Данные*. Просто информационный кадр. Может использоваться как в период состязания, так и в период без состязания.

- *Данные + CF-подтверждение*. Может передаваться только в период без состязания. Помимо данных, в этом кадре имеется подтверждение полученной ранее информации.

- *Данные + CF-опрос*. Используется точечным координатором для доставки данных к мобильной станции и для запроса у мобильной станции информационного кадра, который находится в ее буфере.

- *Данные + CF-подтверждение + CF-опрос*. Объединяет в одном кадре функции двух описанных выше кадров.

Остальные четыре подтипа информационных кадров фактически не переносят данные пользователя. Информационный кадр "нулевая функция" не переносит ни данных, ни запросов, ни подтверждений. Он

используется только для передачи точке доступа бита управления питанием в поле управления кадром, указывая, что станция перешла в режим работы с пониженным энергопотреблением. Оставшиеся три кадра (CF-подтверждение, CF-опрос, CF-подтверждение + CF-опрос) имеют те же функции, что и описанные выше подтипы кадров (данные + CF-подтверждение, данные + CF-опрос, данные + CF-подтверждение + CF-опрос), но не несут пользовательских данных.

Кадры управления

Кадры управления используются для управления связью станций и точек доступа. Возможны следующие подтипы:

- *Запрос ассоциации.* Посыпается станцией к точке доступа с целью запроса ассоциации с данной сетью с базовым набором услуг (*Basic Service Set - BSS*). Кадр включает информацию о возможностях, например, будет ли использоваться шифрование, или способна ли станция отвечать при опросе.
- *Ответ на запрос ассоциации.* Возвращается точкой доступа и указывает, что запрос ассоциации принят.
- *Запрос повторной ассоциации.* Посыпается станцией при переходе между *BSS*, когда требуется установить ассоциацию с точкой доступа в новом *BSS*. Использование повторной ассоциации, а не просто ассоциации, позволяет новой точке доступа договариваться со старой о передаче информационных кадров по новому адресу.
- *Ответ на запрос повторной ассоциации.* Возвращается точкой доступа и указывает, что запрос повторной ассоциации принят.
- *Пробный запрос.* Используется станцией для получения информации от другой станции или точки доступа. Кадр используется для локализации *BSS* стандарта *IEEE 802.11*.
- *Ответ на пробный запрос.* Отклик на пробный запрос.
- *Сигнальный кадр.* Передается периодически, позволяет мобильным станциям локализовать и идентифицировать *BSS*.
- *Объявление наличия трафика.* Посыпается мобильной станцией с целью уведомления других (которые могут находиться в режиме пониженного энергопотребления), что в *буфере данной* станции находятся кадры, адресованные другим.
- *Разрыв ассоциации.* Используется станцией для *аннулирования* ассоциации.
- *Аутентификация.* Для аутентификации станций используются множественные кадры.
- *Отмена аутентификации.* Передается для прекращения безопасного соединения.

Стандарты IEEE 802.11

Из всех существующих стандартов беспроводной передачи данных *IEEE 802.11* на практике чаще всего используются всего три стандарта, определенные Инженерным институтом электротехники и радиоэлектроники (*IEEE*): *802.11b*, *802.11a* и *802.11g*.

В стандарте *IEEE 802.11b* благодаря высокой скорости передачи данных (до 11 Мбит/с), практически эквивалентной пропускной способности обычных проводных локальных сетей *Ethernet*, а также ориентации на диапазон 2,4 ГГц, этот стандарт завоевал наибольшую популярность у производителей оборудования для беспроводных сетей.

Поскольку оборудование, работающее на максимальной скорости 11 Мбит/с, имеет меньший *радиус действия*, чем на более низких скоростях, стандартом *802.11b* предусмотрено автоматическое снижение скорости при ухудшении качества сигнала.

Стандарт *IEEE 802.11a* имеет большую ширину полосы из семейства стандартов *802.11* при скорости передачи данных до 54 Мбит/с.

В отличие от базового стандарта, ориентированного на область частот 2,4 ГГц, спецификациями *802.11a* предусмотрена работа в диапазоне 5 ГГц. В качестве *метода модуляции* сигнала выбрано ортогональное частотное мультиплексирование (*OFDM*).

К недостаткам *802.11a* относятся более высокая потребляемая *мощность* радиопередатчиков для частот 5 ГГц, а также меньший *радиус действия*.

Стандарт *IEEE 802.11g* является логическим развитием *802.11b* и предполагает передачу данных в том же частотном диапазоне. Кроме того, стандарт *802.11g* полностью совместим с *802.11b*, то есть любое устройство *802.11g* должно поддерживать работу с устройствами *802.11b*. Максимальная *скорость передачи* в стандарте *802.11g* составляет 54 Мбит/с, поэтому на сегодня это наиболее перспективный стандарт беспроводной связи.

При разработке стандарта 802.11g рассматривались две отчасти конкурирующие технологии: метод ортогонального частотного разделения *OFDM* и метод двоичного пакетного сверточного кодирования *PBCC*, дополнительно реализованный в стандарте 802.11b. В результате стандарт 802.11g содержит компромиссное решение: в качестве базовых применяются технологии *OFDM* и *CCK*, а дополнительно предусмотрено использование технологии *PBCC*. О технологиях *CCK* и *OFDM* мы расскажем чуть позже.

Набор стандартов 802.11 определяет *целый* ряд технологий реализации физического уровня (*Physical Layer Protocol* - *PHY*), которые могут быть использованы подуровнем 802.11 *MAC*. В этой главе рассматривается каждый из уровней *PHY*:

- Уровень *PHY* стандарта 802.11 со скачкообразной перестройкой частоты (*FHSS*) в диапазоне 2,4 ГГц.
- Уровень *PHY* стандарта 802.11 с расширением спектра методом прямой последовательности (*DSSS*) в диапазоне 2,4 ГГц.
- Уровень *PHY* стандарта 802.11b с комплементарным кодированием в диапазоне 2,4 ГГц.
- Уровень *PHY* стандарта 802.11a с ортогональным частотным мультиплексированием (*OFDM*) в диапазоне 5 ГГц.
- *Расширенный физический уровень* (*Extended Rate Physical Layer* - *ERP*) стандарта 802.11g в диапазоне 2,4 ГГц.

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*. Уровни *MAC* и *PHY* разрабатывались так, чтобы они были независимыми. Именно независимость между *MAC* и подуровнем *PHY* 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. 5.15** показано, как эти подуровни соотносятся между собой и с вышестоящими уровнями в *модели взаимодействия открытых систем* (*Open System Interconnection* - *OSI*).

Подуровень *PLCP* по существу является уровнем обеспечения взаимодействия, 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. Подуровни *PLCP* и *PMD* отличаются для разных вариантов стандарта 802.11.

Перед тем как приступить к изучению физических уровней, рассмотрим одну из составляющих физического уровня, до сих пор не упомянутую, а именно - скремблирование.

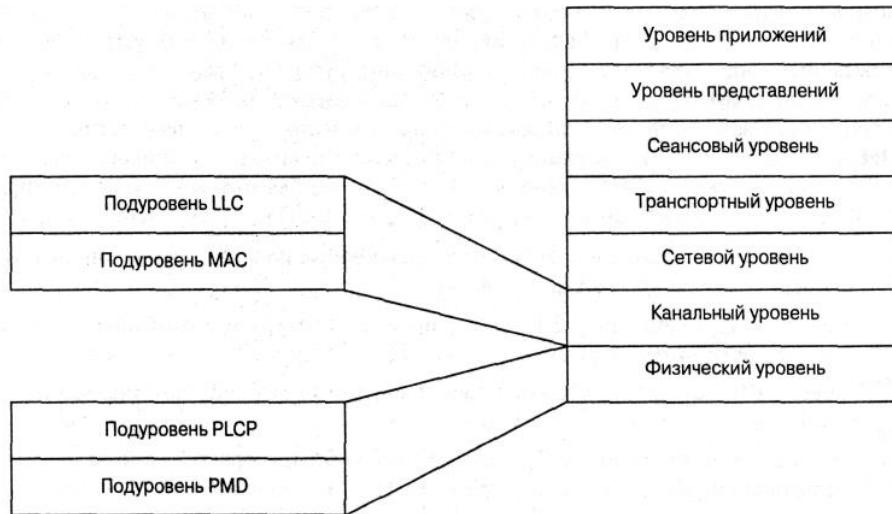


Рис. 5.15. Подуровни уровня *PHY*

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 бывает, 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 "отбеливанием потока данных". Дескремблер приемника затем выполняет *обратное преобразование* этой случайной последовательности с целью получения исходной структурированной последовательности. Большинство способов скремблирования относится к числу самосинхронизирующихся; это означает, что дескремблер способен самостоятельно синхронизироваться со скремблером.

IEEE 802.11

Исходный стандарт 802.11 определяет три метода передачи на физическом уровне:

- передача в диапазоне инфракрасных волн;
- 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.

Передача в диапазоне инфракрасных волн

Средой передачи являются инфракрасные волны диапазона 850 нм, которые генерируются либо полупроводниковым лазерным диодом, либо светодиодом (LED). Так как инфракрасные волны не проникают через стены, область покрытия LAN ограничивается зоной прямой видимости. Стандарт предусматривает три варианта распространения излучения: *ненаправленную антенну*, отражение от потолка и фокусное направленное излучение. В первом случае узкий луч рассеивается с помощью системы линз. Фокусное направленное излучение предназначено для организации двухточечной связи, например между двумя зданиями.

Беспроводные локальные сети со скачкообразной перестройкой частоты (FHSS)

Беспроводные локальные сети FHSS поддерживают скорости передачи 1 и 2 Мбит/с. 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.

Последовательность перестройки частоты должна иметь следующие параметры: частота перескоков не менее 2,5 раз в секунду как минимум между шестью (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 **таблице 5.2** представлены схемы скачкообразной перестройки частоты, обеспечивающие минимальное перекрытие.

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.

Таблица 5.2. 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	{2,5,8,11,14,17,20,23,26,29,32,35,38,41,44,47,50,53,56,59,62,65,68,71,74,77}

После того как уровень MAC пропускает MAC-фрейм, который в локальных беспроводных сетях FHSS называется также служебным элементом данных PLCP, или PSDU (PLCP Service Data Unit), подуровень PLCP добавляет два поля в начало фрейма, чтобы сформировать таким образом фрейм PPDU (PPDU - элемент данных протокола PLCP). На **рис. 5.16** представлен формат фрейма FHSS подуровня PLCP.

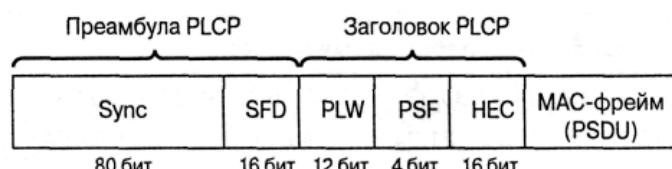


Рис. 5.16. Формат фрейма FHSS подуровня PLCP

Преамбула PLCP состоит из двух подполей:

- *Подполе Sync размером 80 бит.* Стока, 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.

- *HEC (Header Error Check).* Контрольная сумма фрейма.

Служебный элемент данных PLCP (PSDU) проходит через операцию скрэмблирования с целью отбеливания (рандомизации) последовательности входных битов. Получившийся в результате PSDU представлен на **рис. 5.17**. Заполняющие символы вставляются между всеми 32-символьными блоками. Эти заполняющие символы устраняют любые систематические отклонения в данных, например, когда единиц больше, чем нулей, или наоборот, которые могли бы привести к нежелательным эффектам при дальнейшей обработке.

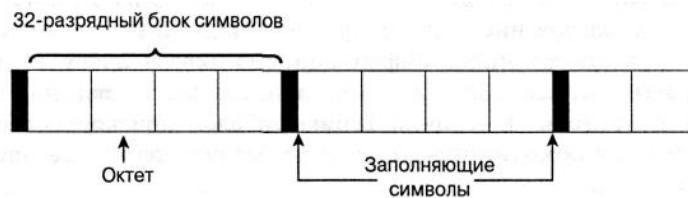


Рис. 5.17. Скрэмблированный PSDU в технологии FHSS

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 гауссовой частотной модуляции (*Gaussian Frequency Shift Keying - GFSK*).

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.

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. 5.18**.

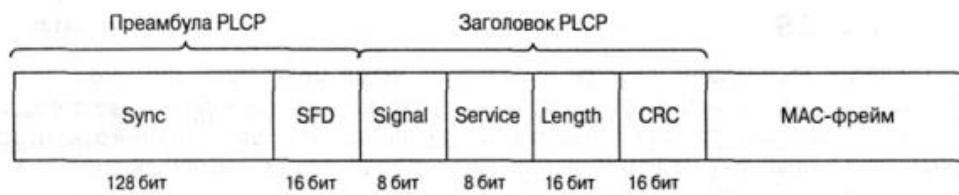


Рис. 5.18. Формат фрейма DSSS подуровня PLCP

Преамбула PLCP состоит из двух подполей:

- *Подполе Sync шириной 128 бит, представляющее собой строку, состоящую из единиц.* Задача этого под поля - 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.*
- *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 16-216), необходимое для передачи части MAC-фрейма.
- Подполе *CRC*. 16-битная контрольная сумма.

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 модуляция (*Differential Binary Phase Shift Keying - DBPSK*) для скорости передачи 1 Мбит/с.
- Квадратурная относительная фазовая модуляция (*Differential Quadrature Phase Shift Key - DQPSK*) для скорости передачи 2 Мбит/с.

IEEE 802.11b

На физическом уровне к MAC-кадрам (MPDU) добавляется заголовок физического уровня, состоящий из преамбулы и собственно PLCP-заголовка (рис. 5.19).

Преамбула содержит стартовую синхропоследовательность (SYNC) для настройки приемника и 16-битный код начала кадра (SFD) - число F3A016. PLCP-заголовок включает поля *SIGNAL* (информация о скорости и типе модуляции), *SERVICE* (дополнительная информация, в том числе о применении высокоскоростных расширений и *PBCC*-модуляции) и *LENGTH* (время в микросекундах, необходимое для передачи следующей за заголовком части кадра). Все три поля заголовка защищены 16-битной контрольной суммой *CRC*.



Рис. 5.19. Структура кадров сети IEEE 802.11b физического уровня

В стандарте *IEEE 802.11b* предусмотрено два типа заголовков: длинный и короткий (рис. 5.20).



Рис. 5.20. Короткий заголовок кадров сети 802.11b

Они отличаются длиной синхропоследовательности (128 и 56 бит), способом ее генерации, а также тем, что символ начала кадра в коротком заголовке передается в обратном порядке. Кроме того, если все поля длинного заголовка передаются со скоростью 1 Мбит/с, то при коротком заголовке преамбула транслируется на скорости 1 Мбит/с, другие поля заголовка - со скоростью 2 Мбит/с. Остальную часть кадра можно передавать на любой из допустимых стандартом скоростей передачи, указанных в полях *SIGNAL* и *SERVICE*. Короткие заголовки физического уровня предусмотрены спецификацией *IEEE 802.11b* для увеличения пропускной способности сети.

Из описания процедур связи сети *IEEE 802.11* видно, что "накладные расходы" в этом стандарте выше, чем в проводной сети *Ethernet*. Поэтому крайне важно обеспечить высокую скорость передачи данных в канале. Повысить пропускную способность канала с заданной шириной полосы частот можно, разрабатывая и применяя новые *методы модуляции*. По этому пути пошла группа разработчиков *IEEE 802.11b*.

Напомним, что изначально стандарт *IEEE 802.11* предусматривал работу в режиме *DSSS* с использованием так называемой Баркеровской последовательности (Barker) длиной 11 бит: $B1 = (10110111000)$. Каждый информационный бит замещается своим произведением по модулю 2 (операция "исключающее ИЛИ") с данной последовательностью, т. е. каждая информационная единица заменяется на $B1$, каждый ноль - на инверсию $B1$. В результате бит заменяется последовательностью 11 чипов. Далее сигнал кодируется посредством дифференциальной двух- или четырехпозиционной фазовой модуляции (*DBPSK* или *DQPSK*, один или два чипа

на символ соответственно). При частоте модуляции несущей 11 МГц общая скорость составляет в зависимости от типа модуляции 1 и 2 Мбит/с.

Стандарт *IEEE 802.11b* дополнительно предусматривает скорости передачи 11 и 5,5 Мбит/с. Для этого используется так называемая ССК-модуляция (*Complementary Code Keying* - кодирование комплементарным кодом).

Хотя механизм расширения спектра, используемый для получения скоростей 5,5 и 11 Мбит/с с применением ССК, 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 ССК расширяющий код представляет собой код из 8 комплексных чипов, 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 добиться скорости передачи данных 5,5 и 11 Мбит/с.

Для того чтобы передавать данные со скоростью 5,5 Мбит/с, нужно сгруппировать скрэмблированный поток битов в символы по 4 бита (b_0, b_1, b_2 и b_3). Последние два бита (b_2 и b_3) используются для определения 8 последовательностей комплексных чипов, как показано в таблице 3.2, где $\{c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8\}$ представляют чипы последовательности. В **таблице 5.3** j представляет мнимое число, корень квадратный из -1 , и откладывается по мнимой, или квадратурной, оси комплексной плоскости.

Таблица 5.3. Последовательность чипов ССК

(b_2, b_3)	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8
00	j	1	j	-1	j	1	- j	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 (b_2, b_3), можно использовать первые два бита (b_0, b_1) для определения поворота фазы, осуществляемого при модуляции по методу *DQPSK*, который будет применен к последовательности (**таблица 5.4**). 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 5.4. Поворот фазы при модуляции ССК

(b_0, b_1)	Изменение фазы четных символов	Изменение фазы нечетных символов
00	0	π
01	$\pi/2$	$-\pi/2$
11	π	0
10	$-\pi/2$	$\pi/2$

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, скрэмблированная 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 (b_2, b_3) для выбора одной из четырех возможных последовательностей. Биты (b_0, b_1) используются таким же образом, как при модуляции ССК на скорости 5,5 Мбит/с для вращения фазы последовательности и дальнейшей модуляции на подходящей несущей частоте.

В чем достоинство ССК-модуляции? Дело в том, что чипы символа определяются на основе последовательностей Уолша-Адамара. Последовательности Уолша-Адамара хорошо изучены, обладают отличными автокорреляционными свойствами. Что немаловажно, каждая такая последовательность мало коррелирует сама с собой при фазовом сдвиге - очень полезное свойство при борьбе с переотраженными

сигналами. Нетрудно заметить, что теоретическое операционное усиление ССК-модуляции - 3 дБ (в два раза), поскольку без кодирования QPSK-модулированный с частотой 11 Мбит/с сигнал может транслировать 22 Мбит/с. Как видно, ССК-модуляция представляет собой вид блочного кода, а потому достаточно проста при аппаратной реализации. Совокупность этих свойств и обеспечила ССК место в стандарте IEEE 802.11b в качестве обязательного вида модуляции.

На практике важно не только операционное усиление. Существенную роль играет и равномерность распределения символов в фазовом пространстве - они должны как можно дальше отстоять друг от друга, чтобы минимизировать ошибки их детектирования. И с этой точки зрения ССК-модуляция не выглядит оптимальной, ее реальное операционное усиление не превышает 2 дБ. Поэтому изначально прорабатывался другой способ модуляции - пакетное бинарное сверточное кодирование PBCC (*Packet Binary Convolutional Coding*). Этот метод вошел в стандарт IEEE 802.11b как дополнительная (необязательная) опция. Механизм PBCC (рис. 5.21) позволяет добиваться в сетях IEEE 802.11b пропускной способности 5,5, 11 и 22 Мбит/с.

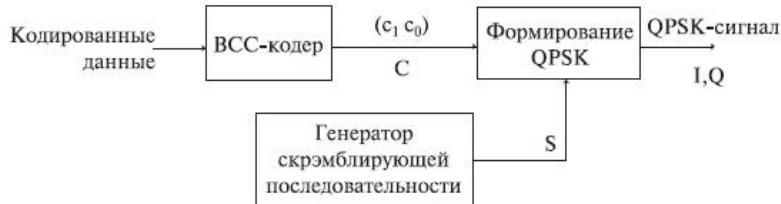


Рис. 5.21. Общая схема PBCC-модуляции

Как следует из названия, метод основан на сверточном кодировании. Для скоростей 5,5 и 11 Мбит/с поток информационных битов поступает в шестиразрядный *сдвиговый регистр* с сумматорами (рис. 5.22). В начальный момент времени все триггеры *сдвигового регистра* инициализируют нулем. В результате каждый исходный бит d заменяется двумя битами кодовой последовательности (c_0, c_1). При скорости 11 Мбит/с c_0 и c_1 задают один символ четырехпозиционной QPSK-модуляции. Для скорости 5,5 Мбит/с используют двухпозиционную BPSK-модуляцию, последовательно передавая кодовые биты c_0 и c_1 . Если же нужна скорость 22 Мбит/с, схема кодирования усложняется (рис. 5.23): три кодовых бита (c_0-c_2) определяют один символ в 8-позиционной 8-PSK-модуляции.

После формирования PSK-символов происходит скремблирование. В зависимости от сигнала s (рис. 3.7) символ остается без изменений ($s = 0$), либо его фаза увеличивается на $\pi/2$ ($s = 1$). Значение s определяет 256-битовая циклически повторяющаяся последовательность S . Она формируется на основе начального вектора $U = 338Bh$, в котором равное число нулей и единиц.

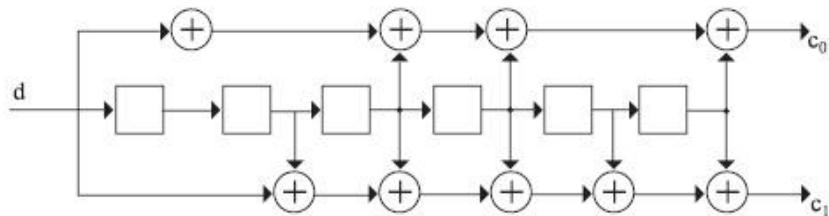


Рис. 5.22. Сверточное кодирование с двумя битами кодовой последовательности

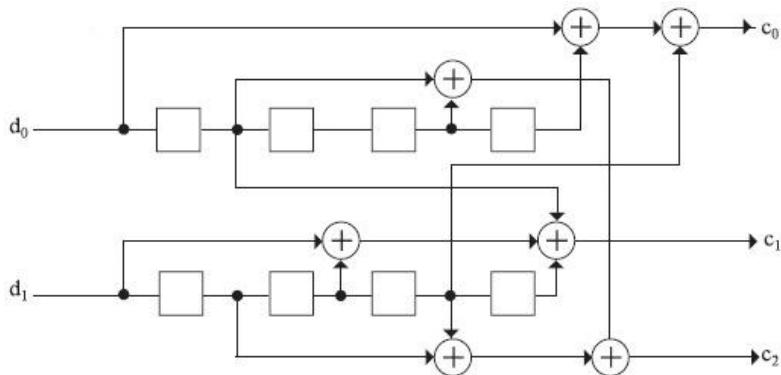


Рис. 5.23. Сверточное кодирование с тремя битами кодовой последовательности

У шестиразрядного *сдвигового регистра*, применяемого в PBCC для скоростей 11 и 5,5 Мбит/с, 64 возможных выходных состояния. Так что при модуляции PBCC информационные биты в фазовом пространстве

оказываются гораздо дальше друг от друга, чем при ССК-модуляции. Поэтому РВСС и позволяет при одном и том же соотношении "сигнал-шум" и уровне ошибок вести передачу с большей скоростью, чем в случае ССК. Однако плата за более эффективное кодирование - сложность аппаратной реализации данного алгоритма.

IEEE 802.11a

Стандарт IEEE 802.11a появился практически одновременно с *IEEE 802.11b*, в сентябре 1999 года. Эта спецификация была ориентирована на работу в диапазоне 5 ГГц и основана на принципиально ином, чем описано выше, механизме кодирования данных - на частотном мультиплексировании посредством ортогональных несущих (*OFDM*).

Стандарт *802.11a* определяет характеристики оборудования, применяемого в офисных или городских условиях, когда распространение сигнала происходит по многолучевым каналам из-за множества отражений.

В IEEE 802.11a каждый кадр передается посредством 52 ортогональных несущих, каждая с шириной полосы порядка 300 КГц (20 МГц/64). Ширина одного канала - 20 МГц. Несущие модулируют посредством *BPSK*, *QPSK*, а также 16- и 64-позиционной квадратурной амплитудной модуляции (*QAM*). В совокупности с различными скоростями кодирования (1/2 и 3/4, для 64-*QAM* - 2/3 и 3/4) образуется набор скоростей передачи 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с. В **таблице 5.5** показано, как необходимая скорость передачи данных преобразуется в соответствующие параметры узлов передатчика *OFDM*.

Таблица 5.5. Параметры передатчика стандарта 802.11a

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

Из 52 несущих 48 предназначены для передачи информационных символов, остальные 4 - служебные. Структура заголовков физического уровня отличается от принятого в спецификации *IEEE 802.11b*, но незначительно (**рис. 5.24**).

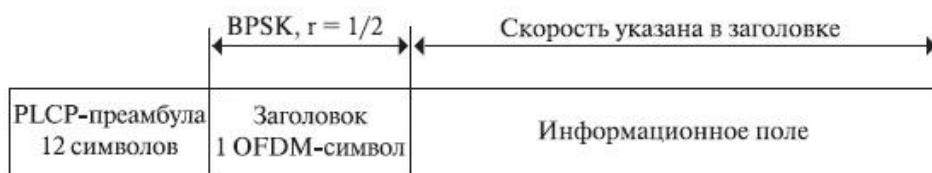


Рис. 5.24. Структура заголовка физического уровня стандарта IEEE 802.11a

Кадр включает преамбулу (12 символов синхропоследовательности), заголовок физического уровня (PLCP-заголовок) и собственно информационное поле, сформированное на МАС-уровне. В заголовке передается информация о скорости кодирования, типе модуляции и длине кадра. Преамбула и заголовок транслируются с минимально возможной скоростью (*BPSK*, скорость кодирования $r = 1/2$), а информационное поле - с указанной в заголовке, как правило, максимальной, скоростью, в зависимости от условий обмена. *OFDM*-символы передаются через каждые 4 мкс, причем каждому символу длительностью 3,2 мкс предшествует защитный интервал 0,8 мкс (повторяющаяся часть символа). Последний необходим для борьбы с многолучевым распространением сигнала - отраженный и пришедший с задержкой символ попадет в защитный интервал и не повредит следующий символ.

Естественно, формирование/декодирование *OFDM*-символов происходит посредством быстрого преобразования Фурье (обратного/прямого, ОБПФ/БПФ). *Функциональная схема* трактов приема/передачи (**рис. 5.25**) достаточно стандартна для данного метода и включает сверточный кодер, механизм

перемежения/перераспределения (защита от пакетных ошибок) и процессор ОБПФ. Фурье-процессор, собственно, и формирует суммарный сигнал, после чего к символу добавляется защитный интервал, окончательно формируется *OFDM*-символ и посредством квадратурного модулятора/конвертера передается в заданную частотную область. При приеме все происходит в обратном порядке.

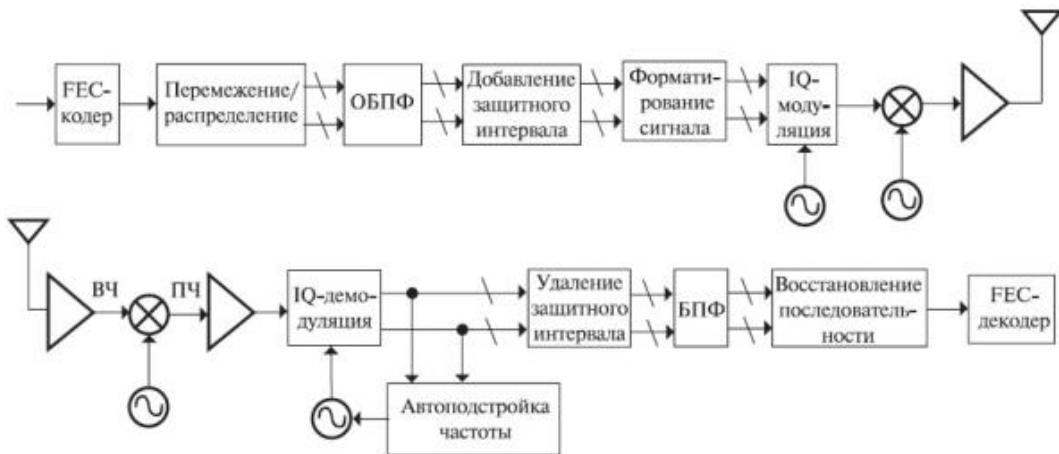


Рис. 5.25. Функциональная схема трактов приема/передачи стандарта IEEE 802.11a

IEEE 802.11g

Стандарт *IEEE 802.11g* по сути представляет собой перенесение схемы модуляции *OFDM*, прекрасно зарекомендовавшей себя в 802.11a, из диапазона 5 ГГц в область 2,4 ГГц при сохранении функциональности устройств стандарта 802.11b. Это возможно, поскольку в стандартах 802.11 ширина одного канала в диапазонах 2,4 и 5 ГГц схожа - 22 МГц.

Одним из основных требований к спецификации 802.11g была обратная совместимость с устройствами 802.11b. Действительно, в стандарте 802.11b в качестве основного способа модуляции принята схема ССК (*Complementary Code Keying*), а в качестве дополнительной возможности допускается модуляция *PBCC* (*Pocket Binary Convolutional Coding*).

Разработчики 802.11g предусмотрели ССК-модуляцию для скоростей до 11 Мбит/с и *OFDM* для более высоких скоростей. Но сети стандарта 802.11 при работе используют принцип *CSMA/CA* - множественный доступ к каналу связи с контролем несущей и предотвращением коллизий. Ни одно устройство 802.11 не должно начинать передачу, пока не убедится, что эфир в его диапазоне свободен от других устройств. Если в зоне слышимости окажутся устройства 802.11b и 802.11g, причем обмен будет происходить между устройствами 802.11g посредством *OFDM*, то оборудование 802.11b просто не поймет, что другие устройства сети ведут передачу, и попытается начать трансляцию. Последствия очевидны.

Чтобы не допустить подобной ситуации, предусмотрена возможность работы в смешанном режиме - *CCK-OFDM*. Информация в сетях 802.11 передается кадрами. Каждый информационный кадр включает два основных поля: преамбулу с заголовком и информационное поле (рис. 5.26).

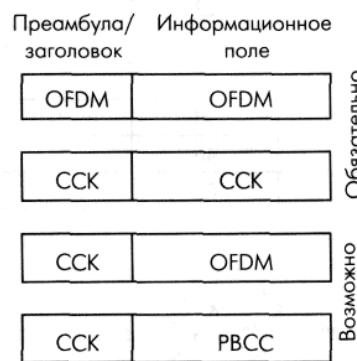


Рис. 5.26. Кадры IEEE 802.11g в различных режимах модуляции

Преамбула содержит синхропоследовательность и код начала кадра, заголовок - служебную информацию, в том числе о типе модуляции, скорости и продолжительности передачи кадра. В режиме *CCK-OFDM* преамбула и заголовок модулируются методом ССК (реально - путем прямого расширения спектра DSSS посредством последовательности Баркера, поэтому в стандарте 802.11g этот режим именуется *DSSS-OFDM*), а информационное поле - методом *OFDM*. Таким образом, все устройства 802.11b, постоянно "прослушивающие"

эфир, принимают заголовки кадров и узнают, сколько времени будет транслироваться кадр $802.11g$. В этот период они "молчат". Естественно, пропускная способность сети падает, поскольку скорость передачи преамбулы и заголовка - 1 Мбит/с.

Видимо, данный подход не устраивал лагерь сторонников технологии $PBCC$, и для достижения компромисса в стандарт $802.11g$ в качестве дополнительной возможности ввели, так же как и в $802.11b$, необязательный режим - $PBCC$, в котором заголовок и преамбула передаются так же, как и при ССК, а информационное поле модулируется по схеме $PBCC$ и передается на скорости 22 или 33 Мбит/с. В результате устройства стандарта $802.11g$ должны оказаться совместимыми со всеми модификациями оборудования $802.11b$ и не создавать взаимных помех. Диапазон поддерживаемых им скоростей отражен в таблице 3.5, зависимость скорости от типа модуляции - на рис. 5.27.

Таблица 5.6. Возможные скорости и тип модуляции в спецификации $IEEE 802.11g$

Скорость, Мбит/с	Тип модуляции	
	Обязательно	Допустимо
1	Последовательность Баркера	
2	Последовательность Баркера	
5,5	<i>CCK</i>	<i>PBCC</i>
6	<i>OFDM</i>	<i>OFDM</i>
9		<i>OFDM, CCK-OFDM</i>
11	<i>CCK</i>	<i>PBCC</i>
12	<i>OFDM</i>	<i>CCK-OFDM</i>
18		<i>OFDM, CCK-OFDM</i>
22		<i>PBCC</i>
24	<i>OFDM</i>	<i>CCK-OFDM</i>
33		<i>PBCC</i>
36		<i>OFDM, CCK-OFDM</i>
48		<i>OFDM, CCK-OFDM</i>
54		<i>OFDM, CCK-OFDM</i>

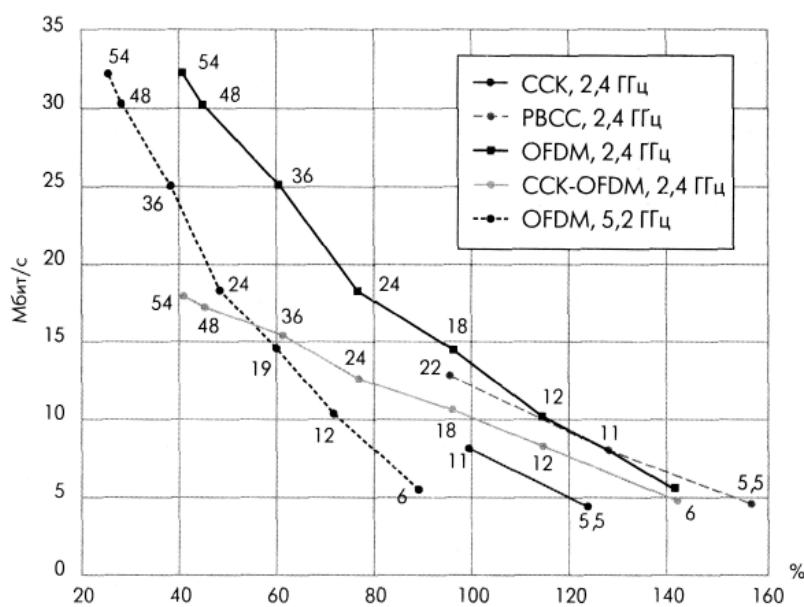


Рис. 5.27. Зависимость скорости передачи от расстояния для различных технологий передачи. Расстояние приведено в процентах, 100% - дальность передачи с модуляцией ССК на скорости 11 Мбит/с

Очевидно, что устройствам стандарта $IEEE 802.11g$ достаточно долго придется работать в одних сетях с оборудованием $802.11b$. Также очевидно, что производители в массе своей не будут поддерживать режимы CCK -

OFDM и *PBCC* в силу их необязательности, ведь почти все решает цена устройства. Поэтому одна из основных проблем данного стандарта - как обеспечить бесконфликтную работу смешанных сетей *802.11b/g*.

Основной принцип работы в сетях *802.11* - "слушать, прежде чем вещать". Но устройства *802.11b* не способны услышать устройства *802.11g* в *OFDM*-режиме. Ситуация аналогична проблеме скрытых станций: два устройства удалены настолько, что не слышат друг друга и пытаются обратиться к третьему, которое находится в зоне слышимости обоих. Для предотвращения конфликтов в подобной ситуации в *802.11* введен защитный механизм, предусматривающий перед началом информационного обмена передачу короткого кадра "запрос на передачу" (*RTS*) и получение кадра подтверждения "можно передавать" (*CTS*). Механизм *RTS/CTS* применим и к смешанным сетям *802.11b/g*. Естественно, эти кадры должны транслироваться в режиме *CCK*, который обязаны понимать все устройства. Однако защитный механизм существенно снижает пропускную способность сети.

В **таблице 5.7** представлена сводная информация по параметрам физических уровней.

Таблица 5.7. Стандарты физического уровня

Параметр	<i>802.11 DSSS</i>	<i>802.11 FHSS</i>	<i>802.11b</i>	<i>802.11a</i>	<i>802.11g</i>
Частотный диапазон (ГГц)	2,4	2,4	2,4	5	2,4
Максимальная скорость передачи данных (Мбит/с)	2	2	11	54	54
Технология	<i>DSSS</i>	<i>FHSS</i>	<i>CCK</i>	<i>OFDM</i>	<i>OFDM</i>
Тип модуляции (для максимальной скорости передачи)	<i>QPSK</i>	<i>GFSK</i>	<i>QPSK</i>	<i>64-QAM</i>	<i>64-QAM</i>
Число неперекрывающихся каналов	3	3	3	15	3

Элементы и инфраструктура WiFi

Основные элементы сети

Для построения беспроводной сети используются Wi-Fi адAPTERы и точки доступа.

АдAPTER представляет собой устройство, которое подключается через слот расширения PCI, PCMCIA, CompactFlash. Существуют также адAPTERы с подключением через порт USB 2.0. **Wi-Fi адAPTER выполняет ту же функцию, что и сетевая карта в проводной сети.** Он служит для подключения компьютера пользователя к беспроводной сети. Благодаря платформе Centrino все современные ноутбуки имеют встроенные адAPTERы Wi-Fi, совместимые со многими современными стандартами. Wi-Fi адAPTERами, как правило, снабжены и КПК (карманные персональные компьютеры), что также позволяет подключать их к беспроводным сетям.

Для доступа к беспроводной сети **адAPTER может устанавливать связь непосредственно с другими адAPTERами. Такая сеть называется беспроводной одноранговой сетью или Ad Hoc ("к случаю"). АдAPTER также может устанавливать связь через специальное устройство - точку доступа. Такой режим называется инфраструктурой.**

Для выбора способа подключения адAPTER должен быть настроен на использование либо Ad Hoc, либо инфраструктурного режима.

Точка доступа представляет собой автономный модуль со встроенным микрокомпьютером и приемно-передающим устройством. Через точку доступа осуществляется взаимодействие и обмен информацией между беспроводными адAPTERами, а также связь с проводным сегментом сети. Таким образом, **точка доступа играет роль коммутатора.**

Точка доступа имеет **сетевой интерфейс (uplink port), при помощи которого она может быть подключена к обычной проводной сети.** Через этот же интерфейс может осуществляться и настройка точки.

Точка доступа может использоваться как для подключения к ней клиентов (базовый режим точки доступа), так и для взаимодействия с другими точками доступа с целью построения распределенной сети (Wireless Distributed System - WDS). Это режимы беспроводного моста "точка-точка" и "точка - много точек", беспроводной клиент и повторитель.

Доступ к сети обеспечивается путем передачи широковещательных сигналов через эфир. Принимающая станция может получать сигналы в диапазоне работы нескольких передающих станций. Станция-приемник использует **идентификатор зоны обслуживания (Service Set Identifier - SSID)** для фильтрации получаемых сигналов и выделения того, который ей нужен.

Зоной обслуживания (Service Set - SS) называются логически сгруппированные устройства, обеспечивающие подключение к беспроводной сети.

Базовая зона обслуживания (Basic Service Set - BSS) - это группа станций, которые связываются друг с другом по беспроводной связи. Технология BSS предполагает наличие особой станции, которая называется точкой доступа (access point).

Основные элементы Wi-Fi сети

Для построения беспроводной сети используются Wi-Fi адAPTERы и точки доступа.

АдAPTER (рис. 1) представляет собой устройство, которое подключается через слот расширения PCI, PCMCIA, CompactFlash. Существуют также адAPTERы с подключением через порт USB 2.0. Wi-Fi адAPTER выполняет ту же функцию, что и сетевая карта в проводной сети. Он служит для подключения компьютера пользователя к беспроводной сети. Благодаря платформе Centrino все современные ноутбуки имеют встроенные адAPTERы Wi-Fi, совместимые со многими современными стандартами. Wi-Fi адAPTERами, как правило, снабжены и КПК (карманные персональные компьютеры), что также позволяет подключать их к беспроводным сетям.



Рис. 1. АдAPTERы

Для доступа к беспроводной сети адаптер может устанавливать связь непосредственно с другими адаптерами. Такая сеть называется *беспроводной одноранговой сетью* или *Ad Hoc*("к случаю"). Адаптер также может устанавливать связь через специальное устройство - *точку доступа*. Такой режим называется *инфраструктурой*.

Для выбора способа подключения адаптер должен быть настроен на использование либо *Ad Hoc*, либо инфраструктурного режима.

Точка доступа (рис. 2) представляет собой автономный модуль со встроенным микрокомпьютером и приемно-передающим устройством.

Через точку доступа осуществляется взаимодействие и обмен информацией между беспроводными адаптерами, а также связь с проводным сегментом сети. Таким образом, точка доступа играет роль коммутатора.



Рис. 2. Точка доступа

Точка доступа имеет сетевой интерфейс (uplink port), при помощи которого она может быть подключена к обычной проводной сети. Через этот же интерфейс может осуществляться и настройка точки.

Точка доступа может использоваться как для подключения к ней клиентов (базовый режим точки доступа), так и для взаимодействия с другими точками доступа с целью построения распределенной сети (Wireless Distributed System - WDS). Это режимы беспроводного моста "точка-точка" и "точка - много точек", беспроводный клиент и повторитель.

Доступ к сети обеспечивается путем передачи широковещательных сигналов через эфир. Принимающая станция может получать сигналы в диапазоне работы нескольких передающих станций. Станция-приемник использует идентификатор зоны обслуживания (Service Set IDentifier - SSID) для фильтрации получаемых сигналов и выделения того, который ей нужен.

Зоной обслуживания(Service Set - SS) называются логически сгруппированные устройства, обеспечивающие подключение к беспроводной сети.

Базовая зона обслуживания(Basic Service Set - BSS) - это группа станций, которые связываются друг с другом по беспроводной связи. Технология BSS предполагает наличие особой станции, которая называется *точкой доступа*(access point).

Обычно схема Wi-Fi сети содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка (Ad-hoc), когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передаёт свой идентификатор сети (SSID (англ.)) с помощью специальных сигнальных пакетов на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с - наименьшая скорость передачи данных для Wi-Fi. Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID приёмник может выбирать между ними на основании данных об уровне сигнала. Стандарт Wi-Fi даёт клиенту полную свободу при выборе критерии для соединения. Более подробно принцип работы описан в официальном тексте стандарта.

