Содержание

1. Введение 3
2. Основы передачи данных в беспроводных сетях 4
2.1. Сигналы для передачи информации 4
2.2. Передача данных 6
Аналоговые и цифровые данные 6
Аналоговые и цифровые сигналы 6
2.3. Модуляция сигналов 6
Амплитудная модуляция 7
Частотная модуляция 7
Фазовая модуляция 8
Квадратурная амплитудная модуляция 9
2.4. Методы доступа к среде в беспроводных сетях 9
Уплотнение с пространственным разделением 10
Уплотнение с частотным разделением (Frequency Division Multiplexing, FDM) 10
Уплотнение с временным разделением (Time Division Multiplexing, TDM) 10
Уплотнение с кодовым разделением (Code Division Multiplexing, CDM) 11
Механизм мультиплексирования посредством ортогональных несущих частот (Orthogonal Frequency Division Multiplexing, OFDM) 12
2.5. Технология расширенного спектра 13
Расширение спектра скачкообразной перестройкой частоты (Frequency Hopping Spread Spectrum, FHSS) 13
Прямое последовательное расширение спектра (Direct Sequence Spread Spectrum, DSSS) 14
2.6. Кодирование и защита от ошибок 16
Методы обнаружения ошибок 17
Контроль по паритету 17
Вертикальный и горизонтальный контроль по паритету 17
Циклический избыточный контроль (Cyclic Redundancy Check, CRC) 18
Методы коррекции ошибок 18
Методы автоматического запроса повторной передачи 19
Расчет дальности работы беспроводного канала связи 20
3. Основные элементы сети Wi-Fi 22
4. Архитектура IEEE 802.11 24
4.1. Стек протоколов IEEE 802.11 24
4.2. Уровень доступа к среде стандарта 802.11 24
Распределенный режим доступа DCF 25
Централизованный режим доступа PCF 29
4.3. Кадр MAC-подуровня 31
Контрольные кадры 32
Информационные кадры 32

Кадры управления 33
5. Стандарты IEEE 802.11 34
5.1. IEEE 802.11 36
Передача в диапазоне инфракрасных волн 36
Беспроводные локальные сети со скачкообразной перестройкой частоты (FHSS) 36
Беспроводные локальные сети, использующие широкополосную модуля-цию DSSS с расширением спектра методом прямой последовательности 38
5.2. IEEE 802.11b 39
5.3. IEEE 802.11a 40
5.4. IEEE 802.11g 42
5.5. IEEE 802.11d 44
5.6. IEEE 802.11e 44
5.7. IEEE 802.11f 44
5.8. IEEE 802.11h 45
5.9. IEEE 802.11i 45
5.10. IEEE 802.11n 45
6. Режимы работы беспроводного оборудования 46
6.1. Точка доступа 46
6.2. Режимы WDS и WDS WITH AP 46
6.3. Режим повторителя 48
6.4. Режим клиента точки доступа 49
6.5. Режим клиента маршрутизатора WISP 50
6.6. Режим повторителя WISP 50
7. Защита информации в беспроводных сетях 51
7.1. Классификация механизмов безопасности в сетях Wi-Fi 51
7.2. Механизмы шифрования 51
Механизм шифрования WEP (IEEE 802.11) 51
Спецификация WPA 55
Стандарт сети 802.11i с повышенной безопасностью (WPA2) 61
7.3. Аутентификация в беспроводных Wi-Fi сетях 63
Принцип аутентификации абонента в IEEE 802.11 63
Открытая аутентификация 64
Аутентификация с общим ключом 64
Аутентификация по MAC-адресу 65
Стандарт IEEE 802.1x/EAP (Enterprise-режим) 65
7.4. Дополнительные механизмы защиты 74
SSID 74

1. Введение

WI-FI – это технология беспроводного объединения компьютеров в локальную сеть. Под аббревиатурой "Wi-Fi" (от английского словосочетания "Wireless Fidelity", которое можно дословно перевести как "высокая точность беспроводной передачи данных") 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). 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 (до 300 Мб/с), что позволяет использовать их для решения очень широкого спектра задач.

Вместе с тем необходимо помнить об ограничениях беспроводных сетей. Это, как правило, все-таки 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.

2. Основы передачи данных в беспроводных сетях

2.1. Сигналы для передачи информации

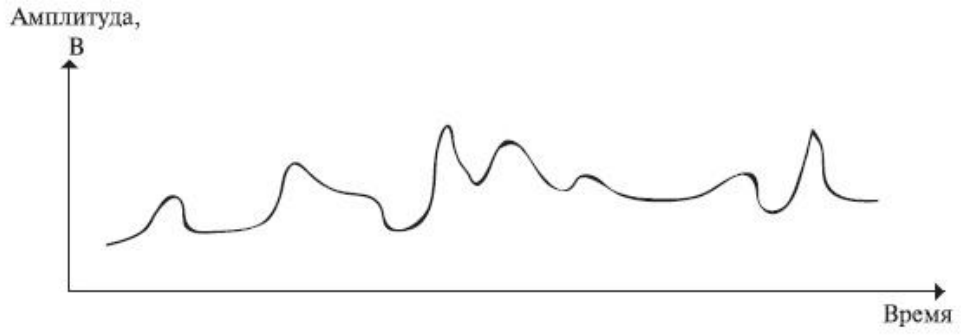
Если рассматривать сигнал как функцию времени, то он может быть либо аналоговым, либо цифровым. Аналоговым называется сигнал, интенсивность которого во времени изменяется постепенно. Другими словами, в сигнале не бывает пауз или разрывов. Цифровым называется сигнал, интенсивность которого в течение некоторого периода поддерживается на постоянном уровне, а затем также изменяется на постоянную величину (это определение идеализировано). На рис. 2.1 приведены примеры сигналов обоих типов. Аналоговый сигнал может представлять речь, а цифровой - набор двоичных единиц и нулей.

Простейшим типом сигнала является периодический сигнал, в котором некоторая структура периодически повторяется во времени. На рис. 2.2 приведен пример периодического аналогового сигнала (синусоида) и периодического цифрового сигнала (прямоугольный сигнал, или меандр). Математическое определение: сигнал s(t) является периодическим тогда и только тогда, когда

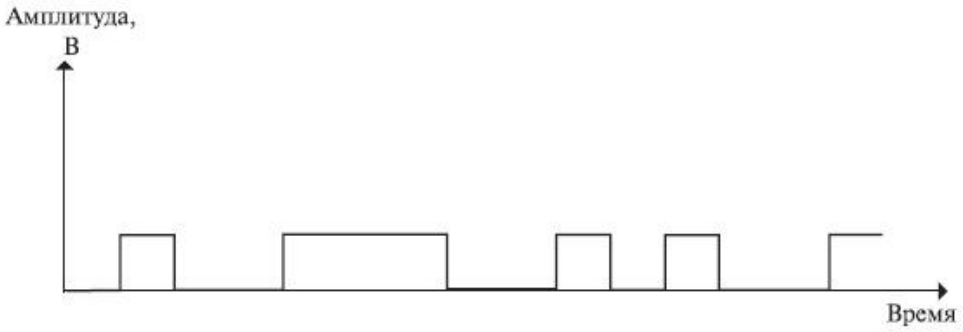
$$s(t + T) = s(t), \text{при} - \infty < t < +\infty,$$

где постоянная ***T*** является периодом сигнала.

Фундаментальным аналоговым сигналом является синусоида. В общем случае такой сигнал можно определить тремя параметрами: максимальной амплитудой ***A***, частотой ***f*** и фазой ***ф***. Максимальной амплитудой называется максимальное значение или интенсивность сигнала во времени; измеряется максимальная амплитуда, как правило, в вольтах. Частотой называется темп повторения сигналов (в периодах за секунду, или герцах). Эквивалентным параметром является период сигнала ***T***, представляющий собой время, за которое происходит повторение сигнала; следовательно, ***T = 1/f*** . Фаза является мерой относительного сдвига по времени в пределах отдельного периода сигнала.



а) Аналоговый сигнал



б) Цифровой сигнал

Рисунок 2.1. Аналоговый и цифровой сигналы.

В общем случае синусоидальный сигнал можно представить в следующем виде:

$$s(t) = A * \sin(2\pi f t + \varphi)$$

Существует соотношение между двумя синусоидальными сигналами, один из которых изменяется во времени, а другой – в пространстве. Определим длину волны сигнала ***λ*** как расстояние, занимаемое одним периодом или, иными словами, как расстояние между двумя точками равных фаз двух последовательных циклов. Предположим, что сигнал распространяется со скоростью ***v***. Тогда длина волны связана с периодом следующим соотношением: ***λ = vT***, что равносильно ***λf = v***. Особое значение для нашего изложения имеет случай ***v = c***, где ***c*** - скорость света в вакууме, приблизительно равная $3*10^8$ м/с.

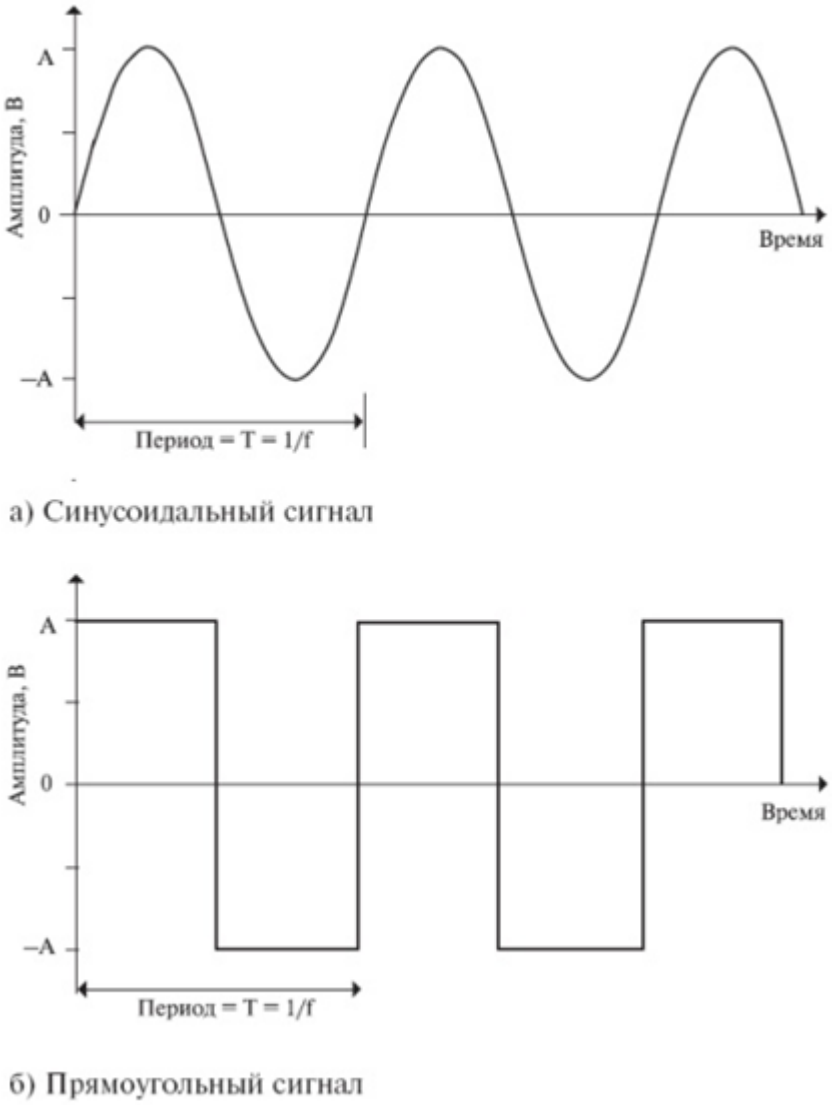


Рисунок 2.2. Периодические сигналы.

Применив преобразование Фурье, то есть сложив вместе достаточное количество синусоидальных сигналов с соответствующими амплитудами, частотами и фазами, можно получить электромагнитный сигнал любой формы. Аналогично, любой электромагнитный сигнал рассматривается как совокупность периодических аналоговых (синусоидальных) сигналов с разными амплитудами, частотами и фазами.

Спектром сигнала называется набор всех синусоид, полученных в результате разложения сигнала. Цифровой сигнал можно представить следующим образом:

$$s(t) = A * \frac{4}{\pi} * \sum_{k=1,3,5\ldots}^{\infty} \frac{\sin(2\pi k f t)}{k}$$

Этот сигнал содержит бесконечное число частотных составляющих и, следовательно, имеет бесконечную ширину полосы.

Таким образом, мы можем сделать следующие выводы. В общем случае любой цифровой сигнал имеет бесконечную ширину спектра частот. Любая линия связи обладает полосой пропускания, которая влияет на качество передаваемого по линии сигнала. Следовательно, необходимо выбирать способ кодирования передаваемого по линии сигнала так, чтобы частоты основных гармоник, составляющие сигнал, попадали в полосу пропускания линии связи, что в свою очередь приводило к наименьшему искажению сигнала на выходе линии.

2.2. Передача данных

Определим данные как объекты, передающие смысл, или информацию. Сигналы – это электромагнитное представление данных. Передача – процесс перемещения данных путем распространения сигналов по передающей среде и их обработки.

Аналоговые и цифровые данные

Понятия "аналоговые данные" и "цифровые данные" достаточно просты. Аналоговые данные принимают непрерывные значения из некоторого диапазона. Например, звуковые сигналы и видеосигналы представляют собой непрерывно изменяющиеся величины. Цифровые данные, напротив, принимают только дискретные значения; примеры – текст и целые числа.

Аналоговые и цифровые сигналы

В системе связи информация распространяется от одной точки к другой посредством электрических сигналов. Аналоговый сигнал представляет собой непрерывно изменяющуюся электромагнитную волну, которая может распространяться через множество сред, в зависимости от частоты; в качестве примеров таких сред можно назвать проводные линии, такие как витая пара и коаксиальный кабель; этот сигнал также может распространяться через атмосферу или космическое пространство. Цифровой сигнал представляет собой последовательность импульсов напряжения, которые могут передаваться по проводной линии; при этом постоянный положительный уровень напряжения может использоваться для представления двоичного нуля, а постоянный отрицательный уровень – для представления двоичной единицы. В беспроводной технологии используются цифровые данные и аналоговые сигналы, так как цифровые сигналы затухают сильнее, чем аналоговые.

2.3. Модуляция сигналов

Исторически модуляция начала применяться для аналоговой информации, и только потом – для дискретной. Необходимость в модуляции аналоговой информации возникает, когда нужно передать низкочастотный (например, голосовой) аналоговый сигнал через канал, находящийся в высокочастотной области спектра.

Для решения этой проблемы амплитуду высокочастотного несущего сигнала изменяют (модулируют) в соответствии с изменением низкочастотного сигнала.

В процессе модулирования задействованы одна или несколько характеристик несущего сигнала: амплитуда, частота и фаза. Соответственно, существуют три основные технологии кодирования или модуляции, выполняющие преобразование цифровых данных в аналоговый сигнал (рисунок 2.3):

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

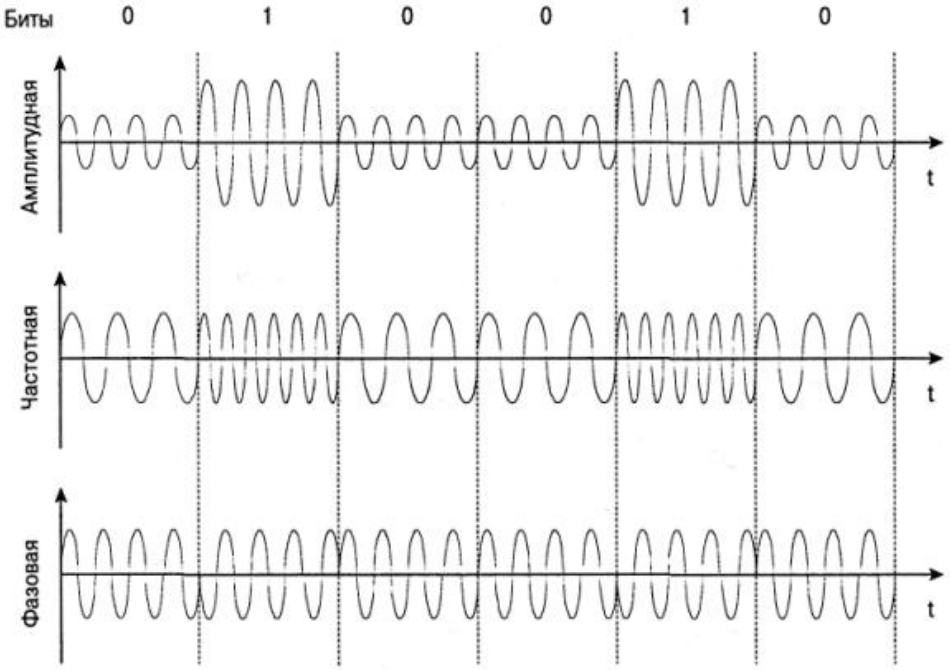


Рисунок 2.3. Модуляция цифровых данных аналоговыми сигналами.