Однако стандарт не описывает всех аспектов построения беспроводных локальных сетей Wi-Fi. Поэтому каждый производитель оборудования решает эту задачу по-своему, применяя те подходы, которые он считает наилучшими с той или иной точки зрения. Поэтому возникает необходимость классификации способов построения беспроводных локальных сетей.

По способу объединения точек доступа в единую систему можно выделить:

- автономные точки доступа (называются также самостоятельные, децентрализованные, умные);
- точки доступа, работающие под управлением контроллера (называются также «легковесные», централизованные);
- бесконтроллерные, но не автономные (управляемые без контроллера).

По способу организации и управления радиоканалами можно выделить беспроводные локальные сети:

- со статическими настройками радиоканалов;
- с динамическими (адаптивными) настройками радиоканалов;
- со «слоистой» или многослойной структурой радиоканалов.

Режимы и особенности организации Wi-Fi сетей

Беспроводные сети Wi-Fi поддерживают несколько различных режимов работы, реализуемых для конкретных целей.

Режим Ad Hoc

В режиме *Ad Hoc* (рис. 3) клиенты устанавливают связь непосредственно друг с другом. Устанавливается одноранговое взаимодействие по типу "точка-точка", и компьютеры взаимодействуют напрямую без применения точек доступа. При этом создается только одна зона обслуживания, не имеющая интерфейса для подключения к проводной локальной сети.

Основное достоинство данного режима - простота организации: он не требует дополнительного оборудования (точки доступа). Режим может применяться для создания временных сетей для передачи данных.

Однако необходимо иметь в виду, что режим *Ad Hoc* позволяет устанавливать соединение на скорости не более 11 Мбит/с, независимо от используемого оборудования. Реальная скорость обмена данными будет ниже и составит не более $11/N$ Мбит/с, где N - число устройств в сети. Дальность связи составляет не более ста метров, а скорость передачи данных быстро падает с увеличением расстояния.

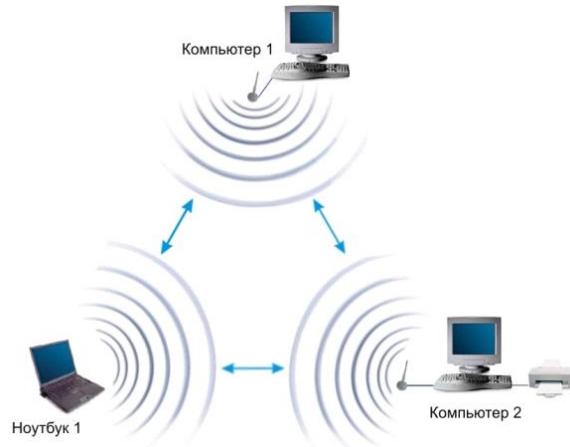


Рис. 3. Ad Hoc

Для организации долговременных беспроводных сетей следует использовать инфраструктурный режим.

Инфраструктурный режим

В этом режиме точки доступа обеспечивают связь клиентских компьютеров (рис. 4). Точку доступа можно рассматривать как беспроводной коммутатор. Клиентские станции не связываются непосредственно одна с другой, а связываются с точкой доступа, и она уже направляет пакеты адресатам.

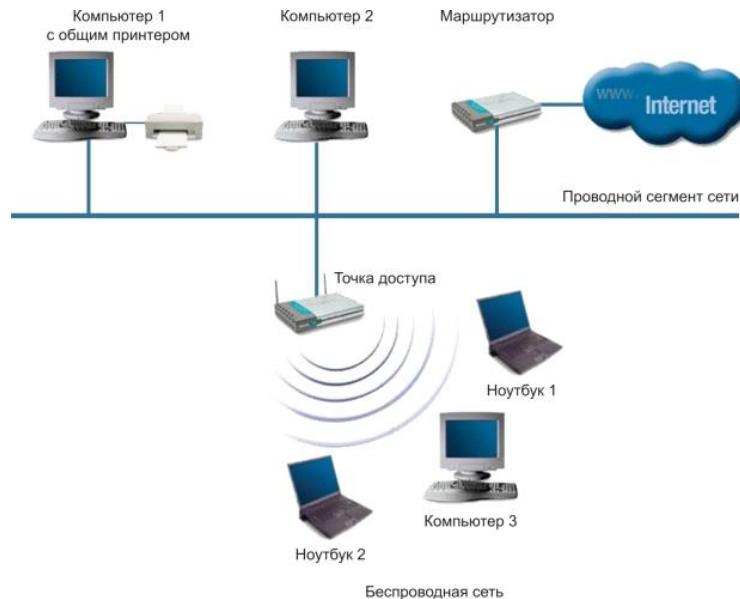


Рис. 4. Инфраструктурный режим

Точка доступа имеет порт Ethernet, через который базовая зона обслуживания подключается к проводной или смешанной сети - к сетевой инфраструктуре.

Режимы WDS и WDS with AP

Термин *WDS* (Wireless Distribution System) расшифровывается как "распределенная беспроводная система". В этом режиме точки доступа соединяются только между собой, образуя мостовое соединение. При этом каждая точка может соединяться с несколькими другими точками. Все точки в этом режиме должны использовать один и тот же канал, поэтому количество точек, участвующих в образовании моста, не должно быть чрезмерно большим. Подключение клиентов осуществляется только по проводной сети через uplink-порты точек (рис. 5).

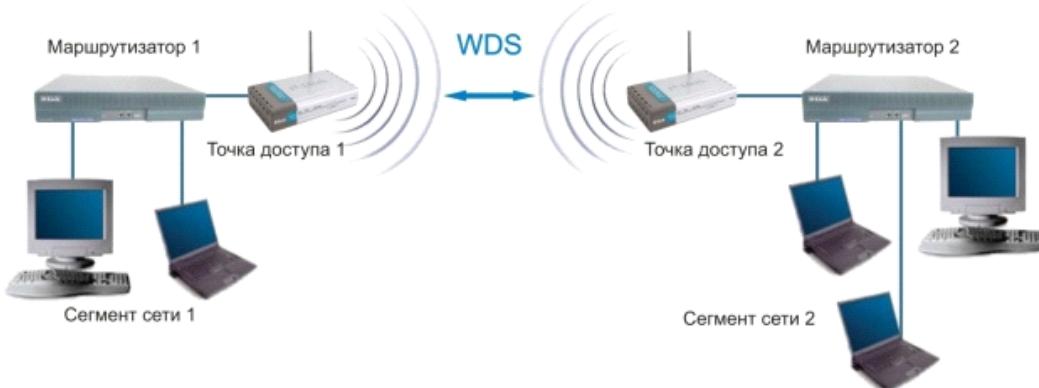


Рис. 5. Мостовой режим

Режим беспроводного моста, аналогично проводным мостам, служит для объединения подсетей в общую сеть. С помощью беспроводных мостов можно объединять проводные LAN, находящиеся как в соседних зданиях, так и на расстоянии до нескольких километров. Это позволяет объединить в сеть филиалы и центральный офис, а также подключать клиентов к сети провайдера Internet (рис. 6).

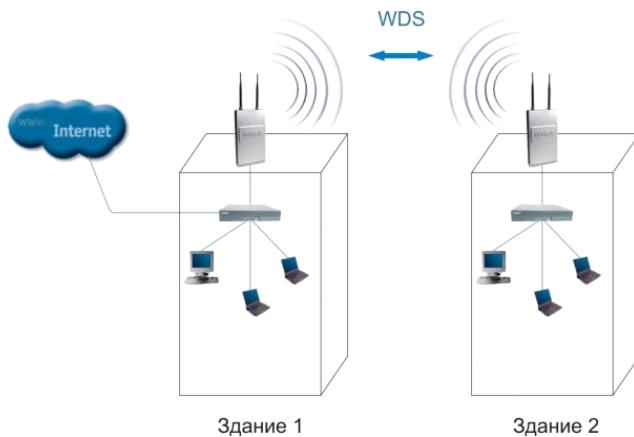


Рис. 6. Мостовой режим между зданиями

Беспроводной мост может использоваться там, где прокладка кабеля между зданиями нежелательна или невозможна. Данное решение позволяет достичь значительной экономии средств и обеспечивает простоту настройки и гибкость конфигурации при перемещении офисов.

К точке доступа, работающей в режиме моста, подключение беспроводных клиентов невозможно. Беспроводная связь осуществляется только между парой точек, реализующих мост.

Термин *WDS with AP* (WDS with Access Point) означает "распределенная беспроводная система, включающая точку доступа", т.е. с помощью этого режима можно не только организовать мостовую связь между точками доступа, но и одновременно подключить клиентские компьютеры (рис. 7). Это позволяет достичь существенной экономии оборудования и упростить топологию сети. Данная технология поддерживается большинством современных точек доступа.

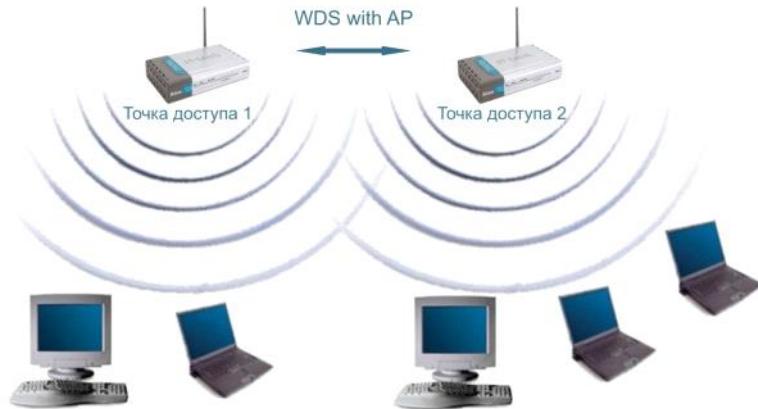


Рис. 7. Режим WDS with AP

Тем не менее, необходимо помнить, что все устройства в составе одной WDS with AP работают на одной частоте и создают взаимные помехи, что ограничивает количество клиентов до 15-20 узлов. Для увеличения количества подключаемых клиентов можно использовать несколько WDS-сетей, настроенных на разные неперекрывающиеся каналы и соединенные проводами через uplink-порты.

Топология организации беспроводных сетей в режиме WDS аналогична обычным проводным топологиям.

Топология типа "шина"

Топология типа "шина" самой своей структурой предполагает идентичность сетевого оборудования компьютеров, а также равноправие всех абонентов (рис. 8).

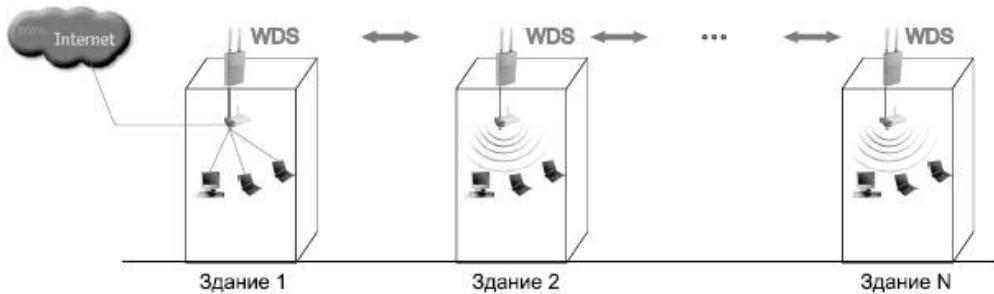


Рис. 8. Топология типа "шина"

Здесь отсутствует центральный абонент, через которого передается вся информация, что увеличивает ее надежность (ведь при отказе любого центра перестает функционировать вся управляемая этим центром система). Добавить новых абонентов в шину довольно просто. Надо ввести параметры новой точки доступа, что приведет только к кратковременной перезагрузке последней точки.

Шине не страшны отказы отдельных точек, так как все остальные компьютеры сети могут нормально продолжать обмен между собой, но при этом оставшаяся часть компьютеров не сможет получить доступ в Internet.

Топология типа "кольцо"

"Кольцо"- это топология, в которой каждая точка доступа соединена только с двумя другими (рис. 9). Четко выделенного центра в данном случае нет, все точки могут быть одинаковыми.

Подключение новых абонентов в "кольцо" обычно осуществлять очень просто, хотя это и требует обязательной остановки работы двух крайних точек от новой точки доступа.

В то же время основное преимущество кольца состоит в том, что ретрансляция сигналов каждым абонентом позволяет существенно увеличить размеры всей сети в целом (порой до нескольких десятков километров). Кольцо в этом отношении существенно превосходит любые другие топологии.

Топология связей между точками в этом режиме представляет собой ациклический граф типа "дерево", то есть данные из Internet от точки 4 к точке 2 проходят по двум направлениям - через точку 1 и 3 (рис. 9). Для устранения лишних связей, способных приводить к появлению циклов в графе, реализуется алгоритм *Spanning tree*. Его использование позволяет выявить и блокировать лишние связи. При изменении топологии сети - например, из-за

отключения некоторых точек или невозможности работы каналов - алгоритм *Spanning tree* запускается заново, и прежде заблокированные лишние связи могут использоваться вместо вышедших из строя.

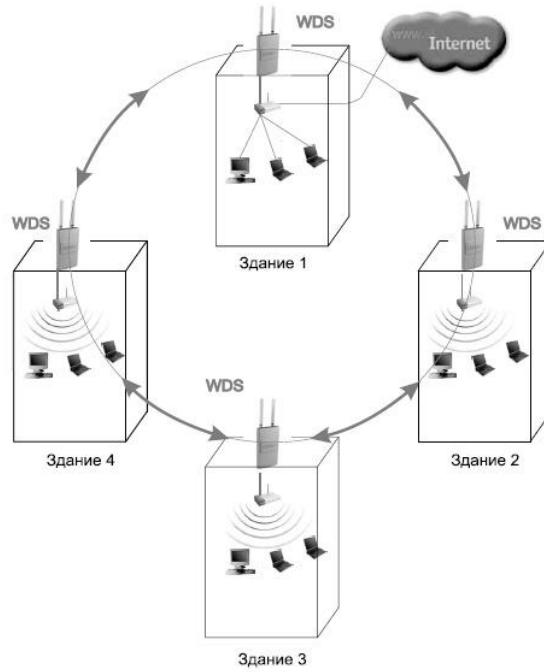


Рис. 9. Топология типа "кольцо"

Топология типа "звезда"

"Звезда"- это топология с явно выделенным центром, к которому подключаются все остальные абоненты (рис. 10). Весь обмен информацией идет исключительно через центральную точку доступа, на которую в результате ложится очень большая нагрузка.

Если говорить об устойчивости звезды к отказам точек, то выход из строя обычной точки доступа никак не отражается на функционировании оставшейся части сети, зато любой отказ центральной точки делает сеть полностью неработоспособной.

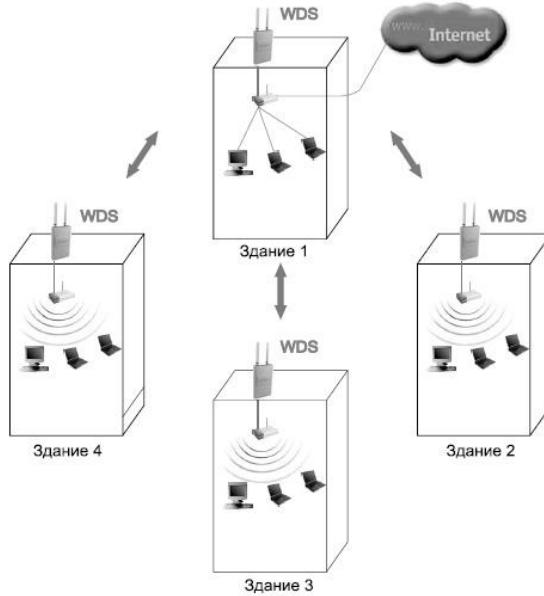


Рис. 10. Топология типа "звезда"

Существенный недостаток топологии "звезда" состоит в жестком ограничении количества абонентов. Так как все точки работают на одном канале, обычно центральный абонент может обслуживать не более 10 периферийных абонентов из-за большого падения скорости.

В большинстве случаев, например, для объединения нескольких районов в городе, используют комбинированные топологии.

Режим повторителя

Может возникнуть ситуация, когда оказывается невозможno (неудобно) соединить точку доступа с проводной инфраструктурой или какое-либо препятствие затрудняет осуществление связи точки доступа с местом расположения беспроводных станций клиентов напрямую. В такой ситуации можно использовать точку в режиме повторителя (Repeater) (рис. 4.11).

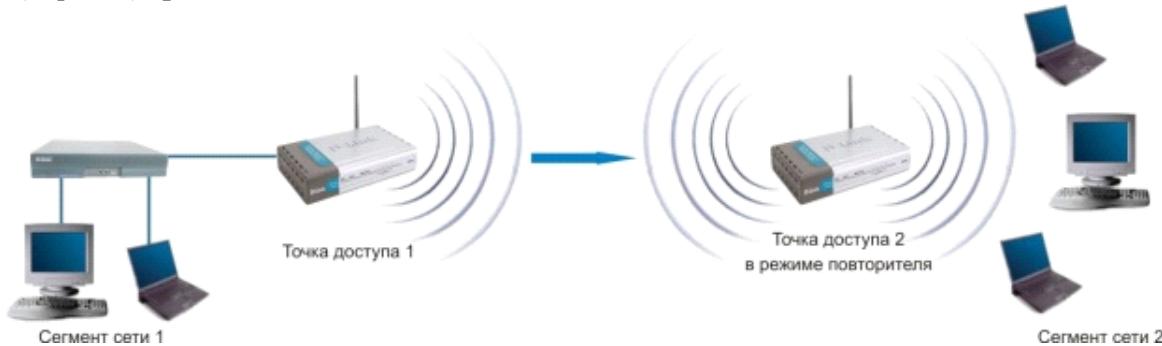


Рис. 11. Режим повторителя

Аналогично проводному повторителю, беспроводной повторитель просто ретранслирует все пакеты, поступившие на его беспроводной интерфейс. Эта ретрансляция осуществляется через тот же канал, через который они были получены.

При применении точки доступа в режиме повторителя следует помнить, что наложение широковещательных доменов может привести к сокращению пропускной способности канала вдвое, потому что начальная точка доступа также "слышит" ретранслированный сигнал.

Режим повторителя не включен в стандарт 802.11, поэтому для его реализации рекомендуется использовать однотипное оборудование (вплоть до версии прошивки) и от одного производителя. С появлением WDS данный режим потерял свою актуальность, потому что WDS заменяет его. Однако его можно встретить в старых версиях прошивок и в устаревшем оборудовании.

Режим клиента

При переходе от проводной архитектуры к беспроводной иногда можно обнаружить, что имеющиеся сетевые устройства поддерживают проводную сеть Ethernet, но не имеют интерфейсных разъемов для беспроводных сетевых адаптеров. Для подключения таких устройств к беспроводной сети можно использовать точку доступа "клиент" (рис. 12).

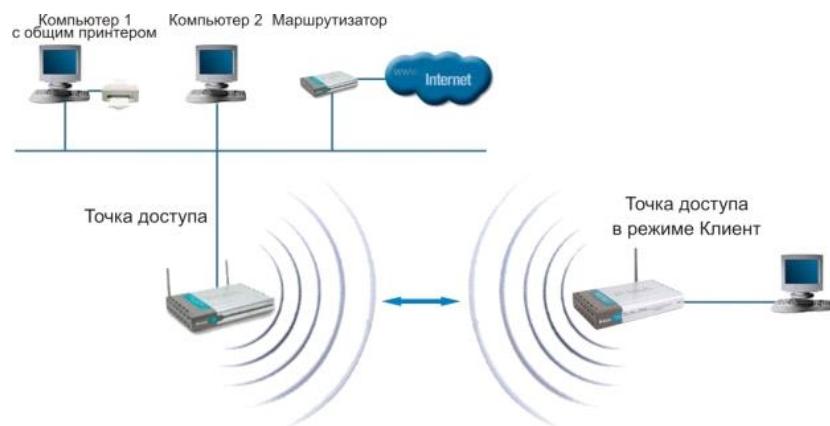


Рис. 12. Режим клиента

При помощи точки доступа, функционирующей в режиме клиента, к беспроводной сети подключается только одно устройство. Этот режим не включен в стандарт 802.11 и поддерживается не всеми производителями.

Организация и планирование беспроводных сетей

При организации беспроводной локальной сети необходимо учитывать некоторые особенности окружающей среды. На качество и дальность работы связи влияет множество физических факторов: число стен, перекрытий и других объектов, через которые должен пройти сигнал. Обычно расстояние зависит от типа материалов и

радиочастотного шума от других электроприборов в помещении. Для улучшения качества связи надо следовать базовым принципам:

- сократить число стен и перекрытий между абонентами беспроводной сети - каждая стена и перекрытие отнимает от максимального радиуса от 1 м до 25 м. Расположить точки доступа и абонентов сети так, чтобы количество преград между ними было минимальным;

- проверить угол между точками доступа и абонентами сети. Стена толщиной 0,5 м при угле в 30 градусов для радиоволны становится стеной толщиной 1 м. При угле в 2 градуса стена становится преградой толщиной в 12 м! Надо стараться расположить абонентов сети так, чтобы сигнал проходил под углом в 90 градусов к перекрытиям или стенам;

- строительные материалы влияют на прохождение сигнала по-разному - целиком металлические двери или алюминиевая облицовка негативно сказываются на передаче радиоволн. Желательно, чтобы между абонентами сети не было металлических или железобетонных препятствий;

- с помощью программного обеспечения проверки мощности сигнала надо позиционировать антенну на лучший прием;

- удалить от абонентов беспроводных сетей, по крайней мере, на 1-2 метра электроприборы, генерирующие радиопомехи, микроволновые печи, мониторы, электромоторы, ИБП. Для уменьшения помех эти приборы должны быть надежно заземлены;

- если используются беспроводные телефоны стандарта 2,4 ГГц или оборудование X-10 (например, системы сигнализации), качество беспроводной связи может заметно ухудшиться или прерваться.

Для типичного жилья расстояние связи не представляет особой проблемы. Если обнаружена неуверенная связь в пределах дома, то надо расположить точку доступа между комнатами, которые следует связать беспроводной сетью.

Для обнаружения точек доступа, попадающих в зону действия беспроводной сети, и определения каналов, на которых они работают, можно использовать программу Network Stumbler (<http://www.stumbler.net/>). С ее помощью также можно оценить соотношение "сигнал-шум" на выбранных каналах.

Офисная сеть

Простая беспроводная сеть для небольшого офиса или домашнего использования (Small Office/Home Office - SOHO) может быть построена на основе одной точки доступа (рис. 13).

Для организации сети адаптеры переводятся в режим инфраструктуры, а точка доступа - в режим точки доступа. При этом создается одна зона обслуживания, в которой находятся все пользователи сети.



Рис. 13. Офисная сеть

При размещении точки доступа при развертывании малой сети следует обеспечить достаточное качество связи на всех рабочих местах, а также удобство в размещении самой точки. Типовое решение - закрепить точку доступа непосредственно на фальш-потолке, при этом провода электропитания и проводной сети будут проходить над фальш-потолком либо в коробах.

Необходимо иметь в виду, что при расширении сети и увеличении количества пользователей скорость связи будет падать (пропорционально числу пользователей). Наибольшее разумное количество пользователей обычно составляет 16-20. Помимо этого скорость и качество связи зависят и от расстояния между клиентом и точкой. Эти соображения могут потребовать расширения базовой сети.

Для расширения сети можно использовать uplink-порт точки доступа. Он может использоваться как для объединения базовых зон обслуживания в сеть, так и для интеграции в имеющуюся проводную или беспроводную инфраструктуру, например для обеспечения пользователей доступом к разделяемым ресурсам других подразделений или для подключения к Internet.

При расширении сети необходимо следить, чтобы частоты соседних точек доступа не перекрывались во избежание взаимных помех и снижения скорости передачи. Это достигается настройкой соседних точек на неперекрывающиеся по частоте каналы 1, 6 и 11. Чередуя каналы таким образом, что соседние точки с каналами 1, 6 и 11 окажутся в вершинах равностороннего треугольника, можно охватить беспроводной связью сколь угодно большую площадь без перекрытия частот (рис. 14).

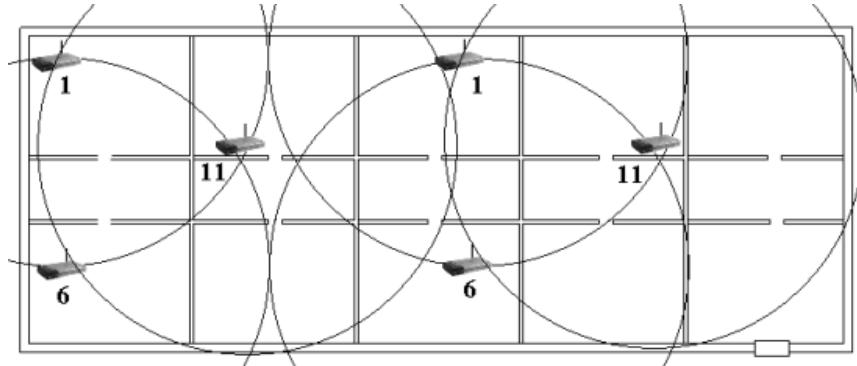


Рис. 14. Расширение беспроводной сети

На развертывание беспроводных сетей используемые приложения оказывают влияние по-разному. Наиболее важные факторы - это:

- расчетная скорость в пересчете на одного клиента;
- типы используемых приложений;
- задержки в передаче данных.

Расчетная скорость каждого клиента уменьшается с вводом в зону обслуживания новых клиентов. Следовательно, если дома или в офисе используются требовательные к скорости приложения (например, программа Internet-телефонии Skype), необходимо увеличить количество точек доступа на единицу площади (рис. 15).

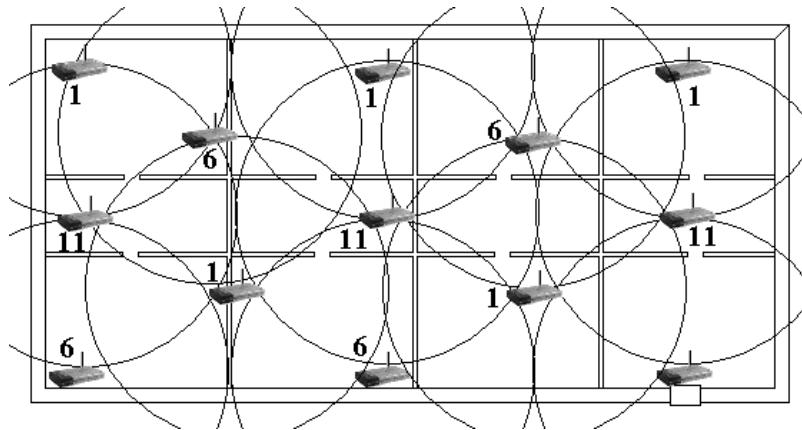


Рис. 15. Расширение беспроводной сети с максимальной скоростью

Для определения границы действия точек доступа используется ноутбук с установленной программой Network Stumbler. Она показывает, на какой скорости будет работать адаптер в зависимости от расстояния от точки доступа. По мере удаления скорость автоматически падает, и при достижении порогового уровня необходимо ставить новую точку.

Объединение всех точек доступа в офисе в локальную сеть можно осуществить несколькими способами. Самым простым и распространенным методом организации является объединение через проводную инфраструктуру (рис. 16).



Рис. 16. Объединение точек доступа через проводную инфраструктуру

В таком случае устанавливается коммутатор, к которому подключаются точки доступа посредством витой пары через uplink-порт. Также к этому коммутатору можно подвести широкополосный Internet. Преимуществом такого подключения является простота настройки зоны действия точек доступа на разные каналы, недостатком - прокладка проводов от точек доступа к коммутатору.

Второй способ - подключение с использованием расширенного режима WDS (рис. 17).

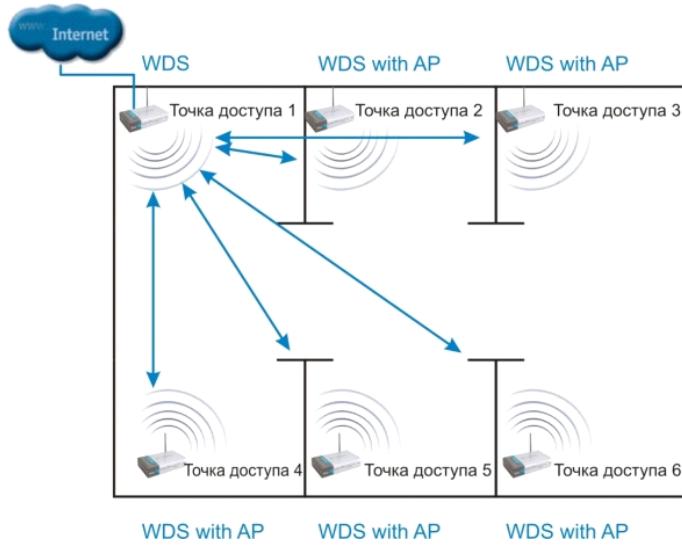


Рис. 17. Объединение точек доступа с использованием расширенного режима WDS

Одна точка доступа, которая имеет подключение к Internet, переводится в мостовой режим WDS, остальные точки настраиваются на тот же канал, что и первая, и устанавливается режим WDS with AP. Использование такого способа нежелательно, т.к. все точки работают на одном канале, и при достаточно большом их количестве резко уменьшается скорость. Рекомендуется устанавливать не более 2-3 точек.

Третий способ подключения аналогичен предыдущему, но дополнительно к каждой точке доступа через проводной интерфейс подключена еще одна точка, работающая на другом канале, для организации связи в одной комнате (рис. 18).

Здесь переводятся те точки доступа в режим WDS, которые будут связаны с первой, а остальные через проводные интерфейсы подключаются к ним. Они должны работать в режиме точки доступа и на других каналах, чтобы не было коллизий. Преимуществом такого способа подключения является полное отсутствие проводной инфраструктуры (за исключением связи между соседними точками), недостатком - высокая стоимость, в связи с большим количеством точек доступа, и использование одного канала для связи с базовой точкой.

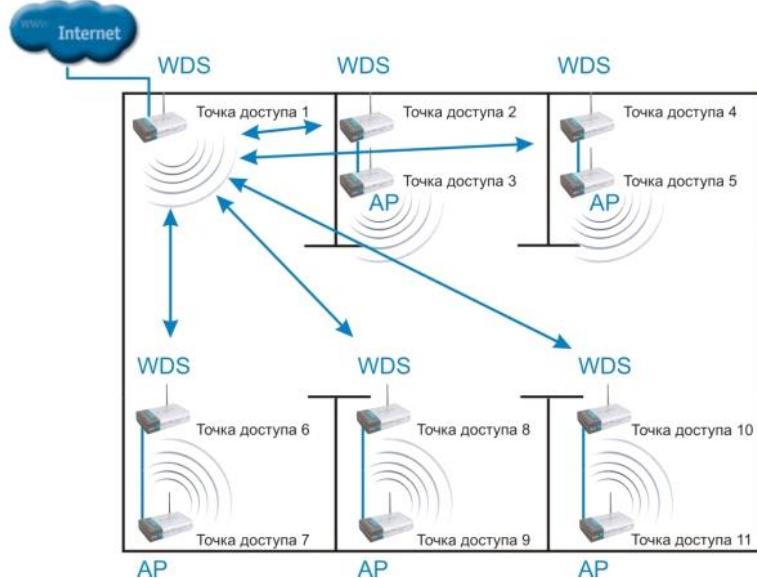


Рис. 18. Объединение точек доступа с дополнительными точками

Чтобы пользователь мог передвигаться от одной точки доступа к другой без потери доступа к сетевым службам и разрыва соединения, во всем оборудовании компании D-Link предусмотрена функция роуминга.

Роуминг - это возможность радиоустройства перемещаться за пределы действия базовой станции и, находясь в зоне действия "гостевой" станции, иметь доступ к "домашней" сети (**рис. 19**).



Рис. 19. Роуминг

При организации роуминга все точки доступа, обеспечивающие роуминг, конфигурируются на использование одинакового идентификатора зоны обслуживания (SSID). Все точки доступа относятся к одному широковещательному домену, или одному *домену роуминга*.

Механизм определения момента времени, когда необходимо начать процесс роуминга, не определен в стандарте 802.11, и, таким образом, оставлен на усмотрение поставщиков оборудования. Наиболее простой широко распространенный алгоритм переключения заключается в том, что адаптер взаимодействует с одной точкой вплоть до того момента, когда уровень сигнала не упадет ниже допустимого предела. После этого осуществляется поиск точки доступа с одинаковым SSID и максимальным уровнем сигнала, и переподключение к ней.

Роуминг включает значительно больше процессов, чем необходимо для поиска точки доступа, с которой можно связаться. Опишем некоторые из задач, которые должны решаться в ходе роуминга на канальном уровне:

- предыдущая точка доступа должна определить, что клиент уходит из ее области действия;
- предыдущая точка доступа должна буферизовать данные, предназначенные для клиента, осуществляющего роуминг;
- новая точка доступа должна показать предыдущей, что клиент успешно переместился в ее зону;
- предыдущая точка доступа должна послать буферизованные данные новой точке доступа;
- предыдущая точка доступа должна определить, что клиент покинул ее зону действия;
- точка доступа должна обновить таблицы MAC-адресов на коммутаторах инфраструктуры, чтобы избежать потери данных перемещающегося клиента.

Сеть между несколькими офисами

Беспроводная связь может использоваться для объединения подсетей отдельных зданий, например центрального офиса и филиалов, там, где прокладка кабеля между зданиями нежелательна или невозможна (рис. 20).

Для организации связи между зданиями могут использоваться внешние беспроводные точки, работающие в режиме моста. Через uplink-порт внешняя точка подключается к обычному коммутатору и через него обеспечивает связь со всеми компьютерами подсети.

Внешние беспроводные точки имеют водонепроницаемый термостатированный корпус, систему грозовой защиты, систему питания Power-over-Ethernet. Благодаря сменной антенне можно обеспечивать устойчивую радиосвязь на расстоянии до нескольких километров на специализированные узконаправленные антенны.

При организации внешней беспроводной связи особое внимание следует обратить на обеспечение безопасности передачи данных, в связи с ее большей уязвимостью, как при прослушивании, так и в случае прямого физического воздействия. Поэтому рекомендуется использовать точки доступа, специально предназначенные для наружного применения и позволяющие задействовать аутентификацию, контроль доступа и шифрование передаваемых данных.

Необходимо также обратить внимание на то, что для внешних точек предусмотрена более сложная процедура получения разрешений на использование частот.

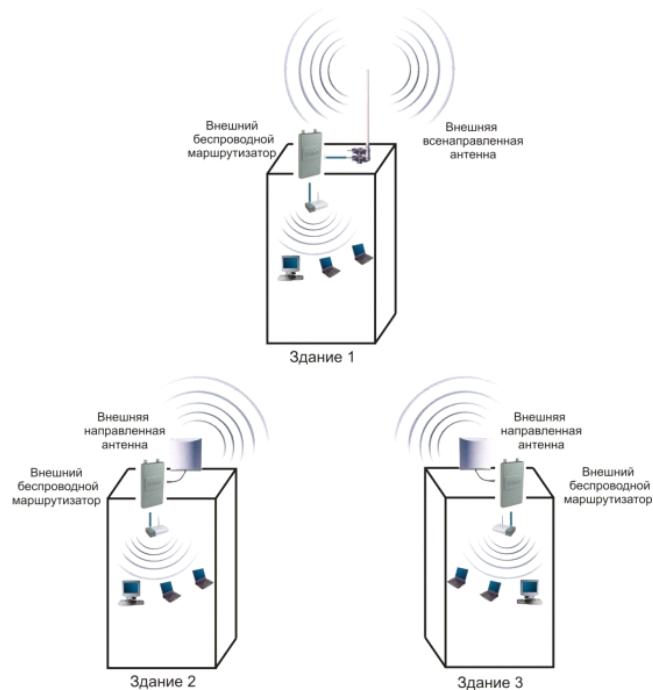


Рис. 20. Сеть между несколькими офисами

Беспроводные технологии в промышленности

Для использования в промышленности технологии Wi-Fi предлагаются пока ограниченным числом поставщиков. Так Siemens, Automation & Drivers предлагает Wi-Fi-решения для своих контроллеров SIMATIC в соответствии со стандартом IEEE 802.11g в свободном ISM-диапазоне 2,4 ГГц и обеспечивающим максимальную скорость передачи 54 Мбит/с. Данные технологии применяются для управления движущимися объектами и в складской логистике, а также в тех случаях, когда по какой-либо причине невозможно прокладывать проводные сети Ethernet. Использование Wi-Fi устройств на предприятиях обусловлено высокой помехоустойчивостью, что обуславливает их применение на предприятиях с множеством металлических конструкций. В свою очередь Wi-Fi приборы не создают существенных помех для узкополосных радиосигналов. В настоящее время технология находит широкое применение на удаленном или опасном производстве, там, где нахождение оперативного персонала связано с повышенной опасностью или вовсе затруднительно. К примеру, для задач телеметрии на нефтегазодобывающих предприятиях, а также для контроля за перемещением персонала и транспортных средств в шахтах и рудниках, для определения нахождения персонала в аварийных ситуациях.

Wi-Fi и телефоны сотовой связи

Некоторые считают, что Wi-Fi и подобные ему технологии со временем могут заменить сотовые сети, такие как GSM. Препятствиями для такого развития событий в ближайшем будущем являются отсутствие глобального роуминга, ограниченность частотного диапазона и сильно ограниченный радиус действия Wi-Fi. Более правильным

выглядит сравнение сотовых сетей с другими стандартами беспроводных сетей, таких как UMTS, CDMA или WiMAX.

Тем не менее, Wi-Fi пригоден для использования VoIP в корпоративных сетях или в среде SOHO. Первые образцы оборудования появились уже в начале 2000-х, однако на рынок они вышли только в 2005 году. Тогда такие компании, как Zyxel, UT Starcomm, Samsung, Hitachi и многие другие, представили Wi-Fi-телефоны на рынок VoIP по «разумным» ценам. В 2005 году ADSL ISP провайдеры начали предоставлять услуги VoIP своим клиентам (например нидерландский ISP XS4All). Когда звонки с помощью VoIP стали очень дешёвыми, а зачастую вообще бесплатными, провайдеры, способные предоставлять услуги VoIP, получили возможность открыть новый рынок — услуг VoIP. Телефоны GSM с интегрированной поддержкой возможностей Wi-Fi и VoIP начали выводиться на рынок, и потенциально они могут заменить проводные телефоны.

В настоящий момент непосредственное сравнение Wi-Fi и сотовых сетей необоснованно. Телефоны, использующие только Wi-Fi, имеют весьма ограниченный радиус действия, поэтому развертывание таких сетей обходится очень дорого. Тем не менее, развертывание таких сетей может быть наилучшим решением для локального использования, например, в корпоративных сетях. Однако устройства, поддерживающие несколько стандартов, могут занять значительную долю рынка.

Стоит заметить, что при наличии в данном конкретном месте покрытия как GSM, так и Wi-Fi, экономически намного более выгодно использовать Wi-Fi, разговаривая посредством сервисов интернет-телефонии. Например, клиент Skype давно существует в версиях, как для смартфонов, так и для КПК.

4 Эволюция технологии 802.11

4.1 Технология 802.11n

С появлением сетевых мультимедийных центров возникают такие задачи, как передача по беспроводной сети потока DVD. Поэтому IEEE одобрил создание рабочей группы по разработке стандарта 802.11n. Целью группы стала разработка нового физического уровня (PHY) и уровня доступа к среде передачи (MAC), которые позволили бы достичь реальной скорости передачи данных, как минимум, в 100 Мбит/с. То есть увеличить её в сравнении с реально существующими сегодня решениями примерно в четыре раза. Всё это, вместе с обратной совместимостью с существующими стандартами, должно было не только сделать работу в беспроводных сетях более комфортной, но и обеспечить достаточный запас скорости на ближайшее будущее.

В основе стандарта 802.11n:

- увеличение скорости передачи данных;
- увеличение зоны покрытия;
- увеличение надежности передачи сигнала;
- увеличение пропускной способности.

В разработке стандарта 802.11n предлагается пойти эволюционным путём, используя уже проверенные технологии, добавив к ним новые разработки, позволяющие достичь высоких скоростей передачи данных. Например, в стандарте 802.11n предлагается использовать такие "наследственные" технологии, как OFDM (ортогональное частотное мультиплексирование) и QAM (квадратурная амплитудная модуляция). Подобный подход обеспечит обратную совместимость и снизит стоимость разработки. Новый стандарт не должен мешать работе старых устройств 11a/g, и в то же время, должен поддерживать высокую скорость работы.

Черновую версию стандарта 802.11n (DRAFT 2.0) поддерживают многие современные сетевые устройства. Итоговая версия IEEE 802.11n (DRAFT 11.0), которая была принята 11 сентября 2009 года, обеспечивает скорость до 300 Мбит/с.

IEEE 802.11n - получила название Wi-Fi 4. Работает в диапазонах 2,4 и 5 ГГц (устройства, поддерживающие диапазон 5 ГГц встречаются реже). Стандарт 802.11n повышает скорость передачи данных в 3-11 раз по сравнению с устройствами стандартов 802.11g (максимальная скорость 54 Мбит/с), при условии использования в режиме 802.11n с другими устройствами 802.11n. Позволяет достигать скоростей до 150 Мбит/с при ширине канала 40 МГц на каждую независимую антенну. Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с.

Реальная скорость передачи данных всегда меньше канальной скорости. Для Wi-Fi реальная скорость передачи данных обычно отличается более чем в два раза в меньшую сторону. Кроме того, существует еще несколько факторов, ограничивающих реальную пропускную способность:

- канал всегда делится между клиентами;
- предавая служебный трафик, точка доступа всегда подстраивается под клиента, работающего на минимальной скорости;
- наличие помех (работающие рядом точки доступа, микроволновые печи, «радио-няни», bluetooth-устройства, радиотелефоны).

Увеличение физической скорости передачи

Первый способ увеличения скорости передачи данных - расширение частотного диапазона каждого канала с 20 МГц до 40 МГц. В спецификации 802.11n предусмотрены стандартные каналы 20 МГц, а также широкополосные 40 МГц. Это решение повышает пропускную способность до 150 Мбит/с на поток. В полосе частот 2.4 ГГц для беспроводных сетей доступны 13 каналов (в некоторых странах 11) с интервалами 5 МГц между ними. Для передачи сигнала беспроводные устройства стандарта 802.11b/g используют каналы шириной 20 МГц.