Амплитудная модуляция

При амплитудной модуляции два двоичных значения представляются сигналами постоянной частоты с двумя различными амплитудами. Одна из амплитуд, как правило, выбирается равной нулю; то есть одно двоичное значение представляется наличием несущей частоты при постоянной амплитуде, а другое – ее отсутствием.

Частотная модуляция

Наиболее распространенной формой частотной модуляции является бинарная (Binary FSK – BFSK), в которой два двоичных числа представляются сигналами двух различных частот, расположенных около несущей.

Бинарная частотная модуляция делает сигнал более помехоустойчивым, чем амплитудная модуляция.

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 собой набор бит.

На рисунке 2.4 представлен пример схемы MFSK с M=4, где fc – несущая частота; fd – разностная частота; M – число различных сигнальных посылок. Входной поток битов

кодируется по два бита, после чего передается одна из четырех возможных двухбитовых комбинаций.

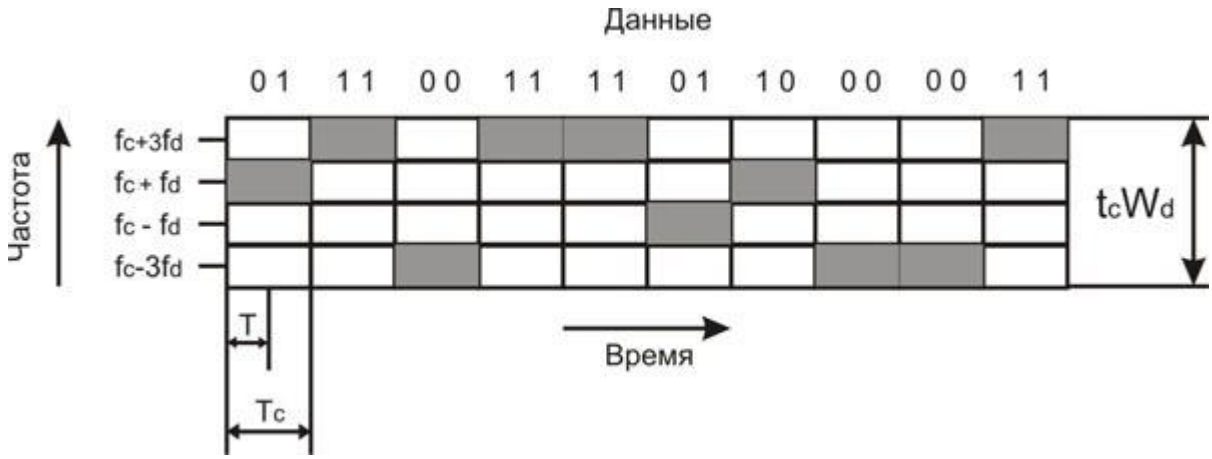


Рисунок 2.4. Использование частоты схемой MFSK (M = 4).

Фазовая модуляция

При фазовой модуляции для представления данных выполняется смещение несущего сигнала.

Самой простой фазовой модуляцией является двухуровневая модуляция (Binary PSK, BPSK), где для представления двух двоичных цифр используются две фазы.

Альтернативной формой двухуровневой PSK является дифференциальная PSK (DPSK), пример которой приведен на рисунке 2.5. В данной системе двоичный 0 представляется сигнальным пакетом, фаза которого совпадает с фазой предыдущего посланного пакета, а двоичная 1 представляется сигнальным пакетом с фазой, противоположной фазе предыдущего пакета. Такая схема называется дифференциальной, поскольку сдвиг фаз выполняется относительно предыдущего переданного бита, а не относительно какого-то эталонного сигнала. При дифференциальном кодировании передаваемая информация представляется не сигнальными посылками, а изменениями между последовательными сигнальными посылками. Схема DPSK делает излишним строгое согласование фазы местного гетеродина приемника и передатчика. До тех пор пока предыдущая полученная фаза точна, точен и фазовый эталон.

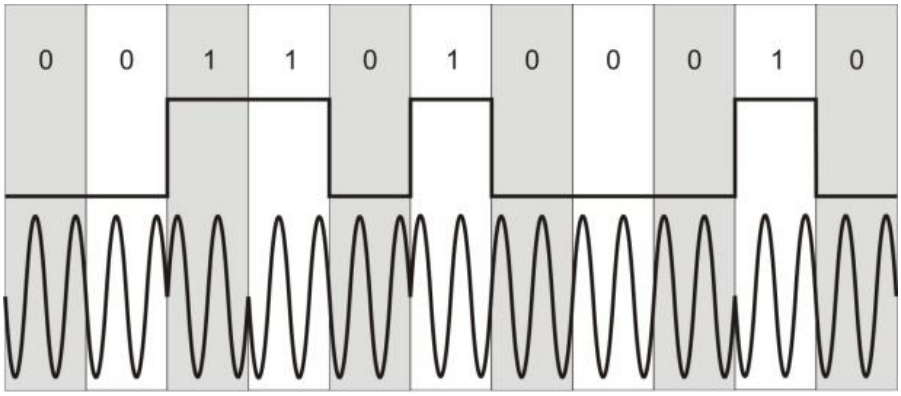


Рисунок 2.5. Дифференциальная фазовая модуляция (DPSK).

Если каждой сигнальной посылкой представить более одного бита, это позволит эффективнее использовать полосу сигнала. Например, в распространенной кодировке, известной как квадратурная фазовая модуляция (Quadrature Phase-Shift Keying, QPSK), вместо сдвига фазы на 180°, как в кодировке BPSK, используются сдвиги фаз, кратные 90°.

Таким образом, каждая сигнальная посылка представляет не один бит, а комбинацию двух бит.

Описанную схему можно расширить: передавать, например, по три бита в каждый момент времени, используя для этого восемь различных углов сдвига фаз. Более того, при каждом угле можно использовать несколько амплитуд. Такая модуляция называется многоуровневой фазовой модуляцией (Multiple FSK, MFSK).

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°. 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 амплитудной модуляции (2QAM) каждый из двух потоков может находиться в одном из двух состояний, а объединенный поток – в одном из 2 * 2 = 4 состояний. При использовании четырехуровневой модуляции (то есть четырех различных уровней амплитуды, 4QAM) объединенный поток будет находиться в одном из 4 * 4 = 16 состояний. Уже реализованы системы, имеющие 64 или даже 256 состояний. Чем больше число состояний, тем выше скорость передачи данных, возможная при определенной ширине полосы. Разумеется, как указывалось ранее, чем больше число состояний, тем выше вероятность возникновения ошибок вследствие помех или поглощения.

2.4. 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 пространственным разделением

Основано на разделении сигналов в пространстве, когда передатчик посылает сигнал, используя код c, время t и частоту f области s_i. То есть каждое беспроводное устройство может вести передачу данных только в границах определенной территории, на которой любому другому устройству запрещено передавать свои сообщения.

К примеру, если радиостанция вещает на строго определенной частоте на закрепленной за ней территории, а какая-либо другая станция в этой же местности также начнет вещать на той же частоте, слушатели радиопередач не смогут получить "чистый" сигнал ни от одной из этих станций. Другое дело, если радиостанции работают на одной частоте в разных городах. Искажений сигналов каждой радиостанции не будет в связи с ограниченной дальностью распространения сигналов этих станций, что исключает их наложение друг на друга. Характерный пример – системы сотовой телефонной связи.

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 (рисунок 2.6). Это один из наиболее известных методов, так или иначе используемый в самых современных системах беспроводной связи.

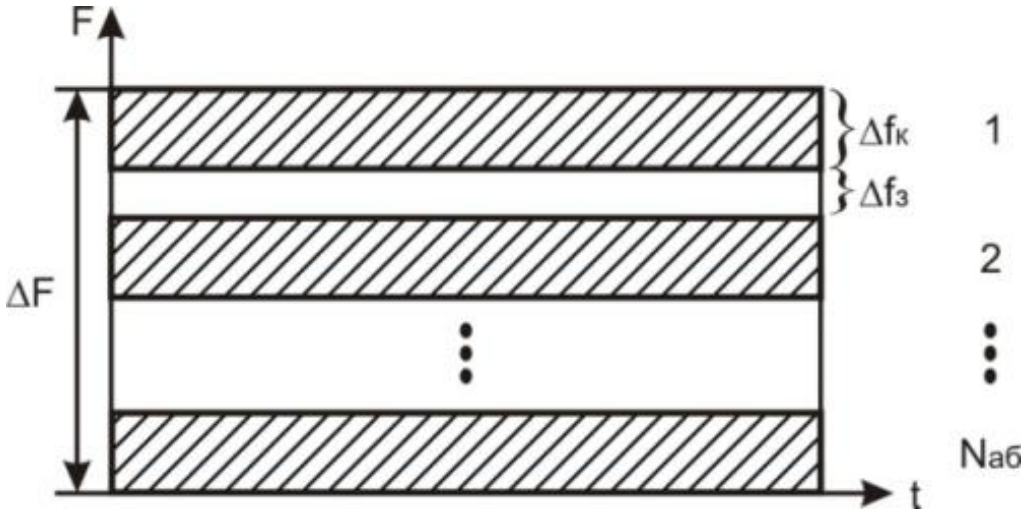


Рисунок 2.6. Принцип частотного разделения каналов.

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.

Уплотнение с временным разделением (Time Division Multiplexing, TDM)

В данной схеме распределение каналов идет по времени, то есть 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 (рисунок 2.7).

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

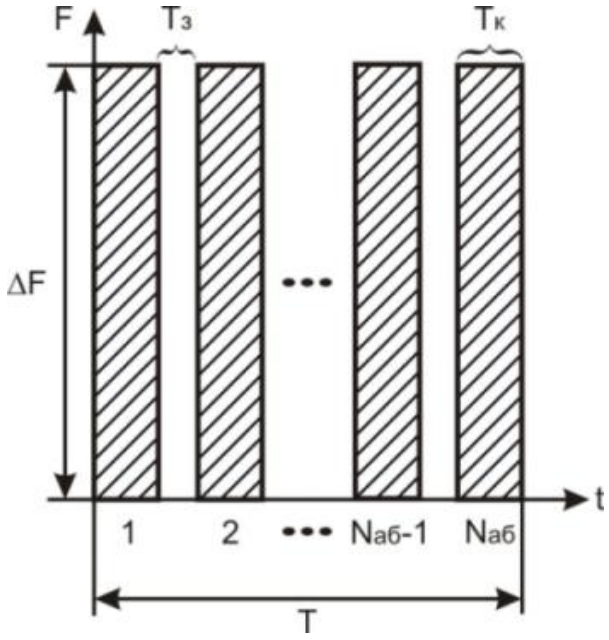


Рисунок 2.7. Принцип временного разделения каналов.

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.

Именем основанного на CDM механизме разделения каналов (CDMA – CDM Access) даже назван стандарт сотовой телефонной связи IS-95a, а также ряд 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.

Приемник знает CDM-код передатчика, сигналы которого должен воспринимать. Он постоянно принимает все сигналы и оцифровывает их. Затем в специальном устройстве (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 принял 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. Более того, 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 (Direct Sequence Spread Spectrum, DSSS).

Наиболее сильная сторона 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 более значительно 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)

Суть этого механизма: весь доступный частотный диапазон разбивается на достаточно много 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, то есть 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 (обусловлена тем, что при высокоскоростной передаче данных информационные символы передаются в виде импульсов с постоянной частотой следования значительно большей полосы частот канала. Поэтому импульсы подвергаются искажениям в виде различных задержек и ослаблении разных частотных составляющих этих импульсов. Это приводит к их расширению во времени, так что принимаемый в каждый момент сигнал представляет собой наложение "размазанных" по времени составляющих множества импульсов. Это явление межсимвольной интерференции еще называется "памятью" канала. Оно затрудняет различение сигналов и, как следствие, требует снижения скорости передачи данных). 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 Ts, то период сигнала OFDM будет

равен N*Ts. Это позволяет существенно снизить влияние межсимвольных помех. При проектировании системы число N выбирается таким образом, чтобы величина N*Ts значительно превышала среднеквадратичный разброс задержек канала.

2.5. 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)

Для того 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 передатчику и приемнику. Попытка подавления сигнала в каком-то узком диапазоне также не слишком ухудшала сигнал, так как подавлялась только небольшая часть информации. Идею этого метода иллюстрирует рисунок 2.8.

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 ASK 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 оказывается меньше из-за постоянных накладных расходов на синхронизацию.

Рисунок 2.8. Расширение спектра скачкообразной перестройкой частоты.

Несущая частота меняется в соответствии с номерами частотных подканалов, вырабатываемых алгоритмом псевдослучайных чисел. Псевдослучайная последовательность зависит от некоторого параметра, который называют начальным числом. Если приемнику и передатчику известны алгоритм и значение начального числа, то они меняют частоты 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 (рисунок 2.9а); в противном случае мы имеем дело с быстрым расширением спектра (рисунок 2.9б).

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 - вместо экономного расходования узкой полосы делается попытка занять весь доступный диапазон. На первый взгляд метод FHSS эффективен только тогда, когда в один момент времени в диапазоне работает только один канал. Однако это 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 в каждый передаваемый информационный бит (логический 0 или 1) в буквальном смысле встраивается последовательность так называемых чипов. Если информационные биты – логические нули или единицы – при потенциальном кодировании информации можно представить в виде последовательности прямоугольных импульсов, то каждый отдельный чип – это тоже прямоугольный импульс, но его длительность в несколько раз меньше длительности информационного бита. Последовательность чипов представляет собой последовательность прямоугольных импульсов, то есть нулей и единиц, однако эти нули и единицы не являются информационными.

Рисунок 2.9. Соотношение между скоростью передачи данных и частотой смены подканалов.

Поскольку длительность одного чипа в n раз меньше длительности информационного бита, то и ширина спектра преобразованного сигнала будет в n-раз больше ширины спектра первоначального сигнала. При этом и амплитуда передаваемого сигнала уменьшится 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 при фиксированной полосе пропускания линии связи передаваемый сигнал будет сильнее затухать. Поэтому обычно коэффициент расширения имеет значение от 10 до 100.

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.

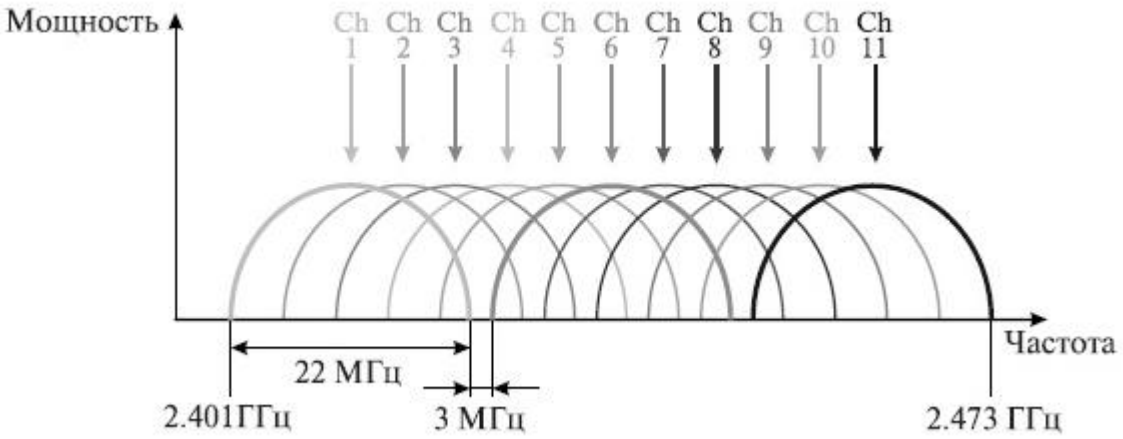


Рисунок 2.10. Каналы, используемые в технологии DSSS.

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 рисунке 2.10.

2.6. Кодирование и защита от ошибок

Существует три наиболее распространенных способа 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.

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 несколько распространенных алгоритмов вычисления контрольной суммы, отличающихся вычислительной сложностью и способностью обнаруживать ошибки передачи 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 пересылается 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-и или 33-х 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 %.

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 мы контролируем три информационных бита, то разрешенными 4-битными кодами с дополнением до нечетного количества единиц будут: 0001, 0010, 0100, 0111, 1000, 1011, 1101, 1110, 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 мы сконструировали 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). Вам может встретиться сверточный код с коэффициентом кодирования 1/2. Этот коэффициент указывает, что на каждый входной бит приходится два выходных. При сравнении кодов обращайте внимание на то, что, хотя коды с более высокой эффективной степенью кодирования позволяют передавать данные с более высокой скоростью, они, соответственно, более чувствительны к шуму.

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.

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).

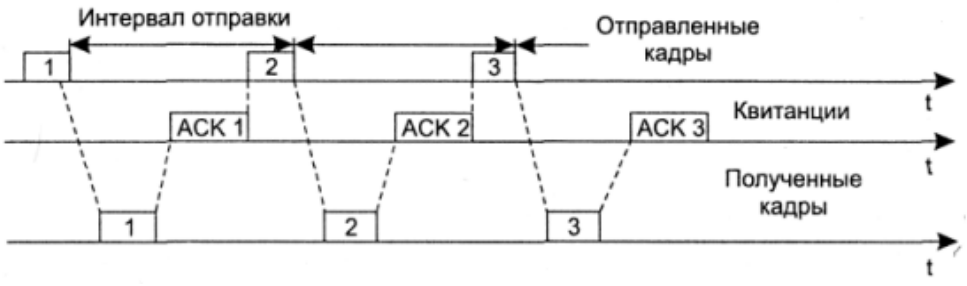


Рисунок 2.11. Процедура запрос ARQ с остановками.

В этом случае источник, пославший кадр, ожидает получения подтверждения (Acknowledgement, ACK), или, как еще его называют, квитанции, от приемника и только после этого посылает следующий кадр. Если же подтверждение не приходит в течение тайм-аута, то кадр (или подтверждение) считается утерянным и его передача повторяется. На рисунке 2.11 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.

Расчет дальности работы беспроводного канала связи

Без вывода приведем формулу расчета дальности. Она берется из инженерной формулы расчета потерь в свободном пространстве:

$$FSL = 33 + 20(lgF + lgD),$$

где FSL (Free Space Loss) – потери в свободном пространстве (дБ);

F – центральная частота канала, на котором работает система связи (МГц);

D – расстояние между двумя точками (км).

FSL определяется суммарным усилением системы. Оно считается следующим образом:

$$Y_{\text{дБ}} = P_{t,\text{дБмВт}} + G_{t,\text{дБи}} + G_{T,\text{дБи}} - P_{min,\text{дБмВт}} - L_{t,\text{дБ}} - L_{T,\text{дБ}},$$

где P_t,дБмВт – мощность передатчика;

G_t,дБи – коэффициент усиления передающей антенны;

G_T,дБи – коэффициент усиления приемной антенны;

P_{min},дБмВт – чувствительность приемника на данной скорости;

L_t,дБ – потери сигнала в коаксиальном кабеле и разъемах передающего тракта;

L_T,дБ – потери сигнала в коаксиальном кабеле и разъемах приемного тракта.

Для каждой скорости приемник имеет определенную чувствительность. Для небольших скоростей (например, 1-2 Мегабита) чувствительность наименьшая: от -90 дБмВт до -94 дБмВт. Для высоких скоростей чувствительность намного выше. В зависимости от марки радиомодулей максимальная чувствительность может немного варьироваться. Ясно, что для разных скоростей максимальная дальность будет разной. FSL вычисляется по следующей формуле:

$$FSL = Y_{\text{дБ}} - SOM,$$

где SOM(System Operating Margin) – запас в энергетике радиосвязи (дБ) учитывает возможные факторы, отрицательно влияющие на дальность связи, такие как:

- температурный дрейф чувствительности приемника и выходной мощности передатчика;
- всевозможные атмосферные явления: туман, снег, дождь;
- рассогласование антенны, приемника, передатчика с антенно-фидерным трактом.

Параметр SOM обычно берется равным 10 дБ. Считается, что 10-децибельный запас по усилению достаточен для инженерного расчета. Центральная частота канала F берется из таблицы 2.1.

Таблица 2.1 – Вычисление центральной частоты.

Канал	**Центральная частота (*МГц*)**
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472
14	2484

В итоге получаем формулу дальность связи:

$$D = 10(\frac{FSL}{20} - \frac{33}{20} - lgF)$$

3. Основные элементы сети Wi-Fi

Для построения беспроводной сети используются адаптеры и точки доступа.

Адаптер (рисунок 3.1) представляет собой устройство, которое подключается через слот расширения PCI, PCMCIA, ExpressCard, CompactFlash. Существуют также адаптеры с подключением через порт USB 2.0. Wi-Fi адаптер 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 адаптеры Wi-Fi, совместимые со многими современными стандартами. Wi-Fi адаптерами, как правило, снабжены и КПК (карманные персональные компьютеры), что также позволяет подключать их к беспроводным сетям.

Рисунок 3.1. Адаптеры.

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 (рисунок 3.2) представляет собой автономный модуль со встроенным микрокомпьютером и приемно-передающим устройством.

Рисунок 3.2. Точка доступа.

Точка доступа имеет сетевой интерфейс, 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).

4. Архитектура IEEE 802.11

Институт инженеров по электротехнике и электронике 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.

4.1. Стек протоколов IEEE 802.11

Естественно, 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 (рисунок 4.1).

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.

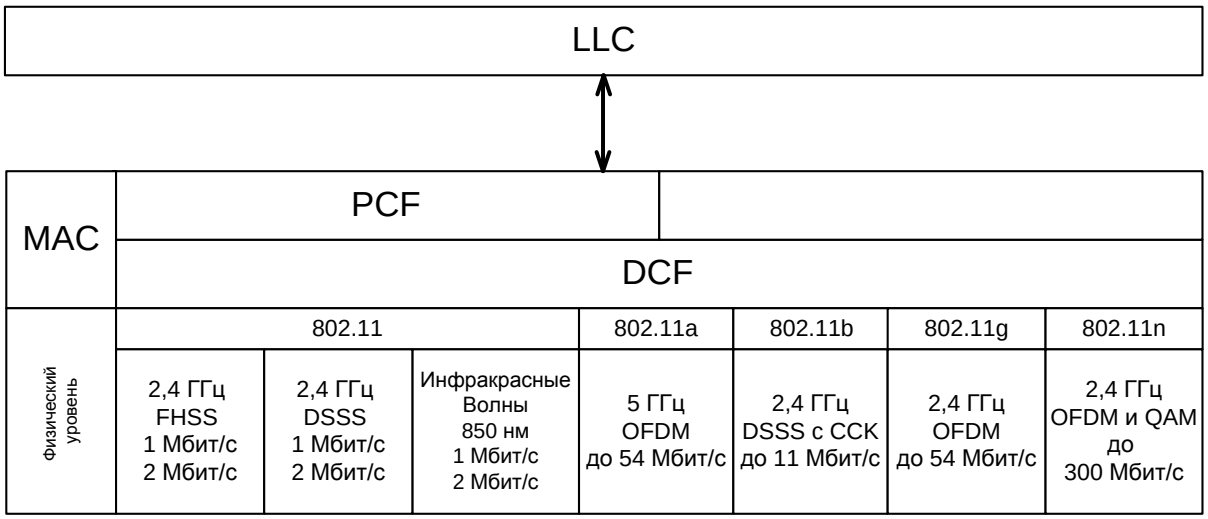


Рисунок 4.1. Стек протоколов IEEE 802.11.

4.2. Уровень доступа к среде стандарта 802.11

В сетях 802.11 уровень MAC обеспечивает два режима доступа к разделяемой среде (рисунок 4.1): распределенный режим DCF (Distributed Coordination Function) и централизованный режим PCF (Point Coordination Function).

Распределенный режим доступа DCF

Логика управления доступа к среде рассмотрена на рисунке 4.2. Рассмотрим сначала, как обеспечивается доступ в распределенном режиме 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, посылаемым 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 следующим образом – временные интервалы начинают отсчитываться от момента окончания передачи очередного кадра (рисунок 4.3). 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.

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 антенне 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 "Contention Window" (конкурентное окно).

Рассмотрим этот довольно непростой метод доступа на примере рисунка 4.3. 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.

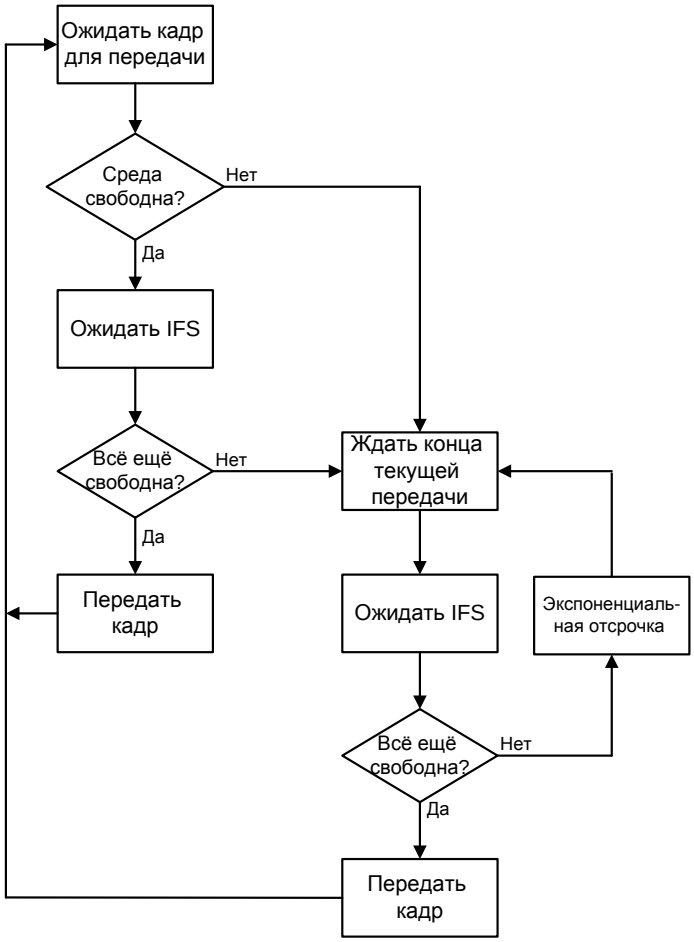


Рисунок 4.2. Логика управления доступом к среде согласно стандарту IEEE 802.11.

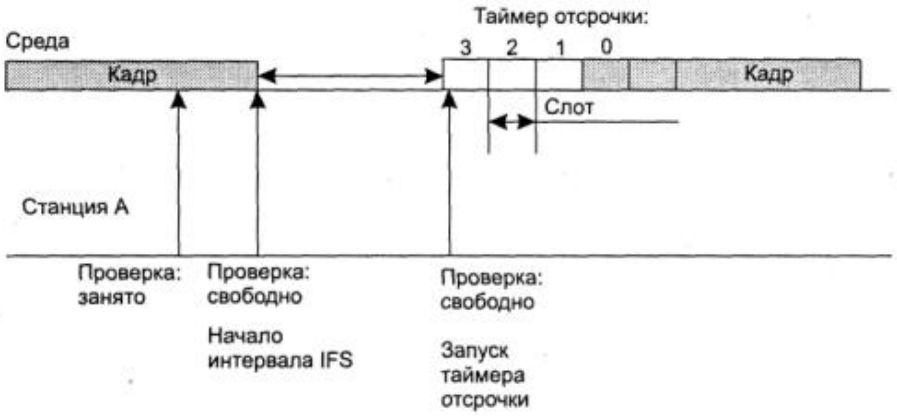


Рисунок 4.3. Режим доступа DCF.

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 нуль. Этот счетчик также устанавливается в нуль, 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 (рисунок 4.4) – 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.

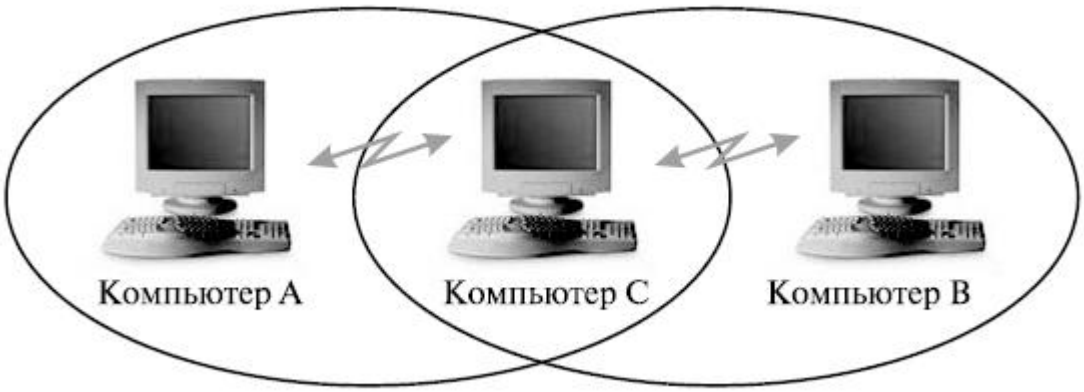


Рисунок 4.4. Проблема скрытого терминала.

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 посылает 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 посылает 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 (рисунок 4.5).

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.

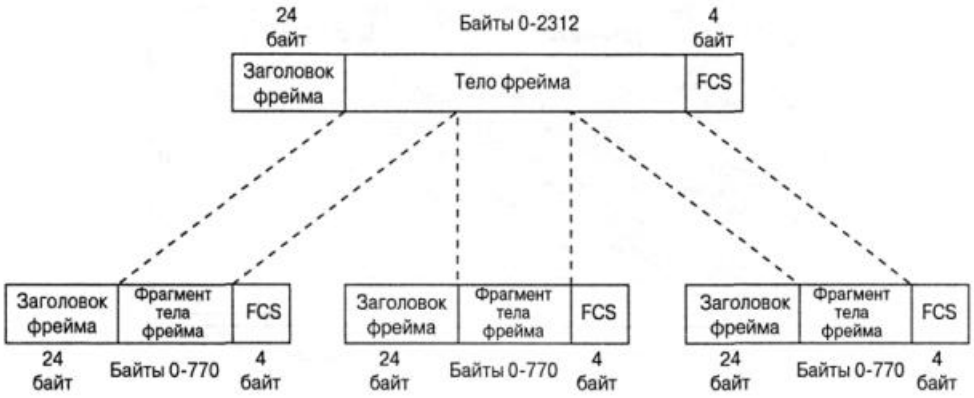


Рисунок 4.5. Фрагментация фрейма.

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.

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 сосуществует с режимом DCF. Оба режима координируются с помощью трех типов межкадровых интервалов (рисунок 4.6).

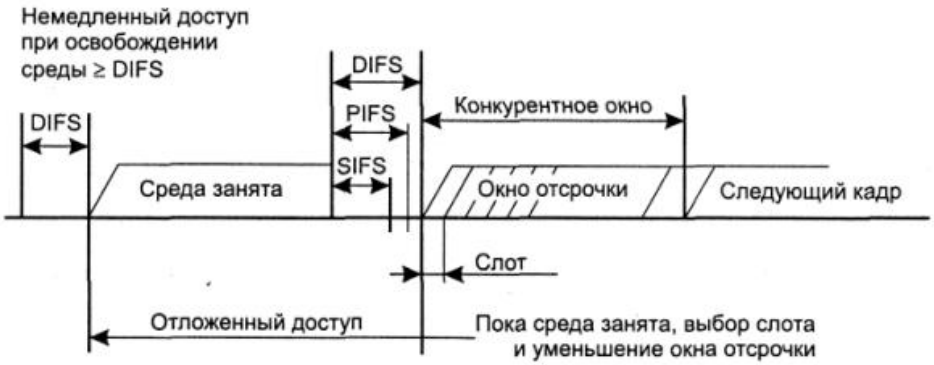


Рисунок 4.6. Сосуществование режимов PCF и DCF.

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.

Рассмотрим следующий предельный случай. Беспроводная сеть сконфигурирована так, что несколько станций с чувствительным ко времени информационным потоком контролируются точечным координатором, тогда как оставшийся поток состязается за доступ с использованием CSMA. Точечный координатор может циклически выпускать запросы ко всем станциям, сконфигурированным для упорядоченного опроса. При запуске запроса опрашиваемая станция может ответить, используя SIFS. Если точечный координатор получает ответ, он выпускает другой запрос, используя PIFS. Если в течение предопределенного времени не получено отклика, координатор выпускает запрос.

Если был реализован порядок, описанный в предыдущем абзаце, точечный координатор может заблокировать весь асинхронный поток, выпуская повторные запросы. Для предотвращения блокировки определяется интервал, известный как суперкадр (superframe). В течение первой части этого интервала точечный координатор циклически выпускает запросы ко всем станциям, сконфигурированным для упорядоченного опроса. Затем точечный координатор выключается на оставшееся время, давая возможность станциям посоревноваться за асинхронный доступ.