Для исключения взаимных помех между каналами необходимо, чтобы их полосы отстояли друг от друга на 25 МГц. Таким образом, остается всего 3 непересекающихся канала на полосе 20 МГц: 1, 6 и 11. С 20 МГц каналами стандарт предоставляет лишь около 72 Мбит/с на поток. С шириной канала 40 МГц непересекающимися являются каналы 3 и 11.

В полосе частот 5 ГГц доступно 19 непересекающихся каналов, которые более пригодны для применения в устройствах стандарта 802.11n, обеспечивающих максимально возможную скорость передачи данных. Сигналы распределяются без взаимного перекрытия каналов с шириной полосы 40 МГц.

Так как у точек доступа стандарта 802.11n, пропускная способность может превысить 100 Мбит/с, каналы Fast Ethernet могут стать узким местом на пути сетевого трафика. Поэтому при разворачивании беспроводной сети желательно использовать коммутаторы Gigabit Ethernet.

Второй способ увеличения скорости - использование MIMO (multiple input multiple output). MIMO системы обеспечивают параллельную передачу множества сигналов, увеличивая суммарную пропускную способность. Число параллельных каналов зависит не может превышать минимального числа антенн, используемых для передачи и приема. Чтобы получить физическую скорость 100 Мбит/с, стандарт 802.11n должен поддерживать технологию MIMO не меньше, чем для двух потоков.

Стандарт 802.11n определяет различные антенные конфигурации "MxN", начиная с "1x1" до "4x4" (самые распространенные на сегодняшний день это конфигурации "3x3" или "2x3"). Первое число (M) определяет количество передающих антенн (T), а второе число (N) определяет количество приемных антенн (R).

Большинство предлагаемых производителями точек доступа поддерживает MIMO 2x2 или 1x1, то есть SISO (одноточковая передача). Встроенные в мобильные устройства Wi-Fi-адAPTERы обычно поддерживают режим SISO. Пользователи с повышенными требованиями к скорости передачи данных смогут приобрести модели с конфигурацией антенн 4x4.

Технологии МИМО включают в себя сложные векторные и матричные алгоритмы обработки в системах со множеством антенн (multi-antenna).

Метод кодирования OFDM по своей структуре в настоящее время является оптимальным для поддержания технологии MIMO. В МИМО используется методика предварительного кодирования и последующего декодирования (Precoding) с формированием пространственной диаграммы направленности (beamforming), которая представляет собой некое векторное расширение стандартной плоской диаграммы направленности. При формировании пространственной диаграммы направленности используется множество антенн для передачи сигналов. Такой подход позволяет значительно улучшить охват и емкость системы, а также уменьшить вероятность нарушения связи. Чтобы обеспечить пространственное разнесение и оптимальный запас времени на замирание, в методе МИМО используются коды «пространство-время» (Space-Time Code, STC).

Методика МИМО включает в себя так называемое «пространственное мультиплексирование» (Spatial Multiplexing, SM), которое повышает скорости передачи и увеличивает пропускную способность по сравнению с отдельной одиночной антенной. При пространственном мультиплексировании множество потоков передаются по множеству антенн.

В методе МИМО необходимо постоянно запрашивать информацию по идентификации канала, его состоянию и конкретным параметрам. В зависимости от текущего состояния канала сигналы передаются по разным подканалам. Специальные сигналы используются для преобразования параметров самих подканалов, таких, например, как диаграмма направленности элементов адаптивной антенны, коррекция ошибок, скорость передачи и др. Для коррекции ошибок используется коэффициент ошибок пакетов (Packet Error Rate, PER). Когда канал находится в плохом состоянии, увеличивается значение этого коэффициента и, как следствие, автоматически зона покрытия ограничивается до величины, где может быть выдержано расчетное значение PER. Следует иметь в виду, что SM и STC обеспечивают большой охват независимо от состояния канала, но не повышают пиковую скорость данных.

Изменения коснулись и MAC-уровня, который получил новые функции. Важно понимать, что скорость передачи существенно ограничивается заголовками физического уровня (PHY) и задержками. Однако они плохо поддаются улучшению. Более того, заголовки физического уровня PHY приходится делать даже больше, чтобы поддержать новые режимы.

В стандарте 802.11n введен новый эффективный подход к увеличению эффективности передачи - составные последовательности обмена (aggregate exchange sequences). Составная последовательность - это объединение нескольких блоков данных протокола MAC (MAC Protocol Data Units, MPDU) в один блок данных протокола PHY (PHY Protocol Data Unit, PPDU). Составные последовательности обмена доступны при использовании протокола, который может подтверждать прием нескольких блоков MPDU одним подтверждением приема блока (Block ACK) в ответ на запрос подтверждения блока (block acknowledgement request, BAR). Такой протокол снимает необходимость инициирования передачи каждого блока MPDU. Если использовать существующие протоколы уровня MAC без составных последовательностей, то для того, чтобы

достичь предписанной группой TGn скорости передачи данных 100 Мбит/с в точке доступа MAC, физическая скорость передачи должна быть равна 500 Мбит/с.

Еще одна возможность повышения эффективности передачи - новые механизмы передачи данных уровня MAC, которые позволяют передавать данные в обоих направлениях без необходимости инициации передачи. Данный подход позволяет посыпать ответ на составной блок MPDU в обратном направлении в ответ на инициацию передачи станцией-инициатором. При обеспечении защиты от конфликтов в BSS можно создать механизмы для минимизации времени реверсирования передачи между инициатором и ответчиком.

Предусматриваются MAC-кадры нового формата, которые позволяют создавать пакеты физического уровня с информацией сразу для нескольких клиентов.

Количество поднесущих в канале определено равным 56 при ширине канала 20 МГц и 114 – при ширине канала 40 МГц. Частотный разнос каналов разрешен как для 20, так и для 40 МГц. В стандарте 802.11n в соответствии с нормативами РФ допускается использование до четырех каналов передачи данных. Подразумевается, что не менее двух каналов могут быть у Wi-Fi-точки доступа и не менее одного канала должно быть у беспроводной абонентской станции.

Еще один параметр, влияющий на скорость передачи, – это длительность охранного интервала GI, введенная в стандарте 802.11a. В стандарте 802.11 длительность охранного интервала может принимать два значения: 800 и 400 нс.

Оборудование Wi-Fi в стандарте 802.11n может работать в трех режимах:

- «чистом» режиме - 802.11n (именно в этом режиме и можно воспользоваться преимуществами повышенной скорости и увеличенной дальностью передачи данных стандарта 802.11n).
- наследуемом (Legacy), в котором обеспечивается поддержка устройств 802.11b/g и 802.11a;
- смешанном (Mixed), в котором поддерживаются устройства 802.11b/g, 802.11a и 802.11n;

Режим с высокой пропускной способностью HT (High Throughput)

Точки доступа 802.11n используют режим High Throughput (HT), известный также как "чистый" режим (Greenfield-режим), который предполагает отсутствие поблизости (в зоне покрытия) работающих устройств 802.11b/g, использующих ту же полосу частот. Если же такие устройства существуют в зоне покрытия, то они не смогут общаться с точкой доступа 802.11n. Таким образом, в этом режиме разрешены к использованию только клиенты 802.11n, что позволяет воспользоваться преимуществами повышенной скорости и увеличенной дальностью передачи данных, обеспечиваемыми стандартом 802.11n.

Режим с невысокой пропускной способностью Non-HT

Точка доступа 802.11n с использованием режима Non-HT (известный также как наследуемый режим), отправляет все кадры в формате 802.11b/g, чтобы устаревшие станции смогли понять их. В этом режиме точка доступа должна использовать ширину каналов 20 МГц и при этом не будет использовать преимущества стандарта 802.11n. Для обеспечения обратной совместимости все устройства должны поддерживать этот режим. Нужно учитывать, что точка доступа 802.11n с использованием режима Non-HT не будет обеспечивать высокую производительность. При использовании этого режима передача данных осуществляется со скоростью, поддерживаемой самым медленным устройством.

Смешанный режим с высокой пропускной способностью HT Mixed

Смешанный режим HT Mixed будет наиболее распространенным режимом для точек доступа 802.11n в ближайшие несколько лет. В этом режиме, усовершенствования стандарта 802.11n могут быть использованы одновременно с существующими станциями 802.11b/g. Режим HT Mixed обеспечит обратную совместимость устройств, но устройства 802.11n получат уменьшение пропускной способности. В этом режиме точка доступа 802.11n распознает наличие старых клиентов и будет использовать более низкую скорость передачи данных, пока старое устройство осуществляет прием-передачу данных.

Беспроводные точки доступа и клиенты 802.11n производят согласование ширины канала и *пространственных потоков* (англ. *spatial streams*). Число пространственных потоков зависит от количества антенн. Так, максимальную теоретическую пропускную способность можно достичь лишь в конфигурации 4x4: четыре передающих и четыре приёмных антенн. Стандарт 802.11n определяет *индекс модуляции и схемы кодирования* (англ. *modulation and Coding Scheme. MCS*) в виде целого числа от 0 (соответствует самому медленному, но надёжному режиму) до 31 (наиболее быстрый, но чувствительный к радиопомехам режим). Индекс определяет тип модуляции радиочастоты (Type), скорость кодирования (англ. *coding rate*), защитный

интервал (англ. *guard interval*) и ширину канала. В сочетании эти параметры определяют теоретическую скорость передачи данных, начиная от 6,5 Мбит/с до 600 Мбит/с (**таблица 4.1**). Максимальная скорость может быть достигнута за счет использования всех возможных опций.

Таблица 4.1 – Индекс модуляции и схемы кодирования MCS

MCS Index	Type	Coding Rate	Spatial Streams	Data Rate (Mbps) with 20 MHz CH		Data Rate (Mbps) with 40 MHz CH	
				800 ns	400 ns (SGI)	800 ns	400 ns (SGI)
0	BPSK	1/2	1	6.50	7.20	13.50	15.00
1	QPSK	1/2	1	13.00	14.40	27.00	30.00
2	QPSK	3/4	1	19.50	21.70	40.50	45.00
3	16-QAM	1/2	1	26.00	28.90	54.00	60.00
4	16-QAM	3/4	1	39.00	43.30	81.00	90.00
5	64-QAM	2/3	1	52.00	57.80	108.00	120.00
6	64-QAM	3/4	1	58.50	65.00	121.50	135.00
7	64-QAM	5/6	1	65.00	72.20	135.00	150.00
8	BPSK	1/2	2	13.00	14.40	27.00	30.00
9	QPSK	1/2	2	26.00	28.90	54.00	60.00
10	QPSK	3/4	2	39.00	43.30	81.00	90.00
11	16-QAM	1/2	2	52.00	57.80	108.00	120.00
12	16-QAM	3/4	2	78.00	86.70	162.00	180.00
13	64-QAM	2/3	2	104.00	115.60	216.00	240.00
14	64-QAM	3/4	2	117.00	130.00	243.00	270.00
15	64-QAM	5/6	2	130.00	144.40	270.00	300.00
16	BPSK	1/2	3	19.50	21.70	40.50	45.00
...
31	64-QAM	5/6	4	260.00	288.90	540.00	600.00

Короткий защитный интервал SGI (Short Guard Interval) определяет интервал времени между передаваемыми символами (наименьшая единица данных, передаваемых за один раз). Этот интервал помогает при приеме данных избежать задержки из-за межсимвольных помех Inter-Symbol Interference (ISI) и преодолеть эхо (отражение звуковых волн). В устройствах стандарта 802.11b/g используется защитный интервал 800 нс, а в устройствах 802.11n есть возможность использования паузы всего в 400 нс. Более короткие интервалы привели бы к большему вмешательству и снижению пропускной способности, в то время как большие интервалы могут привести к нежелательным простоям в беспроводной среде. Короткий защитный интервал (SGI) может повысить скорость передачи данных до 11 процентов.

Точки доступа 802.11n должны поддерживать MCS значения от 0 до 15, в то время как 802.11n станции должны поддерживать MCS значения от 0 до 7. Все другие значения MCS, в том числе связанные с каналами шириной 40 МГц, коротким защитным интервалом (SGI), являются опциональными. Определение значения MCS и SGI для всех устройств 802.11n, является хорошим способом для определения набора скоростей передачи данных, которые могут быть использованы беспроводной сетью.

В **таблице 4.2** приведено сравнение характеристик стандартов 802.11 a/g/n.

Таблица 4.2 - Основные характеристики стандартов группы IEEE 802.11

Стандарт	802.11g	802.11a	802.11n
Частотный диапазон, ГГц	2,4-2,483	5,15-5,25	2,4 или 5,0
Метод передачи	DSSS,OFDM	DSSS,OFDM	MIMO
Скорость, Мбит/с	1-54	6-54	6-300
Совместимость	802.11 b/n	802.11 n	802.11 a/b/g
Метод модуляции	BPSK, QPSK, OFDM	BPSK, QPSK, OFDM	BPSK, 64-QAM
Дальность связи в помещении, м	20-50	10-20	50-100
Дальность связи вне помещения, м	250	150	500

В России стандарт официально сертифицирован. Оборудование стандарта 802.11n разрешено к применению на территории России в диапазонах 2400–2483,5, 5150–5350 и 5650–5725 МГц приказом Министерства связи и массовых коммуникаций России от 14 сентября 2010 г. № 124.

Недостатки решений 802.11n

- исключительно широкополосный сигнал потенциально может создать помехи работе других беспроводных устройств - особенно в перегруженном диапазоне 2,4 ГГц;
- усложнение антенных систем приводит к увеличению габаритов устройств;
- увеличение числа передатчиков приведет к уменьшению времени работы от батарей портативных устройств;
- существенное увеличение производительности беспроводных сетей доступно только в диапазоне 5 ГГц.

4.2 Стандарт 802.11ac

На утверждение стандарта 802.11n в свое время ушло около 5 лет. Его разработка началась в 2004 году, а в 2006 была принята первая предварительная драфт-версия. Окончательно 802.11n был утвержден только в 2009 году. Такая же судьба постигла и нынешнее поколение беспроводных сетей - 802.11ac. Его проектирование стартовало еще в 2008 году, а закончилось лишь в конце 2013. В самом начале 2014 года организация IEEE наконец-то приняла окончательные спецификации стандарта 802.11ac для беспроводных сетей.

Первые 802.11ac девайсы появились еще в 2012 году, хотя дебютная программа сертификации организации Wi-Fi Alliance состоялась лишь в середине 2013 года (Draft 3.0). На рынке были лишь те устройства, которые соответствовали драфт-версии 802.11ac (в дальнейшем будем называть их роутерами первой волны). В некоторых из них (например, в шестиантенном роутере Netgear Nighthawk X6) производители использовали собственные наработки, которые позволяли «выжать» из технологии еще больше производительности. Роутеры второй волны, основанные на окончательной спецификации 802.11ac, появились в 2015 году. Они предлагают более высокую производительность за счет поддержки некоторых новых функций.

Стандарт 802.11ac - стандарт беспроводных локальных сетей WiFi, работающий в диапазоне частот 5 ГГц. Обратно совместим с IEEE 802.11n (в диапазоне 5 ГГц) и IEEE 802.11a. Получил название **Wi-Fi 5**. Устройства с 802.11ac обычно также реализуют стандарт 802.11n в диапазоне 2,4 ГГц.

В настоящее время маршрутизаторы с поддержкой IEEE 802.11ac еще только становятся массовыми, но в организации IEEE уже идет работа над следующим (шестым) поколением беспроводных сетей - 802.11ax. Скорость передачи данных вновь увеличилась, но в IEEE не собираются останавливаться на достигнутом, и уже разрабатывают преемника - стандарт 802.11ax.

Технология 802.11ac до 25 мая 2015 г. формально была не разрешена к использованию на территории РФ. Сама технология имеет целый набор преимуществ, которые обеспечат быструю адаптацию в РФ, как это в настоящее время происходит по всему миру:

- в несколько раз большая скорость пропускания (по сравнению со стандартом WiFi 802.11n). Устройства с 433 Мбит/с на канал уже были доступны летом 2014 года и до 6,77 Гбит/с при 8xMU-MIMO-антеннах;
- большее покрытие (по сравнению со стандартом 11n);
- снижение энергопотребления (Дж/бит), что, в свою очередь, продлит время автономной работы мобильных устройств (в 2-4 раза по сравнению с 11n).

Основными преимуществами стандарта WiFi 802.11ac являются высокие скорости передачи в радиоканале и, соответственно, большая агрегированная полоса пропускания точки доступа, а также более совершенные механизмы контроля активного и пассивного состояния клиентских устройств. Все это вместе ведет к значительной экономии заряда батареи мобильного устройства.

Решения на базе WiFi-стандарта 802.11ac достигает высоких скоростей передачи данных (data transfer) с помощью трехмерной функциональной матрицы:

- а) большее количество объединяемых частотных каналов в сумме до: 80MHz или даже 160MHz (по сравнению с максимумом в 40MHz для 802.11n);
- б) большая доступная модуляция: до QAM256 (в 802.11n максимум QAM64);
- в) больший уровень ММО: до 8 пространственных потоков (в 802.11n до 4 потоков).

Стандарт 802.11ac разработан для диапазона 5 ГГц. Этот диапазон загружен значительно меньше, чем 2,4 ГГц, поэтому сигнал меньше подвержен различным помехам. В новую технологию также перекочевала функция SU-MIMO (single-user multiple input/multiple output), которая была чуть ли не основной отличительной чертой 802.11n. Принцип ее работы заключается в том, что она позволяет передавать одному клиенту (устройству) сразу несколько потоков информации. В 802.11ac технология получила более производительную систему модуляции, которая обеспечивает максимальную пропускную способность каждого потока в 433 Мбит/с.

Первое поколение (Первая волна) устройств стандарта WiFi 802.11ac (Wave-1) продолжает оставаться полудуплексной радиотехнологией. Такие устройства используют, как правило, частотные каналы шириной до 80MHz и чаще всего до трех пространственных потоков. Стоит отметить, что роутеры первой волны поддерживают передачу до трех потоков одновременно, поэтому их суммарная пропускная способность находится в районе 1300 Мбит/с. В стандарте 802.11n также была реализована параллельная передача данных по трем потокам, однако ширина каждого потока равнялась всего лишь 150 Мбит/с, что в совокупности составляло скромные 450 Мбит/с.

Поэтому при относительно грубом делении можно обозначить низкий уровень продуктов 802.11ac со скоростями в радиоканале до 433 Мб/с, средний уровень со скоростями до 867 Мб/с и высокий уровень со скоростями до 1,3Гб/с. Практически доступные скорости передачи данных (transfer) для пользователей будут значительно ниже в силу проблем общей эффективности группы стандартов 802.11. Как правило, практически доступный максимум не выше 60%. Точки доступа и WiFi-маршрутизаторы 802.11ac первой волны сейчас широко доступны в мире и начали официально завозиться в РФ после разрешения в 2015 г.

Вторая волна 802.11ac вначале будет поддерживать частотные каналы до 160 МГц до четырех пространственных потоков и технологию одновременной коммуникации более чем с одним пользователем MU-MIMO (Multi User MIMO). MU-MIMO позволяет отправлять множество фреймов одновременно ко многим пользователям в том же самом частотном спектре.

Тем самым с множественными антennами и с помощью соответствующей технологии точка доступа WiFi может вести себя как беспроводный коммутатор. Но технология ограничена сверху максимальным количеством доступных пространственных потоков. Отсюда в случае трех поддерживаемых пространственных потоках на точке доступа и наличии только трехпоточных клиентов (MacBook Pro), всегда с точкой будет взаимодействовать только один клиент даже при поддержке MU-MIMO.

Поэтому MU-MIMO особенно перспективно выглядит для случая, когда в сети присутствуют в основном персональные мобильные устройства, такие как смартфоны и планшеты, имеющие максимум 2 пространственных потока, но чаще всего один. Для случая смартфонов с одним потоком и точки доступа WiFi с тремя потоками и MU-MIMO будет случай работы один к трем, и точка поддерживает до трех клиентов одновременно и параллельно.

Роутеры второй волны получат несколько важных изменений.

Во-первых, у них появится поддержка технологии MU-MIMO. Она работает по такому же принципу, как и SU-MIMO, однако в отличие от последней умеет передавать данные не одному, а сразу нескольким клиентам.

Во-вторых, новые роутеры смогут объединять несколько каналов на частоте 5 ГГц в единый поток с полосой пропускания с частотой 160 МГц. Роутеры первой волны также умеют объединять несколько каналов, однако частота полосы пропускания составляет 80 МГц.

В-третьих, новые роутеры будут поддерживать передачу по восьми потокам одновременно - вместо текущих трех. Девайсы второй волны будут использовать более широкие каналы и дополнительные потоки, улучшенную технологию формирования направленного сигнала (beamforming) и другие функции. Это позволит нарастить скорость физической передачи данных до 7–10 Гбит/с.

Можно ожидать в начале второй волны стандарта WiFi 802.11ac (Wave-2) появления точек доступа со скоростями в радиоканале до 3.47 Гб/с (4 пространственных потока, QAM256, MU-MIMO). При этом максимум стандарта 802.11ac обеспечивает выход на канальные скорости до 6.93 Гб/с при поддержке до 8-и пространственных потоков. Но 8 потоков потребуют как минимум 8 антенн (а желательно и больше) с необходимым разнесением, что диктует существенное увеличение размеров устройств и требует большее количество энергии для работы через PoE. Анализ скоростей в 802.11 ac (**таблица 4.3**) привела в одной из своих статей компания Aruba.

Важно отметить, что последние два варианта с восемью пространственными потоками на данном этапе развития технологии выглядят маловероятными для массового производства и применения. Тем более что наличия трех неперекрывающихся каналов в 5 ГГц шириной 160 МГц каждый пока не приходилось встречать ни в одной стране мира. Только комиссия FCC в США довольно близко подошла к тому, чтобы расчистить такой участок спектра и обеспечить максимальные возможности для реализации решения стандарта WiFi 802.11ac.

Таблица 4.3 - Достигимые скорости в 802.11ac

Channel bandwidth	Transmit - Receive antennas	Modulation and coding etc	Typical client scenario	Throughput (individual link rate)	Throughput (aggregate link rate)
80 MHz	1x1	256-QAM 5/6, short guard interval	Smartphone	433 Mbps	433 Mbps
80 MHz	2x2	256-QAM 5/6, short guard interval	Tablet, PC	867 Mbps	867 Mbps
160 MHz	1x1	256-QAM 5/6, short guard interval	Smartphone	867 Mbps	867 Mbps
160 MHz	2x2	256-QAM 5/6, short guard interval	Tablet, PC	1.73 Gbps	1.73 Gbps
160 MHz	4x Tx AP, 4 clients of 1x Rx	256-QAM 5/6, short guard interval	Multiple smartphones	867 Mbps per client	3.47 Gbps
160 MHz	8x Tx AP, 4 clients with total of 8x Rx	256-QAM 5/6, short guard interval	Digital TV, set-top box, tablet, PC, smartphone	867 Mbps to two 1x clients 1.73 Gbps to one 2x client 3.47 Gbps to one 4x client	6.93 Gbps
160 MHz	8x Tx AP, 4 clients of 2x Rx	256-QAM 5/6, short guard interval	Multiple set-top boxes, PCs	1.73 Gbps to each client	6.93 Gbps

Характеристики покрытия радиоустройств с 802.11ac значительно выше, чем 802.11n. И хотя максимальные скорости на 802.11ac доступны относительно близко к точке доступа, но общие дистанции предоставления высокоскоростного сервиса значительно больше, чем у устройств 802.11n. Ниже приведен график компании Cisco с анализом Rate vs Range (рисунок 4.1), дистанция отображена в футах.

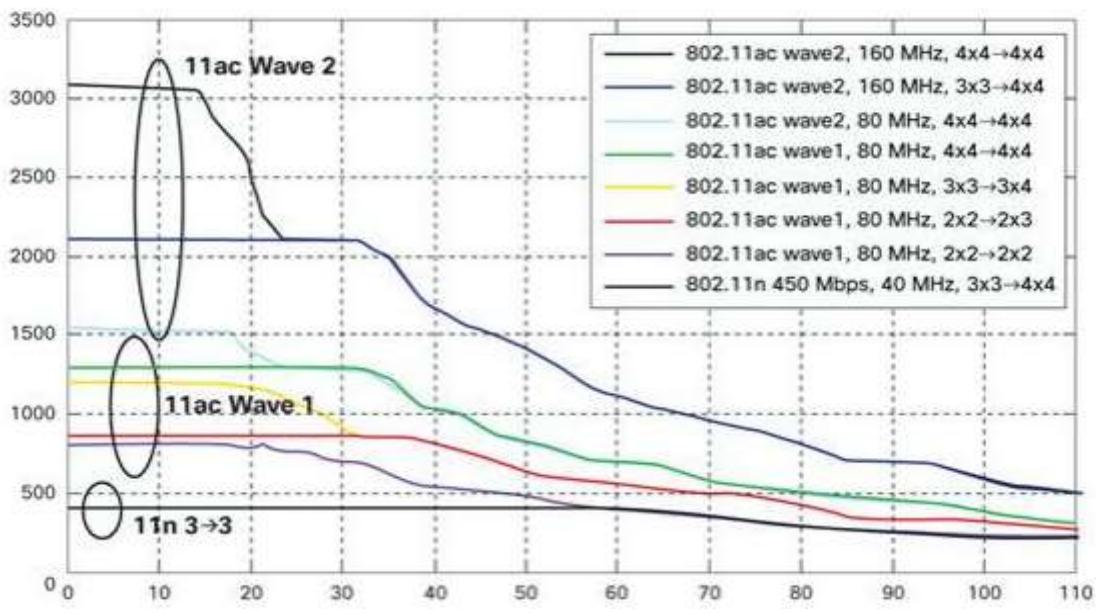


Рисунок 4.1 – Зависимость скорости 802.11ac от дальности

Технология формирования направленного сигнала (beamforming)

В 802.11 эта технология используется не впервые. Стандарт 802.11n поддерживал ее, однако, только на уровне опций. IEEE не обязывала производителей внедрять бимформинг, и когда они решались на это, то четких указаний IEEE о том, как должна работать технология, не было. Возникали ситуации, когда маршрутизаторы и Wi-Fi-адAPTERы по-разному формировали направленный сигнал, и технология не работала. Чтобы избежать этого, некоторые компании даже выпускали наборы устройств, одно из которых подключалось к роутеру, а другое – к компьютеру или какому-либо другому гаджету. Одним из таких наборов был Netgear WNHDB3004 Wireless Home Theater Kit, предназначенный для домашних кинотеатров. Стоимость устройств, была довольно высока и лишь единицы стремились переплачивать за незначительную прибавку производительности.

С появлением 802.11ac ситуация с бимформингом изменилась. IEEE прописала четкие правила для имплементации технологии, хотя и не сделала ее обязательной. Теперь, если одно устройство поддерживает бимформинг, а другое – нет, то они все равно будут работать вместе, хотя раньше это было невозможно.

На практике формирование направленного сигнала позволяет более эффективно использовать полосу пропускания, что положительно отражается на передаче потокового видео, качестве аудиоданных и всех других операциях, чувствительных к пропускной способности и латентности сети.

Как же работает технология? Беспроводные роутеры и адаптеры сети, не поддерживающие бимформинг, одинаково транслируют данные во всех направлениях. В свою очередь, девайсы, которые поддерживают данную технологию, осуществляют передачу данных в конкретном направлении – туда, где находится девайс, принимающий сигнал. Если клиентское устройство также умеет формировать направленный сигнал, то вместе с маршрутизатором они могут обмениваться информацией о своем местоположении и, исходя из этого, определять кратчайший путь к другу.

Среди роутеров первой волны встречалось не так много девайсов, которые поддерживали бимформинг. В основном это были продукты компании Netgear, но свои модели представили компании D-Link и Linksys. Окончательно прижиться бимформинг должен в маршрутизаторах второй волны.

4.3 IEEE 802.11ax – следующее поколение Wi-Fi

Стандарт 802.11ac был окончательно утвержден в 2014 году, но в стенах организации IEEE уже кипит работа по разработке следующего поколения Wi-Fi – 802.11ax. Несмотря на это, по предварительным планам принять финальные спецификации IEEE намерена не раньше 2019 года. Однако, судя по развитию стандартов 802.11n и 802.11ac, первые 802.11ax устройства появятся значительно раньше.

Новая версия стандарта Wi-Fi-802.11ax, которую уже окрестили "Эффективной" (High Efficiency Wireless) предназначена для решения проблем со скоростью доступа в высоконагруженных сетях. Основной задачей HEW Wi-Fi (802.11ax) будет повышение средней пропускной способности в беспроводной сети на одного пользователя. Подобная попытка была сделана ранее в стандарте 802.11ac, когда были предложены различные способы увеличения согласованной работы большого количества устройств, но многие из них, оказывается, работают недостаточно эффективно.

При сравнении с предыдущим стандартом 802.11ac, можно отметить, что с появлением 802.11ax будет осуществлен возврат в диапазон 2.4 ГГц. Ранее из этого диапазона ушли (в 802.11ac он не поддерживался), но, в конечном итоге, поняли, что 5-гигагерцовый диапазон имеет свои недостатки, и в частности, малый радиус действия. Даст ли возврат в диапазон 2.4 ГГц какие-то преимущества, момент спорный: в этом диапазоне хоть и больший радиус действия, но старых устройств b/g/n тоже значительно больше, а значит, придется работать в режиме совместимости с ними. Более подробный список изменений приведен в **таблице 4.4**.

Таблица 4.4 – Сравнение стандартов 802.11ac и 802.11ax

Параметры	802.11ac	802.11ax
Диапазон, ГГц	5	2.4 / 5
Ширина канала, МГц	20,40, 80, 80 + 80, 160	20,40, 80, 80 + 80, 160
Размер FFT в OFDM	62, 128, 256, 512	256, 512, 1024, 2048
Уровень модуляции	256-QAM	1024-QAM
Скорости передачи данных Мбит/сек	433 (ширина канала 80 МГц) 6933 (ширина канала 160 МГц)	600.4 (ширина канала 80 МГц) 9607.8 (ширина канала 160 МГц)

В стандарте 802.11ax предполагаются следующие улучшения:

- как и в ранее выпущенных стандартах, 802.11ax будет иметь обратную совместимость с линейкой ранее выпущенного оборудования Wi-Fi-стандартов: 802.11a / b / g / n / ac;
- сможет работать как в 5 ГГц, так и в 2.4 ГГц;
- поддержка всех основных частотных полос, вплоть до 160 МГц;
- расширен ряд доступных схем кодирования вплоть до 1024QAM;
- скорости передачи данных и ширину канала планируется оставить такой же, как и в 802.11ac, за исключением того, что будут добавлены новые методы кодирования: MCS 10 и MCS 11, поддерживающие модуляцию 1024-QAM;

- MIMO 8x8, до 8 пространственных потоков;
- величина OFDM символа в четыре раза больше, чем в решениях по стандарту 802.11ac;
- в 4 раза будут увеличены размеры OFDM FFT. Это значит, что поднесущие станут ближе друг к другу (расстояние между ними уменьшится в 4 раза - **рисунок 4.2**), кроме того, будет увеличена длительность каждого символа (тоже в 4 раза). Это позволит повысить надежность при передаче данных и производительность беспроводных устройств в условиях многолучевого замирания;

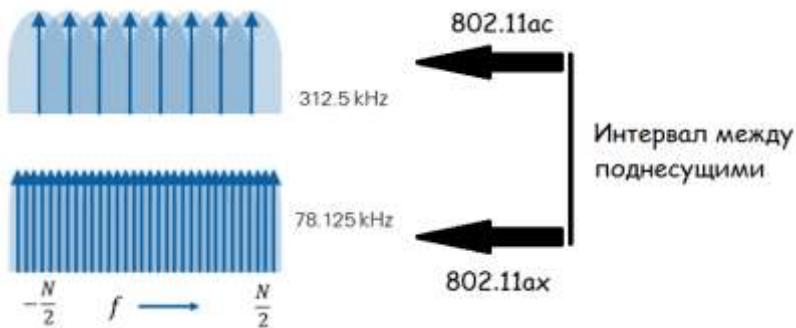


Рисунок 4.2 - Интервалы между поднесущими в 802.11ax

- клиенты с поддержкой MU-MIMO могут взаимодействовать с точкой доступа 802.11ax параллельно в обоих направлениях (DL и UL);
- значительно увеличиваются возможности пространственного мультиплексирования и полностью нивелируются фундаментальные ограничения базового стандарта 802.11, которые имеет полудуплексную природу. Передача данных Uplink и Downlink будет производиться с использованием технологии MU-MIMO и OFDMA;
- новые схемы усиления передачи преамбулы и повторной перепосылки теоретически могут обеспечить несколько дополнительных dB усиления по сравнению с 802.11ac. Это может создать условия для получения лучшего покрытия;
- четырехкратное увеличение средней пропускной способности сети для каждого отдельного пользователя в сильно загруженных хот-спотах (вокзалах, аэропортах, стадионах и др.);
- изменится алгоритм доступа к каналу передачи данных;
- доработан механизм beamforming. Формирователь диаграммы направленности инициирует процедуру зондирования канала с помощью Null Data Packet. При этом он измеряет уровень активности в канале и использует эту информацию для вычисления матрицы каналов. Затем матрица каналов используется для фокусировки радиочастотной энергии в сторону каждого отдельного пользователя.

Многопользовательские MIMO и OFDMA

В стандарте 802.11ax будет определено два режима работы:

Single User (один пользователь). В этом режиме беспроводные станции STA посылают и принимают данные точек доступа AP по одному, как только они получают доступ к среде.

Multi-User (многопользовательский режим). Этот режим позволяет точке доступа одновременно работать с несколькими STA. Стандарт делит этот режим дальше на многопользовательский Downlink и Uplink.

Downlink Multi-User позволяет точке доступа AP одновременно передавать данные нескольким беспроводным STA, которые обслуживаются в зоне радиопокрытия AP. Существующий стандарт 802.11ac уже определяет эту функцию. А вот многопользовательский Uplink является нововведением.

Uplink Multi-User позволяет точке доступа AP одновременно принимать данные от нескольких беспроводных станций STA. Это новая возможность стандарта 802.11ax, которая не существовала ни в одной из предыдущих версий стандарта Wi-Fi.

В многопользовательском режиме работы стандарт также определяет два разных способа мультиплексирования большего числа пользователей в определенной области: Multi-User MIMO и OFDMA. Для обоих этих методов точка доступа AP выступает в качестве центрального контроллера, аналогично тому, как сотовая базовая станция LTE управляет мультиплексированием пользователей в зоне обслуживания.

Многопользовательский MIMO

Устройства 802.11ax будут использовать методы формирования диаграммы направленности (зимствованные из 802.11ac) для одновременного направления пакетов к нескольким пространственно разнесенным пользователям. То есть, точка доступа AP будет вычислять матрицу каналов для каждого

пользователя и управлять параллельными лучами для разных пользователей, причем каждый луч будет содержать пакеты для своего конкретного пользователя.

В 802.11ax поддерживается одновременная отправка до восьми многопользовательских MIMO-потоков. Кроме того, каждый поток MU-MIMO может иметь собственный MCS (скорость передачи и степень модуляции). К разным пользователям может быть организовано произвольное количество потоков. При использовании пространственного мультиплексирования MU-MIMO, точки доступа можно будет сравнивать с коммутатором Ethernet, имеющим несколько портов. Каждый отдельный порт – это отдельный поток MU-MIMO. При этом, до каждого отдельного абонента может быть "проброшено" несколько потоков (рисунок 4.3).

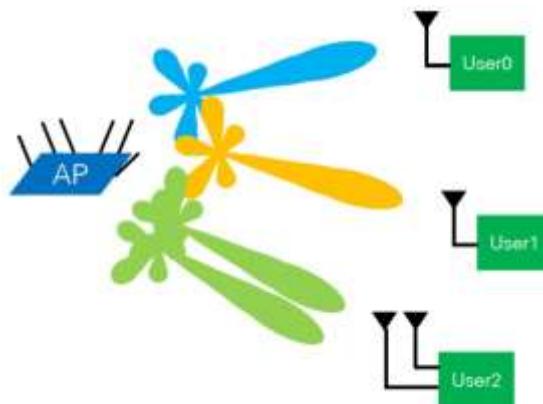


Рисунок 4.3 – MU-MIMO Beamforming для обслуживания множества, пространственно разнесенных пользователей

Новой функциональностью в 802.11ax является MU-MIMO Uplink. Как было указано выше, точка доступа AP может инициировать одновременный прием пакетов от каждой из STA посредством триггерного кадра. Когда несколько STA в ответ на триггерный кадр передают свои собственные пакеты, точка доступа AP применяет матрицу каналов к принятым лучам и отделяет информацию, содержащуюся в каждом луче. Так AP также может инициировать многопользовательский прием одновременный от всех абонентских STA в сети (рисунок 4.4).

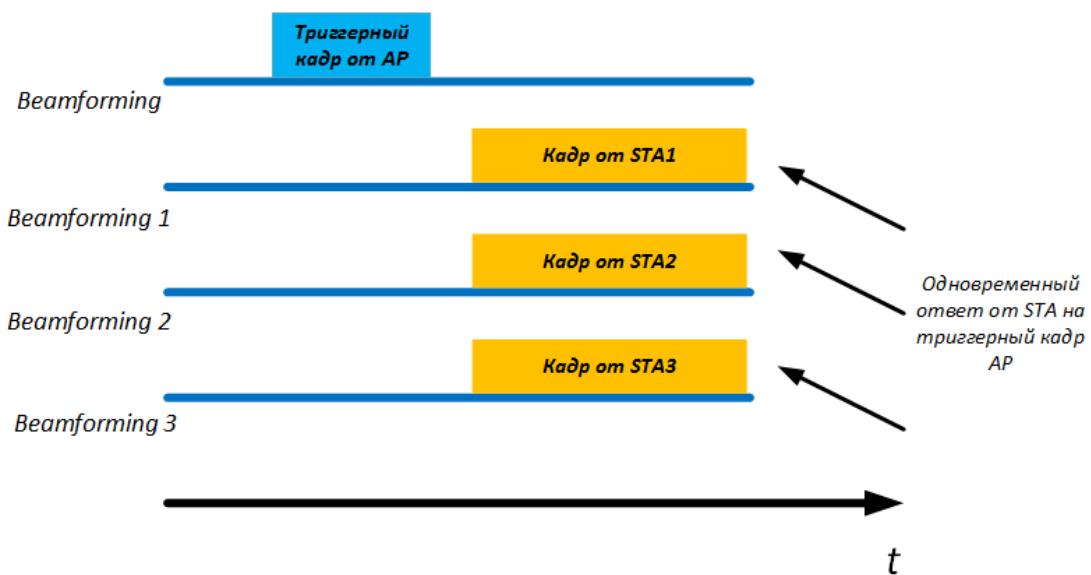


Рисунок 4.4 – MU-MIMO Uplink

Многопользовательский OFDMA

В стандарте 802.11ax появится новая для Wi-Fi, заимствованная из сетей 4G, технология мультиплексирования большого количества абонентов в общей полосе пропускания: Orthogonal Frequency Division Multiple Access (OFDMA). Эта технология основывается на OFDM, которая уже используется в 802.11ac. Суть ее в том, что OFDMA в 802.11ax позволяет дополнительно "нарезать" стандартные каналы шириной 20, 40, 80 и 160 МГц на более мелкие. Таким образом, происходит разделение каналов на более мелкие подканалы с предопределенным количеством поднесущих. Как и в LTE, в стандарте 802.11ax наименьший подканал

называется Resource Unit (RU), имеющий минимальный размер в 26 поднесущих. Для наглядности, на **рисунке 4.5** изображено разделение частотных ресурсов для одного пользователя с использованием OFDM (слева) и мультиплексирование четырех пользователей в одном канале с использованием OFDMA (справа):

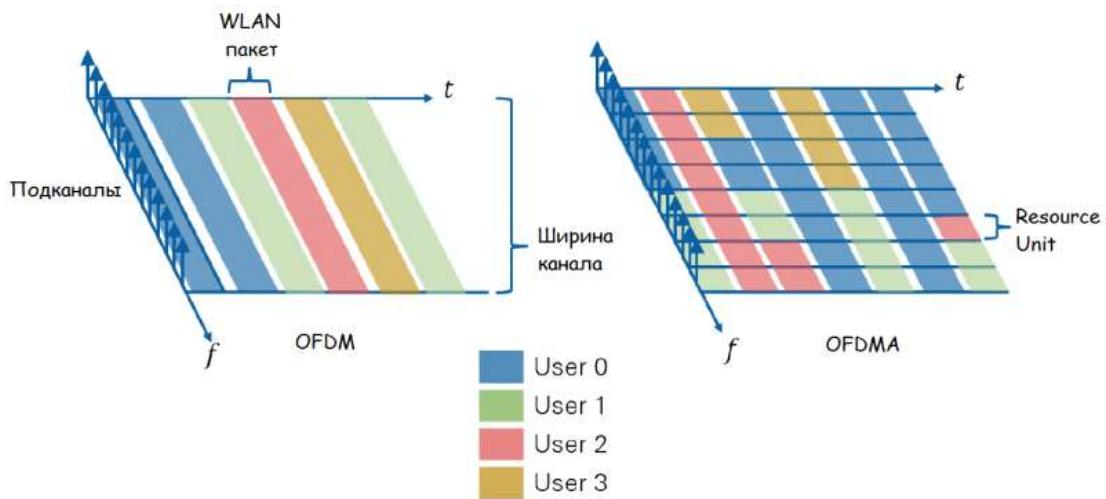


Рисунок 4.5 – OFDMA в 802.11ax

На **рисунке 4.6** показано, как система 802.11ax может мультиплексировать канал, используя разные размеры RU. Обратите внимание, что наименьшее разделение канала вмещает до 9 пользователей на каждые 20 МГц полосы пропускания.



Рисунок 4.6 - Разделение каналов Wi-Fi с использованием каналов шириной 40 МГц:

В **таблице 4.5** показано количество пользователей (для различной ширины каналов), которые теперь могут получать частотно-мультиплексированный доступ OFDMA.

Таблица 4.5 – Количество пользователей при OFDMA

Количество подканалов RU	20 МГц	40 МГц	80 МГц	160 МГц
26	9	18	37	74
52	4	8	16	32
106	2	4	8	16
242	1-SU/MU-MIMO	2	4	8
484	N/A	1-SU/MU-MIMO	2	4
966	N/A	N/A	1-SU/MU-MIMO	4
2x966	N/A	N/A	N/A	1-SU/MU-MIMO

Работа Multi-User Uplink

Как было отмечено выше, в 802.11ax появится возможность одновременной передачи пакетов от нескольких абонентов к точке доступа. Для координации работы MU-MIMO или Uplink OFDMA, точка доступа AP передает триггерный кадр всем пользователям. Этот кадр указывает количество пространственных потоков и / или параметры OFDMA (частоту и размеры RU) каждого пользователя. Триггерный кадр также содержит информацию об управлении мощностью, так что отдельные пользователи могут увеличивать или уменьшать свою передаваемую мощность, стремясь уравнять мощность, получаемую точкой доступа AP от всех пользователей, и улучшать тем самым качество приема кадров.