Использование суперкадра показано на рисунке 4.7. В начале суперкадра точечный координатор может захватить управление и выпускать запросы в течение данного периода времени. Этот промежуток переменный, поскольку опрашиваемые станции выпускают кадры переменного размера. К оставшейся части суперкадра имеется доступ, определяемый состязанием. В конце интервала суперкадра точечный координатор состязается за доступ к среде, используя PIFS. рели среда свободна, точечный координатор получает немедленный доступ, и Начинается новый период суперкадра. Однако среда может быть занята в конце периода суперкадра. В этом случае точечный координатор должен подождать, пока среда не освободится, и лишь затем получить доступ; в результате сокращается период суперкадра на следующий цикл.

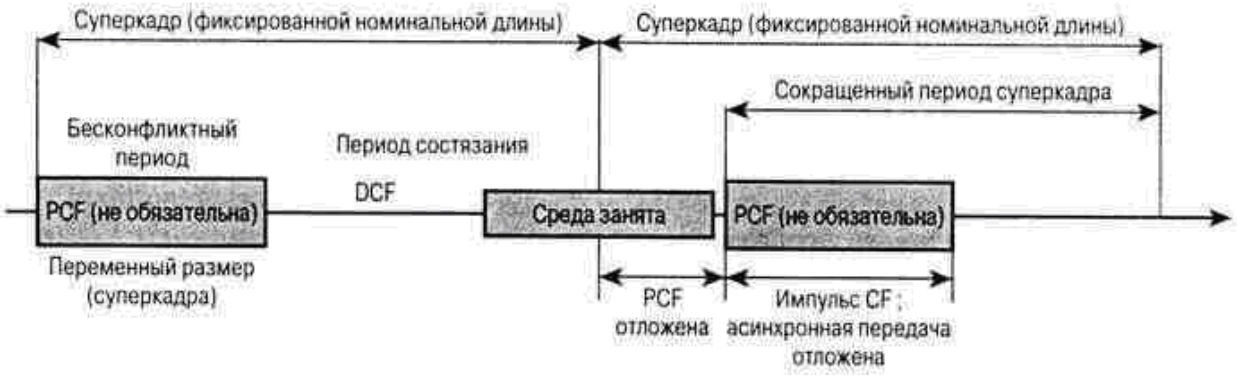
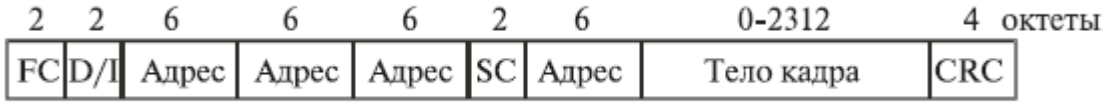


Рисунок 4.7. Структура суперкадра PCF.

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

4.3. Кадр MAC-подуровня

На рисунке 4.8 изображен формат кадра 802.11. Приведенная общая структура применяется для всех информационных и управляющих кадров, хотя не все поля используются во всех случаях.

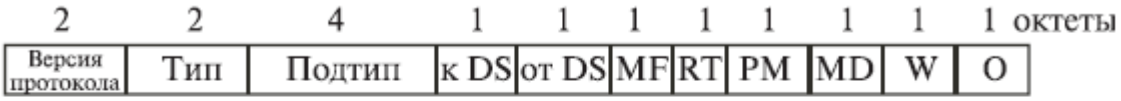


FC — управление кадром
D/I — идентификатор длительности/соединения
SC — управление очередностью

Рисунок 4.8. Формат кадра MAC IEEE 802.11.

Перечислим поля общего кадра:

- ✓ Управление кадром. Указывается тип кадра и предоставляется управляющая информация (объясняется ниже).
- ✓ 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 рисунке 4.9, состоит из следующих полей:
- ✓ Версия протокола.
- ✓ Тип. Определяет тип кадра: контроль, управление или данные.
- ✓ Подтип. Дальнейшая идентификация функций кадра.



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

Рисунок 4.9. Поле управления кадром.

- ✓ К 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.

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. Посылается 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. Посылается 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. Посылается 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 аннуляции ассоциации.
- ✓ Аутентификация. Для аутентификации станций используются множественные кадры.
- ✓ Отмена аутентификации. Передается для прекращения безопасного соединения.

5. 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.

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

Благодаря высокой скорости передачи данных (до 54 Мбит/с), а также ориентации на диапазон 2,4 ГГц, стандарт IEEE 802.11g завоевал наибольшую популярность у производителей оборудования для беспроводных сетей.

Поскольку оборудование, работающее на максимальной скорости 54 Мбит/с, имеет меньший радиус действия, чем на более низких скоростях, стандартом 802.11g предусмотрено автоматическое снижение скорости при ухудшении качества сигнала.

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.

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

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 и позволила использовать дополнительные высокоскоростные физические уровни, описанные в стандартах 802.11b, 802.11a и 802.11g.

Каждый из физических уровней стандарта 802.11 имеет два подуровня:

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

На рисунке 5.1 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.

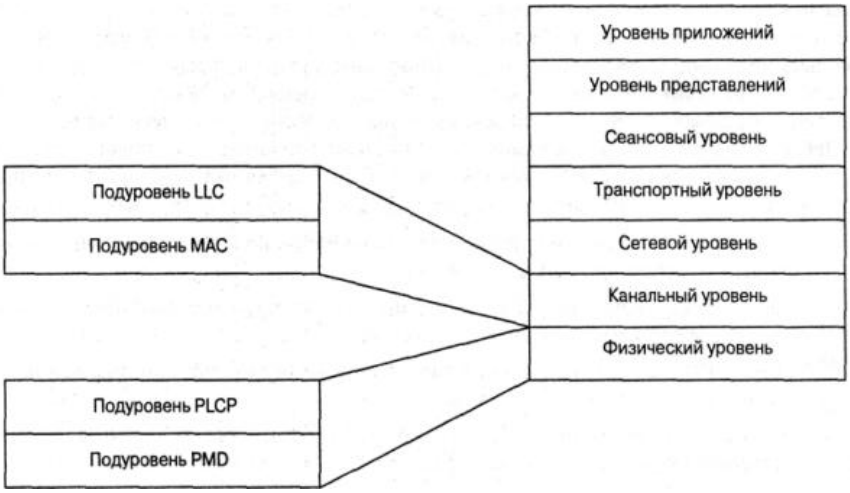


Рисунок 5.1. Подуровни уровня PHY.

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.

5.1. IEEE 802.11

Исходный стандарт IEEE 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.

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.

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 рисунке 5.2 представлен формат фрейма FHSS подуровня PLCP.

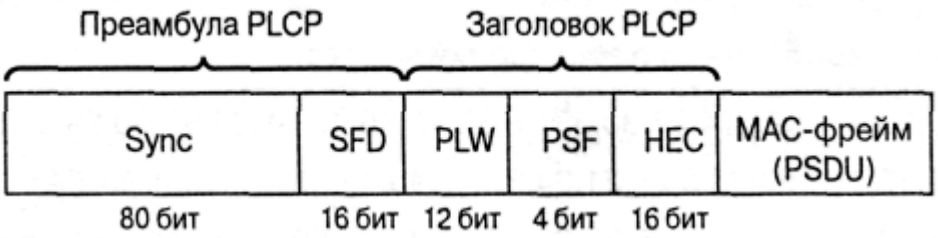


Рисунок 5.2. Формат фрейма FHSS подуровня PLCP.

Преамбула PLCP состоит из двух подполей:

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

Заголовок фрейма PLCP состоит из трех подполей:

- ✓ Слово длины служебного элемента данных PLCP (PSDU), PSDU Length Word (PLW) размером 12 бит. Указывает размер фрейма MAC (PSDU) в октетах.
- ✓ Сигнальное поле PLCP (Signaling Field PLCP - PSF) размером 4 бит. Указывает скорость передачи данных конкретного фрейма.
- ✓ HEC (Header Error Check). Контрольная сумма фрейма.

Служебный элемент данных PLCP (PSDU) проходит через операцию скремблирования с целью отбеливания (рандомизации) последовательности входных битов. Получившийся в результате PSDU представлен на рисунке 5.3. 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.

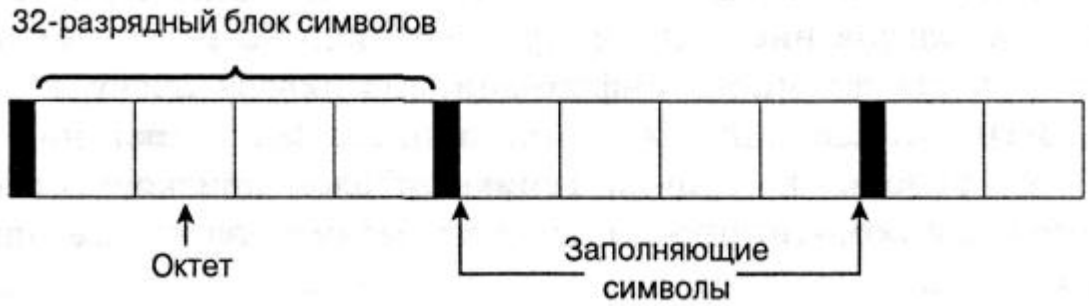


Рисунок 5.3. Скремблированный PSDU в технологии FHSS.

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 рисунке 5.4.

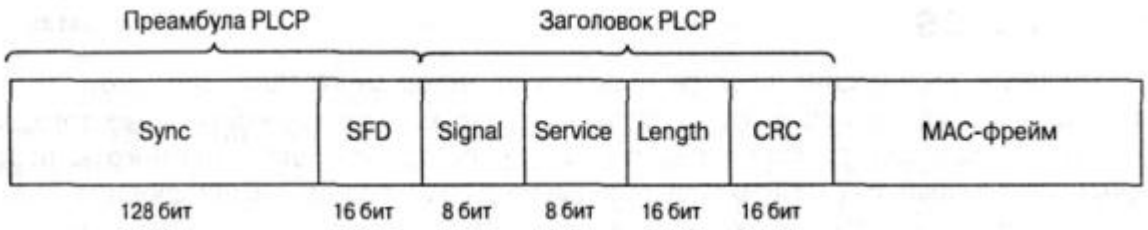


Рисунок 5.4. Формат фрейма DSSS подуровня PLCP.

Преамбула PLCP состоит из двух подполей:

- ✓ Подполе Sync шириной 128 бит, представляющее собой строку, состоящую из единиц. Задача этого подполя - обеспечить синхронизацию для приемной станции.
- ✓ Подполе SFD шириной 16 бит; в нем содержится специфичная строка OxF3A0; 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.

5.2. IEEE 802.11b

На физическом уровне к MAC-кадрам (MPDU) добавляется заголовок физического уровня, состоящий из преамбулы и собственно PLCP-заголовка (рисунок 5.5).

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 PBSS-модуляции) и LENGTH (время в микросекундах, необходимое для передачи следующей за заголовком части кадра). Все три поля заголовка защищены 16-битной контрольной суммой CRC.

Рисунок 5.5. Структура кадров сети IEEE 802.11b физического уровня.

В стандарте IEEE 802.11b предусмотрено два типа заголовков: длинный и короткий (рисунок 5.6).

Рисунок 5.6. 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 CCK-модуляция (Complementary Code Keying - кодирование комплементарным кодом).

5.3. 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 составляет 20 МГц. Несущие модулируют посредством BPSK, QPSK, а также 16- и 64-позиционной квадратурной амплитудной модуляции (QAM). В совокупности с различными скоростями кодирования r (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 5.1 показано, как необходимая скорость передачи данных преобразуется в соответствующие параметры узлов передатчика OFDM.

Таблица 5.1 – 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 OFDM
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48

18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

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 (рисунок 5.7).

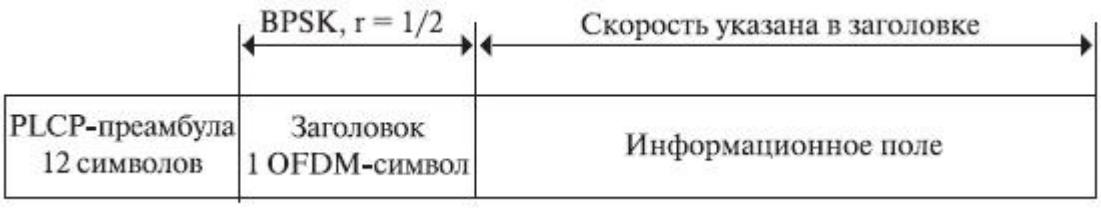


Рисунок 5.7. Структура заголовка физического уровня стандарта IEEE 802.11a.

Кадр включает преамбулу (12 символов синхропоследовательности), заголовок физического уровня (PLCP-заголовок) и собственно информационное поле, сформированное на MAC-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 (рисунок 3.11) 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 переносится в заданную частотную область. При приеме все происходит в обратном порядке.

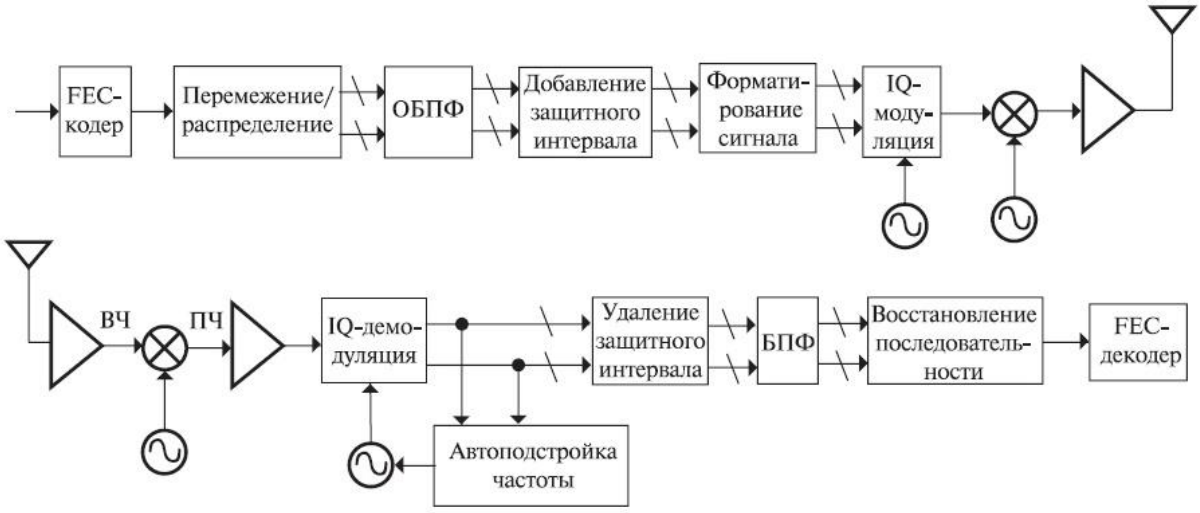


Рисунок 3.11. Функциональная схема трактов приема/передачи стандарта IEEE 802.11a.

5.4. 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 CCK (Complementary Code Keying), а в качестве дополнительной возможности допускается модуляция PBSS.

Разработчики 802.11g предусмотрели CCK-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 (рисунок 5.8).

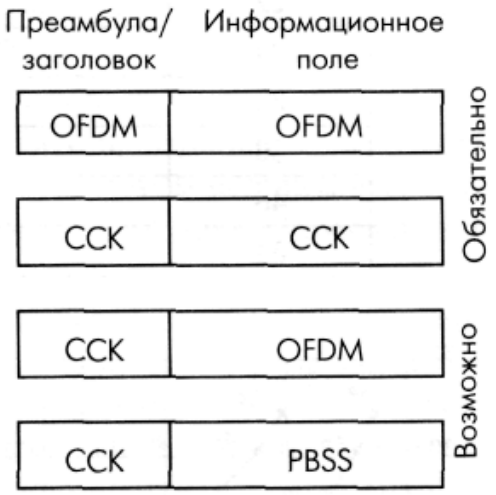


Рисунок 5.8. Кадры IEEE 802.11g в различных режимах модуляции.

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 CCK (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 PBSS, и для достижения компромисса в стандарт 802.11g в качестве дополнительной возможности ввели, так же как и в 802.11b, необязательный режим - PBSS, в котором заголовок и преамбула передаются так же, как и при CCK, а информационное поле модулируется по схеме PBSS 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 5.2.

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 PBSS 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 5.2 представлена сводная информация по параметрам физических уровней.

Таблица 5.2 – Стандарты физического уровня.

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

5.5. IEEE 802.11d

Стандарт IEEE 802.11d определяет параметры физических каналов и сетевого оборудования. Он описывает правила, касающиеся разрешенной мощности излучения передатчиков в диапазонах частот, допустимых законами. Этот стандарт очень важен, поскольку для работы сетевого оборудования используются радиоволны. Если они не будут соответствовать указанным параметрам, то могут помешать другим устройствам, работающим в этом или близлежащем диапазоне частот.

5.6. IEEE 802.11e

Поскольку по сети могут передаваться данные разных форматов и важности, существует потребность в механизме, который бы определял их важность и присваивал необходимый приоритет. За это отвечает стандарт IEEE 802.11e, специально разработанный с целью передачи потоковых видео- или аудиоданных с гарантированными качеством и доставкой.