AP также инструктирует всех пользователей, когда начинать и останавливать передачу. AP отправляет многопользовательский триггерный кадр, который указывает всем пользователям точный момент времени, когда они все должны начать передавать данные, и точную продолжительность их кадров, чтобы гарантировать, что все они завершат передачу одновременно. Как только AP получает кадры от всех пользователей, она отправляет обратно ACK блок, говорящий о завершении передачи (рисунок 4.7).

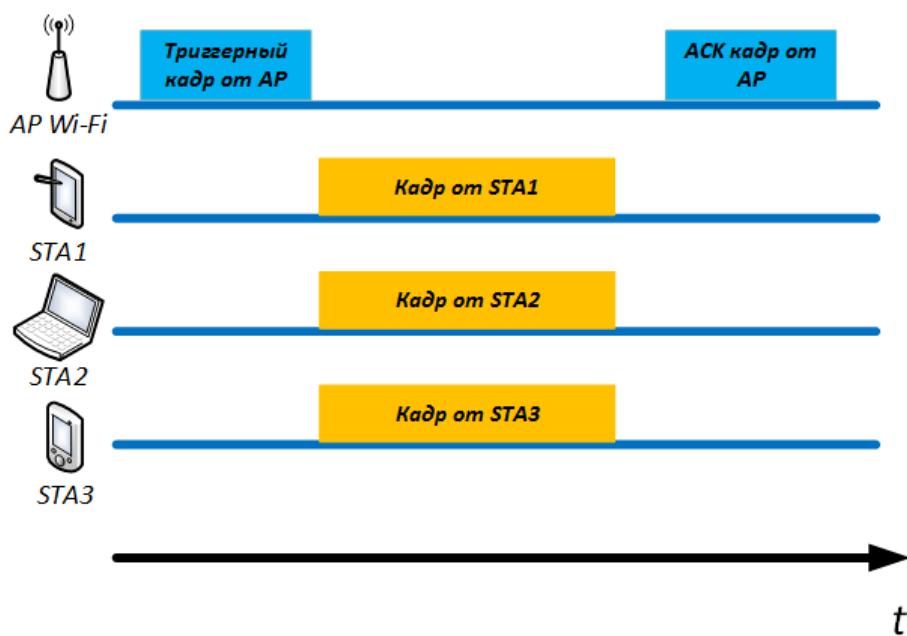


Рисунок 4.7 - Координация многопользовательской работы устройств в Wi-Fi-сети

Одной из основных целей стандарта 802.11ax является обеспечение более высокой средней пропускной способности на каждого пользователя (в среднем в 4 раза) в плотных беспроводных сетях. С этой целью, устройства 802.11ax поддерживают работу многопользовательских технологий MIMO и OFDMA. Также добавлена возможность одновременной передачи от нескольких устройств точке доступа AP, тем самым планируется снижение времени ожидания и простоя оборудования из-за неудачных попыток захватить среду передачи. Можно с уверенностью сказать лишь то, что эффект от 802.11ax будет только в том случае, если в сети все устройства будут поддерживать новый стандарт.

Используя все описанные механизмы в комбинации, новый стандарт 802.11ax способен выходить на физические скорости уровня 10 Гбит/с, обеспечивать полноценную параллельную работу множества клиентских устройств и использовать весь доступный нелицензируемый частотный диапазон. С такими скоростями новый стандарт сможет успешно конкурировать с будущими мобильными сетями пятого поколения 5G в сегменте обеспечения фиксированного беспроводного доступа.

На Wi-Fi по-прежнему возлагают большие надежды, а конкретно к offloading (возможности производить разгрузку сотового трафика с помощью Wi-Fi). По прогнозу, к 2020 году через Wi-Fi-сети операторов связи будет прокачиваться 38.1 эксабайт данных каждый месяц. Еще в прошлом году прогнозируемая цифра не превышала 30 эксабайт. В пересчете на фильмы в формате Blue-ray, это более 6 тысяч фильмов в минуту.

Немного проиллюстрировал свет на новый стандарт вице-президент по технологиям объединения Wi-Fi Alliance Грэг Эннис (Greg Ennis): «Разработка еще очень далека от завершения, ведь производителям нужно договориться о том, какие механизмы и технологии модуляции будут применяться в работе 802.11ax».

По словам Энниса главным приоритетом в процессе разработки является не столько увеличение пропускной способности всей сети, сколько скорость передачи данных каждому отдельному клиенту. По информации, полученной из компании Huawei, которая принимает активное участие в деятельности рабочей группы стандарта 802.11ax, скорость передачи данных уже достигает 10,53 Гбит/с на частоте 5 ГГц.

802.11ax может похвастать увеличенной производительностью в сетях с большим количеством пользователей, например, с точками доступа в общественных местах. Это будет возможно благодаря более эффективному использованию доступного спектра, улучшенной работе с интерференциями и изменения в работе основных протоколов – того же MAC (Medium Access Control). Все это сделает общественные точки доступа не только более производительными, но и более надежными.

Стандарт 802.11ax будет использовать четыре раздельных потока MIMO, каждый из которых поддерживает технологию OFDMA (Orthogonal Frequency-Division Multiple Access). Это позволит роутерам передавать большие объемы данных. Принцип работы технологии OFDMA во многом совпадает с OFDM (Orthogonal Frequency-Division Multiplexing). И OFDMA, и OFDM кодируют информацию на нескольких поднесущих частотах, однако OFDMA делает это эффективнее, размещая больше информации в единице пространства. Фраза Multiple Access как раз и говорит о средствах распределения поднесущих частот между различными пользователями.

Легко подсчитать, что четырехкратное увеличение производительности позволит добиться пропускной способности около 3,5 Гбит/с для каждого отдельного потока. Например, этот же показатель у стандарта 802.11ac не превосходит 866 Мбит/с. А с учетом применения технологии MIMO производительность целой сети может составить 14 Гбит/с. Смартфоны и лэптопы обычно работают с двумя или тремя потоками – в этом случае пропускная способность составит 7 Гбит/с (что приравнивается 900 Мбайт/с) и 10,5 Гбит/с (1344 Мбайт/с) соответственно.

На практике эти показатели будут значительно ниже. Вероятно, что скорость каждого отдельного потока на частоте 80 МГц составит около 1,6 Гбит/с (200 Мбайт/с). Если клиентское устройство поддерживает MIMO, то скорость будет выше в 2-3-4 раза. Что касается людных мест, тех же супермаркетов и парков, то там полоса канала обычно вдвое ниже – 40 МГц. Соответственно, снижается производительность каждого потока до 800 Мбит/с (100 Мбайт/с) и всей сети до 3,2 Гбит/с (400 Мбайт/с).

Главный вопрос заключается в том, сможет ли 802.11ax реализовать весь свой потенциал? Даже самая маленькая пропускная способность 100 Мбайт/с для 40 МГц сетей – это больше показателей чтения/записи для памяти, используемой в современных смартфонах. А для потоков в полосе 80 МГц и 160 МГц очевидно потребуются массивы из твердотельных накопителей.

Интересно сравнить новый стандарт IEEE 802.11ax как с текущим 802.11ac, так и с популярным 802.11n, а также с более старыми стандартами. Ниже представлена **таблица 4.6**, которая дает представление об основных отличиях между всеми основными стандартами, относящимися к семейству Wi-Fi.

Таблица 4.6 – Параметры семейства технологий 802.11

	802.11	802.11b	802.11a	802.11g	802.11n	802.11ac	802.11ax
Год ратификации	1997	1999	1999	2003	2009	2014	2017-2019
Рабочая частота	2.4 GHz/IR	2.4 GHz	5 GHz	2.4 GHz	2.4/5 GHz	5 GHz	2.4/5 GHz
Частотные каналы	20 MHz	20 MHz	20 MHz	20 MHz	20/40 MHz	20/40/80/160 MHz	20/40/80/160 MHz
Пиковая физическая скорость (PHY)	2 Mbps	11 Mbps	54 Mbps	54 Mbps	600 Mbps	6.8 Gbps	10 Gbps
Макс кол SU-потоков (SU Streams)	1	1	1	1	4	8	8
Макс кол MU-потоков (MU Streams)	NA	NA	NA	NA	NA	4	8
Модуляция	DSSS, FHSS	DSSS, CCK	OFDM	OFDM	OFDM	OFDM, OFDMA	
Макс тип и скорость кодирования	DQPSK	CCK	64-QAM, 3/4	64-QAM, 3/4	64-QAM, 5/6	256-QAM, 5/6	1024-QAM, 5/6
Макс кол тонов OFDM	NA	NA	64	64	128	512	2048
Разнесение субтонов	NA	NA	312.5 kHz	312.5 kHz	312.5 kHz	312.5 kHz	78.125 kHz

Можно выделить 3 основные проблемы, которые не позволяют Wi-Fi работать быстро с большим количеством абонентов:

1. Особенности работы протокола доступа к среде передачи CSMA / CD – MAC-уровень модели OSI.
2. Перекрывающиеся области обслуживания различных Wi-Fi-устройств – Физический уровень OSI.
3. Совместное использование каналов шириной до 160 МГц – Физический уровень модели OSI.

Работа протокола CSMA/CA

Протокол 802.11 использует метод множественного доступа к среде с контролем несущих и предотвращением коллизии CSMA, в котором беспроводные станции сначала прослушивают канал связи и стараются передавать данные только тогда, когда канал не активен. Тем самым, они пытаются избежать коллизий при передаче пакетов.

Хотя протокол CSMA хорошо подходит для равноправного разделения канала среди всех участников в общей зоне радиопокрытия, ясно, что с увеличением количества устройств в сети, его эффективность довольно быстро уменьшается. С увеличением количества устройств в сети происходит также и увеличение служебных кадров, а время ожидания для получения доступа нелинейно увеличивается.

Перекрывающиеся области обслуживания

Другим фактором, который приводит к коллизиям в беспроводной Wi-Fi-сети, является наличие множества точек доступа с перекрывающимися областями обслуживания. На **рисунке 4.8** изображено "Устройство А", которое работает в сети My BSS. "Устройство В" также работает в сети My BSS и будет пытаться получить доступ к среде передачи наравне с "Пользователем А" в своей зоне обслуживания. Однако этот В-пользователь может частично находиться в зоне обслуживания другой точки доступа и слышать трафик от Overlapping BSS справа:



Рисунок 4.8 – Перекрывающиеся области обслуживания

В этом случае трафик с OBSS будет вынуждать "Устройство В" вызывать процедуру отсрочки, описанную в предыдущем пункте. Из-за того, что абонентские устройства слышат трафик из других сетей, это приводит к тому, что устройствам приходится дольше ждать своей очереди для передачи, что также снижает среднюю пропускную способность в сети.

Совместное использование каналов

Третий фактор, который следует учитывать, – это совместное использование широких каналов. Как известно, в 802.11ac имеется возможность работать с каналами шириной до 160 МГц (**рисунок 4.9**):

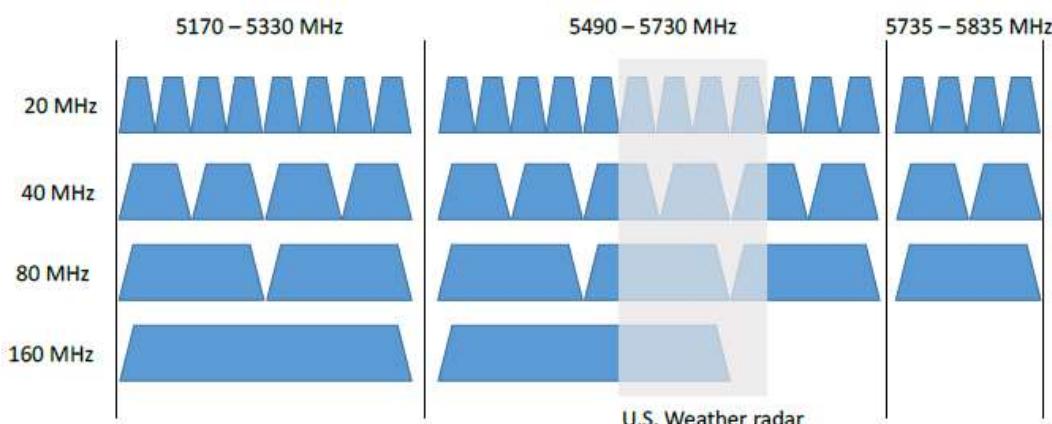


Рисунок 4.9 – Совместное использование широких каналов

Но каналов шириной по 160 МГц в нелицензируемом диапазоне 5 ГГц можно организовать лишь 1 или (в некоторых странах) 2. Это приводит к тому, что устройства в сети должны работать на одном канале, создавая друг другу помехи. Широкие каналы позволяют многократно увеличивать скорости передачи данных, но уже с выходом 802.11ac было ясно, что для больших сетей лучше использовать как можно более узкие каналы, чтобы клиентские устройства как можно меньше мешали друг другу.

Работая на одном канале (пусть даже и очень широком – 160 МГц!), пользователи будут испытывать взаимные помехи, что ухудшает производительность и лишает преимущества от использования Carrier Aggregation в принципе. Это особенно актуально для высоких скоростей передачи данных MCS 8, 9, 10 и 11, которые намного более требовательны к отношению сигнал/шум. Кроме того, при текущей реализации сетей 802.11, довольно много устройств работает на каналах с шириной 20 МГц, что делает каналы в 40, 80 и 160 МГц бесполезным, ведь использующее их оборудование при обнаружении устройств, работающих на узких каналах, должно будет "упасть" в режим совместимости с ними.

Повышение эффективности за счет изменения логики работы на уровне MAC

Какие нововведения для разрешения имеющихся проблем есть в технологии 802.11ax. Для повышения производительности устройств и эффективного использования спектра, на уровне MAC в стандарте 802.11ax беспроводные устройства научат идентифицировать сигналы от перекрывающихся BSS, и на основе этой информации предотвращать конфликтные ситуации. Для того чтобы отличать пакеты от разных BSS в стандарте ввели новое понятие – "Color Code". Для простоты понимания достаточно отметить, что это определенный код, по которому можно будет идентифицировать пакеты разных BSS.

Когда станция, которая активно прослушивает спектр, обнаруживает в нем кадр 802.11ax, она проверяет его Color Code BSS или MAC-адрес в заголовке пакета. Если Color Code BSS в обнаруженном пакете имеет тот же тип, что и в "родной" сети, тогда станция будет обрабатывать этот кадр (рисунок 4.10). Однако если обнаруженный кадр имеет другой Color Code, тогда она его проигнорирует:



Рисунок 4.10 – Использование Color Code

Стандарт будет определять механизмы фильтрации трафика от перекрывающихся BSS. Будет реализовано автоматическое повышение порога обнаружения сигнала для кадров от смежных BSS, при сохранении более низкого порога для трафика внутри зоны BSS (рисунок 4.11).

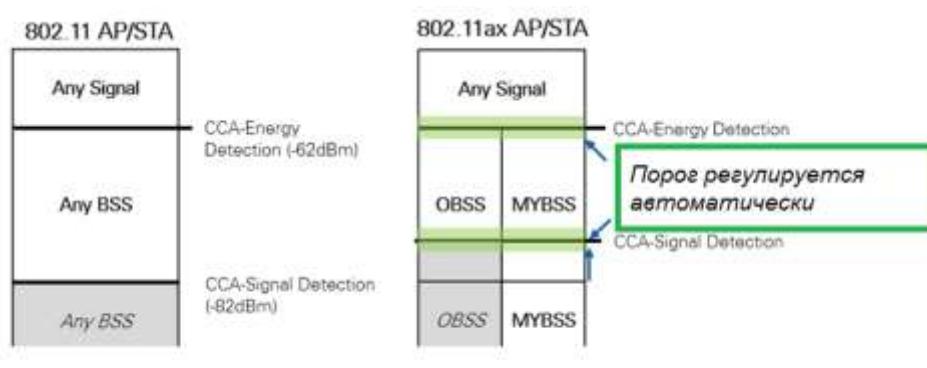


Рисунок 4.11 - Автоматическое регулирование порога

Таким образом, трафик от соседних OBSS не будет создавать ненужные конфликты доступа к каналу:

То есть, станции 802.11ax помимо использования Color Code также смогут самостоятельно регулировать порог обнаружения сигнала OBSS вместе с управлением мощностью передачи. Предполагается, что это улучшит производительность устройств на уровне MAC и обеспечит более оптимальное использование канала.

В дополнение к вышесказанному, в стандарте 802.11 используется алгоритм логического определения доступности среды передачи (Network Allocation Vector, NAV), который работает следующим образом.

Если при прослушивании эфира узел принимает какой-либо пакет, то, исходя из информации, содержащейся в его заголовке (длины пакета), он определяет, сколько времени будет еще длиться данная передача, и устанавливает таймер. Следующее прослушивание среды будет производиться только по истечении интервала времени, отсчитанного этим таймером. Таким образом, NAV обеспечивает среднее резервирование для кадров, критически важных для работы протокола 802.11, таких как управляющие кадры, данные и ACK после обмена RTS / CTS. Целевая группа 802.11, работающая над Wi-Fi HEW, включит в новый стандарт два разных NAV: один NAV будет работать внутри BSS, а второй между перекрывающимися станциями - OBSS NAV. Это поможет станциям прогнозировать трафик в пределах своей собственной BSS и знать состояние трафика из перекрывающейся сети.

Выводы

Распространенный сегодня 802.11ac ознаменовал переход от погони за скоростью одного клиента к погоне за максимальной емкостью сети. Стандарт 802.11 ax полностью поддерживает эту тенденцию (рисунок 4.12). Это связано с тем, что бизнесом востребовано развертывание больших по площади беспроводных сетей.

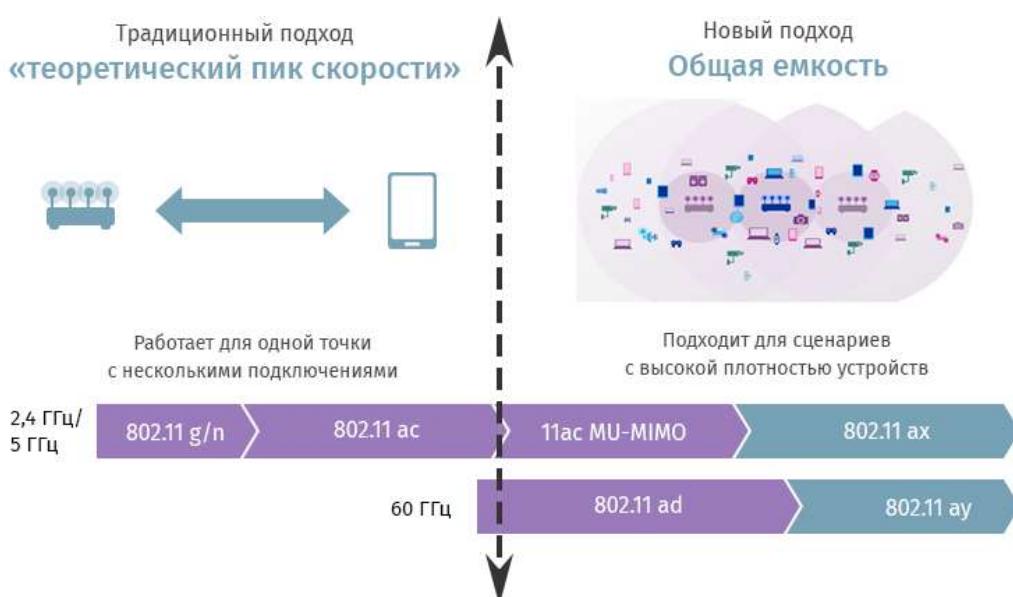


Рисунок 4.12 – Переход от повышения скорости к повышению емкости сети

Согласно прогнозам, в 2022 году более половины устройств будут поддерживать стандарт 802.11ac (рисунок 4.13).



Рисунок 4.13 – Прогноз роста устройств, поддерживающих новые стандарты

Wi-Fi — не единственная технология беспроводной связи. Уже сегодня скорость мобильного интернета по технологии 4G в ряде стран (например, в Австралии, Чехии, Катаре, ОАЭ и других) выше, нежели средняя скорость Wi-Fi подключений. Еще больше частных потребителей предпочитает мобильные сети, когда запустится в массовую коммерческую эксплуатацию 5G. Однако у этих сетей совсем иная экономика и цели, поэтому полностью вытеснить Wi-Fi с рынка они все равно не смогут. А благодаря инициативе Open Roaming 5G станет вполне может стать продолжением и дополнением Wi-Fi, но никак не конкурентом.

Open Roaming — идея вендоронезависимого бесшовного роуминга между сетями Wi-Fi (в том числе 6 версии) и мобильной сетью (в том числе, 5G), которая на данный момент находится на стадии бета-тестирования. Инициатива подразумевает более безопасное подключение к Wi-Fi, где это возможно с помощью одной из существующих учетных записей, например SIM-карты. Это снимет проблему небезопасности передачи данных через «гостевой» Wi-Fi, т.е. частично разгрузит мобильные сети. Open Roaming и новые сервисы для бизнеса поможет создать, поскольку с таким бесшовным переходом из мобильной сети в локальную беспроводную ей будут пользоваться гораздо большая доля клиентов.

4.4 Альтернативные стандарты

Представители IEEE уже нарекли стандарт 802.11ax наследником 802.11ac, однако, в компании ведется работа и над другими проектами (рисунок 4.14).

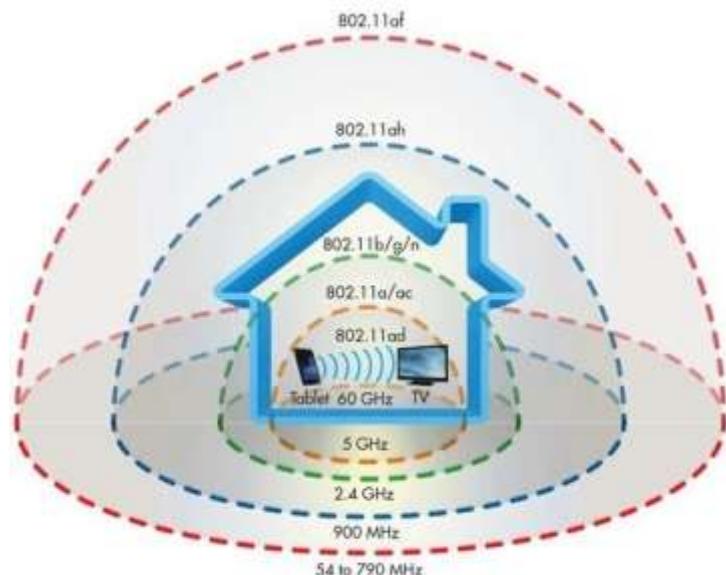


Рисунок 4.14 – Развитие стандарта 802.11

Одним из них является стандарт 802.11ad (рисунок 4.15), отличительной особенностью которого является работа в нелицензированном частотном диапазоне 60 ГГц. Пропускная способность таких сетей сможет достичь примерно 7 Гбит/с, хотя при использовании иных способов формирования направленного сигнала она может составлять и все 25 Гбит/с. Полоса в 60 ГГц предназначена в основном для использования внутри помещений и ориентирована на работу с видео-сервисами и приложениями:



Рисунок 4.15 – Применение 802.11ad

Технология беспроводной сети с частотным спектром 60 ГГц появилась не так давно. В мае 2009 года было объявлено о ее создании, а в декабре того же года были приняты спецификации первого поколения. Разработкой технологии занимался Wireless Gigabit Alliance (WiGig), возглавляемый компаниями Marvell и Wilocity (в июле 2014 года была приобретена компанией Qualcomm Atheros).

Спустя всего лишь год после своего образования альянс WiGig подписал договор о сотрудничестве с организацией Wi-Fi Alliance. Такой ход обеспечил дальнейшую совместимость WiGig и Wi-Fi-девайсов между собой.

Следующая версия стандарта – 802.11ay (WiGig второго поколения), которая является своего рода улучшением выпущенного 802.11ad. Поэтому 802.11ay, как и 11ad, не будет новым типом WLAN сетей, скорее 11ay позволит еще больше оптимизировать использование полосы 60 ГГц и обеспечить скорости передачи данных до 176 Гбит/сек.

Такие скорости стали доступны благодаря использованию 256-QAM модуляции, использованию четырех потоков ММО по 44 Гбит/сек каждый и увеличению ширины полосы пропускания канала до 8,64 ГГц. Также в 11ay добавится технология MU-MIMO. Финальная версия спецификации 802.11ay должна была принять до конца 2017 года, но отложена на 2019 год. Данный стандарт может являться заменой для Ethernet и других проводных сетей внутри офиса или жилого помещения, и обеспечивать внешние транзитные соединения для операторов связи. В будущем эта технология может использоваться, например, для беспроводного подключения мониторов и телевизоров с высоким разрешением. Поэтому, возможно, еще через несколько лет проводов на наших рабочих столах будет еще меньше, если беспроводные карточки будут сразу интегрированы в мониторы. Некоторые эксперты сходятся во мнении, что 802.11ay будет использоваться в AR-очках Apple.

К слову, 802.11ad и ау не являются единственным 60 ГГц стандартом. Конкуренцию ему составляет технология WirelessHD, разрабатываемая одноименным консорциумом, в состав которого входят такие крупные компании, как Intel, LG, Samsung, Silicon Image и другие. Технические характеристики WirelessHD почти ничем не отличаются от таковых у 802.11ad. Теоретическая пропускная способность стандарта равна 28 Гбит/с. Примечательно и то, что эта технология изначально создавалась с прицелом на передачу аудио- и видеоданных в HD, поэтому список поддерживаемых WirelessHD технологий включает в себя всевозможные 3D-форматы, разрешение 4K и защиту HDCP. Кроме этого, поддерживается и режим энергосбережения для мобильных устройств. **В принципе, главным отличием WirelessHD от 802.11ad является то, что технология не совместима с Wi-Fi.** Станет ли это впоследствии минусом стандарта или же, наоборот, сыграет ему на руку, сказать пока что сложно. Ясно одно – WirelessHD будет пытаться занять несколько иную нишу, и, на первый взгляд, несовместимость с Wi-Fi никак не должна повлиять на развитие технологии. Однако, далеко не всегда всё идет по плану.

Стандарты 802.11ad и WirelessHD могут похвастаться высокой производительностью, однако, если говорить в целом про 60-гигагерцовые сети, то у них есть два существенных недостатка.

Во-первых, сверхкороткие волны, используемые в этих технологиях, с трудом проходят сквозь стены.

Во-вторых, на частоте 60 ГГц молекулы кислорода начинают поглощать электромагнитную энергию.

Эти минусы не позволяют WiGig- и WirelessHD-устройствам распространять сигнал на большие расстояния – чаще всего их рабочая площадь не выходит за границы того помещения, где они установлены.

Вот почему на рынке представлено так мало девайсов, соответствующих этому стандарту. Таковыми, к примеру, является устройство Dell Wireless Dock D5000, использующее сеть 802.11ad. А также DVDO Air, которое работает посредством WirelessHD и предназначено для передачи аудио- и видеоконтента высокой четкости с Blu-ray проигрывателя на проектор.

Что касается будущего этих технологий, то эксперты опасаются повторения ситуации с конкуренцией Blu-ray и HD DVD.

Полной противоположностью 802.11ad является стандарт 802.11ah. В отличие от первого, эта технология работает в частотном диапазоне 900 МГц. Это означает, что сигнал такой беспроводной сети легко преодолевает препятствия в виде стен. В то же время его пропускная способность снижается. Скорость 802.11ah может варьироваться от 100 Кбит/с до 347 Мбит/с (ширина канала 16 МГц, четыре потока, 256 QAM, скорость 5/6). Скорее всего, такие беспроводные сети найдут себе применение в домашней автоматизации, где их будут использовать как альтернативу технологиям Z-Wave и Zig Bee. Спецификации стандарта 802.11ah опубликованы в 2017 году.

Уже несколько лет идет работа над приемником 802.11az. Среди поставленных перед разработчиками задач – улучшение определения местоположения пользовательских устройств (при помощи GPS), что позволит быстрее подключаться к ним, не расходуя каждый раз время и ресурсы на поиски правильного направления передачи. Это

важно как для роботов и дронов, так и в потребительском маркетинге, снабжении и Интернете вещей. Кроме того, рабочая группа обещала поработать над энергосбережением. Перспективный стандарт, ожидается к внедрению в 2021 году.

Выводы

Нет никаких сомнений в дальнейшем качественном развитии беспроводных стандартов нет. IEEE не только усовершенствует классические Wi-Fi-сети, но и создаст новые в лице 802.11ad и 802.11ah, которые можно будет использовать во всех сферах жизни. Интересно посмотреть и на технологию WirelessHD: создаст ли она достойную конкуренцию 802.11ad и к чему это приведет? Так или иначе, будущее беспроводных сетей находится в надежных руках.

4.5 Регулирование использования радиочастотного спектра для WiFi

В соответствии со статьей 22 " Регулирование использования радиочастотного спектра " Федерального закона "О связи" в редакции от 09.02.2007 N 14-ФЗ:

Выдержка из статьи 22 ФЗ "О связи"

4. Использование в Российской Федерации радиочастотного спектра осуществляется в соответствии со следующими принципами: разрешительный порядок доступа пользователей к радиочастотному спектру; плотность использования радиочастотного спектра; недопустимость бессрочного выделения полос радиочастот, присвоения радиочастот или радиочастотных каналов; прозрачность и открытость процедур распределения и использования радиочастотного спектра.

5. Средства связи, иные радиоэлектронные средства и высокочастотные устройства, являющиеся источниками электромагнитного излучения, подлежат регистрации. Перечень радиоэлектронных средств и высокочастотных устройств, подлежащих регистрации, и порядок их регистрации определяются Правительством Российской Федерации. Радиоэлектронные средства, используемые для индивидуального приема программ телевизионного вещания и радиовещания, сигналов персональных радиовызовов (радиопейджеры), электронные изделия бытового назначения и средства персональной радионавигации, не содержащие радиоизлучающих устройств, используются на территории Российской Федерации с учетом ограничений, предусмотренных законодательством Российской Федерации, и регистрации не подлежат. Использование без регистрации радиоэлектронных средств и высокочастотных устройств, подлежащих регистрации в соответствии с правилами настоящей статьи, не допускается.

В соответствии со статьей 24 " Выделение полос радиочастот и присвоение (назначение) радиочастот или радиочастотных каналов ", право на использование радиочастотного спектра предоставляется посредством выделения полос радиочастот и присвоения радиочастот или радиочастотных каналов. Использование радиочастотного спектра без соответствующего разрешения не допускается.

Присвоение радиочастот или радиочастотных каналов для радиоэлектронных средств (РЭС) гражданского назначения осуществляется Федеральным агентством связи (Россвязь) по заключению радиочастотной службы при Россвязи на основании заявлений граждан Российской Федерации или заявлений российских юридических лиц.

Порядок получения разрешений для беспроводных сетей в диапазоне 2,4 ГГц в России

1) внутриофисные системы беспроводной передачи данных.

Порядок использования полосы радиочастот 2400-2483,5 МГц для внутриофисных систем передачи данных определен Решением ГКРЧ (Государственной Комиссии по радиочастотам) № 04-03-04-003 от 6 декабря 2004 г. Это Решение значительно упростило процедуру получения разрешительных документов и определило возможность использования внутриофисного оборудования Wi-Fi без оформления разрешений на использование радиочастот.

Выдержка из Решения ГКРЧ № 04-03-04-003 от 6 декабря 2004 г.

3. Разрешить гражданам Российской Федерации и российским юридическим лицам использование на вторичной основе радиочастот в пределах полосы радиочастот 2400-2483,5 МГц для эксплуатации внутриофисных систем передачи данных, указанных в прилагаемом перечне (приложение № 2), на территории Российской Федерации без оформления разрешений на использование радиочастот, при выполнении следующих условий:

- эксплуатации РЭС внутриофисных систем передачи данных только внутри зданий, закрытых складских помещений и производственных территорий;
- регистрации РЭС внутриофисных систем передачи данных установленным в Российской Федерации порядком.

В приложение № 2 к Решению ГКРЧ № 04-03-04-003 включено, в частности, следующее внутриофисное оборудование D-Link:

DWL-1000AP+, DWL-1040AP+, DWL-900AP+, DWL-650+, DWL-520+, DWL-120+, DI-714P+, DI-614+, DWL-G520, DWL-G650, DWL-2100AP, DI-624, DWL-G520+, DWL-G650+, DWL-2000AP+, DI-624+, DI-724P+, DI-824VUP+, DSL-G604T, DWL-G120, DWL-G122, DWL-G510, DWL-G630, DWL-G730AP, DI-524, DWL-3200AP.

2) уличные операторские сети беспроводной передачи данных.

Для получения разрешения на использование полосы частот 2400-2483,5 МГц (стандарты 802.11b/g) для эксплуатации РЭС этой группы применяется частично упрощенный порядок на основе Решения ГКРЧ от 25 сентября 2000 г. (протокол № 2/7). Для этих систем не требуется оформления *частных решений* ГКРЧ для каждого конкретного заявителя, при условии соответствия технических параметров беспроводного оборудования основным тактико-техническим характеристикам, определенным в Решении ГКРЧ №05-10-01-001 от 28 ноября 2005 года.

3) Bluetooth

Порядок использования на территории Российской Федерации радиоэлектронных средств технологии Bluetooth, работающих в полосе частот 2400-2483,5 МГц, определен Решением ГКРЧ № 25/2 от 31.03.03.

Данное Решение ГКРЧ определяет возможность использования, приобретения и эксплуатации радиоэлектронных средств технологии Bluetooth с максимальной излучаемой мощностью не более 2,5 мВт без оформления разрешений органов государственной радиочастотной службы и без последующей регистрации этих РЭС в указанных органах.

Радиоэлектронные средства технологии Bluetooth с максимальной излучаемой мощностью не более 100 мВт разрешается использовать при условии выполнения требований Решения ГКРЧ № 04-03-04-003.

Порядок получения разрешений для беспроводных сетей в диапазоне 5 ГГц в России

В диапазоне 5 ГГц порядок назначения радиочастот одинаковый как для уличных операторских сетей, так и для внутриофисных сетей беспроводной передачи данных.

Получения разрешения на использование радиочастот в диапазоне 5 ГГц (стандарт 802.11a) получать разрешение ГКРЧ не нужно.

Действующие решения ГКРЧ:

Решение ГКРЧ от 30 июля 2001 г., протокол № 11/1;

Решение ГКРЧ от 23 декабря 2002 г., протокол № 23/5;

Решение ГКРЧ № 05-10-01-001 от 28 ноября 2005 г.

Ответственность

Статьи 24 "Выделение полос радиочастот и присвоение (назначение) радиочастот или радиочастотных каналов" и 25 "Контроль за излучениями радиоэлектронных средств и (или) высокочастотных устройств" Федерального закона "О связи" № 126-ФЗ в редакции от 09.02.2007 № 14-ФЗ определяют процедуры, связанные с нарушением условий, установленных при выделении полосы радиочастот и правил использования радиочастотного спектра.

Выдержка из статьи 24 ФЗ "О связи"

10. В случае выявления нарушения условий, установленных при выделении полосы радиочастот либо присвоении (назначении) радиочастоты или радиочастотного канала, разрешение на использование радиочастотного спектра пользователями радиочастотным спектром для радиоэлектронных средств гражданского назначения может быть приостановлено органом, выделившим полосу радиочастот либо присвоившим (назначившим) радиочастоту или радиочастотный канал в соответствии с пунктами 2 и 3 настоящей статьи на срок, необходимый для устранения этого нарушения, но не более чем на девяносто дней.

11. Разрешение на использование радиочастотного спектра прекращается во внесудебном порядке или срок действия такого разрешения не продлевается по следующим основаниям: заявление пользователя радиочастотным спектром; *аннулирование* лицензии на осуществление деятельности в области оказания услуг

связи, если такая деятельность связана с использованием радиочастотного спектра; истечение срока, указанного при присвоении (назначении) радиочастоты или радиочастотного канала, если этот срок не был продлен в установленном порядке или если заблаговременно, не менее чем за тридцать дней, не была подана заявка на его продление; использование радиоэлектронных средств и (или) высокочастотных устройств в противоправных целях, наносящих вред интересам личности, общества и государства; невыполнение пользователем радиочастотным спектром условий, установленных в решении о выделении полосы радиочастот либо присвоении (назначении) радиочастоты или радиочастотного канала; невнесение пользователем радиочастотным спектром платы за его использование в течение тридцати дней со дня установленного срока платежа; ликвидация юридического лица, которому было выдано разрешение на использование радиочастотного спектра; неустранимое нарушение, послужившего основанием для приостановления разрешения на использование радиочастотного спектра.

12. При наличии в документах, представленных заявителем, недостоверной или искаженной информации, повлиявшей на принятие решения о выделении полосы радиочастот либо присвоении (назначении) радиочастоты или радиочастотного канала, орган, выделивший полосу радиочастот либо присвоивший (назначивший) радиочастоту или радиочастотный канал, вправе обратиться в суд с требованием о прекращении или непродлении срока действия разрешения на использование радиочастотного спектра.

13. При прекращении или приостановлении разрешения на использование радиочастотного спектра плата, внесенная за его использование, не возвращается.

Выдержка из статьи 25 ФЗ "О связи"

1. Контроль за излучениями радиоэлектронных средств и (или) высокочастотных устройств (радиоконтроль) осуществляется в целях: проверки соблюдения пользователем радиочастотным спектром правил его использования; выявления неразрешенных для использования радиоэлектронных средств и прекращения их работы; выявления источников радиопомех; выявления нарушения порядка и правил использования радиочастотного спектра, национальных стандартов, требований к параметрам излучения (приема) радиоэлектронных средств и (или) высокочастотных устройств; обеспечения электромагнитной совместимости; обеспечения эксплуатационной готовности радиочастотного спектра.

2. Радиоконтроль является составной частью государственного управления использованием радиочастотного спектра и международно-правовой защиты присвоения (назначения) радиочастот или радиочастотных каналов. Радиоконтроль за радиоэлектронными средствами гражданского назначения осуществляется радиочастотной службой. Порядок осуществления радиоконтроля определяется Правительством Российской Федерации.

В процессе радиоконтроля для изучения параметров излучений радиоэлектронных средств и (или) высокочастотных устройств, подтверждения нарушения установленных правил использования радиочастотного спектра может проводиться запись сигналов контролируемых источников излучений.

Такая запись может служить только в качестве доказательства нарушения порядка использования радиочастотного спектра и подлежит уничтожению в порядке, установленном законодательством Российской Федерации.

Использование такой записи в иных целях не допускается, и виновные в таком использовании лица несут установленную законодательством Российской Федерации ответственность за нарушение неприкосновенности частной жизни, личной, семейной, коммерческой и иной охраняемой законом тайны.

В соответствии с постановлением Правительства РФ от 30 июня 2004 г. № 318 контроль за излучением радиоэлектронных средств осуществляется Федеральной службой по надзору в сфере связи (Россвязьнадзор), территориальными органами Россвязьнадзора и их структурными подразделениями на основании Постановления Правительства РФ от 1 апреля 2005 г. № 175 "Об утверждении правил осуществления радиоконтроля в Российской Федерации".

Согласно статье 68 ФЗ "О связи" "Ответственность за нарушение законодательства Российской Федерации в области связи" в случаях и в порядке, которые установлены законодательством Российской Федерации, лица, нарушившие законодательство Российской Федерации в области связи, несут уголовную, административную и гражданско-правовую ответственность.

Разрешение на использование частот

В России в соответствии с решениями Государственной комиссии по радиочастотам (ГКРЧ) от 7 мая 2007 г. № 07-20-03-001 «О выделении полос радиочастот устройствам малого радиуса действия» и от 20 декабря 2011 г.

№ 11-13-07-1, использование Wi-Fi без получения частного разрешения на использование частот возможно для организации сети внутри зданий, закрытых складских помещений и производственных территорий в полосах 2400–2483,5 МГц (стандарты 802.11b и 802.11g; каналы 1–13) и 5150–5350 МГц (802.11a и 802.11n; каналы 34–64).

Для легального использования внеофисной беспроводной сети Wi-Fi (например, радиоканала между двумя соседними домами) необходимо получение разрешения на использование частот (как в полосе 2,4 ГГц, так и 5 ГГц) на основании заключения экспертизы о возможности использования заявленных РЭС и их электромагнитной совместимости (ЭМС) с действующими и планируемыми для использования РЭС.

В Москве 29 февраля 2016 было принято решение об использовании в России частотного диапазона 57–66 ГГц для устройств стандарта IEEE 802.11ad (WiGig). Принятое решение вносит изменения в решение ГКРЧ от 7 мая 2007 года № 07-20-03-001 «О выделении полос радиочастот устройствам малого радиуса действия». Решением ГКРЧ также разрешено использование нового диапазона частот 5650–5850 МГц (каналы 132–165) устройствами стандарта IEEE 802.11ac (Wi-Fi). Это позволит использовать канал до 160 МГц внутри зданий при развертывании сетей Wi-Fi стандарта 802.11ac. Также для диапазонов 5150–5350 МГц и 5650–5850 МГц вдвое была повышена допустимая мощность излучения. Теперь она составляет 10 мВт на 1 МГц.

Радиоэлектронные средства подлежат регистрации в Роскомнадзоре в соответствии с установленным порядком. В соответствии с Постановлением Правительства Российской Федерации от 13 октября 2011 г. № 837 «О внесении изменений в Постановление Правительства Российской Федерации от 12 октября 2004 г. № 539» не подлежат регистрации, в частности, (из п. 13, 23, 24 приложения):

- пользовательское (окончное) оборудование передающее, включающее в себя приемное устройство, малого радиуса действия стандартов IEEE 802.11, IEEE 802.11.b, IEEE 802.11.g, IEEE 802.11.n (Wi-Fi), работающее в полосе радиочастот 2400—2483,5 МГц, с допустимой мощностью излучения передатчика не более 100 мВт, в том числе встроенное либо входящее в состав других устройств;
- пользовательское (окончное) оборудование передающее, включающее в себя приемное устройство, малого радиуса действия стандартов IEEE 802.11a, IEEE 802.11.n (Wi-Fi), работающее в полосах радиочастот 5150 — 5350 МГц и 5650 — 6425 МГц, с допустимой мощностью излучения передатчика не более 100 мВт, в том числе встроенное либо входящее в состав других устройств;
- устройства малого радиуса действия, используемые внутри закрытых помещений, в полосе радиочастот 5150 — 5250 МГц с максимальной эквивалентной изотропно излучаемой мощностью передатчика не более 200 мВт;
- устройства малого радиуса действия в сетях беспроводной передачи данных внутри закрытых помещений в полосе радиочастот 2400—2483,5 МГц с максимальной эквивалентной изотропно излучаемой мощностью передатчика не более 100 мВт при использовании псевдослучайной перестройки рабочей частоты.