5.7. IEEE 802.11f

Стандарт IEEE 802.11f разработан с целью обеспечения аутентификации сетевого оборудования (рабочей станции) при перемещении компьютера пользователя от одной точки доступа к другой, то есть между сегментами сети. При этом вступает в действие протокол обмена служебной информацией IAPP (Inter-Access Point Protocol), который необходим для передачи данных между точками доступа. При этом достигается эффективная организация работы распределенных беспроводных сетей.

5.8. IEEE 802.11h

Стандарт IEEE 802.11h разработан с целью эффективного управления мощностью излучения передатчика, выбором несущей частоты передачи и генерации нужных отчетов. Он вносит некоторые новые алгоритмы в протокол доступа к среде MAC (Media Access Control, управление доступом к среде), а также в физический уровень стандарта IEEE 802.11a. В первую очередь это связано с тем, что в некоторых странах диапазон 5 ГГц используется для трансляции спутникового телевидения, для радарного слежения за объектами и т. п., что может вносить помехи в работу передатчиков беспроводной сети.

Смысл работы алгоритмов стандарта IEEE 802.11h заключается в том, что при обнаружении отраженных сигналов (интерференции) компьютеры беспроводной сети (или передатчики) могут динамически переходить в другой диапазон, а также понижать или повышать мощность передатчиков. Это позволяет эффективнее организовать работу уличных и офисных радиосетей.

5.9. IEEE 802.11i

Стандарт IEEE 802.11i разработан специально для повышения безопасности работы беспроводной сети. С этой целью созданы разные алгоритмы шифрования и аутентификации, функции защиты при обмене информацией, возможность генерирования ключей и т. д.:

- ✓ AES (Advanced Encryption Standard, передовой алгоритм шифрования данных) – алгоритм шифрования, который позволяет работать с ключами длиной 128, 192 и 256 бит;
- ✓ RADIUS (Remote Authentication Dial-In User Service, служба дистанционной аутентификации пользователя) – система аутентификации с возможностью генерирования ключей для каждой сессии и управления ими, включающая в себя алгоритмы проверки подлинности пакетов и т. д.;
- ✓ TKIP (Temporal Key Integrity Protocol, протокол целостности временных ключей) – алгоритм шифрования данных;
- ✓ WRAP (Wireless Robust Authenticated Protocol, устойчивый беспроводной протокол аутентификации) – алгоритм шифрования данных;
- ✓ CCMP (Counter with Cipher Block Chaining Message Authentication Code Protocol) – алгоритм шифрования данных.

5.10. IEEE 802.11n

На сегодняшний день стандарт IEEE 802.11n – самый перспективный из всех стандартов, касающихся беспроводных сетей. К сожалению, пока он только разрабатывается, но возможности, которые он открывает, выглядят очень заманчиво.

Данный стандарт должен обеспечить скорость передачи данных, минимальным значением которой будет 300 Мбит/с, что фактически равняется наиболее распространенной скоростью в проводных сетях стандарта Fast Ethernet.

IEEE 802.11n будет использовать метод ортогонального частотного мультиплексирования (OFDM) и квадратурную амплитудную модуляцию (QAM). Это должно обеспечить не только высокую скорость передачи данных, но и полную совместимость со стандартами IEEE 802.11a/b/g.

6. Режимы работы беспроводного оборудования

6.1. Точка доступа

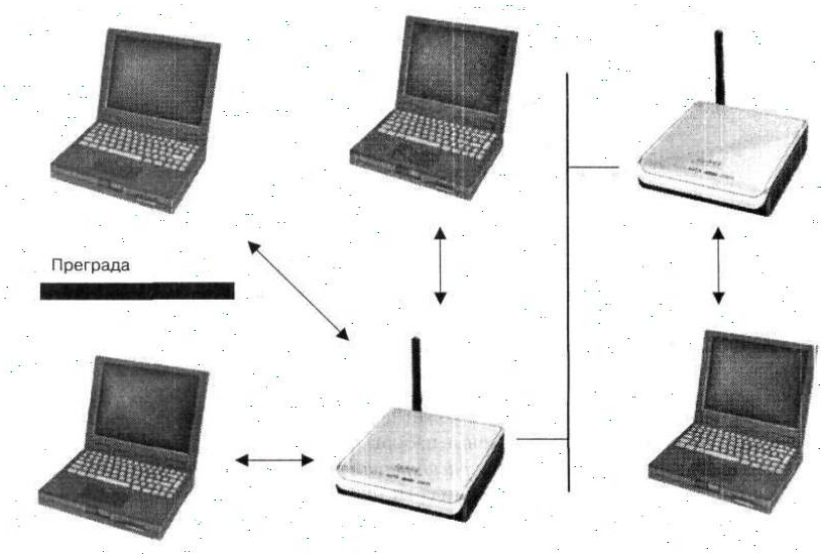


Рисунок 6.1. Точка доступа.

Режим «Точка доступа» обеспечивает подключения устройств в сеть в инфраструктурной конфигурации. Точка доступа имеет сетевой интерфейс, при помощи которого она может быть подключена к обычной проводной сети. В общем случае принцип работы точки доступа прост. Она принимает сигнал на входном интерфейсе, и передает усиленный сигнал на выходной интерфейс.

6.2. 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 (рисунок 6.2).

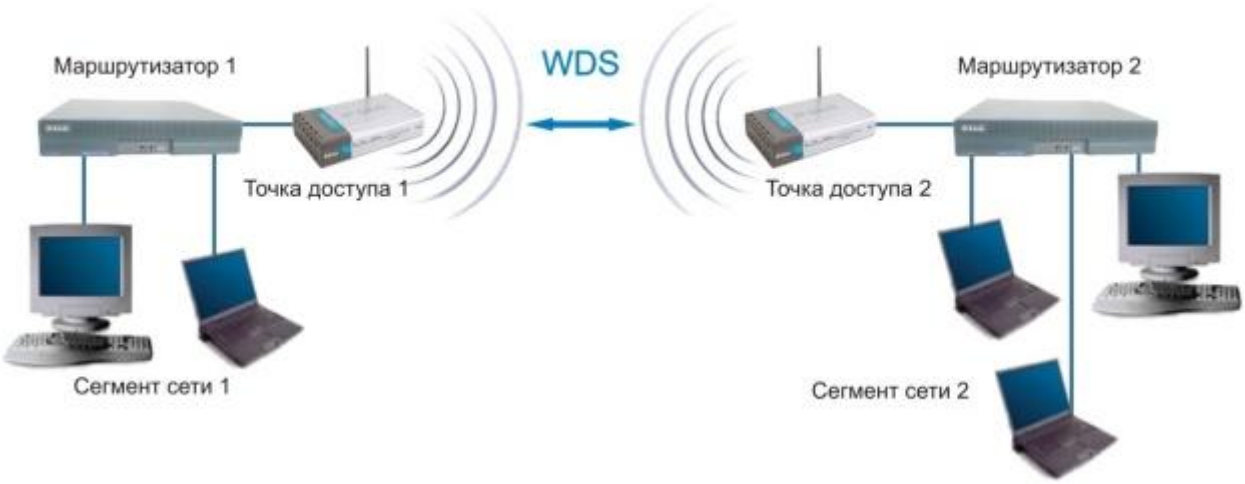


Рисунок 6.2. Режим моста.

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 (рисунок 6.3).

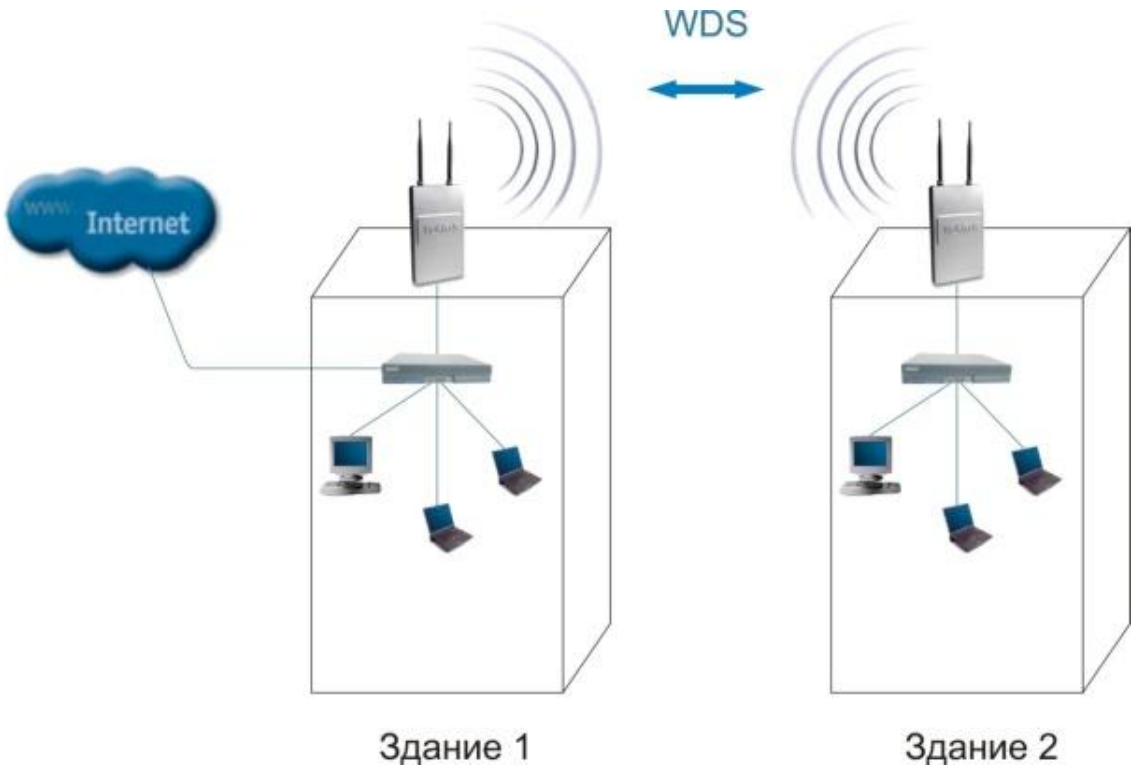


Рисунок 6.3. Мостовой режим между зданиями.

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 (рисунок 6.4). Это позволяет достичь существенной экономии оборудования и упростить топологию сети. Данная технология поддерживается большинством современных точек доступа.

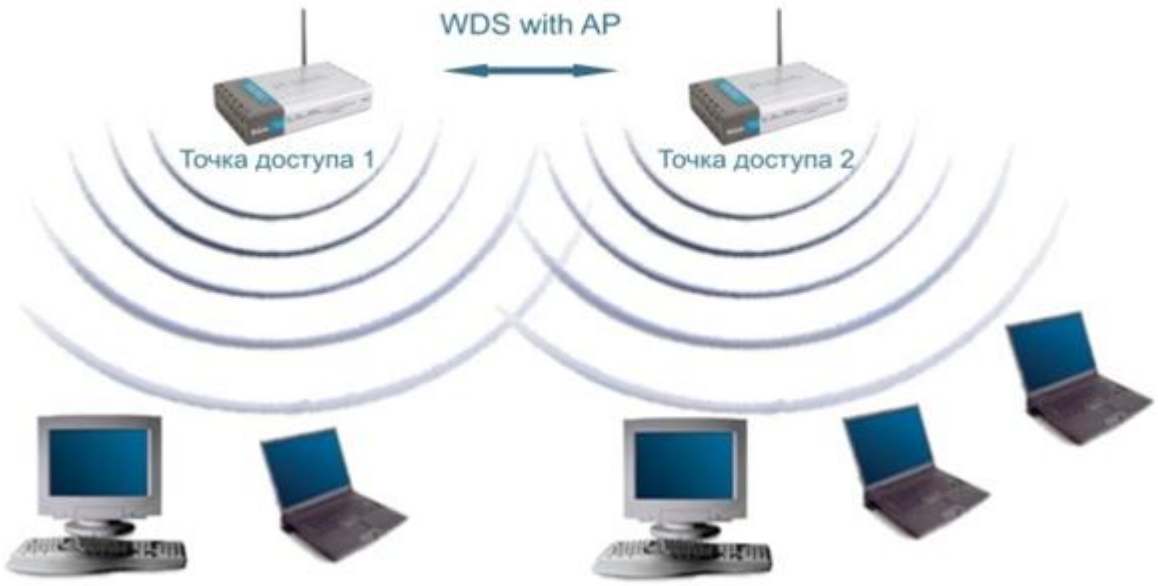


Рисунок 6.4. Режим WDS with AP.

6.3. Режим повторителя

Может возникнуть ситуация, когда оказывается невозможно (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) (рисунок 6.5).

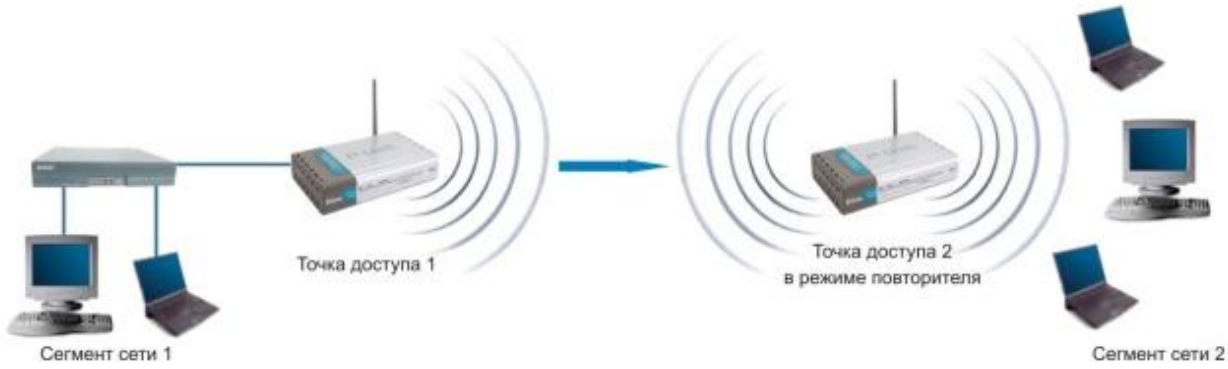


Рисунок 6.5. Режим повторителя.

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.

6.4. Режим клиента точки доступа

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" (рисунок 6.6).

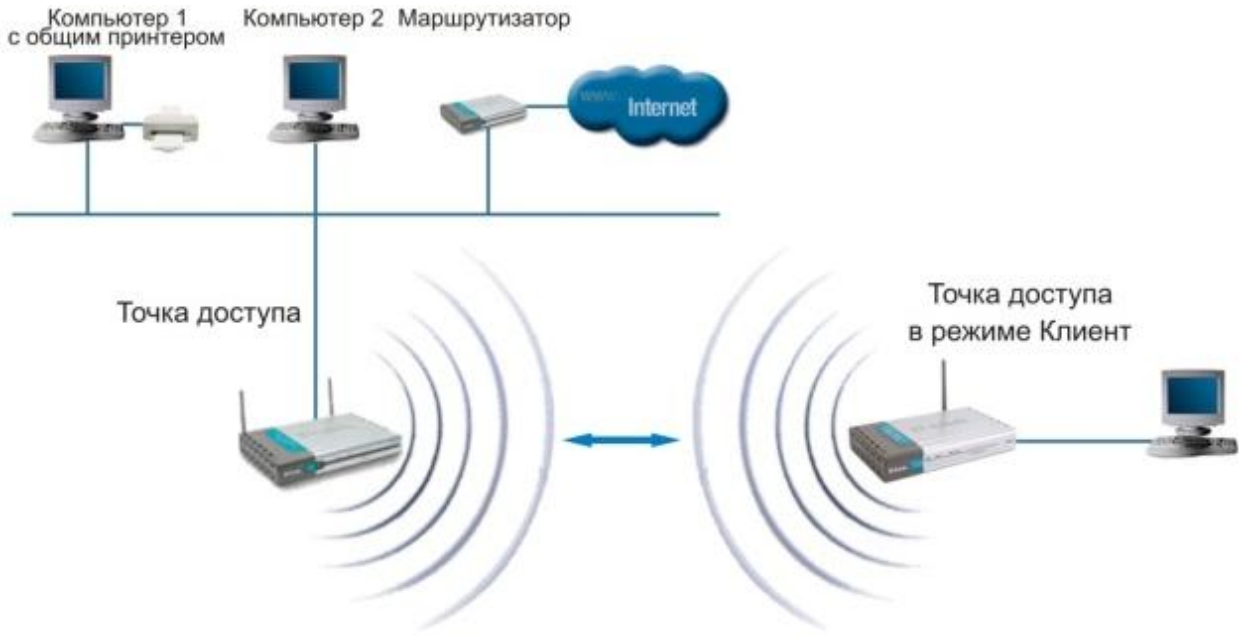


Рисунок 6.6. Режим клиента.