Частотная сетка диапазона 5 ГГц предусматривает использования для Wi-Fi только непересекающихся каналов шириной 20 МГц и с шагом 20 МГц, от начала и конца полосы частотный отступ составляет 30 МГц. Первоначально были разрешены к использованию полосы UNII-1 (Европа, Россия) и дополнительно к ней UNII-3 и один канал из "медицинского" ISM (США), позднее к ним добавили полосу UNII-2.

Канал	36	40	44	48	52	56	60	64	149	153	157	161	165
Центральная частота, МГц	5180	5200	5220	5240	5260	5280	5300	5320	5745	5765	5785	5805	5825
Полоса	UNII-1				UNII-2				UNII-3				ISM

Канал	100	104	108	112	116	120	124	128	132	136	140	144
Центральная частота, МГц	5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700	5720
Полоса	UNII-2 Extended											

Таким образом диапазон содержит 25 непересекающихся каналов. Частотные полосы UNII-2 и UNII-2 Extended выделенные для Wi-Fi пересекаются с частотами, на которых работают авиационные, судовые и военные радары, а также погодные радары аэродромов. Поэтому использование данных диапазонов возможно только при использовании технологии DFS (*Dynamic Frequency Selection*), которая заключается в том, что точка

постоянно мониторит частоту на наличие импульсов от радара и при наличии таковых обязана изменить рабочий канал.

В России на текущий момент времени из диапазона UNII-2 Extended разрешено использование только четырех каналов 132-144, таким образом у нас доступно всего 17 непересекающихся каналов, по четыре в каждой из полос UNII и один в ISM.

Кроме стандартной ширины канала в 20 МГц стандартами Wi-Fi предусмотрено использование каналов шириной в 40 МГц, 80 МГц и 160 МГц. Широкие полосы могут использоваться только в полосах UNII. Таким образом каждая из доступных в России полос может содержать по 4 канала 20 МГц, 2 канала 40 МГц и по одному каналу 80 МГц. Канал шириной в 160 МГц может использоваться только один, получаемый при объединении полос UNII-1 и UNII-2 - занимая всю их ширину.

5 Концептуальное построение Wi-Fi 7 - IEEE 802.11be

Еще только недавно на рынок вышли устройства, поддерживающие технологию Wi-Fi 6 (IEEE 802.11ax), а уже ведётся разработка нового поколения Wi-Fi 7 (IEEE 802.11be).

5.1 Этапы развития Wi-Fi 7

Предистория Wi-Fi 7

В сентябре 2020 года отмечалось 30-летие проекта IEEE 802.11. В настоящее время технология Wi-Fi, определяемая семейством стандартов IEEE 802.11, является самой популярной беспроводной технологией, используемой для подключения к интернету: Wi-Fi передает более половины пользовательского трафика.

В то время как сотовые технологии делают ребрендинг каждое десятилетие, например, заменяя название 4G на 5G, для пользователей Wi-Fi повышение скорости передачи данных, а также внедрение новых услуг и новых функций происходят практически незаметно.

Одним из доказательств развития Wi-Fi является резкое увеличение номинальных скоростей передачи данных: от 2 Мбит/с в версии 1997 г. до почти 10 Гбит/с в стандарте 802.11ax. Современный Wi-Fi достигает такого прироста производительности благодаря более быстрым сигнально-кодовым конструкциям, более широким каналам и использованию технологий MIMO.

Помимо основного направления высокоскоростных беспроводных локальных сетей, эволюция Wi-Fi включает в себя несколько нишевых проектов. Например, Wi-Fi HaLow (802.11ah) стал попыткой вывести Wi-Fi на рынок беспроводного Интернета вещей. Wi-Fi миллиметрового диапазона (802.11ad/ay) поддерживает номинальные скорости передачи данных до 275 Гбит/с, правда на очень небольшие расстояния.

Новые приложения и услуги, связанные с видеопотоками высокого разрешения, виртуальной и дополненной реальностью, играми, удаленным офисом и облачными вычислениями, а также необходимостью поддержки большого количества пользователей с интенсивным трафиком в беспроводных сетях требуют высокой производительности.

Современное состояние разработки Wi-Fi 7

В мае 2019 года подгруппа BE (TGbe) рабочей группы 802.11 комитета по стандартизации локальных и городских сетей начала работу над новым дополнением к стандарту Wi-Fi, которое увеличит **номинальную пропускную способность более, чем до 40 Гбит/с** в одном частотном канале «типичного» для Wi-Fi диапазона ≤ 7 ГГц. Хотя во многих документах фигурирует «максимальная пропускная способность не менее 30 Гбит/с», новый протокол физического уровня будет обеспечивать номинальную скорость свыше 40 Гбит/с.

Еще одним важным направлением разработки Wi-Fi 7 является **поддержка приложений реального времени** (игры, виртуальная и дополненная реальность, управление роботами). Примечательно, что хотя Wi-Fi по-особому обслуживает аудио- и видеотрафик, долгое время считалось, что обеспечение на уровне стандарта гарантированно малых задержек (единиц миллисекунд), также известное как TSN (Time-Sensitive Networking), в сетях Wi-Fi принципиально невозможно.

В ноябре 2017 г. коллектив из ИППИ РАН и НИУ ВШЭ выступил с соответствующим предложением в группе IEEE 802.11. Предложение вызвало большой интерес, и в июле 2018 года была запущена специальная подгруппа для дальнейшего изучения этого вопроса. Поскольку для поддержки приложений реального времени требуются как высокие номинальные скорости передачи данных, так и расширение функционала канального уровня, рабочая группа 802.11 решила разрабатывать методы поддержки приложений реального времени в рамках Wi-Fi 7.

Важным вопросом, связанным с Wi-Fi 7, является его сосуществование с технологиями сотовых сетей (4G/5G), разрабатываемыми 3GPP и работающими в тех же нелицензируемых полосах частот. Речь идет о LTELAA/NR-U. Для изучения проблем, связанных с сосуществованием Wi-Fi и сотовых сетей, IEEE 802.11 создал Coexisting Standing Committee (Coex SC).

Несмотря на многочисленные встречи и даже совместный семинар участников 3GPP и IEEE 802.11 в июле 2019 года в Вене, технические решения еще не были утверждены. Возможное объяснение такой бесплодной деятельности состоит в том, что как IEEE 802, так и 3GPP не хотят изменять свои собственные технологии, чтобы привести их в соответствие с другой. Таким образом, на данный момент не ясно, повлияют ли обсуждения в рамках Coex SC на стандарт Wi-Fi 7.

Этапы процесса разработки

Хотя процесс разработки Wi-Fi 7 находится на самой начальной стадии, к настоящему времени было внесено около 500 предложений нового функционала для будущего Wi-Fi 7, также известного как IEEE 802.11be. Большая часть идей только обсуждаются в подгруппе be и решение по ним еще не было принято. Другие идеи были недавно одобрены. Ниже указано, какие предложения являются утвержденными, а какие только обсуждаются (рисунок 5.1).

5.1).

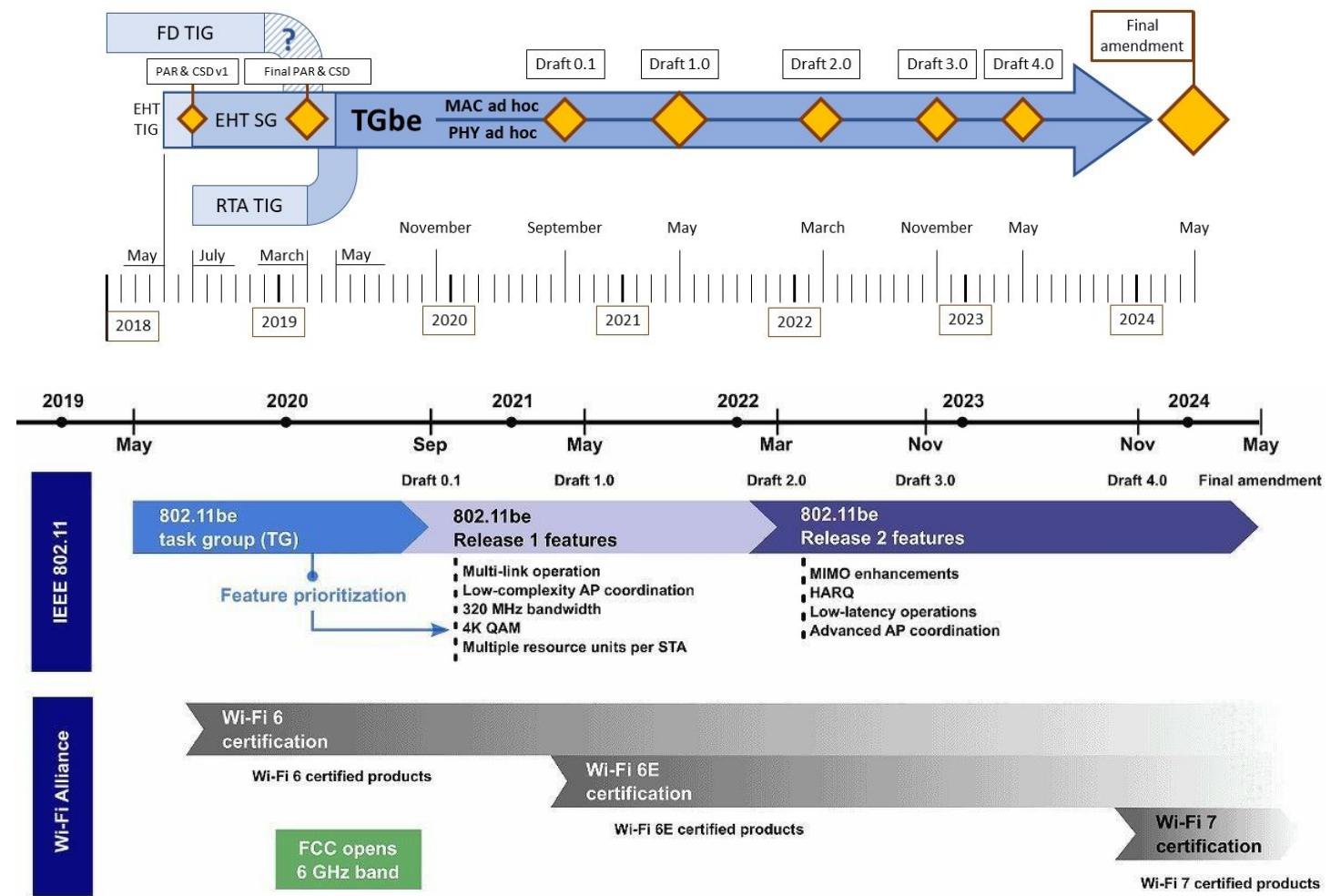


Рисунок 5.1 - Таймлайн разработки и принятия стандарта Wi-Fi 7

Изначально планировалось, что разработка основных новых механизмов завершится к марта 2021 года. Окончательный вариант стандарта ожидается к началу 2024 года. В январе 2020 в подгруппе 11be была выражена обеспокоенность тем, будет ли разработка соответствовать графику при нынешнем темпе работы. Чтобы ускорить процесс разработки стандарта, подгруппа согласилась выбрать небольшой набор высокоприоритетных функций, которые могут быть выпущены к 2021 году (Release 1), а остальные оставить на Release 2. Высокоприоритетные функции должны обеспечивать основной прирост производительности и включают в себя поддержку 320 МГц, 4KQAM, очевидные улучшения OFDMA от Wi-Fi 6, MU-MIMO с 16 потоками.

Из-за коронавируса группа сейчас очно не собирается, но регулярно проводит телеконференции. Разработка

несколько замедлилась, но не прекратилась.

5.2 Концепция и задачи технологии Wi-Fi 7

Основные новшества Wi-Fi 7 (рисунок 5.2)

1. Новый протокол физического уровня является развитием протокола Wi-Fi 6 с **двухкратным увеличением ширины полосы до 320 МГц, двухкратным увеличением числа пространственных потоков MU-MIMO**, что увеличивает номинальную пропускную способность в $2 \times 2 = 4$ раза. Wi-Fi 7 также начинает использовать модуляцию **4K-QAM**, что добавляет еще 20% к номинальной пропускной способности. Таким образом, Wi-Fi 7 будет обеспечивать номинальную скорость передачи данных в $2 \times 2 \times 1,2 = 4,8$ раз выше по сравнению с Wi-Fi 6: максимальная номинальная пропускная способность Wi-Fi 7 составляет $9,6 \text{ Гбит/с} \times 4,8 = 46 \text{ Гбит/с}$. Кроме того, будет сделано революционное изменение в протоколе физического уровня, связанное с обеспечением совместимости с будущими версиями Wi-Fi, но оно останется незаметным для пользователей.

Удвоение максимальной ширины каналов соответственно позволит удвоить производительность сетей Wi-Fi 7. Для увеличения пропускной способности стандарт также предусматривает комбинированное сочетание канальных полос 160+160 МГц, 240+180 МГц и 160+80 МГц, в том числе, с возможностью объединения частотных блоков в несмежных участках спектра. Расчет на возможность использования столь широких частотных полос под каждый канал обусловлен перспективами адаптации частотного диапазона 6 ГГц нужд беспроводных сетей на безлицензионной основе.

Отношение сигнал / шум (SNR), необходимое на стороне приемника, чтобы принять 4096-QAM составляет около 40 дБ. Такой высокий SNR может быть достигнут формированием луча. Так что эта модуляция может быть полезной, когда точка доступа имеет много антенн и обслуживает только одну клиентскую STA с несколькими антеннами.

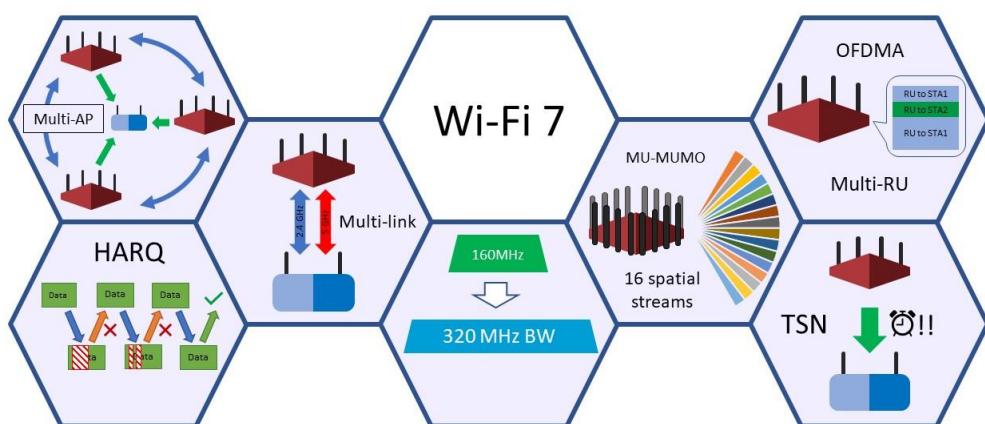


Рисунок 5.2 - Усовершенствования стандарта 802.11be (Wi-Fi 7)

2. **Изменение метода доступа к каналу для поддержки приложений реального времени** будет проведено с учётом опыта IEEE 802 TSN для проводных сетей. Продолжающиеся обсуждения в комитете по стандартизации связаны с процедурой случайной отсрочки при доступе к каналу, категориями обслуживания трафика и, соответственно, отдельными очередями для трафика реального времени, а также политиками обслуживания пакетов.

3. Введенный в Wi-Fi 6 (802.11ax) **OFDMA** – метод доступа к каналу с разделением по времени и частоте

(аналогичный тому, что используется в сетях 4G и 5G) – предоставляет новые возможности для оптимального распределения ресурсов. Однако в 11ax OFDMA недостаточно гибок. Во-первых, он позволяет точке доступа выделять для клиентского устройства только один ресурсный блок заранее определенного размера. Во-вторых, он не поддерживает прямую передачу между клиентскими станциями. Оба недостатка снижают спектральную эффективность. Кроме того, отсутствие гибкости унаследованного от Wi-Fi 6 OFDMA ухудшает производительность в плотных сетях и увеличивает задержку, что критично для приложений реального времени. 11be решит эти проблемы OFDMA.

4. Одним из утвержденных революционных изменений Wi-Fi 7 является встроенная поддержка **одновременного использования нескольких параллельных соединений на различных частотах**, которая очень полезна как для огромных скоростей передачи данных, так и для чрезвычайно низкой задержки. Хотя современные чипсеты уже могут использовать несколько соединений одновременно, например, в диапазоне 2.4 и 5 ГГц, эти соединения независимы, что ограничивает эффективность такой операции. В 11be будет найден такой уровень синхронизации между каналами, который позволяет эффективно использовать ресурсы канала и повлечёт существенные изменения в правилах протокола доступа к каналу.

5. Использованием очень широких каналов и большого числа пространственных потоков приводит к проблеме высоких накладных расходов, связанных с процедурой оценивания состояния канала, необходимой для MIMO и OFDMA. Эти накладные расходы сводят на нет весь выигрыш от повышения номинальных скоростей передачи данных. Ожидается, что **процедура оценки состояния канала будет пересмотрена**.

6. В контексте Wi-Fi 7 в комитете по стандартизации обсуждается **использование некоторых «продвинутых» методов передачи данных**. В теории эти методы повышают спектральную эффективность в случае повторных попыток передачи, а также при одновременных передачах в одном и том же или противоположных направлениях. Речь идет о гибридном автоматическом запросе повторения HARQ (Hybrid Automatic Repeat Request), используемом сейчас в сотовых сетях, о режиме FD (full-duplex) и о неортогональном множественном доступе NOMA (Non-Orthogonal Multiple Access). Эти методы хорошо изучены в литературе в теории, однако пока не ясно, окупит ли прирост производительности, который они обеспечивают, усилия, направленные на их реализацию.

- Использование **HARQ** осложнено следующей проблемой. В Wi-Fi для снижения накладных расходов пакеты склеиваются. В текущих версиях Wi-Fi доставка каждого пакета внутри склеенного подтверждается и, если подтверждение не приходит, передача пакета повторяется методами протокола доступа к каналу. HARQ переносит повторные попытки с канального на физический уровень, где пакетов больше нет, а есть кодовые слова, причём границы кодовых слов не совпадают с границей пакетов. Такая рассинхронизация усложняет реализацию HARQ в Wi-Fi. • Что касается **Full-Duplex**, то в настоящее время ни в сотовых сетях, ни в сетях Wi-Fi нельзя

одновременно в одном и том же частотном канале передавать данные и к точке доступа (базовой станции), и от неё. С технической точки зрения это связано с большой разницей в мощности передаваемого и принимаемого сигнала. Хотя существуют прототипы, сочетающие цифровое и аналоговое вычитание передаваемого сигнала из принятого, способные получить сигнал Wi-Fi во время своей передачи, выигрыш, который они могут дать на практике, может быть незначительный из-за того, что в каждый момент времени нисходящий поток не равен восходящему (в среднем нисходящий существенно больше). При этом такая двухсторонняя передача существенно усложнит протокол.

- Если для передачи нескольких потоков с использованием MIMO нужно иметь несколько антенн для отправителя и получателя, то в случае неортогонального доступа точка доступа может одновременно передавать данные двум получателям с одной антенны. Различные варианты неортогонального доступа включены в последние спецификации 5G. Прототип **NOMA** Wi-Fi был впервые создан в 2018 г. в ИППИ РАН. Он продемонстрировал прирост производительности 30-40%. Достоинствами разработанной технологии является её обратная совместимость: один из двух получателей может быть устаревшим устройством, не поддерживающим Wi-Fi 7. Вообще проблема обратной совместимости очень важна, так как в сети Wi-Fi могут одновременно работать устройства различных поколений. В настоящее время несколько команд в мире анализируют эффективность от совместного использования NOMA и MU-MIMO, результаты которых определят дальнейшую судьбу подхода.

7. Еще одним важным нововведением, но с неясной судьбой, является **координированная работа точек доступа (рисунок 5.3)**. Хотя многие поставщики имеют свои собственные централизованные контроллеры для корпоративных сетей Wi-Fi, возможности таких контроллеров были, как правило, ограничены настройкой долгосрочных параметров и выбором канала. Комитет по стандартизации обсуждает более тесное сотрудничество между соседними точками доступа, которое включает в себя координированные планирование передач,

beamforming (направленную передачу сигнала) и даже распределенные системы MIMO. Некоторые из рассматриваемых подходов используют последовательное подавление помех (примерно то же, что и в NOMA).

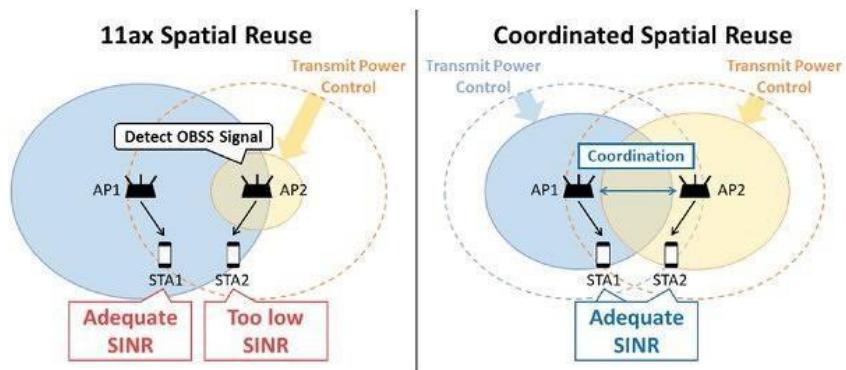


Рисунок 5.2 - Координированный обмен данными в Wi-Fi 7

Хотя подходы для координации 802.11be еще не проработаны, нет сомнения, что стандарт разрешит точкам доступа разных производителей координировать между собой расписание передач, чтобы снизить взаимную интерференцию. Что касается других, более сложных, подходов, например, распределенное MU-MIMO (рисунок 5.4), то их внедрить в стандарт будет сложнее, хотя отдельные члены группы полны решимости сделать это в рамках Release 2. Вне зависимости от исхода судьба методов координации точек доступа туманна. Даже будучи включёнными в стандарт, они могут не дойти до рынка. Похожее случалось и раньше при попытке навести порядок в передачах Wi-Fi с помощью таких решений, как HCCA (Hybrid coordination function Controlled Channel Access -802.11e) и HCCA TXOP (Transmission Opportunity Negotiation (11be)).

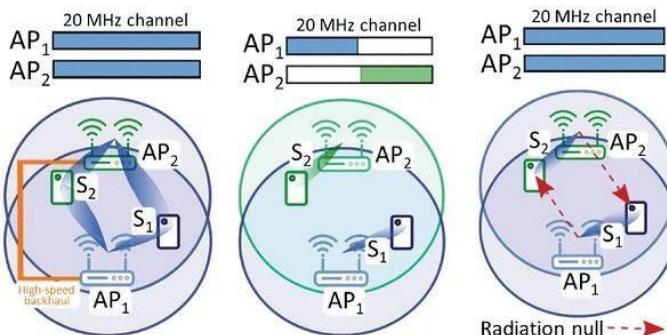


Рисунок 5.4 - Преимущества «кооперативного» MU-MIMO (CMU-MIMO)

Создатели Wi-Fi 7 также учитывают тот факт, что к моменту коммерциализации стандарта частотный диапазон 6 ГГц будет изрядно загружен трафиком других беспроводных сервисов, включая сотовые сети 5G. По этой причине в финальных спецификациях Wi-Fi 7 также появится разрабатываемый в настоящее время «автоматический частотный координатор» – AFC (Automated Frequency Coordinator), задачей которого является эффективное использование частотного спектра.

Скорее всего большинство предложений, связанных с первыми пятью группами, станут частью Wi-Fi 7, в то время как предложения, связанные с двумя последними группами, требуют значительных дополнительных исследований, чтобы доказать свою эффективность.

5.3 Перспективы технологии Wi-Fi 7

Привлекательность технологии Wi-Fi 7 видна из таблицы 1, в которой приведено сравнение характеристик технологий Wi-Fi.

Таблица 5.1 – Характеристики поколений Wi-Fi

Wi-Fi generations					
	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6	Wi-Fi 6E	Wi-Fi 7 (expected)
Launch date	2007	2013	2019	2021	2024
IEEE standard	802.11n	802.11ac	802.11ax		802.11be
Max data rate	1.2 Gbps	3.5 Gbps	9.6 Gbps		46 Gbps
Bands	2.4 GHz and 5 GHz	5 GHz	2.4 GHz and 5 GHz	6 GHz	1–7.25 GHz (including 2.4 GHz, 5 GHz, 6 GHz bands)
Security	WPA 2	WPA 2	WPA 3		WPA3
Channel size	20, 40 MHz	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 80+80, 160 MHz	Up to 320 MHz
Modulation	64-QAM OFDM	256-QAM OFDM	1024-QAM OFDMA		4096-QAM OFDMA (with extensions)
MIMO	4x4 MIMO	4x4 MIMO, DL MU-MIMO	8x8 UL/DL MU-MIMO		16x16 MU-MIMO

Выделение для Wi-Fi 7 частотного диапазона 6 ГГц

Выделение частот в диапазоне 6 ГГц для нужд беспроводных сетей в настоящее время в разных странах находится на разных и порой противоречивых стадиях. Так, несмотря на уже выданное Федеральной комиссии по связи США (FCC) разрешение на использование диапазона 6 ГГц для устройств стандарта Wi-Fi 6 и Wi-Fi 6E, а также позитивные сдвиги в этом направлении со стороны регуляторов Южной Кореи и Великобритании, Европе в этом плане пока находится на перепутье.

По словам **Андреаса Гайсса** (Andreas Geiss), главы департамента политики в отношении распределении радиочастотного спектра GD CONNECT при Еврокомиссии, процесс ратификации нового частотного диапазона осложняется участием в нем не только 26 стран Евросоюза (за вычетом Великобритании), но также всех 48 стран Европы в составе Европейской конференции администраций почтовых служб и служб связи (CEPT, Conference of European Posts and Telecommunications).

Регуляторы полны оптимизма согласовать уже к апрелю 2021 г. протокол по использованию частотного диапазона шириной 500 МГц – в промежутке между 5945 МГц и 6425 МГц, для целей Wi-Fi. Ожидается, что к апрелю 2021 г. европейские регуляторы согласуют и примут две версии правил для использования беспроводного оборудования в диапазоне. Одна из этих версий – с низким энергопотреблением для помещений (Low Power Indoor, LPI), будет предназначена для оборудования с размещением только внутри зданий, с полным доступом к частотам в полосе 480 МГц.

Оборудование категории с очень низким энергопотреблением – Very Low Power (VLP), можно будет использовать как внутри, так и вне помещений, при этом спектральные полосы для этого будут разделены на две категории - 400 МГц и 80 МГц, соответственно.

Ожидается, что большинство техники Wi-Fi с поддержкой диапазона 6 ГГц будет поставляться в категории LPI. В только недавно разработанной и представленной категории VLP будут появляться в основном потребительские устройства – такие как виртуальные очки VR/AR и другие гаджеты с подключением к смартфонам.

Перспективы Wi-Fi 7 в России

В России правила сертификации устройств стандарта Wi-Fi 6 (802.11ax) в диапазонах частот 2400-2483,5 МГц, 5150-5350 МГц и новом 5650-6425 МГц урегулированы приказом Минцифры России №321 от 6 июля 2020 г. «О внесении изменений в Правила применения оборудования радиодоступа. Часть I. Правила применения оборудования радиодоступа для беспроводной передачи данных в диапазоне от 30 МГц до 66 ГГц, утвержденные

приказом Министерства связи и массовых коммуникаций Российской Федерации от 14.09.2010 N 124», Приложение 10.3.

В частности, новыми правилами для оборудования стандарта Wi-Fi 6 устанавливается требование не менее четырех потоков MIMO для базовой станции и не менее двух для абонента, и не более восьми в обоих случаях. Поддерживаемая ширина канала может составлять 20 МГц, 40 МГц, 80 МГц, 80+80 МГц или 160 МГц, с модуляцией BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM и 1024-QAM.

С точки зрения адаптации нового стандарта в России, при появлении финальных спецификаций Wi-Fi 7 в документе российского регулятора понадобятся лишь минимальные дополнения, поскольку частотный диапазон 6 ГГц уже разрешен для использования устройствами Wi-Fi на территории страны.

УГРОЗЫ И РИСКИ БЕСПРОВОДНЫХ СЕТЕЙ

Главное отличие беспроводных сетей от проводных связано с абсолютно неконтролируемой областью между конечными точками сети. В достаточно широком пространстве сетей беспроводная среда никак не контролируется. Современные беспроводные технологии предлагают ограниченный набор средств управления всей областью развертывания сети. Это позволяет атакующим, находящимся в непосредственной близости от беспроводных структур, производить целый ряд нападений, которые были невозможны в проводной сети. Обсудим характерные только для беспроводного окружения угрозы безопасности, оборудование, которое используется при атаках, проблемы, возникающие при роуминге от одной точки доступа к другой, укрытия для беспроводных каналов и криптографическую защиту открытых коммуникаций.

Подслушивание

Наиболее распространенная проблема в таких открытых и неуправляемых средах, как беспроводные сети, - возможность анонимных атак. Анонимные вредители могут перехватывать радиосигнал и расшифровывать передаваемые данные, как показано на рис. 7.1.

Оборудование, используемое для подслушивания в сети, может быть не сложнее того, которое используется для обычного доступа к этой сети. Чтобы перехватить передачу, злоумышленник должен находиться вблизи от передатчика. Перехваты такого типа практически невозможно зарегистрировать, и еще труднее помешать им. Использование антенн и усилителей дает злоумышленнику возможность находиться на значительном расстоянии от цели в процессе перехвата.

Подслушивание позволяет собрать информацию в сети, которую впоследствии предполагается атаковать. Первичная цель злоумышленника - понять, кто использует сеть, какие данные в ней доступны, каковы возможности сетевого оборудования, в какие моменты его эксплуатируют наиболее и наименее интенсивно и какова территория развертывания сети. Все это пригодится для того, чтобы организовать атаку на сеть. Многие общедоступные сетевые протоколы передают такую важную информацию, как имя пользователя и пароль, открытым текстом. Перехватчик может использовать добытые данные для того, чтобы получить доступ к сетевым ресурсам. Даже если передаваемая информация зашифрована, в руках злоумышленника оказывается текст, который можно запомнить, а потом уже раскодировать.

Атака "подслушивание"



Рис. 7.1. Атака "подслушивание"

Другой способ подслушивания - подключение к беспроводной сети. Активное подслушивание в локальной беспроводной сети обычно основано на неправильном использовании протокола Address Resolution Protocol (ARP). Изначально эта технология была создана для "прослушивания" сети. В действительности мы имеем дело с атакой типа MITM (Man In The Middle - "человек посередине") на уровне связи данных. Они могут принимать различные формы и используются для разрушения конфиденциальности и целостности сеанса связи. Атаки MITM более сложны, чем большинство других атак: для их проведения требуется подробная информация о сети.

Злоумышленник обычно подменяет идентификацию одного из сетевых ресурсов. Когда жертва атаки инициирует соединение, мошенник перехватывает его и затем завершает соединение с требуемым ресурсом, а потом пропускает все соединения с этим ресурсом через свою станцию. При этом атакующий может посылать и изменять информацию или подслушивать все переговоры и потом расшифровывать их.

Атакующий посылает ARP-ответы, на которые не было запроса, к целевой станции локальной сети, которая отправляет ему весь проходящий через нее трафик. Затем злоумышленник будет отсылать пакеты указанным адресатам.

Таким образом, беспроводная станция может перехватывать трафик другого беспроводного клиента (или проводного клиента в локальной сети).

Отказ в обслуживании (Denial of Service - DOS)

Полную парализацию сети может вызвать атака типа DOS. Во всей сети, включая базовые станции и клиентские терминалы, возникает такая сильная интерференция, что станции не могут связываться друг с другом (рис. 7.2). Эта атака выключает все коммуникации в определенном районе. Если она проводится в достаточно широкой области, то может потребовать значительных мощностей. Атаку DOS на беспроводные сети трудно предотвратить или остановить. Большинство беспроводных сетевых технологий использует нелицензированные частоты - следовательно, допустима интерференция от целого ряда электронных устройств.

Атака "отказ в обслуживании" в беспроводных коммуникациях



Рис. 7.2. Атака "отказ в обслуживании" в беспроводных коммуникациях

Глушение клиентской станции

Глушение в сетях происходит тогда, когда преднамеренная или непреднамеренная интерференция превышает возможности отправителя или получателя в канале связи, и канал выходит из строя. Атакующий может использовать различные способы глушения.

Глушение клиентской станции дает мошеннику возможность подставить себя на место заглушенного клиента, как показано на рис. 7.3. Также глушение может использоваться для отказа в обслуживании клиента, чтобы ему не удавалось реализовать соединение. Более изощренные атаки прерывают соединение с базовой станцией, чтобы затем она была присоединена к станции злоумышленника.

Глушение базовой станции

Глушение базовой станции предоставляет возможность подменить ее атакующей станцией, как показано на рис. 7.4. Такое глушение лишает пользователей доступа к услугам.

Атака глушения клиента для перехвата соединения



Рис. 7.3. Атака глушения клиента для перехвата соединения

Атака глушения базовой станции для перехвата соединения



Рис. 7.4. Атака глушения базовой станции для перехвата соединения

Как отмечалось выше, большинство беспроводных сетевых технологий использует нелицензированные частоты. Поэтому многие устройства, такие как радиотелефоны, системы слежения и микроволновые печи, могут влиять на работу беспроводных сетей и глушить беспроводное соединение. Чтобы предотвратить такие случаи непреднамеренного глушения, прежде чем покупать дорогостоящее беспроводное оборудование, надо тщательно проанализировать место его установки. Такой анализ поможет убедиться в том, что другие устройства не помешают коммуникациям.

Угрозы криптозащиты

В беспроводных сетях применяются криптографические средства для обеспечения целостности и конфиденциальности информации. Однако оплошности приводят к нарушению коммуникаций и использованию информации злоумышленниками.

WEP - это криптографический механизм, созданный для обеспечения безопасности сетей стандарта 802.11. Этот механизм разработан с единственным статическим ключом, который применяется всеми пользователями. Управляющий доступ к ключам, частое их изменение и обнаружение нарушений практически невозможны. Исследование WEP-шифрования выявило уязвимые места, из-за которых атакующий может полностью восстановить ключ после захвата минимального сетевого трафика. В Internet есть средства, которые позволяют злоумышленнику восстановить ключ в течение нескольких часов. Поэтому на WEP нельзя полагаться как на средство аутентификации и конфиденциальности в беспроводной сети. Использовать описанные криптографические механизмы лучше, чем не использовать никаких, но, с учетом известной уязвимости, необходимы другие методы защиты от атак. Все беспроводные коммуникационные сети подвержены атакам прослушивания в период контакта (установки соединения, сессии связи и прекращения соединения). Сама природа беспроводного соединения не позволяет его контролировать, и потому оно требует защиты. Управление ключом, как правило, вызывает дополнительные проблемы, когда применяется при роуминге и в случае общего пользования открытой средой. Далее мы более внимательно рассмотрим проблемы криптографии и их решения.

Анонимность атак

Беспроводной доступ обеспечивает полную анонимность атаки. Без соответствующего оборудования в сети, позволяющего определять местоположение, атакующий может легко сохранять анонимность и прятаться где угодно на территории действия беспроводной сети. В таком случае злоумышленника трудно поймать и еще сложнее передать дело в суд.

В недалеком будущем прогнозируется ухудшение распознаваемости атак в Internet из-за широкого распространения анонимных входов через небезопасные точки доступа. Уже существует много сайтов, где публикуются списки таких точек, которые можно использовать с целью вторжения. Важно отметить, что многие мошенники изучают сети не для атак на их внутренние ресурсы, а для получения бесплатного анонимного доступа в Internet, прикрываясь которым, они атакуют другие сети. Если операторы связи не принимают мер предосторожности против таких нападений, они должны нести ответственность за вред, причиняемый другим сетям при использовании их доступа к Internet.

Физическая защита

Устройства беспроводного доступа к сети должны быть маленькими и переносимыми (КПК, ноутбуки), как и точки доступа. Кража таких устройств во многом приводит к тому, что злоумышленник может попасть в сеть, не

предпринимая сложных атак, т. к. основные механизмы аутентификации в стандарте 802.11 рассчитаны на регистрацию именно физического аппаратного устройства, а не учетной записи пользователя. Так что потеря одного сетевого интерфейса и несвоевременное извещение администратора может привести к тому, что злоумышленник получит доступ к сети без особых хлопот.

Протоколы безопасности беспроводных сетей

Существует множество технологий безопасности, и все они предлагают решения для важнейших компонентов политики в области защиты данных: аутентификации, поддержания целостности данных и активной проверки. Мы определяем аутентификацию как аутентификацию пользователя или конечного устройства (клиента, сервера, коммутатора, маршрутизатора, межсетевого экрана и т. д.) и его местоположения с последующей авторизацией пользователей и конечных устройств.

Целостность данных включает такие области, как безопасность сетевой инфраструктуры, безопасность периметра и конфиденциальность данных. Активная проверка помогает удостовериться в том, что установленная политика в области безопасности соблюдается, и отследить все аномальные случаи и попытки несанкционированного доступа.

Механизм шифрования WEP

Шифрование WEP (Wired Equivalent Privacy - секретность на уровне проводной связи) основано на алгоритме RC4 (Rivest's Cipher v.4 - код Ривеста), который представляет собой симметричное потоковое шифрование. Как было отмечено ранее, для нормального обмена пользовательскими данными ключи шифрования у абонента и точки радиодоступа должны быть идентичными.

Ядро алгоритма состоит из функции генерации ключевого потока. Эта функция генерирует последовательность битов, которая затем объединяется с открытым текстом посредством суммирования по модулю два. Дешифрация состоит из регенерации этого ключевого потока и суммирования его с шифрограммой по модулю два для восстановления исходного текста. Другая главная часть алгоритма - функция инициализации, которая использует ключ переменной длины для создания начального состояния генератора ключевого потока.

RC4 - фактически класс алгоритмов, определяемых размером его блока. Этот параметр n является размером слова для алгоритма. Обычно, $n = 8$, но в целях анализа можно уменьшить его. Однако для повышения уровня безопасности необходимо задать большее значение этой величины. Внутреннее состояние RC4 состоит из массива размером $2n$ слов и двух счетчиков, каждый размером в одно слово. Массив известен как S-бокс, и далее он будет обозначаться как S. Он всегда содержит перестановку $2n$ возможных значений слова. Два счетчика обозначены через i и j .

Этот алгоритм использует ключ, сохраненный в Key и имеющий длину l байт. Инициализация начинается с заполнения массива S, далее этот массив перемешивается путем перестановок, определяемых ключом. Так как над S выполняется только одно действие, должно выполняться утверждение, что S всегда содержит все значения кодового слова.

Генератор ключевого потока RC4 переставляет значения, хранящиеся в S, и каждый раз выбирает новое значение из S в качестве результата. В одном цикле RC4 определяется одно n -битное слово K из ключевого потока, которое в дальнейшем суммируется с исходным текстом для получения зашифрованного текста.

Особенности WEP-протокола:

- Достаточно устойчив к атакам, связанным с простым перебором ключей шифрования, что обеспечивается необходимой длиной ключа и частотой смены ключей и инициализирующего вектора;
- Самосинхронизация для каждого сообщения. Это свойство является ключевым для протоколов уровня доступа к среде передачи, где велико число искаженных и потерянных пакетов;
- Эффективность: WEP легко реализовать;
- Открытость;
- Использование WEP-шифрования не является обязательным в сетях стандарта IEEE 802.11.
- Для непрерывного шифрования потока данных используется потоковое и блочное шифрование.

Потоковое шифрование

При потоковом шифровании выполняется побитовое сложение по модулю 2 (функция "исключающее ИЛИ", XOR) ключевой последовательности, генерируемой алгоритмом шифрования на основе заранее заданного ключа, и исходного сообщения. Ключевая последовательность имеет длину, соответствующую длине исходного сообщения, подлежащего шифрованию (рис. 8.1).

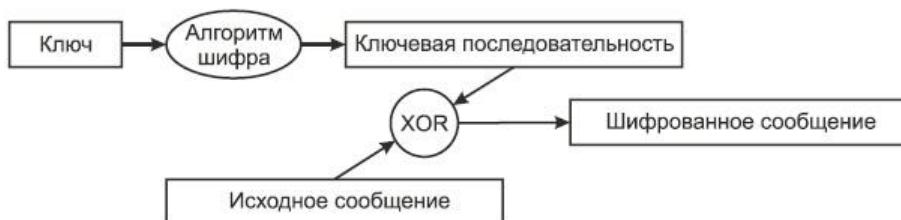


Рис. 8.1. Потоковое шифрование

Блочное шифрование

Блочное шифрование работает с блоками заранее определенной длины, не меняющимися в процессе шифрования. Исходное сообщение фрагментируется на блоки, и функция XOR вычисляется над ключевой последовательностью и каждым блоком. Размер блока фиксирован, а последний фрагмент исходного сообщения дополняется пустыми символами до длины нормального блока (рис. 8.2). Например, при блочном шифровании с 16-байтовыми блоками исходное сообщение длиной в 38 байтов фрагментируется на два блока длиной по 16 байтов и 1 блок длиной 6 байтов, который затем дополняется 10 байтами пустых символов до длины нормального блока.

Потоковое шифрование и блочное шифрование используют метод электронной кодовой книги (ECB). Метод ECB характеризуется тем, что одно и то же исходное сообщение на входе всегда порождает одно и то же зашифрованное сообщение на выходе. Это потенциальная брешь в системе безопасности, ибо сторонний наблюдатель, обнаружив повторяющиеся последовательности в зашифрованном сообщении, в состоянии сделать обоснованные предположения относительно идентичности содержания исходного сообщения.

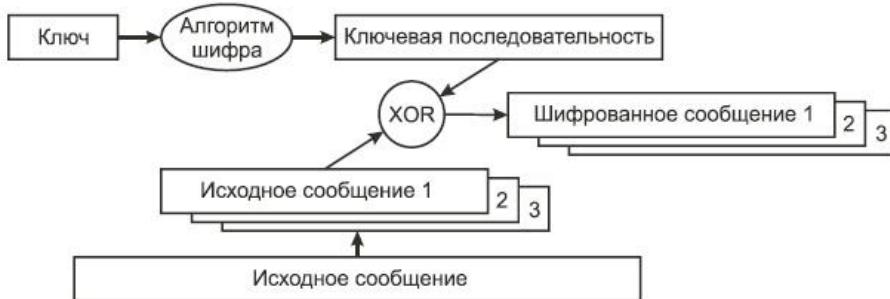


Рис. 8.2. Блочное шифрование

Для устранения указанной проблемы используют:

Векторы инициализации (Initialization Vectors - IVs).

Обратную связь (feedback modes).

До начала процесса шифрования 40- или 104-битный секретный ключ распределяется между всеми станциями, входящими в беспроводную сеть. К секретному ключу добавляется вектор инициализации (IV).

Вектор инициализации (Initialization Vector - IV)

Вектор инициализации используется для модификации ключевой последовательности. При использовании вектора инициализации ключевая последовательность генерируется алгоритмом шифрования, на вход которого подается секретный ключ, совмещенный с IV. При изменении вектора инициализации ключевая последовательность также меняется. На рис. 8.3 исходное сообщение шифруется с использованием новой ключевой последовательности, сгенерированной алгоритмом шифрования после подачи на его вход комбинации из секретного ключа и вектора инициализации, что порождает на выходе шифрованное сообщение.

Стандарт IEEE 802.11 рекомендует использовать новое значение вектора инициализации для каждого нового фрейма, передаваемого в радиоканал.

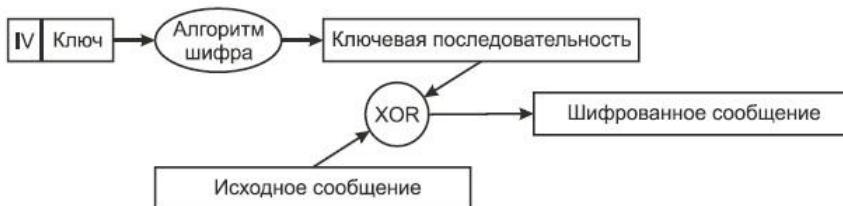


Рис. 8.3. Алгоритм шифрования WEP

Таким образом, один и тот же нешифрованный фрейм, передаваемый многократно, каждый раз будет порождать уникальный шифрованный фрейм.

Вектор инициализации имеет длину 24 бита и совмещается с 40- или 104-битовым базовым ключом шифрования WEP таким образом, что на вход алгоритма шифрования подается 64- или 128-битовый ключ. Вектор инициализации присутствует в нешифрованном виде в заголовке фрейма в радиоканале, с тем чтобы принимающая сторона могла успешно декодировать этот фрейм. Несмотря на то, что обычно говорят об использовании шифрования WEP с ключами длиной 64 или 128 битов, эффективная длина ключа составляет лишь 40 или 104 бита по причине передачи вектора инициализации в нешифрованном виде. При настройках шифрования в оборудовании при 40-битном эффективном ключе вводятся 5 байтовых ASCII-символов ($5 \times 8 = 40$) или 10 шестнадцатеричных чисел ($10 \times 4 = 40$), и при 104-битном эффективном ключе вводятся 13 байтовых ASCII-символов ($13 \times 8 = 104$) или 26 шестнадцатеричных чисел ($26 \times 4 = 104$). Некоторое оборудование может работать со 128-битным ключом.

Обратная связь

Обратная связь модифицирует процесс шифрования и предотвращает порождение одним и тем же исходным сообщением одного и того же шифрованного сообщения. Обратная связь обычно используется при блочном шифровании. Чаще всего встречается тип обратной связи, известный как цепочка шифрованных блоков (CBC).

В основе использования цепочки шифрованных блоков лежит идея вычисления двоичной функции XOR между блоком исходного сообщения и предшествовавшим ему блоком шифрованного сообщения. Поскольку самый первый блок не имеет предшественника, для модификации ключевой последовательности используют вектор инициализации. Работу цепочки шифрованных блоков иллюстрирует рис. 8.4.

Уязвимость шифрования WEP

Атаки на зашифрованные данные с помощью технологии WEP можно подразделить на два метода: пассивные и активные.

Пассивные сетевые атаки

В августе 2001 года криптоаналитики Флурер С., Мантин И. и Шамир А. (Fluhrer S., Mantin I., Shamir A.) установили, что секретный ключ шифрования WEP может быть вычислен с использованием определенных фреймов, пассивно собранных в беспроводной локальной сети. Причиной уязвимости послужила реализация в WEP метода планирования ключей (Key Scheduling Algorithm - KSA) алгоритма потокового шифрования RC4. Некоторые векторы инициализации (так называемые "слабые" векторы) дают возможность установить побайтовый состав секретного ключа, применяя статистический анализ.

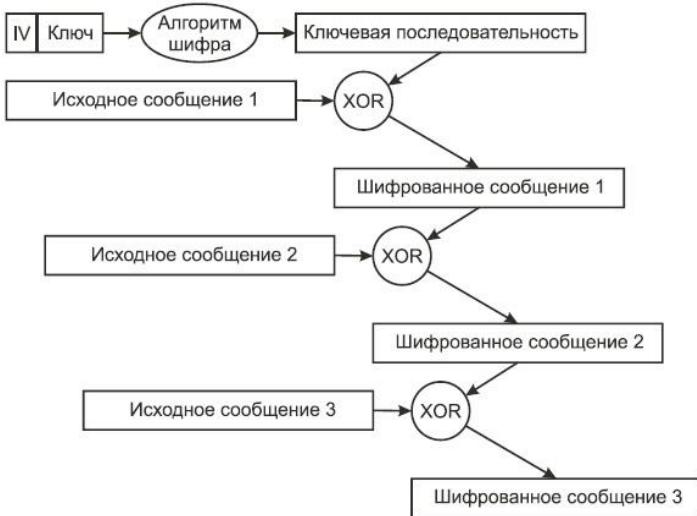


Рис. 8.4. Шифрование с обратной связью

Исследователями из AT&T/Rice University и авторами программы AirSnort была продемонстрирована возможность определения секретного ключа длиной 40 и 104 битов после анализа всего лишь 4 миллионов фреймов. Для загруженной беспроводной локальной сети это эквивалентно приблизительно 4 часам работы, после чего ключ шифрования станет известен пассивному наблюдателю.

Подобная уязвимость делает шифрование с использованием WEP неэффективным. Использование динамических секретных ключей шифрования WEP решает проблему лишь частично, для полного устранения уязвимости требуется усиление самого ключа.

Активные сетевые атаки

Индуктивное вычисление секретного ключа шифрования WEP представляет собой процесс воздействия на беспроводную локальную сеть для получения определенной информации и относится к классу активных сетевых атак. Как было сказано ранее, при потоковом шифровании выполняется двоичное сложение по модулю 2 (XOR) исходного сообщения с ключевой последовательностью с целью получения шифрованного сообщения. Этот факт лег в основу данной атаки.

Высокая эффективность атаки индуктивного вычисления ключа, предпринимаемой в беспроводной локальной сети IEEE 802.11, объясняется отсутствием действенных средств контроля целостности сообщений (Message Integrity Check, MIC). Принимающая сторона не в состоянии распознать факт модификации содержимого фрейма в процессе передачи по общедоступному радиоканалу. Более того, значение ICV (Integrity Check Value), предусмотренное стандартом для контроля целостности сообщений, вычисляется с помощью функции CRC32 (32-bit Cyclical Redundancy Check, контроль с помощью циклического 32-битного избыточного кода), которая подвержена атакам с манипуляцией битами. Таким образом, в отсутствии механизмов контроля целостности сообщений беспроводные локальные сети подвержены активным атакам: повторному использованию вектора инициализации (IV Replay) и манипуляции битами (Bit-Flipping).

1) **Повторное использование вектора инициализации** (Initialization Vector Replay Attacks), представляет собой разработанную теоретически и реализованную практически активную сетевую атаку в беспроводной локальной сети, существующую в нескольких разновидностях, одна из которых описана ниже и проиллюстрирована рис. 8.5.

1. Хакер многократно отправляет абоненту беспроводной локальной сети по проводной сети сообщение известного содержания (например, IP-пакет, письмо по электронной почте и т. п.).
2. Хакер пассивно прослушивает радиоканал связи абонента с точкой радиодоступа и собирает фреймы, предположительно содержащие шифрованное сообщение.
3. Хакер вычисляет ключевую последовательность, применяя функцию XOR к предполагаемому шифрованному и известному нешифрованному сообщениям.
4. Хакер "выращивает" ключевую последовательность для пары вектора инициализации и секретного ключа, породившей ключевую последовательность, вычисленную на предыдущем шаге.

Атакующий знает, что пара вектора инициализации и секретного ключа шифрования, а значит и порождаемая ими ключевая последовательность, может быть повторно использована для воссоздания ключевой последовательности достаточной длины для нарушения конфиденциальности в беспроводной локальной сети в условиях использования шифрования WEP.

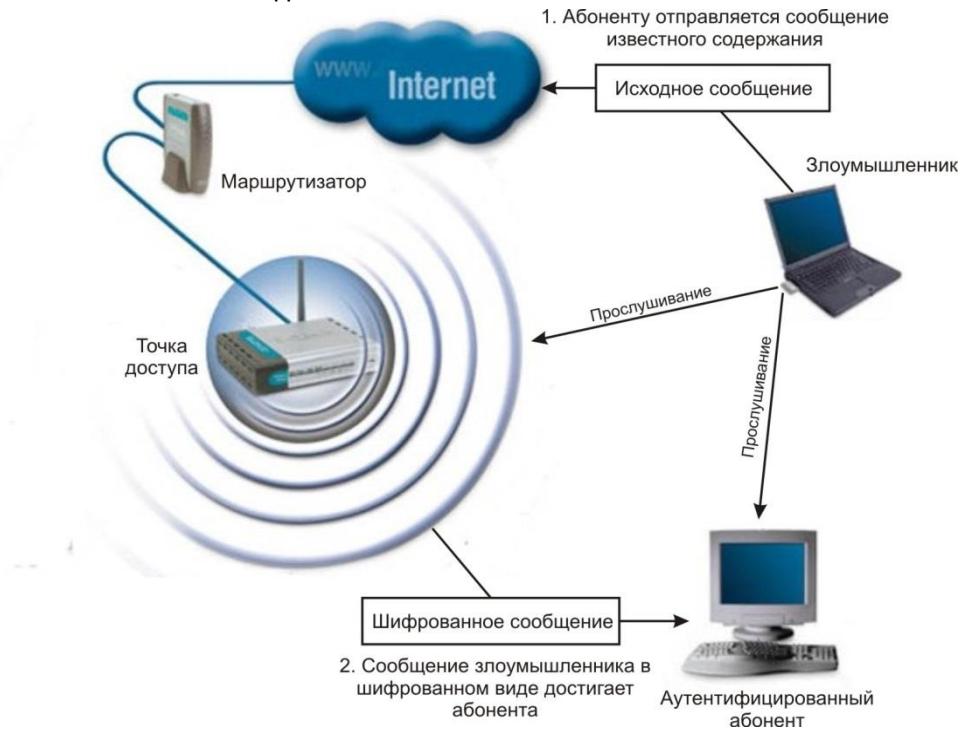


Рис. 8.5. Повторное использование вектора инициализации

После того, как ключевая последовательность вычислена для фреймов некоторой длины, ее можно "вырастить" до любого размера, как описано ниже и показано на рис. 8.6.

1. Хакер создает фрейм на один байт длиннее, чем длина уже известной ключевой последовательности. Пакеты ICMP (Internet Control Message Protocol - протокол управляющих сообщений Internet), посылаемые командой ping, идеальны для этих целей, ибо точка радиодоступа вынуждена на них отвечать.
2. Хакер увеличивает длину ключевой последовательности на один байт.
3. Значение дополнительного байта выбирается случайным образом из 256 возможных ASCII-символов.

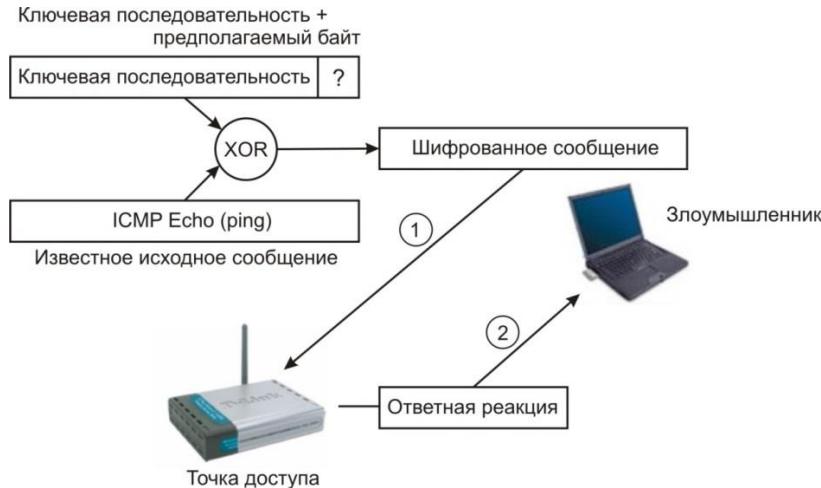


Рис. 8.6. "Выращивание" ключевой последовательности

Если предполагаемое значение дополнительного байта ключевой последовательности верно, то будет получен ожидаемый ответ от точки радиодоступа, в данном примере это ICMP

Процесс повторяется до тех пор, пока не будет подобрана ключевая последовательность нужной длины.

2) Манипуляция битами (Bit-Flipping Attacks)

Манипуляция битами преследует ту же цель, что и повторное использование вектора инициализации, и опирается на уязвимость вектора контроля целостности фрейма ICV. Пользовательские данные могут различаться от фрейма к фрейму, в то же время многие служебные поля и их положение внутри фрейма остаются неизменными.

Хакер манипулирует битами пользовательских данных внутри фрейма 2-го (канального) уровня модели OSI (Open Systems Interconnection) с целью искажения 3-го (сетевого) уровня пакета. Процесс манипуляции показан на рис. 8.7.

1. Хакер пассивно наблюдает фреймы беспроводной локальной сети с помощью средств анализа трафика протокола 802.11.

2. Хакер захватывает фрейм и произвольно изменяет биты в поле данных протокола 3-го уровня.

3. Хакер модифицирует значение вектора контроля целостности фрейма ICV (как именно, будет описано ниже).

4. Хакер передает модифицированный фрейм в беспроводную локальную сеть.

5. Принимающая сторона (абонент либо точка радиодоступа) вычисляет значение вектора контроля целостности фрейма ICV для полученного модифицированного фрейма.

6. Принимающая сторона сравнивает вычисленное значение вектора ICV с имеющимся в полученном модифицированном фрейме.

7. Значения векторов совпадают, фрейм считается неискаженным и не отбрасывается.

8. Принимающая сторона деинкапсулирует содержимое фрейма и обрабатывает пакет сетевого уровня.

9. Поскольку манипуляция битами происходила на канальном уровне, контрольная сумма сетевого уровня оказывается неверной.

10. Стек протокола сетевого уровня на принимающей стороне генерирует предсказуемое сообщение об ошибке.

11. Хакер наблюдает за беспроводной локальной сетью в ожидании зашифрованного фрейма с сообщением об ошибке.

12. Хакер захватывает фрейм, содержащий зашифрованное сообщение об ошибке, и вычисляет ключевую последовательность, как было описано ранее для атаки с повторным использованием вектора инициализации.

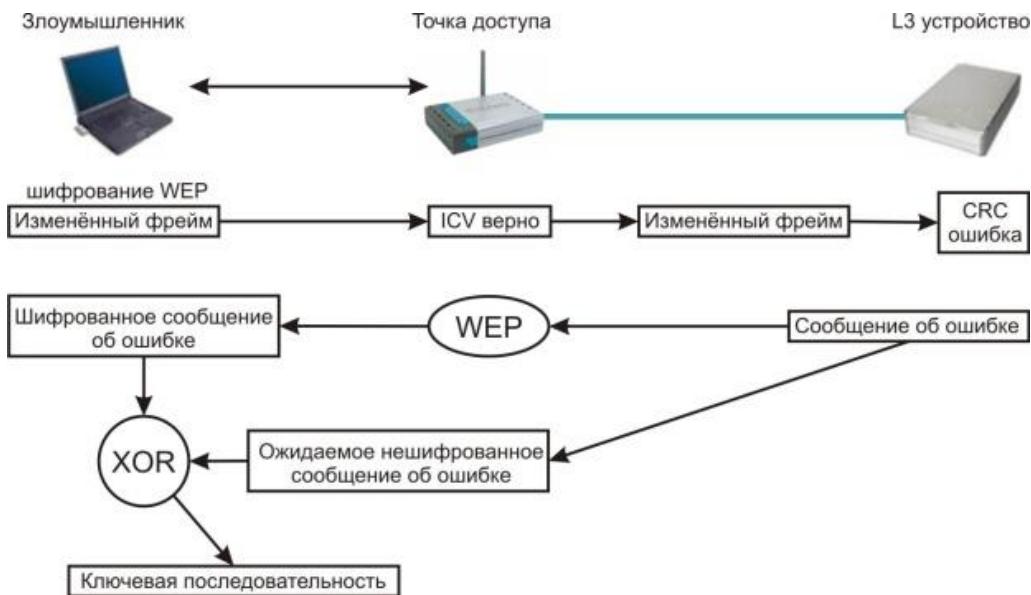


Рис. 8.7. Атака с манипуляцией битами

Вектор ICV находится в шифрованной части фрейма. С помощью следующей процедуры хакер манипулирует битами шифрованного вектора ICV и таким образом обеспечивает корректность самого вектора для нового, модифицированного фрейма (рис. 8.8):

1. Исходный фрейм F1 имеет вектор C1.

2. Создается фрейм F2 такой же длины, что и F1, служащий маской для модификации битов фрейма F1.
3. Создается фрейм F3 путем выполнения двоичной функции XOR над фреймами F1 и F2.
4. Вычисляется промежуточный вектор C2 для фрейма F3.
5. Вектор C3 для фрейма F3 вычисляется путем выполнения двоичной функции XOR над C1 и C2.

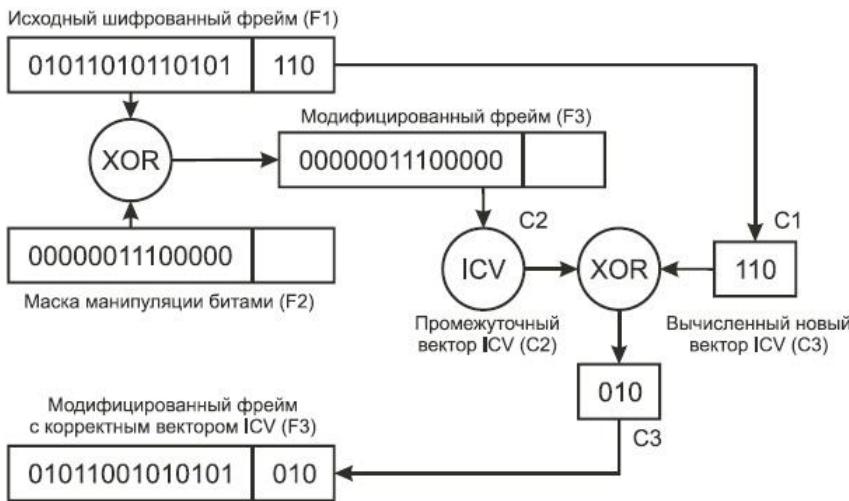


Рис. 8.8. Вычисление поля контроля целостности сообщений

Проблемы управления статическими WEP-ключами

Стандартом IEEE 802.11 не предусмотрены какие-либо механизмы управления ключами шифрования. По определению, алгоритм WEP поддерживает лишь статические ключи, которые заранее распространяются тем или иным способом между абонентами и точками радиодоступа беспроводной локальной сети. Поскольку IEEE 802.11 аутентифицирует физическое устройство, а не его пользователя, утрата абонентского адаптера, точки радиодоступа или собственно секретного ключа представляют опасность для системы безопасности беспроводной локальной сети. В результате при каждом подобном инциденте администратор сети будет вынужден вручную произвести смену ключей у всех абонентов и в точках доступа. Для этого во всем оборудовании D-Link отведено четыре поля для ввода ключей. И при смене всех ключей необходимо только поменять номер используемого ключа.

Эти административные действия годятся для небольшой беспроводной локальной сети, но совершенно неприемлемы для сетей, в которых абоненты исчисляются сотнями и тысячами и/или распределены территориально. В условиях отсутствия механизмов генерации и распространения ключей администратор вынужден тщательно охранять абонентские адаптеры и оборудование инфраструктуры сети.

Аутентификация в беспроводных сетях

Основными стандартами аутентификации в беспроводных сетях являются стандарты IEEE 802.11, WPA, WPA2 и 802.1x. Рассмотрим основы этих стандартов.

Стандарт IEEE 802.11 сети с традиционной безопасностью

Стандарт IEEE 802.11 с традиционной безопасностью (Traditional Security Network - TSN) предусматривает два механизма аутентификации беспроводных абонентов: открытую аутентификацию (Open Authentication) и аутентификацию с общим ключом (Shared Key Authentication). В аутентификации в беспроводных сетях также широко используются два других механизма, выходящих за рамки стандарта 802.11, а именно назначение идентификатора беспроводной локальной сети (Service Set Identifier - SSID) и аутентификация абонента по его MAC-адресу (MAC Address Authentication).

Идентификатор беспроводной локальной сети (SSID) представляет собой атрибут беспроводной сети, позволяющий логически отличать сети друг от друга. В общем случае абонент беспроводной сети должен задать у себя соответствующий SSID для того, чтобы получить доступ к требуемой беспроводной локальной сети. SSID ни в коей мере не обеспечивает конфиденциальность данных, равно как и не аутентифицирует абонента по

отношению к точке радиодоступа беспроводной локальной сети. Существуют точки доступа, позволяющие разделить абонентов, подключаемых к точке на несколько сегментов, - это достигается тем, что точка доступа может иметь не один, а несколько SSID.

Принцип аутентификации абонента в IEEE 802.11

Аутентификация в стандарте IEEE 802.11 ориентирована на аутентификацию абонентского устройства радиодоступа, а не конкретного абонента как пользователя сетевых ресурсов. Процесс аутентификации абонента беспроводной локальной сети IEEE 802.11 состоит из следующих этапов (рис. 9.1):

1. Абонент (Client) посыпает фрейм Probe Request во все радиоканалы.
2. Каждая точка радиодоступа (Access Point - AP), в зоне радиовидимости которой находится абонент, посыпает в ответ фрейм Probe Response.
3. Абонент выбирает предпочтительную для него точку радиодоступа и посыпает в обслуживаемый ею радиоканал запрос на аутентификацию (Authentication Request).
4. Точка радиодоступа посыпает подтверждение аутентификации (Authentication Reply).
5. В случае успешной аутентификации абонент посыпает точке радиодоступа фрейм ассоциации (Association Request).
6. Точка радиодоступа посыпает в ответ фрейм подтверждения ассоциации (Association Response).
7. Абонент может теперь осуществлять обмен пользовательским трафиком с точкой радиодоступа и проводной сетью.



Рис. 9.1. Аутентификация по стандарту 802.11

При активизации беспроводный абонент начинает поиск точек радиодоступа в своей зоне радиовидимости с помощью управляющих фреймов Probe Request. Фреймы Probe Request посыпаются в каждый из радиоканалов, поддерживаемых абонентским радиоинтерфейсом, чтобы найти все точки радиодоступа с необходимыми клиенту идентификатором SSID и поддерживаемыми скоростями радиообмена. Каждая точка радиодоступа из находящихся в зоне радиовидимости абонента, удовлетворяющая запрашиваемым во фрейме Probe Request параметрам, отвечает фреймом Probe Response, содержащим синхронизирующую информацию и данные о текущей загрузке точки радиодоступа. Абонент определяет, с какой точкой радиодоступа он будет работать, путем сопоставления поддерживаемых ими скоростей радиообмена и загрузки. После того как предпочтительная точка радиодоступа определена, абонент переходит в фазу аутентификации.

Открытая аутентификация

Открытая аутентификация по сути не является алгоритмом аутентификации в привычном понимании. Точка радиодоступа удовлетворит любой запрос открытой аутентификации. На первый взгляд использование этого алгоритма может показаться бессмысленным, однако следует учитывать, что разработанные в 1997 году методы аутентификации IEEE 802.11 ориентированы на быстрое логическое подключение к беспроводной локальной сети. Вдобавок к этому многие IEEE 802.11-совместимые устройства представляют собой портативные блоки сбора информации (сканеры штрих-кодов и т. п.), не имеющие достаточной процессорной мощности, необходимой для реализации сложных алгоритмов аутентификации.

В процессе открытой аутентификации происходит обмен сообщениями двух типов:

- запрос аутентификации (Authentication Request);
- подтверждение аутентификации (Authentication Response).

Таким образом, при открытой аутентификации возможен доступ любого абонента к беспроводной локальной сети. Если в беспроводной сети шифрование не используется, любой абонент, знающий

идентификатор SSID точки радиодоступа, получит доступ к сети. При использовании точками радиодоступа шифрования WEP сами ключи шифрования становятся средством контроля доступа. Если абонент не располагает корректным WEP-ключом, то даже в случае успешной аутентификации он не сможет ни передавать данные через точку радиодоступа, ни расшифровывать данные, переданные точкой радиодоступа (рис. 9.2).

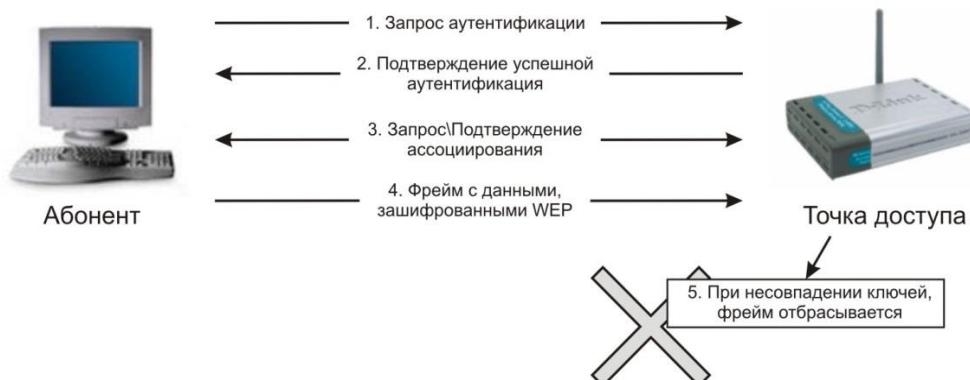


Рис. 9.2. Открытая аутентификация

Аутентификация с общим ключом

Аутентификация с общим ключом является вторым методом аутентификации стандарта IEEE 802.11. Аутентификация с общим ключом требует настройки у абонента статического ключа шифрования WEP. Процесс аутентификации иллюстрирует [рис. 9.3:](#)

1. Абонент посылает точке радиодоступа запрос аутентификации, указывая при этом необходимость использования режима аутентификации с общим ключом.
2. Точка радиодоступа посылает подтверждение аутентификации, содержащее *Challenge Text*.
3. Абонент шифрует *Challenge Text* своим статическим WEP-ключом и посылает точке радиодоступа запрос аутентификации.
4. Если точка радиодоступа в состоянии успешно расшифровать запрос аутентификации и содержащийся в нем *Challenge Text*, она посылает абоненту подтверждение аутентификации, таким образом предоставляя доступ к сети.



Рис. 9.3. Аутентификация с общим ключом

Аутентификация по MAC-адресу

Аутентификация абонента по его MAC-адресу не предусмотрена стандартом IEEE 802.11, однако поддерживается многими производителями оборудования для беспроводных сетей, в том числе D-Link. При аутентификации по MAC-адресу происходит сравнение MAC-адреса абонента либо с хранящимся локально списком разрешенных адресов легитимных абонентов, либо с помощью внешнего сервера аутентификации (рис. 9.4). Аутентификация по MAC-адресу используется в дополнение к открытой аутентификации и аутентификации с общим ключом стандарта IEEE 802.11 для уменьшения вероятности доступа посторонних абонентов.



Рис. 9.4. Аутентификация с помощью внешнего сервера

Пример 9.1

Настроим точку доступа на *WEP*-шифрование.

1. Подключаемся к точке доступа, вводим режим, *SSID*, канал, как было описано в примере 1.4. Далее в поле Authentication (Аутентификация) ставим Shared Key (с общим ключом) (рис. 9.5).

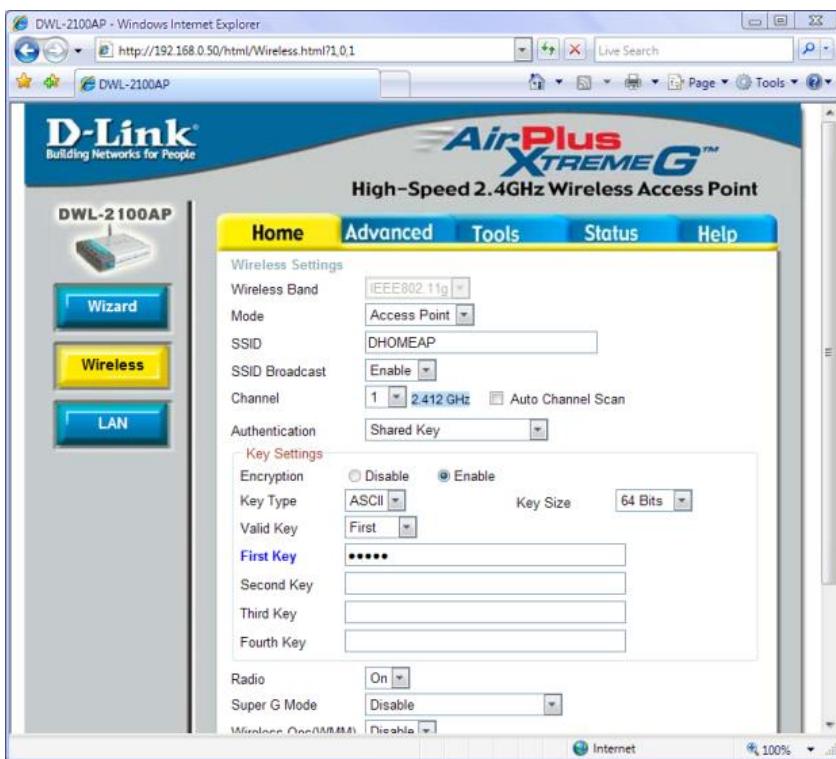


Рис. 9.5.

2. Так как аутентификация с общим ключом предполагает еще и шифрование данных по *WEP*, то в поле Encryption (Шифрование) активно будет только Enable.

3. Выбираем тип ключа (Key Type) и размер ключа (Key Size).

4. Вводим несколько ключей, последовательно выбирая в поле Valid Key (Действующий ключ). При 64-битном ключе с типом ключа ASCII нужно ввести пятизначную последовательность, например pass1.

Теперь, после применения настроек, на клиентской стороне надо выставить те же самые параметры и подключиться к ней.

Уязвимость механизмов аутентификации 802.11

Проблемы идентификатора беспроводной ЛВС

Идентификатор *SSID* регулярно передается точками радиодоступа в специальных фреймах Beacon. Несмотря на то, что эти фреймы играют чисто информационную роль в радиосети, т. е. совершенно "прозрачны" для абонента, сторонний наблюдатель в состоянии с легкостью определить *SSID* с помощью анализатора трафика протокола 802.11, например *Sniffer Pro Wireless*. Некоторые точки радиодоступа, в том числе D-Link, позволяют административно запретить широковещательную передачу *SSID* внутри фреймов Beacon. Однако и в этом случае *SSID* можно легко определить путем захвата фреймов *Probe Response*, посыпаемых точками радиодоступа. Идентификатор *SSID* не разрабатывался для использования в качестве механизма обеспечения безопасности. Вдобавок к этому отключение широковещательной передачи *SSID* точками радиодоступа может отразиться на совместимости оборудования беспроводных сетей различных производителей при использовании в одной радиосети.

Уязвимость открытой аутентификации

Открытая аутентификация не позволяет точке радиодоступа определить, является абонент легитимным или нет. Это становится заметной брешью в системе безопасности в том случае, если в беспроводной локальной сети не используется шифрование *WEP*.

D-Link не рекомендует эксплуатацию беспроводных сетей без шифрования *WEP*. В тех случаях, когда использование шифрования *WEP* не требуется или невозможно (например, в беспроводных локальных сетях публичного доступа), методы аутентификации более высокого уровня могут быть реализованы посредством Internet-шлюзов.

Уязвимость аутентификации с общим ключом

Аутентификация с общим ключом требует настройки у абонента статического *WEP*-ключа для шифрования *Challenge Text*, отправленного точкой радиодоступа. Точка радиодоступа аутентифицирует абонента посредством дешифрации его ответа на *Challenge* и сравнения его с отправленным оригиналом. Обмен фреймами, содержащими *Challenge Text*, происходит по открытому радиоканалу, а значит, подвержен атакам со стороны наблюдателя (*Man in the middle Attack*). Наблюдатель может принять как нешифрованный *Challenge Text*, так и тот же *Challenge Text*, но уже в шифрованном виде (рис. 9.6). Шифрование *WEP* производится путем выполнения побитовой операции XOR над текстом сообщения и ключевой последовательностью, в результате чего получается зашифрованное сообщение (*Cipher-Text*). Важно понимать, что в результате выполнения побитовой операции XOR над зашифрованным сообщением и ключевой последовательностью мы имеем текст исходного сообщения. Таким образом, наблюдатель может легко вычислить сегмент ключевой последовательности путем анализа фреймов в процессе аутентификации абонента.

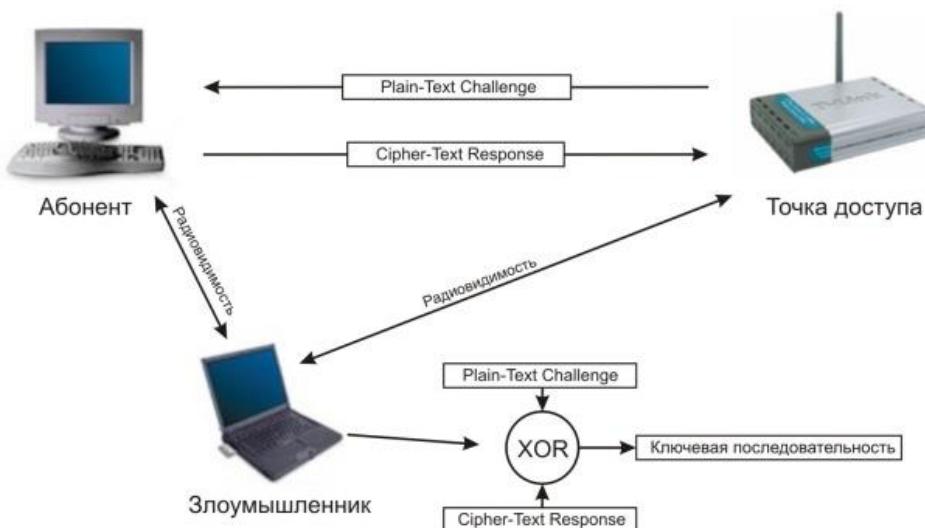


Рис. 9.6. Уязвимость аутентификации с общим ключом

Уязвимость аутентификации по MAC-адресу

Стандарт *IEEE 802.11* требует передачи MAC-адресов абонента и точки радиодоступа в открытом виде. В результате в беспроводной сети, использующей аутентификацию по MAC-адресу, злоумышленник может обмануть метод аутентификации путем подмены своего MAC-адреса легитимным. Подмена MAC-адреса возможна в беспроводных адаптерах, допускающих использование локально администрируемых MAC-адресов. Злоумышленник может воспользоваться анализатором трафика протокола *IEEE 802.11* для выявления MAC-адресов легитимных абонентов.

Спецификация WPA

До мая 2001 г. стандартизация средств информационной безопасности для беспроводных сетей *802.11* относилась к ведению рабочей группы *IEEE 802.11e*, но затем эта проблематика была выделена в самостоятельное подразделение. Разработанный стандарт *802.11i* призван расширить возможности протокола *802.11*, предусматривая средства шифрования передаваемых данных, а также централизованной аутентификации пользователей и рабочих станций.

Основные производители Wi-Fi оборудования в лице организации *WECA (Wireless Ethernet Compatibility Alliance)*, иначе именуемой *Wi-Fi Alliance*, устав ждать ратификации стандарта *IEEE 802.11i*, совместно с *IEEE* в ноябре 2002 г. анонсировали спецификацию *Wi-Fi Protected Access (WPA)*, соответствие которой обеспечивает совместимость оборудования различных производителей.

Новый стандарт безопасности *WPA* обеспечивает уровень безопасности куда больший, чем может предложить *WEP*. Он перебрасывает мостик между стандартами *WEP* и *802.11i* и имеет немаловажное преимущество, которое заключается в том, что микропрограммное обеспечение более старого оборудования может быть заменено без внесения аппаратных изменений.

IEEE предложила временный протокол целостности ключа (*Temporal Key Integrity Protocol, TKIP*).

Основные усовершенствования, внесенные протоколом *TKIP*:

- *Пофреймовое изменение ключей шифрования.* *WEP*-ключ быстро изменяется, и для каждого фрейма он другой;
- *Контроль целостности сообщения.* Обеспечивается эффективный контроль целостности фреймов данных с целью предотвращения скрытых манипуляций с фреймами и воспроизведения фреймов;
- *Усовершенствованный механизм управления ключами.*
-

Пофреймовое изменение ключей шифрования

Атаки, применяемые в *WEP*, использующие уязвимость слабых IV (*Initialization Vectors*), 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). 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.

На рис. 9.7 представлен образец 48-разрядного IV и показано, как он разбивается на части для использования при пофреймовом изменении ключа.



Рис. 9.7. Разбиение 48-разрядного IV

Процесс пофреймового изменения ключа можно разбить на следующие этапы (рис. 9.8):

1. Базовый *WEP*-ключ 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*. Этот процесс позволяет занести ключ 1-й фазы в кэш и также напрямую поместить в ключ.
2. Ключ 1-й фазы снова перемешивается с IV и MAC-адресом передатчика 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 (в стандартном 24-битовом IV) представляют собой фиксированное значение, используемое как заполнитель.
4. Пофреймовый ключ применяется 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.
6. Значение пофреймового ключа вычисляется заново, как на этапе 2.

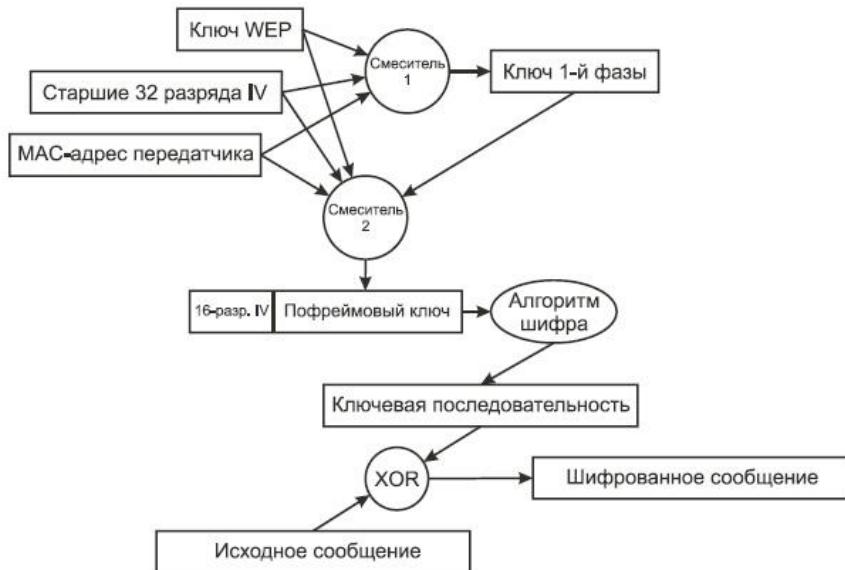


Рис. 9.8. Процесс создания шифрованного сообщения в WPA

Процесс пофреймового изменения ключа можно разбить на следующие этапы.

Устройство инициализирует IV, присваивая ему значение 0. В двоичном представлении это будет значение 00000000000000000000000000000000 000000000000000000000000.

Первые 32 разряда IV (в рассматриваемом случае - первые 32 нуля) перемешиваются с WEP-ключом (например, 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. 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) и т. д.

Этот алгоритм усиливает WEP до такой степени, что почти все известные сейчас возможности атак устраниются без замены существующего оборудования. Следует отметить, что этот алгоритм (и TKIP в целом) разработан с целью устраниить уязвимые места в системе аутентификации WEP и стандарта 802.11. Он жертвует слабыми алгоритмами, вместо того чтобы заменять оборудование.

Контроль целостности сообщения

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 манипуляции битами. 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 шифрования фреймов данных. Этот **уникальный ключ** перемешивается с назначенным MAC-адресом и исходным MAC-адресом фрейма, а также со всей незашифрованной частью фрейма. На [рис. 9.9](#) показана работа алгоритма Michael MIC.



Рис. 9.9. Работа алгоритма Michael MIC

Механизм шифрования *TKIP* в целом осуществляется следующим образом:

1. С помощью алгоритма пофреймового назначения ключей генерируется пофреймовый ключ (рис. 9.10).
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.
- 6.



Рис. 9.10. Механизм шифрования TKIP

Аналогично процессу шифрования по алгоритму *TKIP*, процесс дешифрования по этому алгоритму выполняется следующим образом (рис. 9.11):

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, 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*.

10.

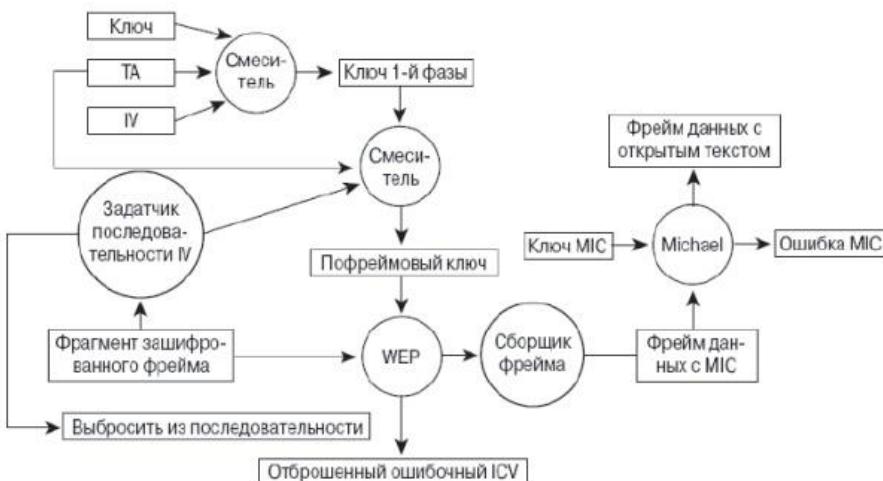


Рис. 9.11. Механизм дешифровки TKIP

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. Клиент запрашивает новый ключ.