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.

Рисунок 6.7. Режим клиента маршрутизатора WISP.

6.5. Режим клиента маршрутизатора WISP

В такой схеме компьютеры подключаются к точке доступа по обычной витой паре, а к поставщику Интернет-услуг устройство подключается уже по Wi-Fi.

6.6. Режим повторителя WISP

В такой схеме компьютеры подключаются к точке доступа по обычной витой паре и так же портативные компьютеры, а к поставщику Интернет-услуг устройство подключается уже по Wi-Fi.

Рисунок 6.8. Режим повторителя WISP.

7. Защита информации в беспроводных сетях

7.1. Классификация механизмов безопасности в сетях Wi-Fi

В современных беспроводных Wi-Fi сетях имеется следующий набор механизмов, обеспечивающих безопасность работы пользователя и конфиденциальность передаваемой информации. Данный набор представлен на рисунке 7.1.

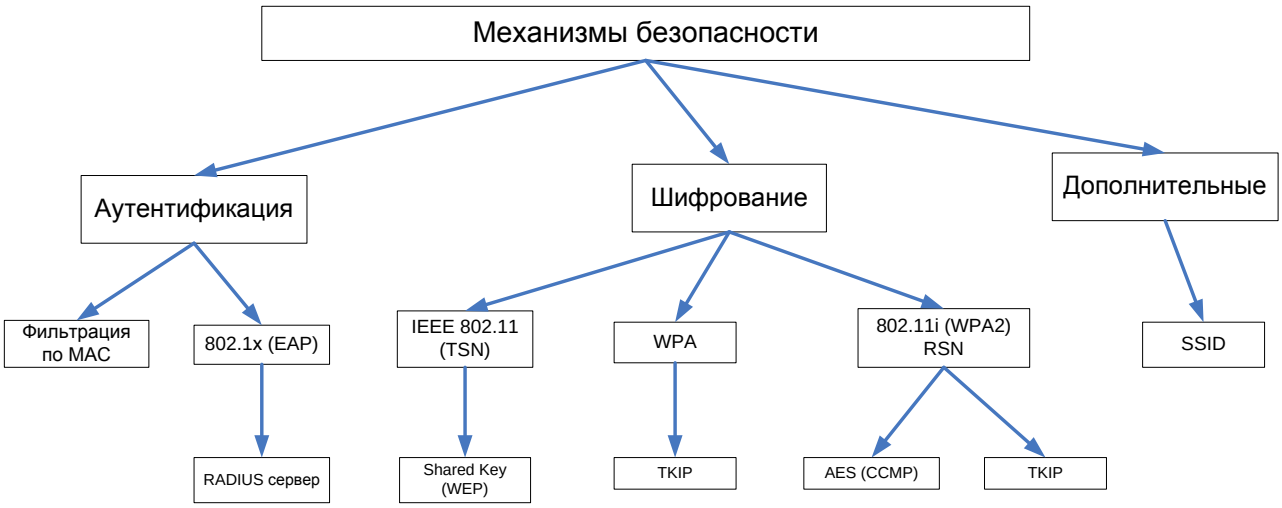


Рисунок 7.1. Классификация механизмов безопасности в Wi-Fi сетях.

7.2. Механизмы шифрования

Механизм шифрования WEP (IEEE 802.11)

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.

Алгоритм инициализации RC4 приведен ниже.

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.

Начальное заполнение массива:

```
for i = 0 to 2n – 1
{
      S[i] = i
      j = 0
}
```

Скрэмблирование:

```
for i = 0 to 2n – 1
{
      j = j + S[i] + Key[i mod l]
      Перестановка (S[i], S[j])
}
```

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.

Инициализация:

```
i = 0
j = 0
```

Цикл генерации:

```
i = i + 1
j = j + S[i]
```

Перестановка `(S[i], S[j])`

Результат: `K = S[S[i] + S[j]]`.

Особенности WEP-протокола:

1. Достаточно устойчив к атакам, связанным с простым перебором ключей шифрования, что обеспечивается необходимой длиной ключа и частотой смены ключей и инициализирующего вектора.

2. Самосинхронизация для каждого сообщения. Это свойство является ключевым для протоколов уровня доступа к среде передачи, где велико число искаженных и потерянных пакетов.
3. Эффективность: WEP легко реализовать.
4. Открытость.
5. 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 (рисунок 7.2).

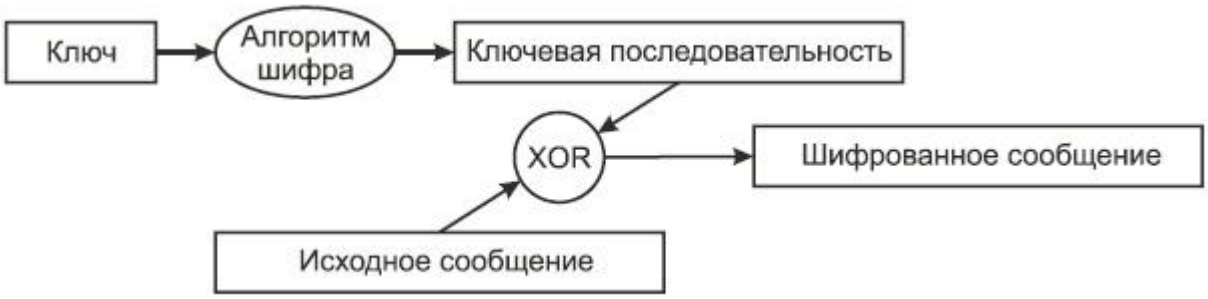


Рисунок 7.2. Потоковое шифрование.

Блочное шифрование

Блочное шифрование работает с блоками заранее определенной длины, не меняющейся 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 (рисунок 7.3). 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.

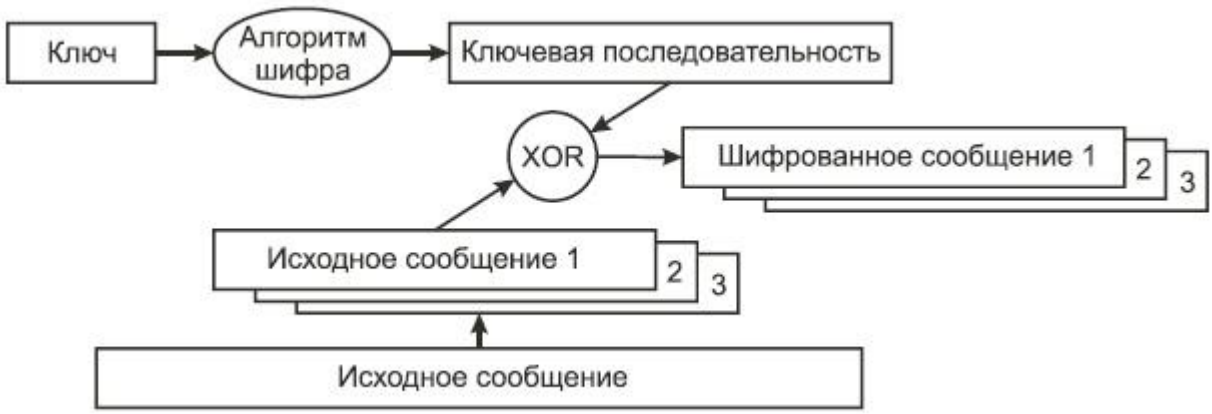


Рисунок 7.3. Блочное шифрование.

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 рисунке 7.4 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.

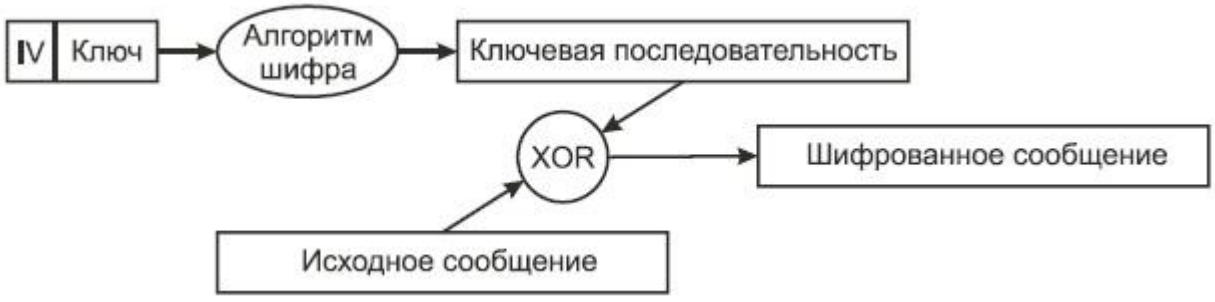


Рисунок 7.4. Алгоритм шифрования WEP.

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*8 = 40) или 10 шестнадцатеричных чисел (10*4 = 40), и при 104-битном эффективном ключе вводятся 13 байтовых ASCII-символов (13*8 = 104) или 26 шестнадцатеричных чисел (26*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.

Спецификация WPA

До мая 2001г. 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, предусмотрев 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 W-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:

- ✓ покадровое изменение ключей шифрования. WEP-ключ быстро изменяется, и для каждого кадра 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 рисунке 7.5 представлен образец 48-разрядного IV и показано, как он разбивается на части для использования при пофреймовом изменении ключа.

Рисунок 7.5. Разбиение 48-разрядного IV.

Процесс пофреймового изменения ключа можно разбить на следующие этапы (рисунок 7.6):

- ✓ 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;
- ✓ ключ 1-й фазы снова перемешивается с IV и MAC-адресом передатчика для выработки значения пофреймового ключа;
- ✓ 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;
- ✓ пофреймовый ключ применяется для WEP-шифрования фрейма данных.

Когда 16-битовое пространство IV оказывается исчерпанным, ключ 1-й фазы отбрасывается и 32 старших разряда увеличиваются на 1. Значение пофреймового ключа вычисляется заново, как на этапе 2.

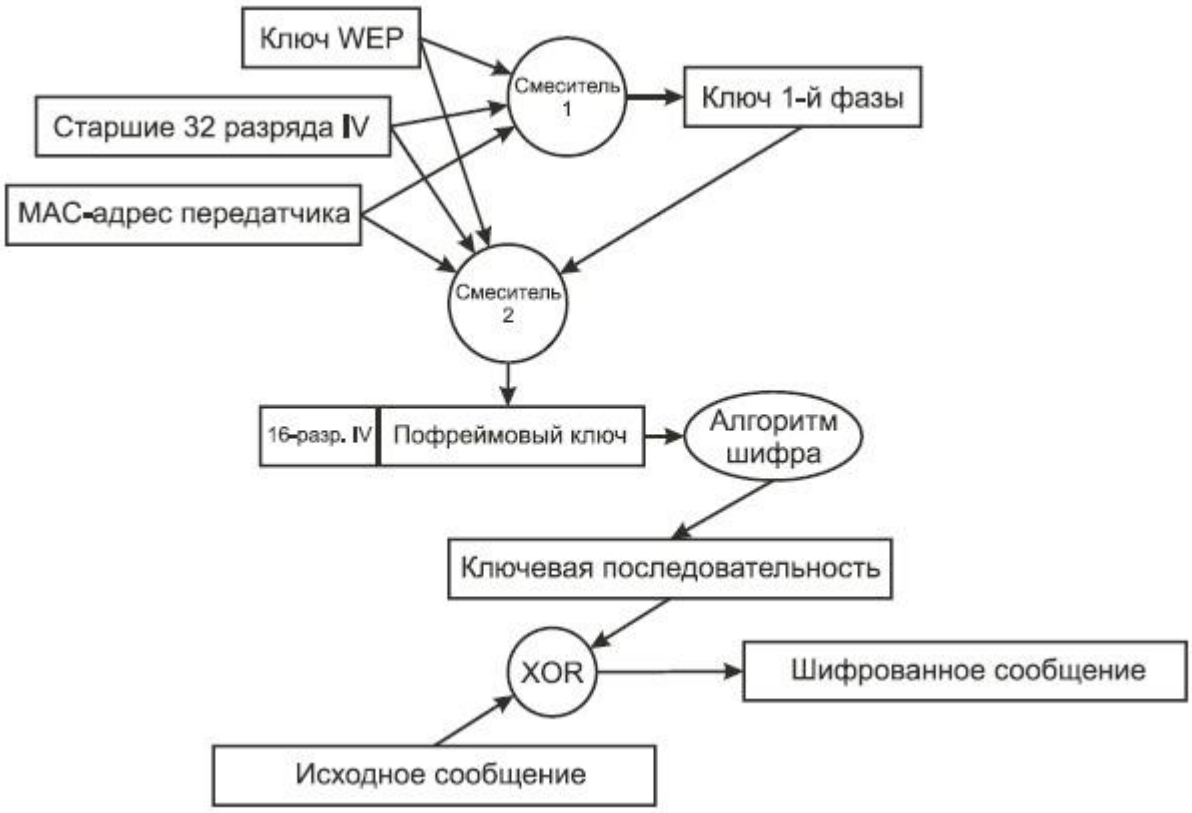


Рисунок 7.6. Процесс создания шифрованного сообщения в WPA.

Процесс пофреймового изменения ключа можно разбить на следующие этапы.

- ✓ устройство инициализирует IV, присваивая ему значение 0. В двоичном представлении это будет значение 00000000000000000000000000000000 00000000000000000;
- ✓ 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 устраняются без замены существующего оборудования. Следует отметить, что этот алгоритм (и TKIP в целом) разработан с целью устранить 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 рисунке 7.7 показана работа алгоритма Michael MIC.

Рисунок 7.7. Работа алгоритма Michael MIC.

Механизм шифрования TKIP в целом осуществляется следующим образом:

1. С помощью алгоритма пофреймового назначения ключей генерируется пофреймовый ключ (рисунок 7.8).
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.

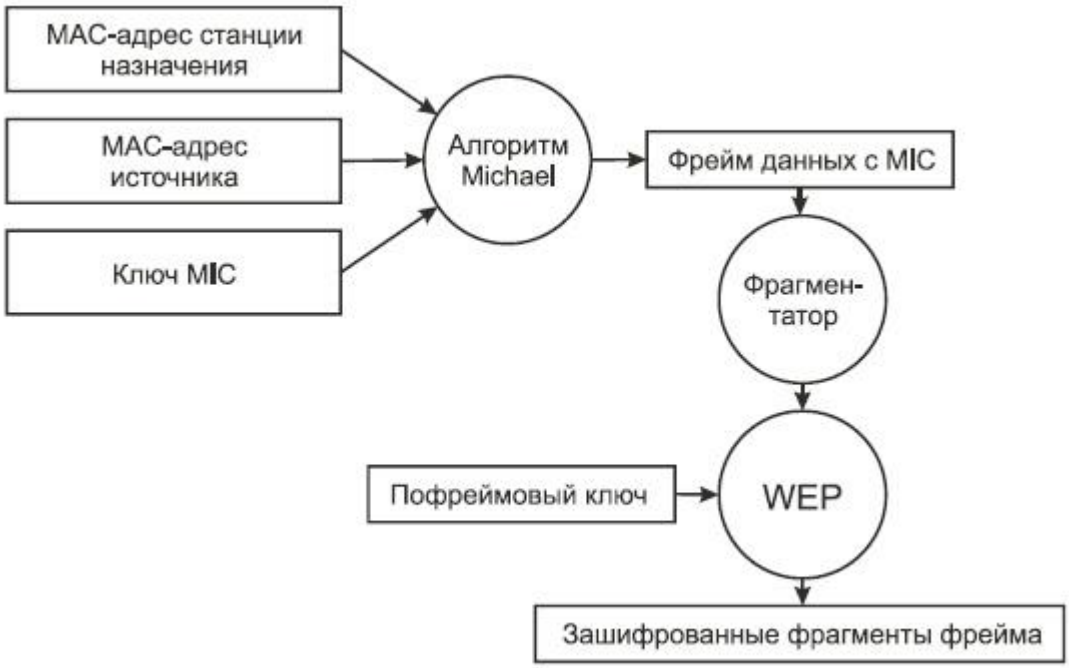


Рисунок 7.8. Механизм шифрования TKIP.

Аналогично процессу шифрования по алгоритму TKIP, процесс дешифрования по этому алгоритму выполняется следующим образом (рисунок 7.9):

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.