WPA может работать в двух режимах: *Enterprise* (корпоративный) и *Pre-Shared Key* (персональный).

В первом случае хранение базы данных и проверка *аутентичности* по стандарту 802.1x в больших сетях обычно осуществляются специальным сервером, чаще всего RADIUS (Remote Authentication Dial-In User Service). *Enterprise*-режим мы рассмотрим далее.

Во втором случае подразумевается применение *WPA* всеми категориями пользователей беспроводных сетей, т.е. имеет место упрощенный режим, не требующий сложных механизмов. Этот режим называется *WPA-PSK* и предполагает введение одного пароля на каждый узел беспроводной сети (точку доступа, беспроводной маршрутизатор, клиентский адаптер, мост). До тех пор, пока пароли совпадают, клиенту будет разрешен доступ в сеть. Можно заметить, что подход с использованием пароля делает *WPA-PSK* уязвимым для атаки методом подбора, однако этот режим избавляет от путаницы с ключами *WEP*, заменяя их целостной и четкой системой на основе цифро-буквенного пароля.

Таким образом, *WPA/TKIP* - это решение, предоставляющее больший по сравнению с *WEP* уровень безопасности, направленное на устранение слабостей предшественника и обеспечивающее совместимость с более старым оборудованием сетей 802.11 без внесения аппаратных изменений в устройства.

Рассмотрение пофреймового назначения ключей и *MIC* касалось в основном ключа шифрования и ключа *MIC*. Но ничего не было сказано о том, как ключи генерируются и пересылаются от клиента к точке доступа и наоборот. В разделе, посвященном *Enterprise*-режиму мы рассмотрим предлагаемый стандартом 802.11i механизм управления ключами.

Стандарт сети 802.11i с повышенной безопасностью (WPA2)

В июне 2004 г. IEEEratифицировал давно ожидаемый стандарт обеспечения безопасности в беспроводных локальных сетях - 802.11i.

Действительно, *WPA* достоин восхищения как шедевр ретроинжиниринга. Созданный с учетом слабых мест *WEP*, он представляет собой очень надежную систему безопасности и, как правило, обратно совместим с существующим Wi-Fi-оборудованием. *WPA* - практическое решение, обеспечивающее достаточный уровень безопасности для беспроводных сетей.

Однако *WPA* - компромиссное решение. Оно все еще основано на алгоритме шифрования *RC4* и протоколе *TKIP*. Вероятность выявления каких-либо слабых мест хотя и мала, но все же существует.

Абсолютно новая система безопасности, лишенная недостатков *WEP*, представляет собой лучшее долгосрочное и к тому же расширяемое решение для безопасности беспроводных сетей. С этой целью комитет по стандартам принял решение разработать систему безопасности с нуля. Это новый стандарт *802.11i*, также известный как *WPA2* и выпущенный тем же *Wi-Fi Alliance*.

Стандарт *802.11i* использует концепцию повышенной безопасности (*Robust Security Network - RSN*), предусматривающую, что беспроводные устройства должны обеспечивать дополнительные возможности. Это потребует изменений в аппаратной части и программном обеспечении, т.е. сеть, полностью соответствующая *RSN*, станет несовместимой с существующим оборудованием *WEP*. В переходный период будет поддерживаться как оборудование *RSN*, так и *WEP* (на самом деле *WPA/TKIP* было решением, направленным на сохранение инвестиций в оборудование), но в дальнейшем устройства *WEP* начнут отмирать.

802.11i приложим к различным сетевым реализациям и может действовать *TKIP*, но по умолчанию *RSN* использует *AES* (Advanced Encryption Standard) и *CCMP* (Counter Mode CBC MAC Protocol) и, таким образом, является более мощным расширяемым решением.

В концепции *RSN* применяется *AES* в качестве системы шифрования, подобно тому как алгоритм *RC4* задействован в *WPA*. Однако механизм шифрования куда более сложен и не страдает от проблем, свойственных *WEP AES* - блочный шифр, оперирующий блоками данных по 128 бит. *CCMP*, в свою очередь, - протокол безопасности, используемый *AES*. Он является эквивалентом *TKIP* в *WPA*. *CCMP* вычисляет *MIC*, прибегая к хорошо известному и проверенному методу *Cipher Block Chaining Message Authentication Code (CBC-MAC)*. Изменение даже одного бита в сообщении приводит к совершенно другому результату.

Одной из слабых сторон *WEP* было управление секретными ключами. Многие администраторы больших сетей находили его неудобным. Ключи *WEP* не менялись длительное время (или никогда), что облегчало задачу злоумышленникам.

RSN определяет иерархию ключей с ограниченным сроком действия, сходную с *TKIP* в *AES/CCMP*, чтобы вместить все ключи, требуется 512 бит - меньше, чем в *TKIP*. В обоих случаях мастер-ключи используются не прямо, а для вывода других ключей. К счастью, администратор должен обеспечить единственный мастер-ключ. Сообщения составляются из 128-битного блока данных, зашифрованного секретным ключом такой же длины (128 бит). Хотя процесс шифрования сложен, администратор опять-таки не должен вникать в нюансы вычислений. Конечным результатом является шифр, который гораздо сложнее, чем даже *WPA*.

802.11i (WPA2) - это наиболее устойчивое, расширяемое и безопасное решение, предназначенное в первую очередь для крупных предприятий, где управление ключами и администрирование доставляет множество хлопот.

Стандарт *802.11i* разработан на базе проверенных технологий. *Механизмы безопасности* были спроектированы с нуля в тесном сотрудничестве с лучшими специалистами по криптографии и имеют все шансы стать тем решением, которое необходимо беспроводным сетям. Хотя ни одна система безопасности от взлома не застрахована, *802.11i* - это решение, на которое можно полагаться, в нем нет недостатков предыдущих систем. И, конечно, *WPA* пригоден для адаптации уже существующего оборудования, и только когда его ресурсы будут окончательно исчерпаны, вы сможете заменить его новым, полностью соответствующим концепции *RSN*.

Производительность канала связи, как свидетельствуют результаты тестирования оборудования различных производителей, падает на 5-20% при включении как *WEP*, так и *WPA*. Однако испытания того оборудования, в котором включено шифрование *AES* вместо *TKIP*, не показали сколько-нибудь заметного падения скорости. Это позволяет надеяться, что *WPA2*-совместимое оборудование предоставит нам долгожданный надежно защищенный канал без потерь в производительности.

WPA2, как и *WPA*, может работать в двух режимах: *Enterprise* (корпоративный) и *Pre-Shared Key* (персональный).

Пример 2.2

Настроим точку доступа с применением персональной спецификации *WPA2-PSK*.

1. Для этого подключаемся к точке доступа по проводному интерфейсу, вводим режим, *SSID*, канал, как было описано в примере 1.4. Далее в поле *Authentication* (Аутентификация) ставим *WPA2-PSK* (рис. 9.12).

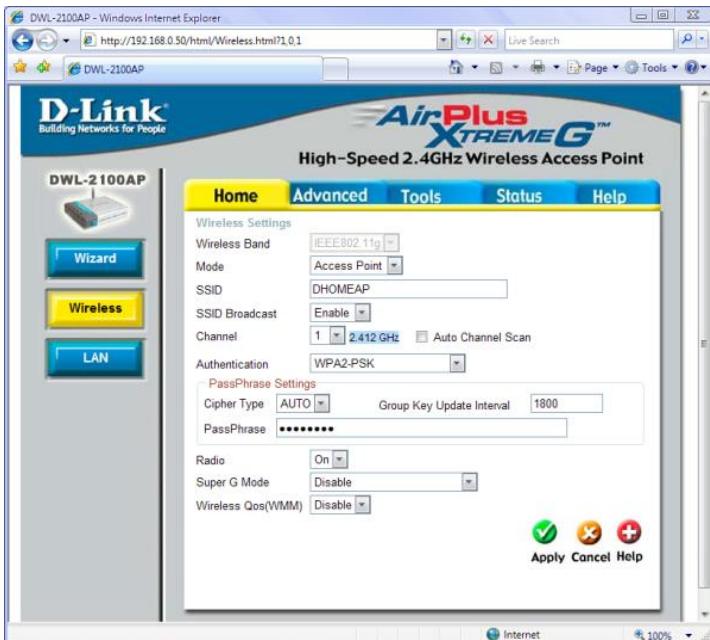


Рис. 9.12.

2. Выбираем тип шифрования (*Cipher Type*). Возможные варианты: AUTO, TKIP, AES. Если выставлено AUTO, точка доступа будет подстраивать тип шифрования под первого подключившегося клиента.

3. Выставляем интервал обновления группового ключа (Group Key Update Interval), который задается в секундах.

4. Вводим в поле PassPhrase ключ любой длины, но не менее 8 символов, например *secretpass*.

Теперь, после применения настроек, на клиентской стороне надо выставить те же самые параметры и подключиться к ней.

Стандарт 802.1x/EAP (Enterprise-режим)

Проблемы, с которыми столкнулись разработчики и пользователи сетей на основе стандарта 802.11, вынудили искать новые решения защиты беспроводных сетей. Были выявлены компоненты, влияющие на системы безопасности беспроводной локальной сети:

1. Архитектура аутентификации.
2. Механизм аутентификации.
3. Механизм обеспечения конфиденциальности и целостности данных.

Архитектура аутентификации IEEE 802.1x - стандарт IEEE 802.1x описывает единую архитектуру контроля доступа к портам с использованием разнообразных методов аутентификации абонентов.

Алгоритм аутентификации Extensible Authentication Protocol или EAP (расширяемый протокол идентификации) поддерживает централизованную аутентификацию элементов инфраструктуры беспроводной сети и ее пользователей с возможностью динамической генерации ключей шифрования.

Архитектура IEEE 802.1x

Архитектура IEEE 802.1x включает в себя следующие обязательные логические элементы (рис. 9.13):

- Клиент (Supplicant) - находится в операционной системе абонента;
- Аутентификатор (Authenticator) - находится в программном обеспечении точки радиодоступа;
- Сервер аутентификации (Authentication Server) - находится на RADIUS-сервере.

IEEE 802.1x предоставляет абоненту беспроводной локальной сети лишь средства передачи атрибутов серверу аутентификации и допускает использование различных методов и алгоритмов аутентификации. Задачей сервера аутентификации является поддержка разрешенных политикой сетевой безопасности методов аутентификации.

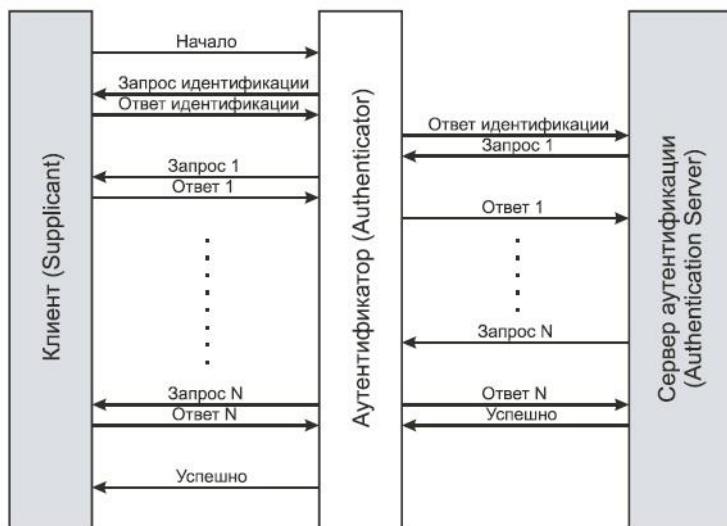


Рис. 9.13. Архитектура IEEE 802.1x

Аутентификатор, находясь в точке радиодоступа, создает логический порт для каждого клиента на основе его идентификатора ассоциирования. Логический порт имеет два канала для обмена данными. Неконтролируемый канал беспрепятственно пропускает трафик из беспроводного сегмента в проводной и обратно, в то время как контролируемый канал требует успешной аутентификации для прохождения фреймов.

Таким образом, в терминологии стандарта 802.1x точка доступа играет роль коммутатора в проводных сетях Ethernet. Очевидно, что проводной сегмент сети, к которому подключена точка доступа, нуждается в сервере аутентификации. Его функции обычно выполняет RADIUS-сервер, интегрированный с той или иной базой данных пользователей, в качестве которой может выступать стандартный RADIUS, LDAP, NDS или Windows Active Directory. Коммерческие беспроводные шлюзы высокого класса могут реализовывать как функции сервера аутентификации, так и аутентификатора.

Клиент активизируется и ассоциируется с точкой радиодоступа (или физически подключается к сегменту в случае проводной локальной сети). Аутентификатор распознает факт подключения и активизирует логический порт для клиента, сразу переводя его в состояние "неавторизован". В результате через клиентский порт возможен лишь обмен трафиком протокола IEEE 802.1x, для всего остального трафика порт заблокирован. Клиент также может (но не обязан) отправить сообщение EAP Start (начало аутентификации EAP) (рис. 9.14) для запуска процесса аутентификации.

Аутентификатор отправляет сообщение EAP Request Identity (запрос имени EAP) и ожидает от клиента его имя (Identity). Ответное сообщение клиента EAP Response (ответ EAP), содержащее атрибуты, перенаправляется серверу аутентификации.

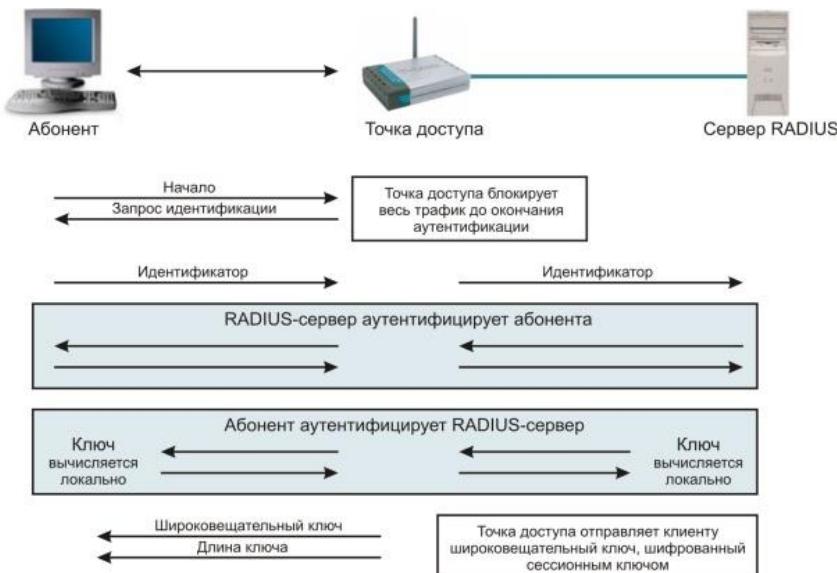


Рис. 9.14. Обмен сообщениями в 802.1x/EAP

После завершения аутентификации сервер отправляет сообщение RADIUS-ACCEPT (принять) или RADIUS-REJECT (отклонить) аутентификатору. При получении сообщения RADIUS-ACCEPT аутентификатор переводит порт клиента в состояние "авторизован", и начинается передача всего трафика абонента.

Механизм аутентификации

Первоначально стандарт 802.1x задумывался для того, чтобы обеспечить аутентификацию пользователей на канальном уровне в коммутируемых проводных сетях.

Алгоритмы аутентификации стандарта 802.11 могут обеспечить 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 WPA для получения всех ключей используется так называемый *мастер-ключ* (Master Key). На рис. 9.15 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 посыпает клиенту секретное случайное число, которое называется *временный аутентификатор* (Authenticator Nonce - ANonce), используя для этого сообщение EAPoL-Key стандарта 802.1x.
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 "выстроит" MAC-адреса одинаковым образом (рис. 9.16).
5. Это комбинированное значение пропускается через псевдослучайную функцию (Pseudo Random Function - PRF), чтобы получить 512-разрядный PTK.
6. Клиент посыпает число SNonce, сгенерированное им на этапе 3, точке доступа с помощью сообщения EAPoL-Key стандарта 802.1x, защищенного 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 посыпает 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 посыпает сообщение EAPoL-Key, защищенное ключом EAPoL-Key MIC, указывающее, что ключи установлены.

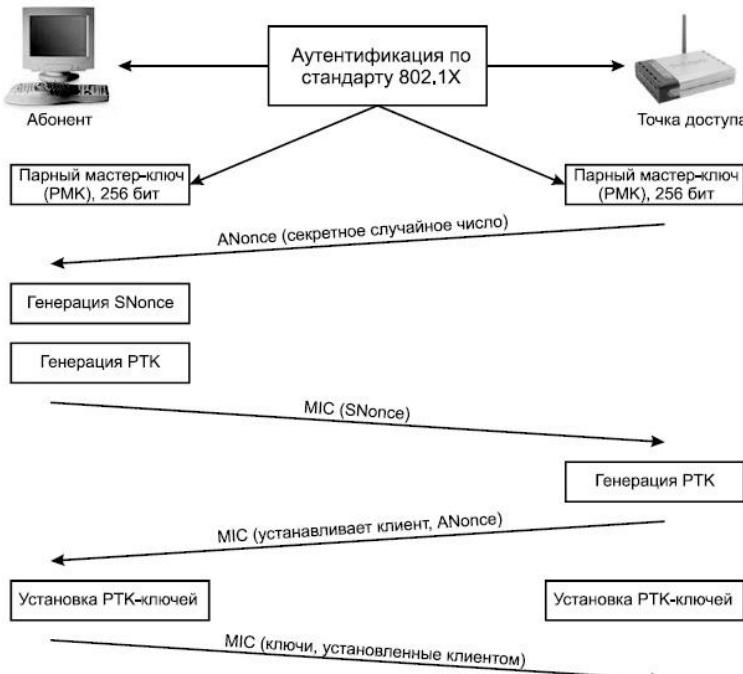


Рис. 9.15. Создание ключей

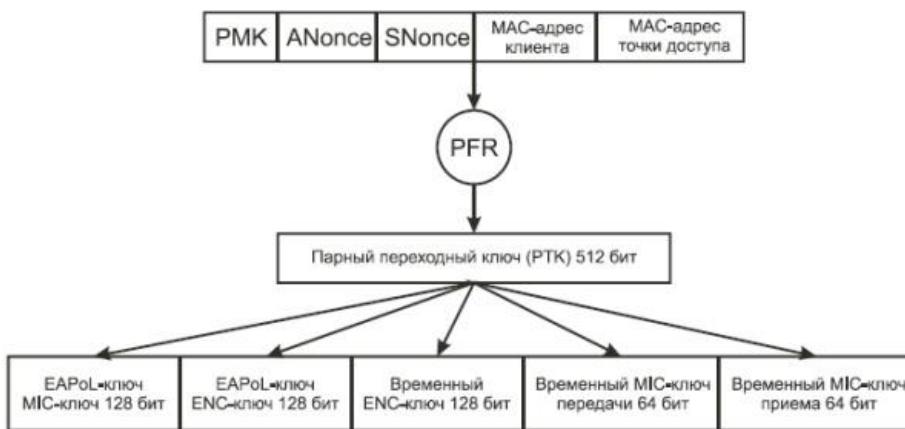


Рис. 9.16. Генерация парного переходного ключа

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

Широковещательные или многоадресные фреймы используют иерархию групповых ключей. Групповой мастер-ключ (Group Master Key - GMK) находится на вершине этой иерархии и выводится в точке доступа. 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. 9.17 представлена иерархия групповых ключей.



Рис. 9.17. 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/многоадресных фреймов, 64-разрядный ключ передачи *MIC* (transmit *MIC* key) и 64-разрядный ключ приема *MIC* (*MIC receive key*).

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

Клиент обновляется с помощью групповых ключей шифрования через сообщения EAPoL-Key. Точка доступа посыпает такому клиенту сообщение EAPoL, зашифрованное с помощью одноадресного 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.

В домашних сетях или сетях, предназначенных для малых офисов, развертывание RADIUS-сервера с базой данных конечных пользователей маловероятно. В таком случае для генерирования сеансовых ключей используется только предварительно разделенный PMK (вводится вручную). Это аналогично тому, что делается в оригинальном протоколе *WEP*.

Поскольку в локальных сетях 802.11 нет физических портов, ассоциация между беспроводным клиентским устройством и точкой доступа считается сетевым портом доступа. Беспроводный клиент рассматривается как претендент, а точка доступа - как *аутентификатор*.

В стандарте 802.1x аутентификация пользователей на канальном уровне выполняется по протоколу *EAP*, который был разработан Группой по проблемам проектирования Internet (IETF). Протокол *EAP* - это замена протокола CHAP (*Challenge Handshake Authentication Protocol* - протокол взаимной аутентификации), который применяется в PPP (*Point to Point Protocol* - протокол соединения "точка-точка"), он предназначен для использования в локальных сетях. Спецификация EAPOL определяет, как фреймы EAP инкапсулируются во фреймы 802.3, 802.5 и 802.11. Обмен фреймами между объектами, определенными в стандарте 802.1x, схематично изображен на рис. 9.18.

EAP является "обобщенным" протоколом в системе аутентификации, авторизации и учета (Authentication, Authorization, and Accounting - AAA), обеспечивающим работу разнообразных методов аутентификации. AAA-клиент (сервер доступа в терминологии AAA, в беспроводной сети представлен точкой радиодоступа), поддерживающий *EAP*, может не понимать конкретных методов, используемых абонентом и сетью в процессе аутентификации. Сервер доступа туннелирует сообщения протокола аутентификации, циркулирующие между абонентом и сервером аутентификации. Сервер доступа интересует лишь факт начала и окончания процесса аутентификации.

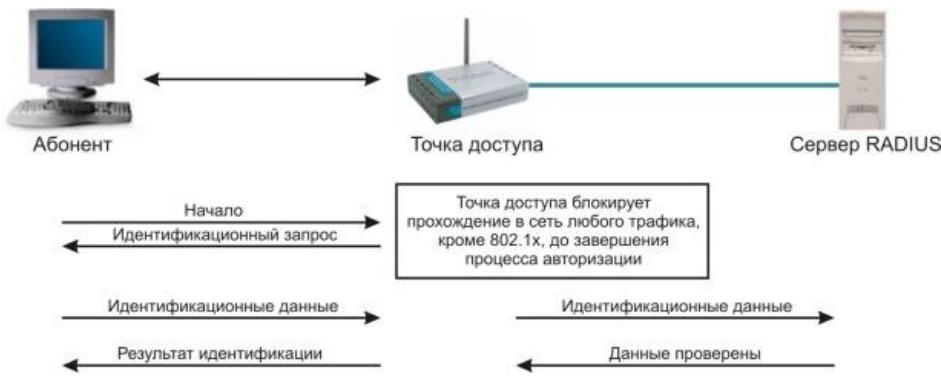


Рис. 9.18. Механизм аутентификации в 802.1x/EAP

Есть несколько вариантов EAP, спроектированных с участием различных компаний-производителей. Такое разнообразие вносит дополнительные проблемы совместимости, так что выбор подходящего оборудования и программного обеспечения для беспроводной сети становится нетривиальной задачей. При конфигурировании способа аутентификации пользователей в беспроводной сети вам, вероятно, придется столкнуться со следующими вариантами EAP:

- *EAP-MD5* - это обязательный уровень EAP, который должен присутствовать во всех реализациях стандарта 802.1x, именно он был разработан первым. С точки зрения работы он дублирует протокол CHAP. Мы не рекомендуем пользоваться протоколом *EAP-MD5* по трем причинам. Во-первых, он не поддерживает динамическое распределение ключей. Во-вторых, он уязвим для атаки "человек посередине" с применением фальшивой точки доступа и для атаки на сервер аутентификации, так как аутентифицируются только клиенты. И наконец, в ходе аутентификации противник может подслушать запрос и зашифрованный ответ, после чего предпринять атаку с известным открытым или шифрованным текстом;
- *EAP-TLS* (*EAP-Transport Layer Security* - протокол защиты транспортного уровня) поддерживает взаимную аутентификацию на базе сертификатов. *EAP-TLS* основан на протоколе SSLv3 и требует наличия удостоверяющего центра. Протоколы TLS и SSL используют ряд элементов инфраструктуры PKI (Public Key Infrastructure): Абонент должен иметь действующий сертификат для аутентификации по отношению к сети. AAA-сервер должен иметь действующий сертификат для аутентификации по отношению к абоненту. Орган сертификации с сопутствующей инфраструктурой управляет сертификатами субъектов PKI. Клиент и RADIUS-сервер должны поддерживать метод аутентификации *EAP-TLS*. Точка радиодоступа должна поддерживать процесс аутентификации в рамках 802.1x/EAP, хотя может и не знать деталей конкретного метода аутентификации. Общий вид *EAP-TLS* выглядит примерно так (рис. 9.19):

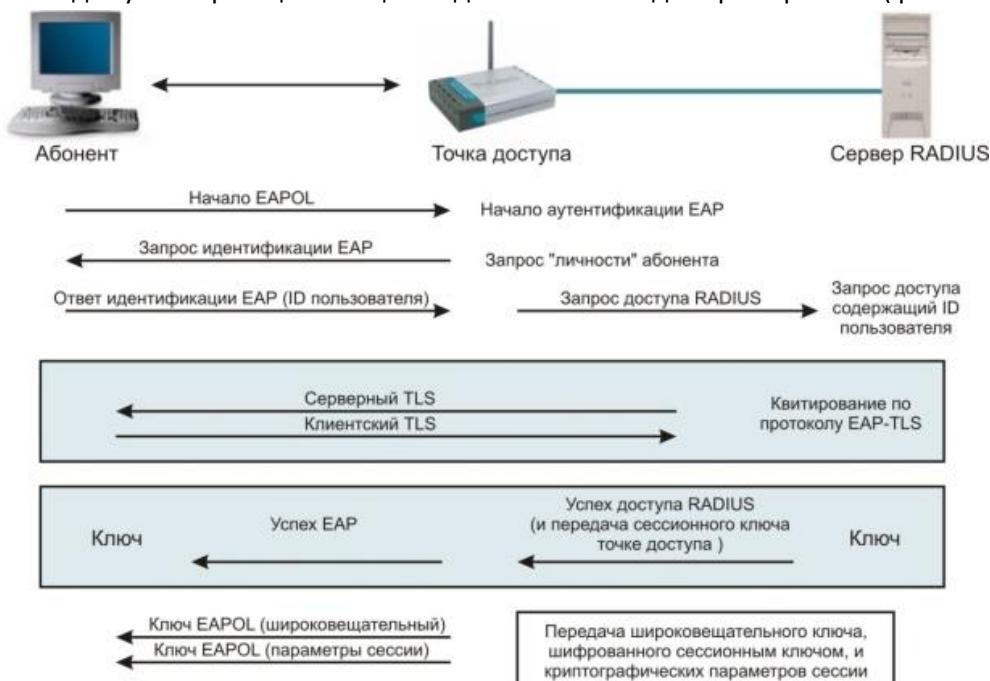


Рис. 9.19. Процесс аутентификации EAP-TLS

- *EAP-LEAP* (Lightweight EAP, облегченный EAP) - это запатентованный компанией Cisco вариант EAP, реализованный в точках доступа и беспроводных клиентских картах Cisco. LEAP был первой (и на протяжении длительного времени единственной) схемой аутентификации в стандарте 802.1x, основанной на паролях. Поэтому LEAP приобрел огромную популярность и даже поддержан в сервере Free-RADIUS, несмотря на то, что это запатентованное решение. Сервер аутентификации посыпает клиенту запрос, а тот должен вернуть пароль, предварительно выполнив его свертку со строкой запроса. Основанный на применении паролей, *EAP-LEAP* аутентифицирует пользователя, а не устройство. В то же время очевидна уязвимость этого варианта для атак методом полного перебора и по словарю, нехарактерная для методов аутентификации с применением сертификатов.
- *PEAP* (Protected EAP - защищенный EAP) и *EAP-TTLS* (Tunneled Transport Layer Security EAP, протокол защиты транспортного уровня EAP), разработанный компанией Certicom and Funk Software. Эти варианты также достаточно развиты, и поддерживаются производителями, в частности D-link. Для работы *EAP-TTLS* требуется, чтобы был сертифицирован только сервер аутентификации, а у претендента сертификата может и не быть, так что процедура развертывания упрощается. *EAP-TTLS* поддерживает также ряд устаревших методов аутентификации, в том числе PAP, CHAP, MS-CHAP, MS-CHAPv2 и даже *EAP-MD5*. Чтобы обеспечить безопасность при использовании этих методов, *EAP-TTLS* создает зашифрованный по протоколу TLS туннель, внутри которого эти протоколы и работают. Примером практической реализации *EAP-TTLS* может служить программное обеспечение для управления доступом в беспроводную сеть *Odyssey* от компании Funk Software. Протокол *PEAP* очень похож на *EAP-TTLS*, только он не поддерживает устаревших методов аутентификации типа PAP и CHAP. Вместо них поддерживаются протоколы *PEAP-MS-CHAPv2* и *PEAP-EAP-TLS*, работающие внутри безопасного туннеля. Поддержка *PEAP* реализована в пакете программ точек доступа D-link и успешно реализована в Windows XP, начиная с Service Pack 2. В общем виде схема обмена *PEAP* выглядит следующим образом (рис. 9.20):

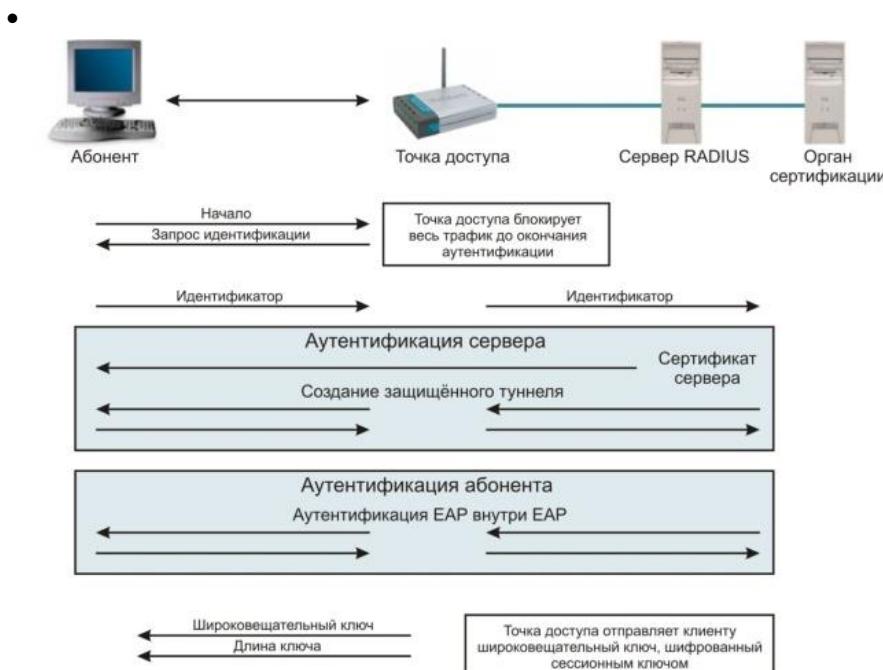


Рис. 9.20. Процесс аутентификации PEAP

- Еще два варианта EAP - это *EAP-SIM* и *EAP-AKA* для аутентификации на базе SIM и USIM. В настоящий момент оба имеют статус предварительных документов IETF и в основном предназначены для аутентификации в сетях GSM, а не в беспроводных сетях 802.11. Тем не менее протокол *EAP-SIM* поддержан в точках доступа и клиентских устройствах некоторых производителей.

Наглядно уровни архитектуры 802.1x показаны на рис. 9.21. Здесь в качестве механизма обеспечения конфиденциальности и целостности данных выступают стандарты шифрования *WPA* и *WPA2*.

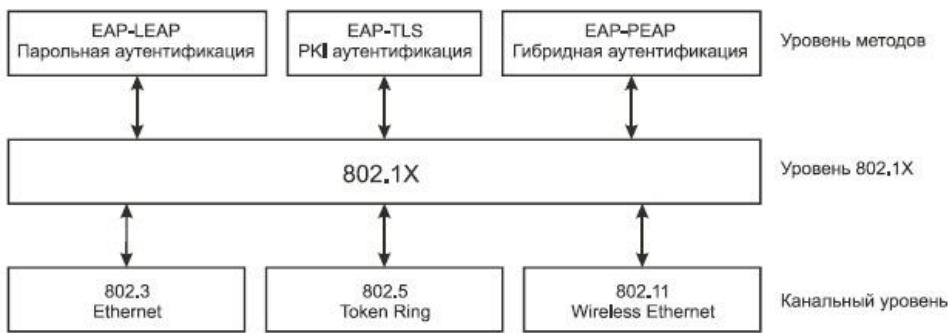


Рис. 9.21. Уровни архитектуры 802.1x

Технологии целостности и конфиденциальности передаваемых данных

Разворачивание беспроводных виртуальных сетей

Виртуальная частная сеть (*Virtual Private Network - VPN*) - это метод, позволяющий воспользоваться общедоступной телекоммуникационной инфраструктурой, например *Internet*, для предоставления удаленным офисам или отдельным пользователям безопасного доступа к сети организации. Поскольку беспроводные сети 802.11 работают в нелицензируемом диапазоне частот и доступны для прослушивания, именно в них *развертывание* и обслуживание *VPN* приобретает особую важность, если необходимо обеспечить высокий уровень защиты информации.

Защищать нужно как соединения между хостами в беспроводной локальной сети, так и двухточечные каналы между беспроводными мостами. Для обеспечения безопасности особо секретных данных нельзя полагаться на какой-то один механизм или на защиту лишь одного уровня сети. В случае двухточечных каналов проще и экономичнее развернуть *VPN*, покрывающую две сети, чем реализовывать защиту на базе стандарта 802.11i, включающую RADIUS-сервер и базу данных о пользователях.

Пользоваться же реализацией стандарта на базе предварительно разделенных ключей (*PSK*) и протокола 802.1x при наличии *высокоскоростного канала* между сетями - не самый *безопасный метод*. *VPN* - это полная противоположность дорогостоящей системе собственных или арендованных линий, которые могут использоваться только одной организацией. Задача *VPN* - предоставить организации те же возможности, но за гораздо меньшие деньги. Сравните это с обеспечением связи за счет двухточечных беспроводных каналов с мостами вместо дорогих выделенных линий.

VPN и беспроводные технологии не конкурируют, а дополняют друг друга. *VPN* работает поверх разделяемых сетей общего пользования, обеспечивая в то же время *конфиденциальность* за счет специальных мер безопасности и применения туннельных протоколов, таких как туннельный протокол на канальном уровне (*Layer Two Tunneling Protocol - L2TP*). Смысл их в том, что, осуществляя *шифрование данных* на отправляющем конце и *десифрирование* на принимающем, протокол организует "туннель", в который не могут проникнуть данные, не зашифрованные должным образом. Дополнительную *безопасность* может обеспечить *шифрование* не только самих данных, но и сетевых адресов отправителя и получателя. Беспроводную локальную сеть можно сравнить с разделяемой сетью общего пользования, а в некоторых случаях (хот-споты, узлы, принадлежащие сообществам) она таковой и является.

VPN отвечает трем условиям: *конфиденциальность*, *целостность* и *доступность*. Следует отметить, что никакая *VPN* не является устойчивой к *DoS*- или *DDoS*-атакам и не может гарантировать доступность на физическом уровне просто в силу своей виртуальной природы и зависимости от нижележащих протоколов.

Две наиболее важные особенности *VPN*, особенно в беспроводных средах, где имеется лишь ограниченный контроль над распространением сигнала, - это *целостность* и, что еще более существенно, *конфиденциальность* данных. Возьмем жизненную ситуацию, когда злоумышленнику удалось преодолеть *шифрование* по протоколу *WEP* и присоединиться к беспроводной локальной сети. Если *VPN* отсутствует, то он сможет прослушивать данные и вмешиваться в работу сети. Но если пакеты аутентифицированы, атака "человек посередине" становится практически невозможной, хотя *перехватить данные* по-прежнему легко. Включение в *VPN* элемента *шифрования* уменьшает негативные

последствия перехвата данных. VPN обеспечивает не столько полную изоляцию всех сетевых взаимодействий, сколько осуществление таких взаимодействий в более контролируемых условиях с четко определенными группами допущенных участников.

Есть много способов классификации VPN, но основные три вида - это "сеть-сеть", "хост-сеть" и "хост-хост".

Топология "сеть-сеть"

Этим термином иногда описывают VPN-туннель между двумя географически разнесенными частными сетями (рис. 10.1).



Рис. 10.1. Топология "сеть-сеть"

VPN такого типа обычно применяются, когда нужно объединить локальные сети с помощью сети общего пользования так, как будто они находятся внутри одного здания.

Основное достоинство такой конфигурации состоит в том, что сети выглядят как смежные, а работа VPN-шлюзов прозрачна для пользователей. В этом случае также важно туннелирование, поскольку в частных сетях обычно используются описанные в RFC 1918 зарезервированные адреса, которые не могут маршрутизироваться через Internet. Поэтому для успешного взаимодействия трафик необходимо инкапсулировать в туннель.

Типичным примером такой сети может быть соединение двух филиалов одной организации по двухточечному беспроводному каналу. Хотя трафик и не выходит за пределы внутренней инфраструктуры организации, к ее беспроводной части нужно относиться так же внимательно, как если бы трафик маршрутизировался через сеть общего пользования. Вы уже видели, что протокол WEP можно легко преодолеть и даже TKIP иногда уязвим, поэтому мы настоятельно рекомендуем всюду, где возможно, реализовывать дополнительное шифрование.

Топология "хост-сеть"

При такой конфигурации удаленные пользователи подключаются к корпоративной сети через Internet.

Сначала мобильный клиент устанавливает соединение с Internet, а затем инициирует запрос на организацию зашифрованного туннеля с корпоративным VPN-шлюзом. После успешной аутентификации создается туннель поверх сети общего пользования, и клиент становится просто еще одной машиной во внутренней сети. Все более широкое распространение надомной работы стимулирует интерес к такому применению VPN.

В отличие от VPN типа "сеть-сеть", где число участников невелико и более или менее предсказуемо, VPN типа "хост-сеть" легко может вырасти до необъятных размеров. Поэтому системный администратор должен заранее продумать масштабируемый механизм аутентификации клиентов и управления ключами.

Топология "хост-хост"

Такая топология, по-видимому, встречается реже всего. Речь идет о двух хостах, обменивающихся друг с другом шифрованными и нешифрованными данными. В такой конфигурации туннель организуется между двумя хостами и весь трафик между ними инкапсулируется внутри VPN. У таких сетей не много практических применений, но в качестве примера можно назвать географически удаленный сервер резервного хранения. Оба

хоста подключены к Internet, и данные с центрального сервера зеркально копируются на резервный. Например, простые сети VPN типа "хост-хост" можно использовать для защиты одноранговых (Ad Hoc) сетей.

Распространенные туннельные протоколы

Протокол IPSec

IPSec - это наиболее широко признанный, поддерживаемый и стандартизованный из всех протоколов VPN. Для обеспечения совместной работы он подходит лучше остальных. *IPSec* лежит в основе открытых стандартов, в которых описан целый набор безопасных протоколов, работающих поверх существующего стека IP. Он предоставляет службы аутентификации и шифрования данных на сетевом уровне (уровень 3) модели OSI и может быть реализован на любом устройстве, которое работает по протоколу IP. В отличие от многих других схем шифрования, которые защищают конкретный протокол верхнего уровня, *IPSec*, работающий на нижнем уровне, может защитить весь IP-трафик. Он применяется также в сочетании с туннельными протоколами на канальном уровне (уровень 2) для шифрования и аутентификации трафика, передаваемого по протоколам, отличным от IP.

Протокол *IPSec* состоит из трех основных частей:

- заголовка аутентификации (Authentication Header - AH);
- безопасно инкапсулированной полезной нагрузки (*Encapsulating Security Payload - ESP*);
- схемы обмена ключами через Internet (Internet Key Exchange - IKE).

Заголовок AH добавляется после заголовка IP и обеспечивает аутентификацию на уровне пакета и целостность данных. Иными словами, гарантируется, что пакет не был изменен на пути следования и поступил из ожидаемого источника. *ESP* обеспечивает конфиденциальность, аутентификацию источника данных, целостность, опциональную защиту от атаки повторного сеанса и до некоторой степени скрытность механизма управления потоком. Наконец, *IKE* обеспечивает согласование настроек служб безопасности между сторонами-участниками.

Протокол PPTP

Двухточечный туннельный протокол (Point-to-Point Tunneling Protocol - PPTP) - это запатентованная разработка компании Microsoft, он предназначен для организации взаимодействия по типу VPN. PPTP обеспечивает аутентификацию пользователей с помощью таких протоколов, как MS-CHAP, CHAP, SPAP и PAP. Этому протоколу недостает гибкости, присущей другим решениям, он не слишком хорошо приспособлен для совместной работы с другими протоколами VPN, зато прост и широко распространен во всем мире.

Протокол определяет следующие типы коммуникаций:

- PPTP-соединение, по которому клиент организует PPP-канал с провайдером;
- Управляющее PPTP-соединение, которое клиент организует с VPN-сервером и по которому согласует характеристики туннеля;
- PPTP-туннель, по которому клиент и сервер обмениваются зашифрованными данными.

Протокол PPTP обычно применяется для создания безопасных каналов связи между многими Windows-машинами в сети *Intranet*.

Протокол L2TP

Этот протокол, совместно разработанный компаниями Cisco, Microsoft и 3Com, обещает заменить PPTP в качестве основного туннельного протокола. По существу *L2TP* (Layer Two Tunneling Protocol, протокол туннелирования канального уровня) представляет собой комбинацию PPTP и созданного Cisco протокола Layer Two Forwarding (L2F). Протокол *L2TP* применяется для туннелирования PPP-трафика поверх IP-сети общего пользования. Для установления соединения по коммутируемой линии в нем используется PPP с аутентификацией по протоколу PAP или CHAP, но, в отличие от PPTP, *L2TP* определяет собственный туннельный протокол.

Поскольку *L2TP* работает на канальном уровне (уровень 2), через туннель можно пропускать и не-IP трафик. Вместе с тем *L2TP* совместим с любым канальным протоколом, например ATM, *Frame Relay* или 802.11.