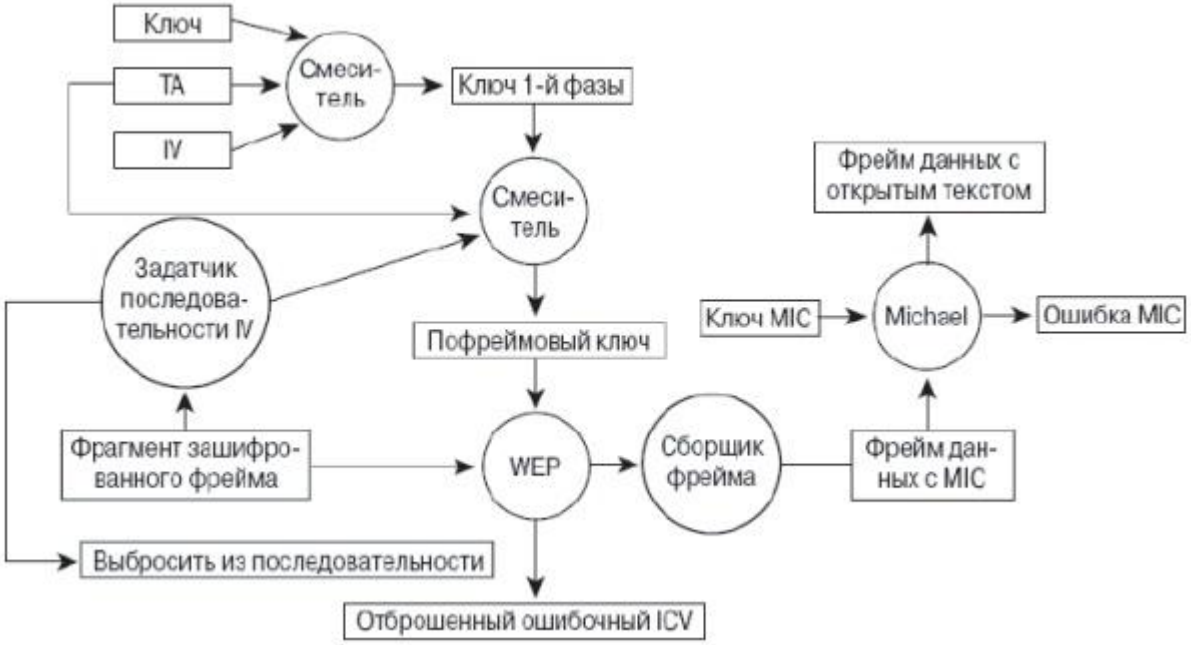


Рисунок 7.9. Механизм дешифровки TKIP.

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.

Стандарт сети 802.11i с повышенной безопасностью (WPA2)

В июне 2004 г. IEEE ратифицировал 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 задействовать 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.

IEEE 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 IEEE 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, IEEE 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.

Шифрование по алгоритму AES

Известно, что шифрование и аутентификация, проводимые в соответствии со стандартом 802.11, имеют слабые стороны, IEEE и WPA усилили алгоритм WEP протоколом TKIP и предлагает сильный механизм шифрования по стандарту 802.11i , обеспечивающий защиту беспроводных LAN стандарта. В тоже время IEEE адаптировал механизм AES для применения его по отношению к разделу, касающемуся защищаемых данных предлагаемого стандарта 802.11i. Компоненты WPA не обеспечивают поддержку шифрования по алгоритму AES.

Алгоритм AES представляет собой следующее поколение средств шифрования. Национальным институтом стандартов и технологий (NITS) США. Названный институт предложил сообществу криптологов разработать новые алгоритмы шифрования. Эти алгоритмы должны быть полностью открыты и использоваться бесплатно. Финалистом и принятым методом стал так называемый алгоритм Рийндела. Как и многие другие шифры, AES требует режима обратной связи во избежание риска, связанного с режимом ECB(режим шифрования с помощью электронных кодов). IEEE разработал режим AES, предназначенный специально для применения в беспроводных локальных сетях. Этот режим называется режим счета сцеплений блоков шифра (Chiper Block Chaining Counter Mode, CBC-CTR) с контролем аутентичности сообщений о сцеплениях блоков шифра (Chiper Block Chaining Message Authenticity Check, CCB-MAC), все вместе это обозначается аббревиатурой AES-CCM. Режим CCM представляет собой комбинацию режима шифрования CBC-CTR и алгоритма контроля аутентичности сообщений CBK-MAC. Эти функции скомбинированы для обеспечения шифрования и проверки целостности сообщений в одном решении.

Алгоритм шифрования CBC-CTR работает с использованием счетчика для пополнения ключевого потока. Значение этого счетчика увеличивается на единицу после шифрования каждого блока. Такой процесс обеспечивает получение уникального ключевого потока для каждого блока. Фрейм с открытым текстом делится на 16-байтовые блоки. После шифрования каждого блока значение счетчика увеличивается на единицу, и так до тех

пор, пока не будут зашифрованы все блоки. Для каждого нового фрейма счетчик переустанавливается.

Алгоритм шифрования CBC-MAC выполняется с использованием результата шифрования CBC по отношению ко всему фрейму, к адресу назначения, адресу источника и данным. Результирующий 128 разрядный выход усекается до 64 бит для использования в передаваемом фрейме.

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

7.3. Аутентификация в беспроводных Wi-Fi сетях

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 (рисунок 7.10):

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

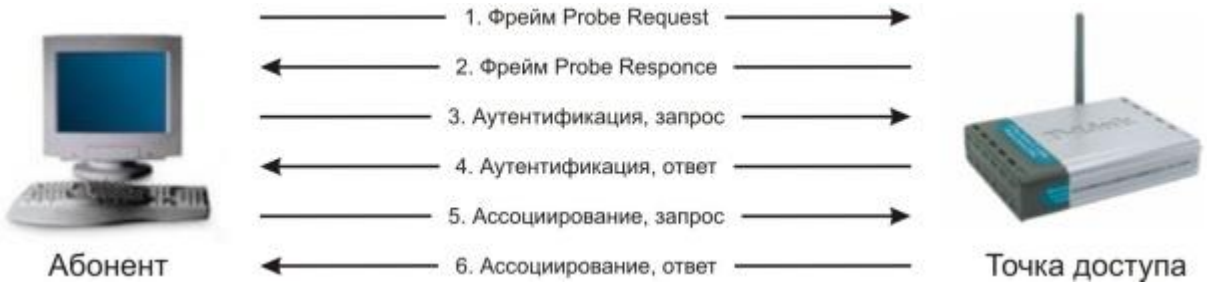


Рисунок 7.10. Аутентификация по стандарту IEEE 802.11.

При активизации беспроводный абонент начинает поиск точек радиодоступа в своей зоне радиовидимости с помощью управляющих фреймов Probe Request. Фреймы Probe Request посылаются 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 (рисунок 7.11).

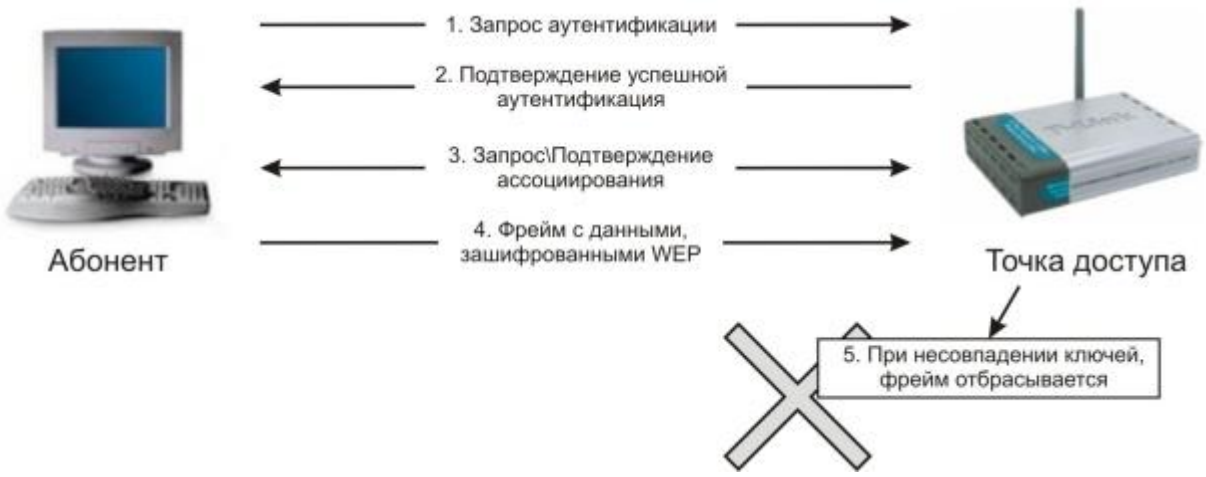


Рисунок 7.11. Открытая аутентификация.

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 рисунок 7.12:

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.

Рисунок 7.12. 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 (рисунок 7.13). 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.

Рисунок 7.13. Аутентификация с помощью внешнего сервера.

Стандарт IEEE 802.1x/EAP (Enterprise-режим)

Проблемы, с которыми столкнулись разработчики и пользователи сетей на основе стандарта IEEE 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 (рисунок 7.14):

1. Клиент (Supplicant) находится в операционной системе абонента.
2. Аутентификатор (Authenticator) находится в программном обеспечении точки радиодоступа.
3. 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.

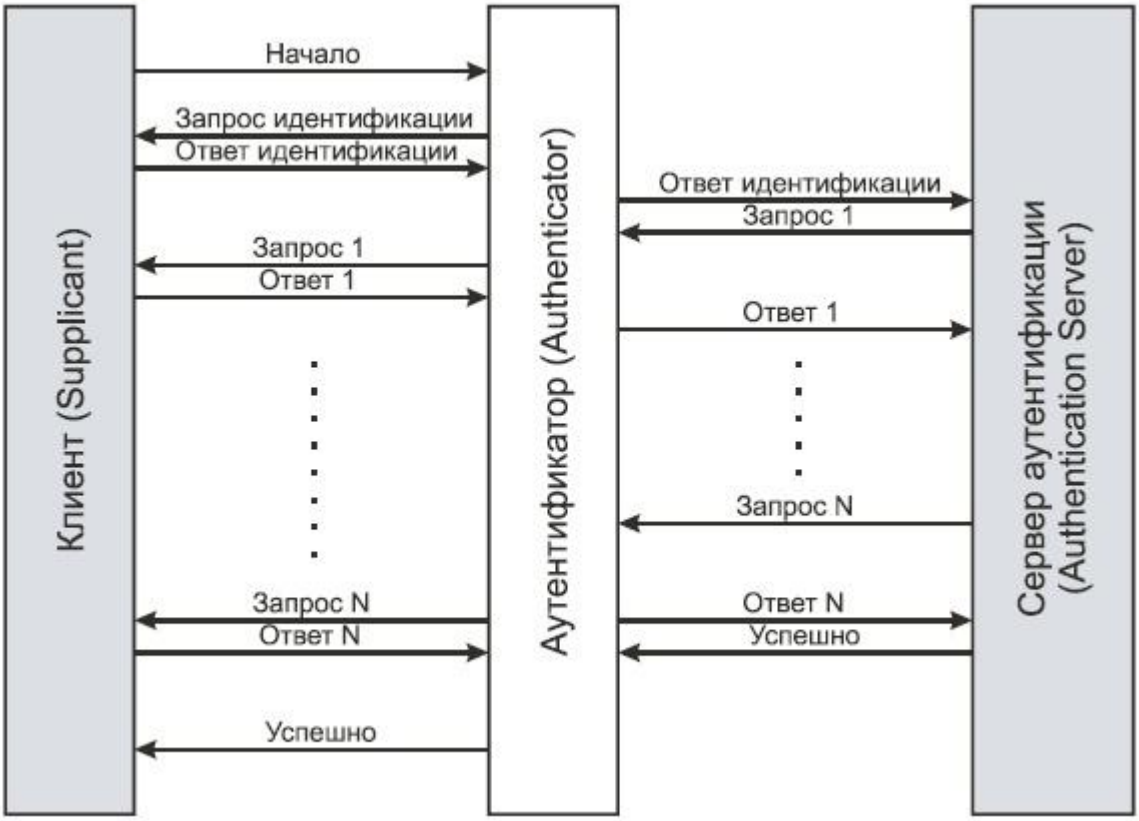


Рисунок 7.14. Архитектура IEEE 802.1x.

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) (рисунок 7.15) 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.

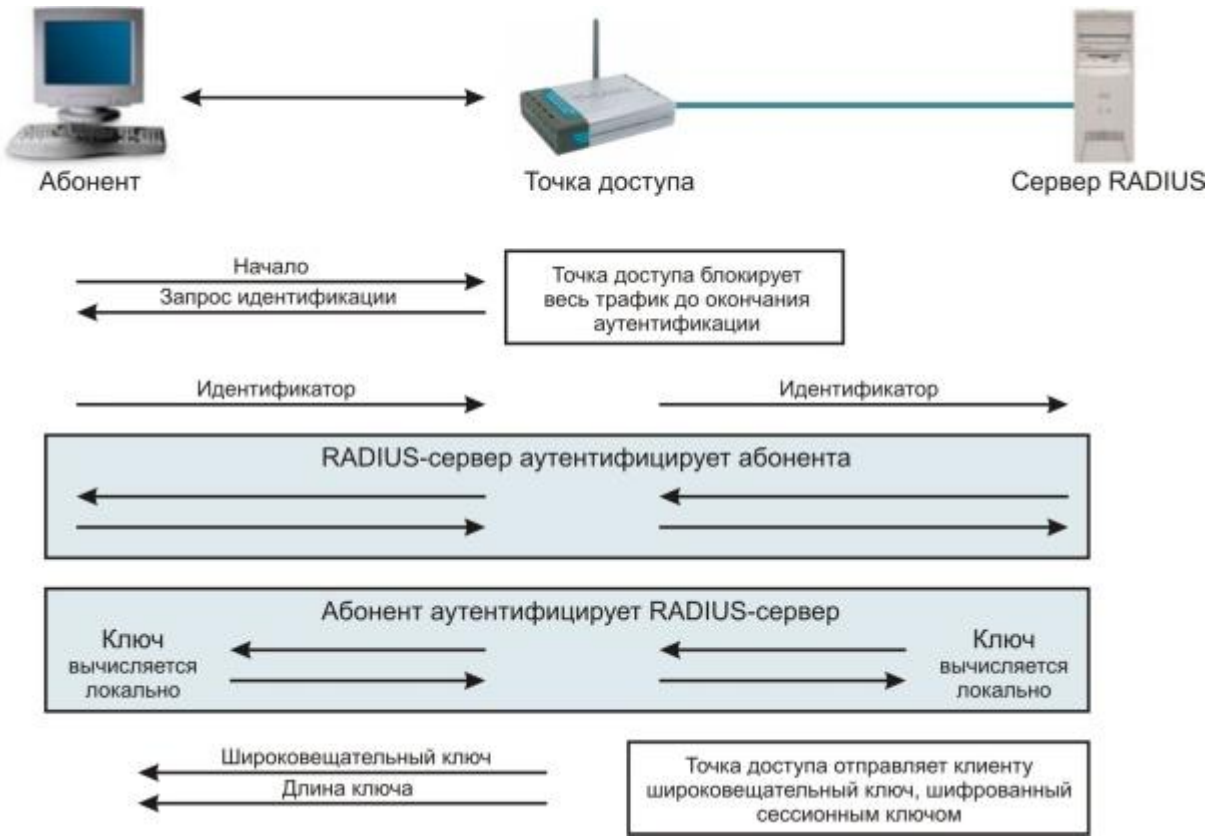


Рисунок 7.15. Обмен сообщениями в 802.1x/EAP.

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).

Механизм генерации ключей шифрования осуществляется следующим образом:

1. Клиент и точка доступа устанавливают динамический ключ (он называется парный мастер-ключ, или PMK, Pairwise Master Key), полученный в процессе аутентификации по стандарту 802.1x.
2. Точка доступа посылает клиенту секретное случайное число, которое называется временный аутентификатор (Authenticator Nonce, ANonce), используя для этого сообщение EAPoL-Key стандарта 802.1x.
3. Этот клиент локально генерирует секретное случайное число, называемое временный проситель (Supplicant Nonce, SNonce).
4. Клиент генерирует парный переходный ключ (Pairwise Transient Key, PTK) путем комбинирования PMK, SNonce, ANonce, MAC-адреса клиента, MAC-адреса точки доступа и строки инициализации. MAC-адреса упорядочены, MAC-адреса низшего порядка предшествуют MAC-адресам высшего порядка. Благодаря этому гарантируется, что клиент и точка доступа "выстроят" MAC-адреса одинаковым образом (рисунок 7.16).
5. Это комбинированное значение пропускается через псевдослучайную функцию (Pseudo Random Function, PRF), чтобы получить 512-разрядный PTK.
6. Клиент посылает число SNonce, сгенерированное им на этапе 3, точке доступа с помощью сообщения EAPoL-Key стандарта 802.1x, 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 посылает сообщение EAPoL-Key, показывающее, что клиент может установить PTK и его ANonce, защищенные ключом EAPoL-Key MIC. Данный этап позволяет клиенту удостовериться в том, что число ANonce, полученное на этапе 2, действительно.
10. Клиент посылает сообщение EAPoL-Key, защищенное ключом EAPoL-Key MIC, указывающее, что ключи установлены.