Сам по себе протокол не содержит средств шифрования, но может быть использован в сочетании с другими протоколами или механизмами шифрования на прикладном уровне.

Системы обнаружения вторжения в беспроводные сети

Системы обнаружения вторжения (*Intrusion Detection System - IDS*) - это устройства, с помощью которых можно выявлять и своевременно предотвращать вторжения в вычислительные сети. Они делятся на два вида: на базе сети и на базе хоста.

Сетевые системы (*Network Intrusion Detection Systems - NIDS*) анализируют трафик с целью обнаружения известных атак на основании имеющихся у них наборов правил (экспертные системы). Исключение с точки зрения принципов анализа составляют системы на базе нейросетей и искусственного интеллекта. Подмножеством сетевых систем обнаружения вторжений являются системы для наблюдения только за одним узлом сети (*Network Node IDS*).

Другой вид систем обнаружения вторжений представляют системы на базе хоста (*Host Intrusion Detection Systems - HIDS*). Они устанавливаются непосредственно на узлах и осуществляют наблюдение за целостностью файловой системы, системных журналов и т. д.

NIDS делятся в свою очередь на две большие категории: на основе сигнатур и на основе базы знаний. Сигнатурные *IDS* наиболее распространены и проще реализуются, но их легко обойти и они не способны распознавать новые атаки. В таких системах события, происходящие в сети, сравниваются с признаками известных атак, которые и называются сигнатурами. Если инструмент взлома модифицировать с целью изменения какой-либо части сигнатур атаки, то скорее всего атака останется незамеченной. Кроме того, базы данных, содержащие сигнтуры, необходимо надежно защищать и часто обновлять. *IDS* на основе базы знаний следят за сетью, собирают статистику о ее поведении в нормальных условиях, обнаруживают различные особенности и помечают их как подозрительные. Поэтому такие *IDS* еще называют основанными на поведении или статистическими.

Простейшая архитектура *IDS* представлена на рис. 10.2.



Рис. 10.2. Основные элементы архитектуры систем обнаружения вторжений

Для эффективной работы статистической *IDS* необходимо иметь надежную информацию о том, как ведет себя сеть в нормальных условиях, - точку отсчета. Хотя такую *IDS* обмануть сложнее, но и у нее есть свои слабые места - ложные срабатывания и трудности при обнаружении некоторых видов коммуникаций по скрытому каналу. Ложные срабатывания особенно вероятны в беспроводных сетях из-за нестабильности передающей среды. Кроме того, атаки, проведенные на ранних стадиях периода фиксации точки отсчета, могут исказить процедуру обучения статистической *IDS*, поэтому ее развертывание в промышленной сети - занятие рискованное. Как быть, если нормальное поведение сети уже изменено взломщиком в момент развертывания?

Хорошая *IDS* для беспроводной сети должна быть одновременно сигнатурной и статистической. Некоторые инструменты для проведения атак на беспроводные сети имеют четко выраженные сигнатуры. Если они обнаруживаются в базе данных, то можно поднимать тревогу. С другой стороны, у многих атак очевидных сигнатур нет, зато они вызывают отклонения от нормальной работы сети на нижних уровнях стека протоколов. Отклонение может быть малозаметным, например несколько пришедших не по порядку фреймов, или бросающимся в глаза, скажем, выросшая в несколько раз нагрузка. Обнаружение таких аномалий - непростая задача, поскольку не существует двух одинаковых беспроводных сетей. То же относится и к проводным локальным сетям, но там хотя бы нет радиопомех, отражения, рефракции и рассеивания сигнала. Поэтому эффективное применение *IDS* в беспроводных сетях возможно только после длительного периода детального исследования сети. При развертывании системы необходимо четко понимать, что, как и зачем мы хотим анализировать, и постараться ответить на эти вопросы, чтобы сконструировать нужную нам систему *IDS* (рис. 10.3).



Рис. 10.3. Характеристики систем обнаружения вторжений

Только собрав значительный объем статистических данных о работе конкретной сети, можно решить, что является аномальным поведением, а что - нет, и идентифицировать проблемы со связью, ошибки пользователей и атаки. Многократные запросы на аутентификацию по протоколу 802.1x/*LEAP* могут свидетельствовать о попытке атаки методом полного перебора. Но это может объясняться и тем, что пользователь забыл свой пароль, или работой плохо написанного клиентского приложения, которое продолжает предпринимать попытки войти в сеть, пока не будет введен правильный пароль. Увеличение числа фреймов-маяков может быть признаком *DoS-атаки* или присутствия в сети фальшивой точки доступа, но не исключено, что все дело в неисправной или неправильно сконфигурированной законной точке доступа. События, фиксируемые *IDS* на верхних уровнях стека протоколов, например большое число фрагментированных пакетов или запросов *TCP SYN*, может указывать на сканирование портов или *DoS-атаку*, но, возможно, это просто результат плохой связи на физическом уровне (уровень 1).

1. События на физическом уровне:

- - наличие дополнительных передатчиков в зоне действия сети;
- - использование каналов, которые не должны быть задействованы в защищаемой сети;
- - перекрывающиеся каналы;
- - внезапное изменение рабочего канала одним или несколькими устройствами, за которыми ведется наблюдение;
- - ухудшение качества сигнала, высокий уровень шума или низкое значение *отношения "сигнал-шум"*.

Эти события могут свидетельствовать о наличии проблем со связью или с сетью, об ошибках, допущенных при конфигурировании сети, о появлении мошеннических устройств, о преднамеренном глушении либо об атаках "человек посередине" на уровень 1 или 2.

2. События, связанные с административными или управляющими фреймами:

- повышенная частота появления некоторых типов фреймов;
- фреймы необычного размера;
- фреймы неизвестных типов;
- неполные, испорченные или неправильно сформированные фреймы;
- поток фреймов с запросами на отсоединение и прекращение сеанса;

- частое появление фреймов с запросом на повторное присоединение в сетях, где не включен роуминг;
- фреймы с неправильными порядковыми номерами;
- частое появление пробных фреймов;
- фреймы, в которых *SSID* отличается от *SSID* данной сети;
- фреймы с широковещательным *SSID*;
- фреймы с часто изменяющимися или случайными *SSID*;
- фреймы со значениями в поле *SSID* или других полях, типичными для некоторых инструментов вторжения;
- фреймы с MAC-адресами, отсутствующими в списке контроля доступа;
- фреймы с дублирующимися MAC-адресами;
- фреймы с часто изменяющимися или случайными MAC-адресами.

Эти события могут указывать на неправильную конфигурацию сети, проблемы со связью, сильные помехи, попытки применения инструментов активного сканирования сети, подделку MAC-адресов, присутствие в сети посторонних клиентов, попытки угадать или подобрать методом полного перебора закрытый *SSID* или на более изощренные атаки "человек посередине" на уровень 2, связанные с манипуляцией управляющими или административными фреймами.

3. События, связанные с фреймами протоколов 802.1x/EAP:

- неполные, испорченные или неправильно сформированные фреймы протокола 802.1x;
- фреймы с такими типами протокола EAP, которые не реализованы в данной беспроводной сети;
- многократные фреймы запроса и ответа процедуры аутентификации EAP;
- многократные фреймы с извещением о неудачной аутентификации EAP;
- затопление фреймами начала и завершения сеанса EAP;
- фреймы EAP аномального размера;
- фреймы EAP с некорректным значением длины;
- фреймы EAP с неправильными "верительными грамотами";
- фреймы EAP, приходящие от неизвестных аутентификаторов (фальшивая точка доступа);
- незавершенная процедура аутентификации по протоколу 802.1x/EAP.

Эти события могут указывать на попытки прорваться через процедуру аутентификации, описанную в протоколе 802.1x, в том числе и путем размещения фальшивого устройства и проникновения в сеть с помощью атаки методом полного перебора или проведения изощренной *DoS-атаки*, направленной на вывод из строя механизмов аутентификации. Разумеется, неправильно сформированные фреймы могут возникать и в результате сильных радиопомех или других проблем на уровне 1.

4. События, связанные с протоколом *WEP*:

- наличие незашифрованного беспроводного трафика;
- наличие трафика, зашифрованного неизвестными *WEP*-ключами;
- наличие трафика, зашифрованного *WEP*-ключами разной длины;
- фреймы со слабыми IV;
- идущие подряд фреймы с повторяющимися IV;
- не изменяющиеся IV;
- откат к *WEP* от более безопасного протокола, например *TKIP*;
- ошибки при ротировании *WEP*-ключей.

Эти события могут указывать на серьезные ошибки при конфигурировании сети, на применение небезопасного устаревшего оборудования или на использование инструментов внедрения трафика опытным взломщиком.

5. События, связанные с общими проблемами связи:

- потеря связи;
- внезапный всплеск нагрузки на сеть;
- внезапное уменьшение пропускной способности сети;
- внезапное увеличение задержек в двухточечном канале;

- повышенный уровень фрагментации пакетов;
- частые повторные передачи.

Эти события заслуживают более пристального изучения для выявления истинной причины ошибок. Механизм построения выводов, встроенный в IDS, должен уметь связывать события с различными возможными причинами, тем самым упрощая расследование.

6. Прочие события:

- присоединившиеся, но не аутентифицированные хосты;
- атаки на верхние уровни стека протоколов, вызывающие срабатывание "традиционной" IDS;
- посторонний административный трафик, адресованный точке доступа;
- постоянное дублирование или повтор пакетов с данными;
- пакеты с данными, в которых испорчены контрольные суммы или MIC, формируемые на канальном уровне;
- затопление многократными попытками одновременного присоединения к сети.

Эти события могут свидетельствовать об успешной или неудачной атаке, о наличии хоста с неправильными настройками безопасности, о попытках получить контроль над точкой доступа и изменить ее конфигурацию, о применении инструментов для внедрения трафика, о DoS-атаке против хостов с включенным протоколом 802.11i или о попытках переполнить буферы точки доступа большим числом запросов на соединение со стороны проводной или беспроводной части сети. Но, как и раньше, искажение фрейма или пакета может быть обусловлено проблемами на физическом уровне, например наличием помех или слабым уровнем сигнала.

Коммерческие системы *IDS* для беспроводных сетей.

Из коммерческих решений хорошо известны программы *AirDefense Guard* и *Isomair Wireless Sentry*. Они основаны на размещении сенсоров на территории.

Анонс WPA3: Wi-Fi Alliance представил обновление безопасности

11 января 2018 в 13:50

Группа Wi-Fi Alliance, в которую входят Apple, Microsoft и Qualcomm, [представила](#) новый протокол безопасности для беспроводных сетей — WPA3. Подробности его реализации появятся позднее (в этом году), однако уже есть информация о нескольких функциях. Например, в WPA3 появится защита от атак полным перебором (brute-force) и возможность «персонализированного шифрования данных». Подробнее об этих и нескольких других особенностях мы расскажем под катом.

/ Flickr / [Metropolitan Transportation Authority](#) / [CC](#)

Почему потребовался апгрейд

Обновление в каком-то смысле стало ответом на баг в протоколе WPA2, используемом в миллиардах устройств по всему миру. Критическая уязвимость получила название [KRACK](#), а обнаружил её бельгийский исследователь Мэтти Ванхоеф (Mathy Vanhoef) осенью прошлого года.

KRACK — это атака повторного воспроизведения на беспроводную сеть, которая [позволяет злоумышленникам](#) провести MITM-атаку и «прослушивать» канал между клиентом и Wi-Fi-точкой.

При установлении соединения по WPA2 выполняется четырехэтапное рукопожатие, во время которого генерируется криптографический ключ для шифрования трафика. Хакер, путем манипулирования сообщениями рукопожатий, [принуждает](#) жертву переопределить уже «утвержденный» ключ. Далее, номера переданного и принятого пакета устанавливаются в начальные значения. После чего злоумышленник может расшифровывать информацию и даже внедрять свой код в TCP.

Новые функции WPA3

Чтобы исключить эту уязвимость и усилить защищенность Wi-Fi-сетей в целом, Альянс внедряет несколько обновлений безопасности, которые станут частью WPA3.

Первая функция — это [брютфорс-защита](#). Новые правила ограничивают количество попыток ввода пароля, что повышает защиту от [словарных атак](#) (подобрать пароль онлайн также не получится).

Еще появится возможность настраивать Wi-Fi-совместимые устройства с помощью сторонних гаджетов. Например, можно будет сконфигурировать WPA3 на устройстве интернета вещей со смартфона или планшета.

В WPA3 также будет внедрена поддержка «персонализированного шифрования данных». Мэтти Ванхоеф в Твиттере [предположил](#), что речь идет о реализации [Opportunistic Wireless Encryption](#) (OWE). Это улучшение, предложенное для стандарта 802.11. OWE использует для получения общего секретного ключа криптографический [протокол Диффи — Хеллмана](#), который заменяет уязвимый метод PSK.

Ванхоеф также [предположил](#), что улучшенная защита паролей будет реализована с помощью механизмов [SAE](#) или [Dragonfly](#), используемого в mesh-сетях.

Наконец, представители Wi-Fi Alliance представили 192-разрядный пакет безопасности, реализованный согласно требованиям Commercial National Security Algorithm (CNSA) Suite. Их [разработал](#) Комитет по национальным системам безопасности (CNSS) для защиты государственных и индустриальных беспроводных сетей.

Когда ждать стандарт

И хотя подробная спецификация протокола будет опубликована уже в этом году, [пройдет](#) некоторое время, прежде чем появится возможность купить сертифицированное оборудование с поддержкой WPA3.

Из-за массовости WPA2, внедрение WPA3 [пройдет](#) поэтапно, поэтому старый протокол пока останется востребован. Для тех, кто продолжит использовать WPA2, Альянс составит список советов для повышения защищенности сетей.

Как [говорят](#) Мэтти Ванхеф (Mathy Vanhoef), внедряемые в WPA3 стандарты существуют уже продолжительное время, но не всегда используются в реальных системах. Мэтти надеется, что желание производителей получить спецификацию WPA3 (хотя бы из коммерческих соображений) изменит ситуацию и окажет положительное влияние на защищенность экосистемы беспроводных сетей.

Началась сертификация устройств WPA3: слабые пароли стали более безопасными

27 июня 2018 в 10:40

25 июня 2018 года Wi-Fi Alliance [официально представил](#) программу сертификации [Wi-Fi CERTIFIED WPA3](#).

Это первое за последние 14 лет обновление протоколов безопасности Wi-Fi.

По заявлению альянса, WPA3 (Wi-Fi Protected Access 3) «добавляет новые функции для упрощения безопасности Wi-Fi, обеспечения более надёжной аутентификации, повышения криптографической стойкости для высокочувствительных рынков данных и обеспечения отказоустойчивости критически важных сетей». Во всех сетях WPA3:

- Используются последние методы безопасности
- Запрещены устаревшие протоколы
- Обязательна функция защиты управляющих фреймов от компрометации PMF (Protected Management Frames)

Поскольку сети Wi-Fi отличаются потребностями в использовании и безопасности, WPA3 как и WPA2 предлагает два стандартных профиля для личных и корпоративных сетей: WPA3-Personal и WPA3-Enterprise.

Пользователи **WPA3-Personal** получают более надёжную парольную аутентификацию и защиту от брутфорса даже в тех случаях, если выбирают слишком короткий или простой пароль. Это реализуется за счёт замены старого протокола Pre-shared Key (PSK) на протокол [Simultaneous Authentication of Equals](#) (SAE) от Дэна Перкинса. SAE относится к протоколам типа [PAKE](#) (password-authenticated key agreement): интерактивный метод, где две или более стороны устанавливают криптографические ключи, основанные на знании одной или несколькими сторонами пароля.

Ключевое свойство PAKE — человек в середине *не может* получить достаточно информации, чтобы провести полноценный «оффлайновый» брутфорс в пассивном режиме. Ему обязательно требуется взаимодействие со сторонами для проверки каждого варианта. Это означает, что даже со слабыми паролями обеспечивается гораздо лучшая безопасность, чем раньше.

WPA3-Personal больше ориентирован на простоту в использовании. Пользователи по-прежнему могут выбирать произвольные пароли.

WPA3-Enterprise предоставляет гораздо более высокие требования к безопасности и теперь позволяет использовать особо стойкие протоколы безопасности для конфиденциальных сетей передачи данных. Предлагаются криптографические протоколы с использованием минимум 192-битных ключей и следующие криптографические инструменты для защиты данных:

- **Аутентичное шифрование:** 256-битный Galois/Counter Mode Protocol (GCMP-256)
- **Формирование ключа и подтверждение:** 384-битный Hashed Message Authentication Mode (HMAC) с хэшированием по протоколу Secure Hash Algorithm (HMAC-SHA384)
- **Обмен ключами и аутентификация:** обмен по протоколу Elliptic Curve Diffie-Hellman (ECDH) и цифровая подпись по алгоритму Elliptic Curve Digital Signature Algorithm (ECDSA) на 384-битной эллиптической кривой
- **Надёжное управление защитой трафика:** 256-битный Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

Предполагается, что при выборе 192-битного режима будут использоваться все перечисленные инструменты, что гарантирует правильную комбинацию протоколов как базовую платформу безопасности внутри сети WPA3.

WPA3 сохраняет обратную совместимость с устройствами WPA2 и в настоящее время является необязательной дополнительной сертификацией для устройств Wi-Fi CERTIFIED.

WPA3 основан на криптографическом протоколе [Simultaneous Authentication of Equals \(SAE\)](#) от Дэна Харкинса (Dan Harkins). Этот специалист также является автором [печально известного](#) протокола [Dragonfly \(RFC 7664\)](#). Нужно сказать, что процедура утверждения RFC 7664 в IETF [сопровождалась бурными дебатами](#). Председатель рабочей группы по криптостандартам CFRG, которая утверждала Dragonfly, Кевин Айгоу (Kevin Igoue) предположительно [является сотрудником АНБ](#). В результате всё-таки в глобальном смысле нельзя со всей уверенностью говорить о криптографической стойкости и общей надёжности протокола SAE и стандарта WPA3 в целом.

Wi-Fi Alliance ожидает, что устройства с поддержкой WPA3 получат распространение на рынке в 2019 году, вместе с устройствами, которые поддерживают новую, более быструю версию самого Wi-Fi — [802.11ax](#). После этого поддержка WPA3 может стать обязательным условием для сертификации любого устройства Wi-Fi.

Wi-Fi становится безопаснее: всё, что вам нужно знать про WPA3

2 октября 2018 в 10:00

Недавно Wi-Fi Alliance [обнародовал](#) крупнейшее обновление безопасности Wi-Fi за последние 14 лет. Протокол безопасности Wi-Fi Protected Access 3 (WPA3) вводит очень нужные обновления в протокол WPA2, представленный в 2004 году. Вместо того, чтобы полностью переработать безопасность Wi-Fi, WPA3 концентрируется на новых технологиях, которые должны закрыть щели, начавшие появляться в WPA2.

Wi-Fi Alliance также объявил о двух дополнительных, отдельных протоколах сертификации, вводящихся в строй параллельно WPA3. Протоколы Enhanced Open и Easy Connect не зависят от WPA3, но улучшают безопасность для определённых типов сетей и ситуаций.

Все протоколы доступны для внедрения производителями в их устройства. Если WPA2 можно считать показателем, то эти протоколы в конечном итоге будут приняты повсеместно, но Wi-Fi Alliance не даёт никакого графика, по которому это должно будет происходить. Скорее всего, с внедрением новых устройств на рынок мы в итоге достигнем этапа, после которого WPA3, Enhanced Open и Easy Connect станут новыми опорами безопасности.

Что же делают все эти новые протоколы? Деталей много, и поскольку большинство из них связано с беспроводным шифрованием, встречается и сложная математика — но вот примерное описание четырёх основных изменений, которые они принесут с собой в дело беспроводной безопасности.

Одновременная аутентификация равных [Simultaneous Authentication of Equals, SAE]

Самое крупное изменение, которое принесёт [WPA3](#). Самый главный момент в защите сети наступает, когда новое устройство пытается установить соединение. Враг должен оставаться за воротами, поэтому WPA2 и WPA3 уделяют много внимания аутентификации новых соединений и гарантии того, что они не будут являться попытками хакера получить доступ.

[SAE](#) — новый метод аутентификации устройства, пытающегося подключиться к сети. SAE — это вариант т.н. [dragonfly handshake](#) [установления связи по методу стрекозы], использующего криптографию для предотвращения угадывания пароля злоумышленником. Он говорит о том, как именно новое устройство, или пользователь, должен «приветствовать» сетевой маршрутизатор при обмене криптографическими ключами.

SAE идёт на замену методу Pre-Shared Key (PSK) [предварительно розданного ключа], используемого с момента презентации WPA2 в 2004-м. PSK также известен, как четырёхэтапное установление связи, поскольку столько именно сообщений, или двусторонних «рукопожатий», необходимо передать между маршрутизатором и подсоединяющимся устройством, чтобы подтвердить, что они договорились по поводу пароля, при том, что ни одна из сторон не сообщает его другой. До 2016 года PSK казался безопасным, а потом была открыта [атака с переустановкой ключа](#) (Key Reinstallation Attacks, [KRACK](#)).

KRACK прерывает серию рукопожатий, притворяясь, что соединение с маршрутизатором временно прервалось. На самом деле он использует повторяющиеся возможности соединения для анализа рукопожатий, пока не сможет догадаться о том, какой был пароль. SAE блокирует возможность такой атаки, а также наиболее распространённые онлайн-атаки по словарю, когда компьютер перебирает миллионы паролей, чтобы определить, какой из них подходит к информации, полученной во время PSK-соединений.

Как следует из названия, SAE работает на основании предположения о равноправности устройств, вместо того, чтобы считать одно устройство отправляющим запросы, а второе – устанавливающим право на подключение (традиционно это были устройство, пытающееся соединиться, и маршрутизатор, соответственно). Любая из сторон может отправить запрос на соединение, и потом они начинают независимо отправлять удостоверяющую их информацию, вместо того, чтобы обмениваться сообщениями по очереди, туда-сюда. А без такого обмена у атаки KRACK не будет возможности «вставить ногу между дверью и косяком», и атаки по словарю станут бесполезными.

SAE предлагает дополнительное усиление безопасности, которого не было в PSK: [прямую секретность](#)[forward secrecy]. Допустим, атакующий получает доступ к зашифрованным данным, которые маршрутизатор отправляет и получает из интернета. Раньше атакующий мог сохранить эти данные, а потом, в случае успешного подбора пароля, расшифровать их. С использованием SAE при каждом новом соединении устанавливается новый шифрующий пароль, поэтому даже если атакующий в какой-то момент и проникнет в сеть, он сможет украсть только пароль от данных, переданных после этого момента.

192-битные протоколы безопасности

[WPA3-Enterprise](#), версия WPA3, предназначенная для работы в правительственные и финансовых учреждениях, а также в корпоративной среде, обладает шифрованием в 192 бита. Такой уровень шифрования для домашнего маршрутизатора будет избыточным, но его имеет смысл использовать в сетях, работающих с особо чувствительной информацией.

Сейчас Wi-Fi работает с безопасностью в 128 бит. Безопасность в 192 бита не будет обязательной к использованию – это будет вариант настроек для тех организаций, сетям которых она будет нужна. Wi-Fi Alliance также подчёркивает, что в промышленных сетях необходимо усиливать безопасность по всем фронтам: стойкость системы определяется стойкостью самого слабого звена.

Чтобы гарантировать подобающий уровень безопасности всей сети, от начала до конца, WPA3-Enterprise будет использовать 256-битный протокол Galois/Counter Mode для шифрования, 384-битный Hashed Message Authentication Mode режим для создания и подтверждения ключей, и алгоритмы Elliptic Curve Diffie-Hellman exchange, Elliptic Curve Digital Signature Algorithm для аутентификации ключей. В них много сложной математики, но плюс в том, что на каждом шагу будет поддерживаться шифрование в 192 бита.

Easy Connect

[Easy Connect](#) – это признание наличия в мире огромного количества устройств, присоединённых к сети. И хотя, возможно, не все люди захотят обзавестись умными домами, у среднего человека к домашнему маршрутизатору сегодня, скорее всего, подключено больше устройств, чем в 2004 году. Easy Connect – попытка Wi-Fi альянса сделать подсоединение всех этих устройств более интуитивным.

Вместо того, чтобы каждый раз при добавлении устройства вводить пароль, у устройств будут уникальные QR-коды – и каждый код устройства будет работать как публичный ключ. Для добавления устройства можно будет просканировать код при помощи смартфона, уже соединённого с сетью.

После сканирования устройство обменяется с сетью ключами аутентификации для установления последующей связи. Протокол Easy Connect не связан с WPA3 – устройства, сертифицированные для него, должны иметь сертификат для WPA2, но не обязательно сертификат для WPA3.

Enhanced Open

[Enhanced Open](#) – ещё один отдельный протокол, разработанный для защиты пользователя в открытой сети. Открытые сети – такие, которыми вы пользуетесь в кафе или аэропорту – несут в себе целый комплекс проблем, которые обычно не касаются вас, когда вы устанавливаете соединение дома или на работе.

Многие атаки, происходящие в открытой сети, относятся к пассивным. Когда к сети подключается куча людей, атакующий может собрать очень много данных, просто фильтруя проходящую мимо информацию.

Enhanced Open использует [оппортунистическое](#) беспроводное шифрование (Opportunistic Wireless Encryption, OWE), определённое в стандарте [Internet Engineering Task Force RFC 8110](#), чтобы защищаться от

пассивного подслушивания. Для OWE не требуется дополнительная защита с аутентификацией – оно концентрируется на улучшении шифрования данных, передаваемых по публичным сетям, с целью предотвратить их кражу. Оно также предотвращает т.н. простую инъекцию пакетов [unsophisticated packet injection], в которой атакующий пытается нарушить работу сети, создавая и передавая особые пакеты данных, выглядящие, как часть нормальной работы сети.

Enhanced Open не даёт защиты с аутентификацией из-за особенностей организации открытых сетей – они по определению предназначены для всеобщего использования. Enhanced Open был разработан для улучшения защиты открытых сетей против пассивных атак, так, чтобы не требовать от пользователей ввода дополнительных паролей или прохождения дополнительных шагов.

Пройдёт, по меньшей мере, несколько лет, до того, как WPA3, Easy Connect и Enhanced Open станут нормой. Широкое распространение WPA3 произойдёт только после замены или обновления маршрутизаторов. Однако если вас беспокоит безопасность вашей личной сети, вы сможете заменить свой текущий маршрутизатор на другой, поддерживающий WPA3, как только производители начнут продавать их, что может произойти уже через несколько месяцев.

WPA3 мог бы быть и безопаснее: мнение экспертов

4 октября 2018 в 10:00

Новые планы альянса Wi-Fi делают упор на безопасности, но независимые исследователи находят в них упущеные возможности

Wi-Fi Protected Access 2, или WPA2, успешно и долго работал. Но после 14 лет в качестве основного беспроводного протокола безопасности неизбежно начали появляться прорехи. Поэтому Wi-Fi Alliance и [объявил](#) [планы](#) на преемника этого протокола, WPA3, с начала года понемногу выдавая информацию о грядущих переменах.

Но [Wi-Fi Alliance](#) – организация, отвечающая за сертификацию продуктов, использующих Wi-Fi, возможно, сделала не всё, что могла, для того, чтобы сделать беспроводную безопасность истинно современной – по крайней мере, так считает сторонний исследователь безопасности. [Мэти Ванхоф](#), исследователь из Лёвенского католического университета в Бельгии, в 2016-м обнаруживший атаку KRACK, позволяющую взломать WPA2, считает, что Wi-Fi Alliance мог бы сработать и лучше, изучив альтернативные протоколы безопасности и их сертификаты.

Серьёзное различие между WPA2 и WPA3 состоит в способе, которым устройства приветствуют маршрутизатор или другие точки доступа, к которым они пытаются присоединиться. WPA3 вводит приветствие, или хэндшейк, под названием одновременная аутентификация равных [Simultaneous Authentication of Equals, SAE]. Его преимущество в том, что оно предотвращает такие атаки, как KRACK, прерывающие приветствие в WPA2. Оно гарантирует, что обмен ключами, доказывающими идентичность обоих устройств, нельзя прервать. Для этого оно приравнивает в правах устройство и маршрутизатор. До этого в таком обмене приветствиями участвовали опрашивающее устройство (пытающееся подключиться к сети) и авторизующее устройство (маршрутизатор).

SAE решает большие проблемы с уязвимостью WPA2 – это важный шаг, но, возможно, недостаточно большой. Ванхоф утверждает, что, по слухам, распространяющимся в сообществе специалистов по безопасности, хотя такое приветствие и предотвратит вредные атаки типа KRACK, остаются вопросы о том, способно ли оно на что-то большее.

Ванхов говорит, что математический анализ приветствия вроде бы подтверждает его безопасность. «С другой стороны, раздаются комментарии и критика, из которых ясно, что существуют и другие варианты, – говорит он. – Вероятность возникновения небольших проблем выше, чем у других типов приветствий».

Одно из опасений состоит в вероятности [атаки по сторонним каналам](#), в частности, [атака по времени](#). Хотя SAE устойчив к атакам, прерывающим приветствие напрямую, он может оказаться уязвимым к более пассивным атакам, наблюдающим за временем авторизации и извлекающим на этом основании некоторую информацию о пароле.

В 2013 году исследователи из Университета Ньюкасла во время [криптоанализа SAE](#) обнаружили, что приветствие уязвимо к т.н. [атакам малых подгрупп](#). Такие атаки сводят ключи, которыми обмениваются

маршрутизатор и подсоединяющееся устройство, к мелкой, ограниченной подгруппе вариантов, которую легче взломать, чем обычно доступный набор из множества вариантов. Чтобы устраниТЬ эту уязвимость, исследователи предлагают дополнить SAE ещё одним этапом проверки ключей, пожертвовав некоторой эффективностью приветствия.

Однако SAE защищает от атак, использовавших недостатки WPA2. [Кевин Робинсон](#), вице-президент по маркетингу Wi-Fi Alliance, говорит, что он делает невозможными офлайн-атаки по словарю. Такие атаки можно проводить, когда атакующий способен проверить тысячи и сотни тысяч возможных паролей подряд, не возбуждая подозрений у сети. SAE предлагает и [прямую секретность](#) – если атакующий получил доступ к сети, все данные, отправленные по ней до этого, останутся в безопасности – в случае с WPA2 это было не так.

Когда Wi-Fi Alliance впервые объявил о выходе WPA3 в пресс-релизе в январе, он упомянул «набор свойств» для улучшения безопасности. В релизе содержался намёк на четыре конкретных свойства. Одно из них, SAE, стало основой WPA3. Второе, 192-битное шифрование, возможно использовать в крупных корпорациях или финансовых учреждениях, переходящих на WPA3. А два другие свойства так и не попали в WPA3.

Туда не попали свойства, существующие в отдельных сертификационных программах. Первое, Easy Connect, упрощает процедуру соединения устройств из интернета вещей с домашней сетью. Второе, Enhanced Open, сильнее защищает открытые сети – такие, как сети в аэропортах и кафе.

«Я думаю, что Wi-Fi Alliance специально сформулировал январский пресс-релиз так туманно, — говорит Ванхоф. — Они не обещали, что всё это будет включено в WPA3. Были рассуждения о том, что все эти свойства станут обязательными. Однако обязательным стало только приветствие – и это, я считаю, плохо».

Ванхоф беспокоится, что три отдельных программы сертификации, WPA3, Easy Connect и Enhanced Open, будут путать пользователей, а не накрывать их зонтиком WPA3. «Придётся говорить обычным пользователям, чтобы они использовали Easy Connect и Enhanced Open», — говорит он.

Wi-Fi Alliance считает, что раздельные программы сертификации уменьшат путаницу пользователей. «Важно, чтобы пользователь понимал разницу между WPA3 и протоколом Enhanced Open, предназначенным для открытой сети», — говорит Робинсон. Точно так же, говорит он, представители индустрии, входящие в Wi-Fi Alliance, посчитали очень важным сделать так, чтобы протокол Easy Connect предлагал беспроблемный метод подсоединения устройств, всё ещё использующих WPA2, а не ограничивал эту возможность только для новых устройств».

И всё же, вне зависимости от того, будут ли пользователи новых сертификационных программ от Wi-Fi Alliance запутаны или успокоены, Ванхоф считает, что Wi-Fi Alliance мог бы более открыто освещать свой процесс выбора протоколов. «Они работали в закрытом режиме, — говорит он. — Из-за этого экспертам по безопасности и шифровальщикам было тяжело комментировать этот процесс», из-за чего возникают опасения по поводу потенциальных уязвимостей SAE и нескольких программ сертификации.

Ванхоф также указывает на то, что открытый процесс мог бы привести к созданию более надёжного протокола WPA3. «Мы часто сталкиваемся с секретностью, — говорит он. — А потом мы обнаруживаем, что в результате безопасность оказалась слабой. В общем, мы поняли, что всегда лучше работать открыто».

WPA3 – Крупнейшее обновление безопасности Wi-Fi за последние 14 лет

Дата публикации: 21.11.2018 Автор: [Дмитрий Денисов](#)

В 2017 году в протоколе WPA2 была обнаружена серьезная уязвимость, получившая название KRACK (Key Reinstallation Attack) – атака с переустановкой ключа. Этот факт, наряду со всеми ранее известными недостатками WPA2, подтолкнул Wi-Fi Alliance к разработке нового стандарта безопасности - WPA3.

Wi-Fi уже давно стал неотъемлемой частью жизни миллионов людей, а с появлением IoT число беспроводных устройств во всем мире постоянно растет, поэтому вопросы защиты Wi-Fi сетей не теряют своей актуальности. Предыдущая версия протокола WPA2 была введена в 2004 году и за последние несколько лет неоднократно была дискредитирована. По этой причине в июле 2018 года Wi-Fi Alliance объявил о начале сертификации устройств, поддерживающих WPA3 (Wi-Fi Protected Access 3) - самого большого обновления безопасности за последние 14 лет.

Новый механизм аутентификации - SAE (Simultaneous Authentication of Equals)

В WPA2 всегда острой проблемой оставалось использование слабых паролей. Если пользователи ставят легкий пароль на беспроводную сеть, то его без труда можно было подобрать с помощью автоматизированных атак с использованием словарей, таких как [Dictionary](#) и [Brute-Force](#). Протокол WPA2 никогда не предлагал вариантов для решения этой проблемы. От разработчиков были лишь рекомендации использовать сложные и более надежные пароли. В WPA3 будут приняты меры, позволяющие противодействовать таким атакам.

Для этого в WPA3 был реализован новый механизм аутентификации SAE (Simultaneous Authentication of Equals), который заменяет используемый в WPA2 метод PSK (Pre-Shared Key). Именно в PSK описано четырехступенчатое рукопожатие для установления связи. Этот метод был скомпрометирован KRACK-атакой, которая прерывает серию рукопожатий и пытается повторить запрос на подключение. Неоднократная повторная отправка приветственных сообщений вынуждает участников сети переустановить уже согласованный ключ. Когда жертва переустанавливает ключ, ассоциированные с ним параметры сбрасываются, что нарушает безопасность, которую должен гарантировать WPA2. Таким образом, злоумышленник получает возможность прослушивать трафик и внедрять свои пакеты.

SAE переводится как "одновременная аутентификация равных", и как понятно из названия, согласно этому алгоритму аутентификация устройств производится одновременно и на равных правах. Что это значит?

Разработчики отказались от строгой последовательности действий при авторизации и ушли от того, чтобы считать точку доступа главным устройством в сети при авторизации. Согласно механизму SAE, все устройства в сети (точки доступа и абонентские устройства) работают на равных правах. Поэтому любое устройство может начать отправлять запросы на аутентификацию и в произвольном порядке отправлять информацию по установлению ключей. В результате чего, возможность реализации KRACK-атаки была устранена. С появлением SAE у злоумышленника принципиально не будет возможности прервать процесс аутентификации, "влезая" между точкой доступа и абонентским устройством.

WPA3-Personal и WPA3-Enterprise

В WPA3 по аналогии с WPA2 останется два режима работы: WPA3-Enterprise и WPA3-Personal.

Устройства, использующие WPA3-Personal, получат повышенную защиту от перебора паролей в виде SAE. Даже когда пользователи выбирают пароли, не соответствующие типичным рекомендациям сложности, SAE гарантирует безопасность. Эта технология устойчива к офлайновым брутфорс-атакам, когда взломщик пытается определить сетевой пароль, пытаясь подобрать пароли без сетевого взаимодействия (оффлайн).

Кроме этого WPA3-Personal получит дополнительное усиление безопасности в виде "Forward Secrecy". Это решение позволяет устанавливать новый ключ шифрования при каждом новом соединении. При WPA2 можно прослушивать трафик и сохранять зашифрованные данные долгое время, после чего, получив ключ доступа, полученные ранее данные можно расшифровать. С появлением Forward Secrecy это стало невозможно, так как даже если атакующий рано или поздно получит ключ от сети, то он сможет расшифровать только те данные, которые передавались после генерации последнего ключа.

Достоинства WPA3-Personal:

- Пользователи могут выбирать пароли, которые легче запомнить, не задумываясь о безопасности;
- Новый алгоритм SAE обеспечивающий улучшенную защиту за счет изменения алгоритма авторизации;
- Шифрование данные Forward Secrecy, защищает трафик данных, даже если пароль был скомпрометирован;

Корпоративные сети чаще используют Enterprise-протокол безопасности. WPA3-Enterprise также будет улучшен за счет усиления ключа шифрования с 128 бит до 192 битов. Разработчики считают такую длину ключа избыточной для большинства сетей, однако, его будет более чем достаточно для особо ценной информации.

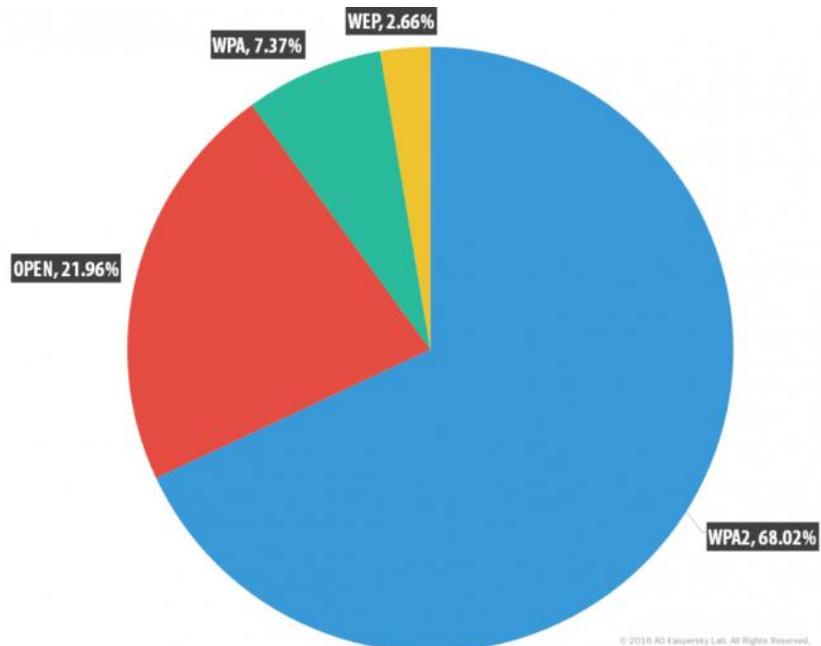
При 192-разрядном шифровании будет использоваться целый ряд сложных криптографических инструментов, протоколов аутентификации и функций формирования ключей:

- 256-bit Galois/Counter Mode Protocol (GCMP-256)
- 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
- Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve
- 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

При этом WPA3 сохраняет обратную совместимость с устройствами, использующими WPA2.

Открытые Wi-Fi сети станут безопасными благодаря Enhanced Open

Пользователи получают доступ к сетям Wi-Fi повсюду: дома, в офисе, в гостиницах, на остановках и в торговых центрах. Доступ к незащищенным сетям в этих местах представляет собой риск того, что кто-то может перехватить персональные данные. Согласно [статистики](#) лаборатории Касперского, проанализировавшей 32 миллиона точек доступа Wi-Fi, более 20% устройств используют открытые беспроводные сети:



Стоит ли говорить о том, что следует подключаться только к безопасным и защищенным сетям? Всегда существуют ситуации, когда открытая Wi-Fi сеть является единственным возможным вариантом получения доступа к сети Интернет. Не редки случаи, когда в открытой сети среди большого количества устройств оказывается атакующий, прослушивающий трафик в фоновом режиме. Чтобы устранить эти риски, Wi-Fi Alliance разработал решение для открытых сетей, которое получило название Enhanced Open.

Сети Wi-Fi Enhanced Open предоставляют пользователям неавторизованное шифрование данных, что значительно усиливает безопасность. Защита прозрачна для пользователя и основана на шифровании Opportunistic Wireless Encryption (OWE), определенного в спецификации Internet Engineering Task Force RFC8110 и спецификации беспроводного шифрования Wi-Fi Alliance, Opportunistic Wireless Encryption Specification, которые были разработаны для защиты от пассивного прослушивания. Таким образом, даже просто подключившись к открытой сети с защитой WPA3 весь трафик по умолчанию будет шифроваться.

Конец эпохи "забывания паролей". Разработан простой способ авторизации в сети Wi-Fi - Easy Connect

Wi-Fi Alliance разработал простой способ аутентификации Wi-Fi Easy Connect. Изначально он сделан для малопроизводительных IoT-устройств, но скорее всего этот способ авторизации понравится и простым пользователям. Подключить устройство к беспроводной сети можно будет путем сканирования его QR-кода.

Wi-Fi Easy Connect позволяет пользователям безопасно добавлять новое устройство в существующую Wi-Fi сеть, используя терминал с более надежным интерфейсом, например смартфон или планшет. По сути это может быть любое устройство, способное сканировать QR-код и запускать протокол Device Provisioning Protocol (DPP) разработанный Wi-Fi Alliance.

Выбранное устройство считается конфигуратором, а все остальные устройства являются дочерними для него и используют конфигуратор для подключения к сети:

Пользователь устанавливает безопасное соединение с дочерним устройством, сканируя его QR-код. Это запускает протокол DPP и автоматически предоставляет ключи, необходимые для доступа к сети.

Easy Connect обеспечивает простоту и гибкость сетей Wi-Fi:

- Не нужно запоминать и вводить пароли при подключении новых устройств;
- Упрощает настройку и подключение устройств с помощью QR-кода;
- Позволяет подключать к Wi-Fi сети устройства с отсутствующим пользовательским интерфейсом (датчики умных домов и элементы IoT);

- Easy Connect не связан с WPA3 поэтому его смогут использовать устройства, поддерживающие как WPA2 так и WPA3;
- Позволяет заменять точку доступа без необходимости повторной регистрации всех устройств;