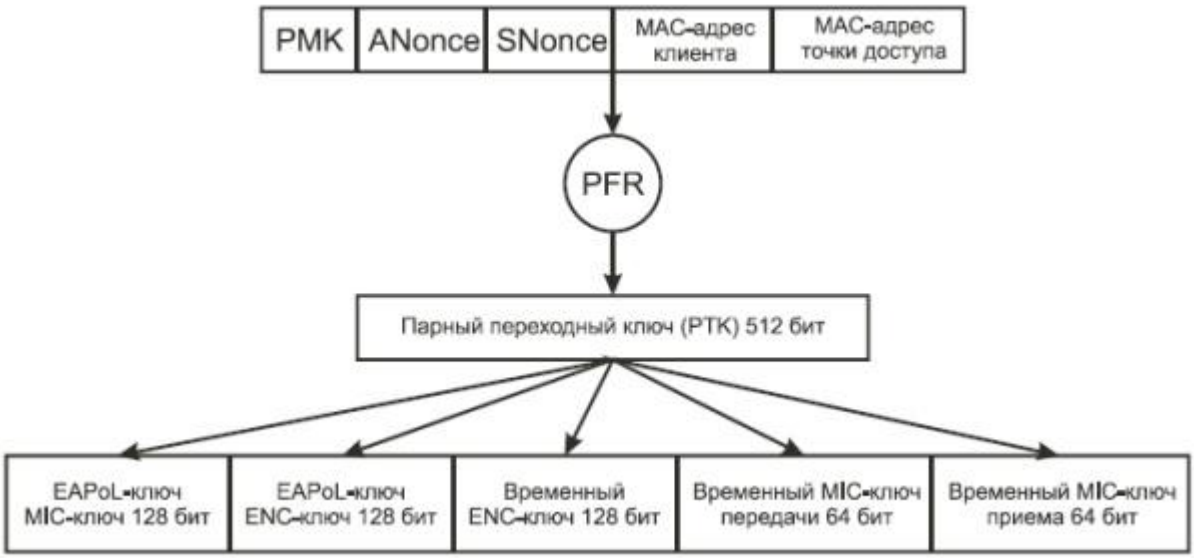


Рисунок 7.16. Генерация парного переходного ключа.

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 посылать 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 рисунке 7.17 представлена иерархия групповых ключей.

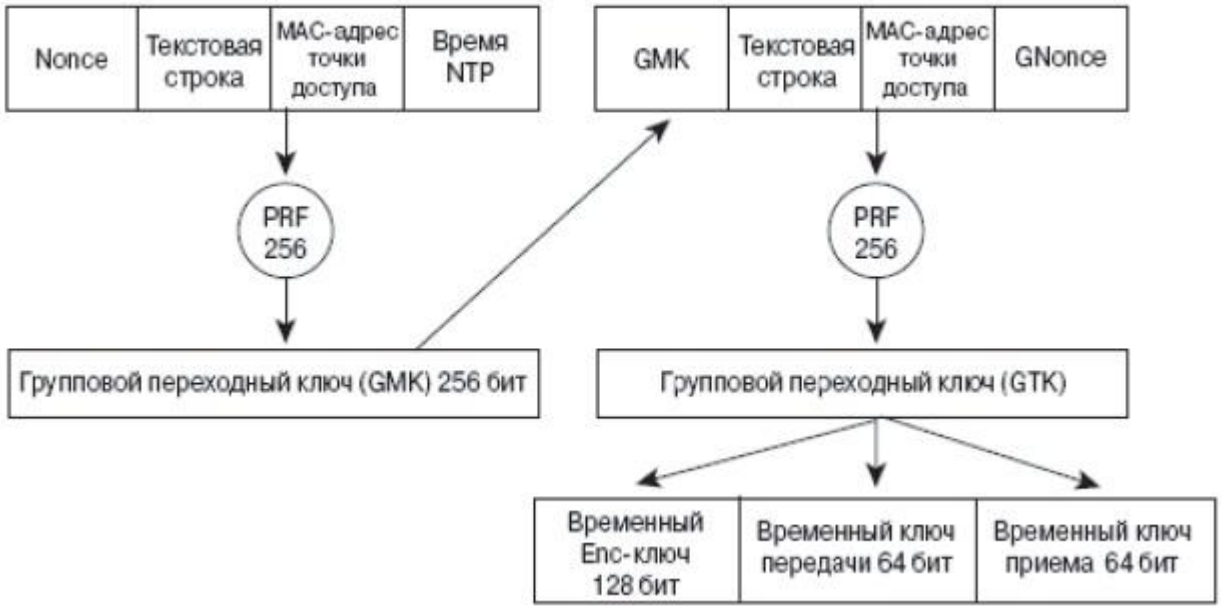


Рисунок 7.17. Иерархия групповых ключей.

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 посылает 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 рисунке 7.18.

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.

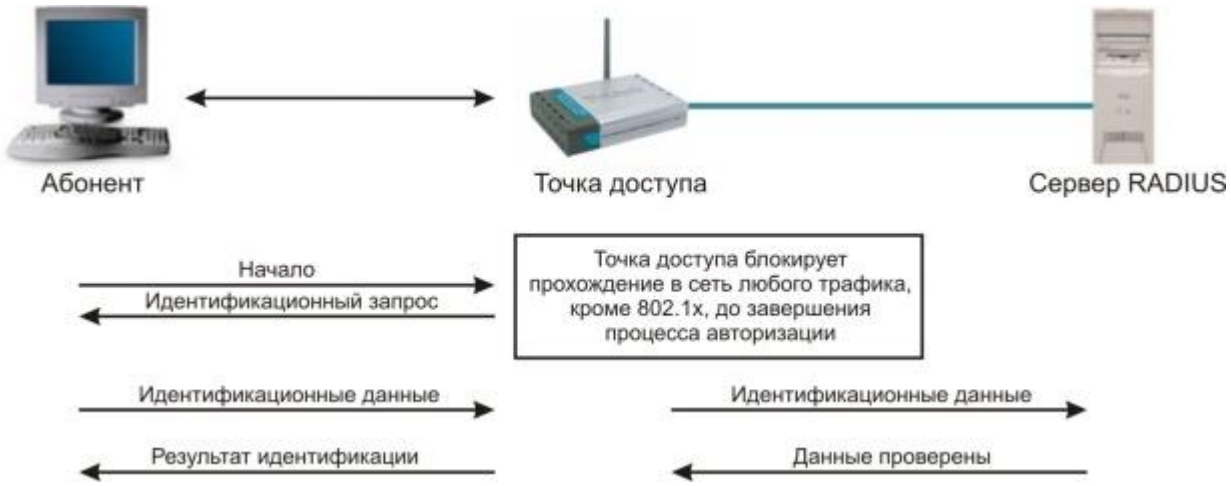


Рис. 7.18. Механизм аутентификации в 802.1x/EAP.

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 (рисунок X).

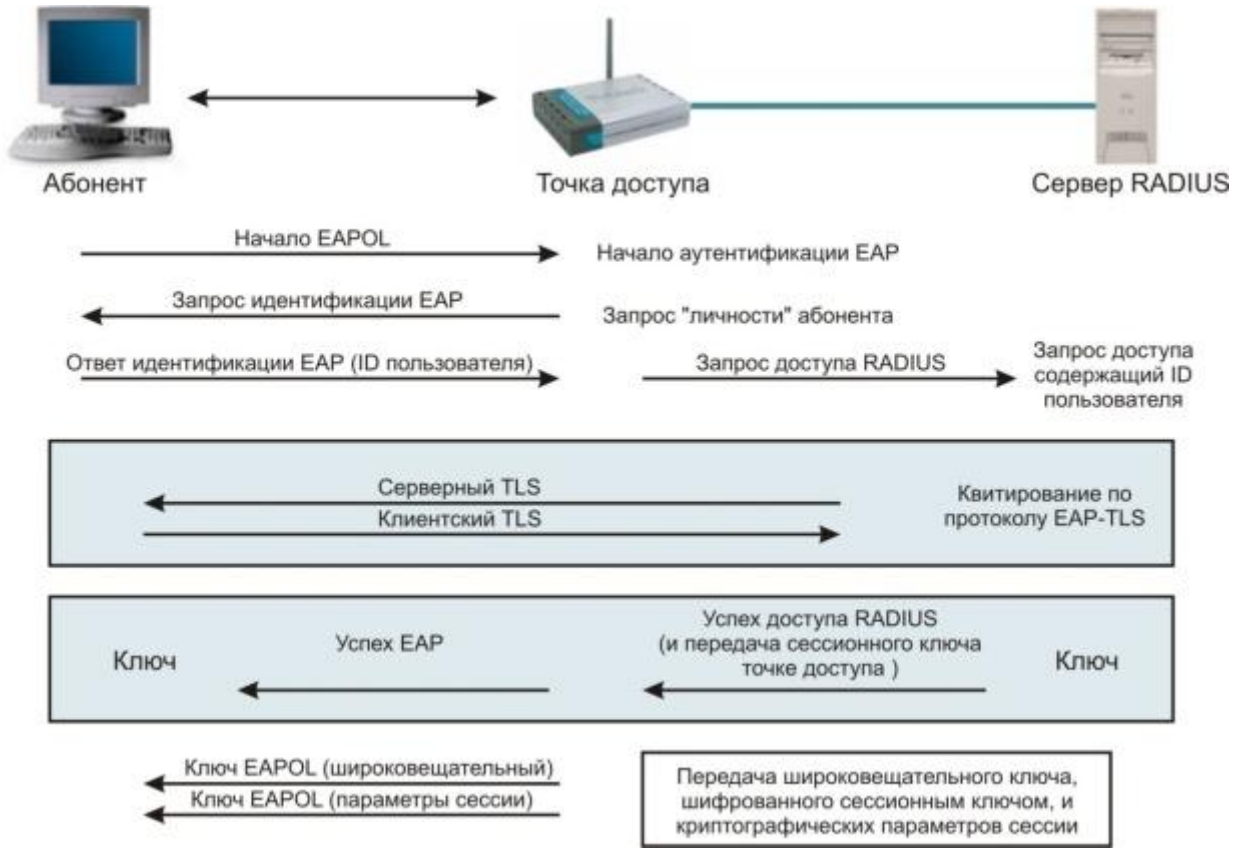


Рисунок X. Процесс аутентификации EAP-TLS.

- ✓ 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 посылает 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 (рисунок X).

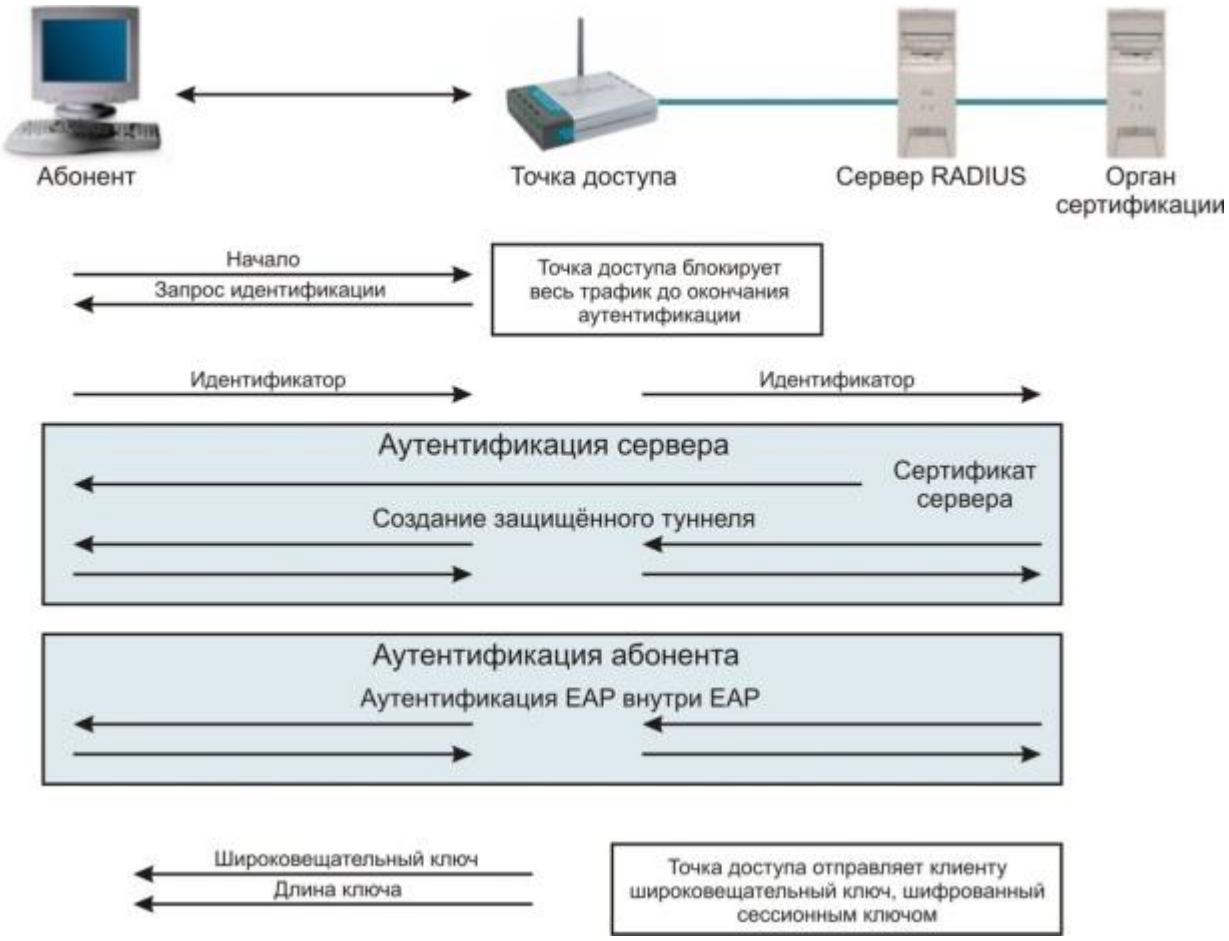


Рисунок X. Процесс аутентификации PEAP.

- ✓ 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 рисунке 7.21. Здесь в качестве механизма обеспечения конфиденциальности и целостности данных выступают стандарты шифрования WPA и WPA2.

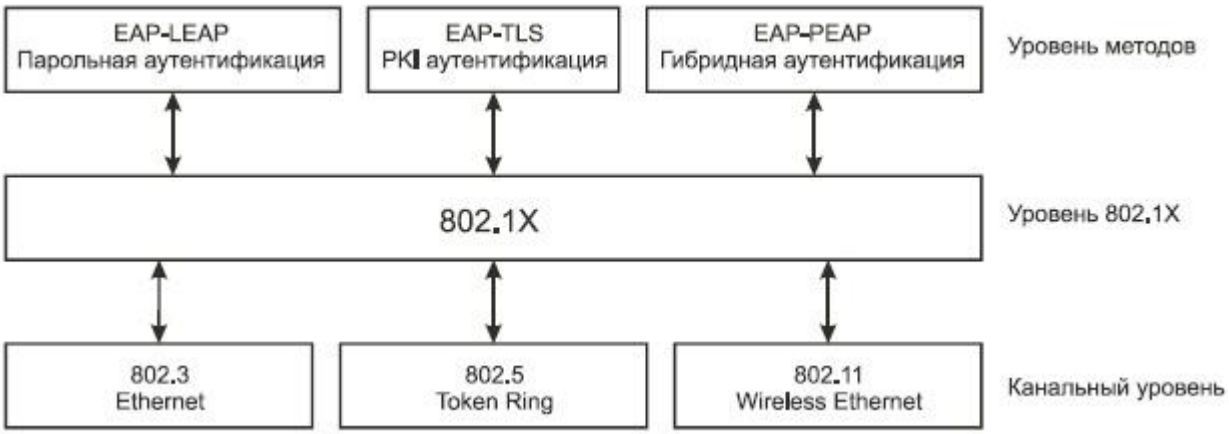


Рисунок X. Уровни архитектуры 802.1x.

7.4. Дополнительные механизмы защиты

SSID

Идентификатор беспроводной сети (SSID) изначально не вошел в состав IEEE 802.11 как базовый механизм защиты. Для подключения к беспроводной сети, нужно знать её имя или SSID. Современные точки доступа оснащены функцией отключения широковещания SSID, т.е. подключится к сети могут только те клиенты которым известен SSID. SSID представляет собой элементарный механизм защиты, но уже сейчас многие сканеры беспроводных сетей способны извлекать имя сети даже при отключение широковещания. Поэтому применения данного механизма хорошо сочетается с другими методами защиты для уменьшения риска взлома беспроводной сети.