

Лекция №3: WI-FI 4/5/6

План лекции:

- I Введение.
- II Топологии сетей стандарта IEEE 802.11.
- III Модель взаимодействия открытых систем OSI и стандарты IEEE 802.11.
- IV Канальный уровень сетей стандарта IEEE 802.11.
- V Формат кадра IEEE 802.11
- VI Набор стандартов IEEE 802.11a/b/g/n/ac/ad.
- VII Дополнительные стандарты IEEE 802.11.
- VIII Безопасность в сетях Wi-Fi. Стандарт IEEE 802.11i.
- IX Мобильность в сетях Wi-Fi. Стандарт IEEE 802.11r/k.
- X Качество обслуживания в сетях Wi-Fi. Стандарт IEEE 802.11e.
- XI Voice Enterprise.
- XII WI-FI 6 vs WI-FI 5, WI-FI 6E.
- XIII Wi-Fi 6E.
- XIV Итог.



I ВВЕДЕНИЕ

Беспроводная локальная сеть WLAN (англ. *Wireless Local Area Network*) – это система передачи данных, которая служит для обеспечения доступа к сети независимо от местоположения абонента, т.к. соединение осуществляется с помощью радиоволн.

Построение локальных беспроводных сетей происходит на основе стандарта IEEE 802.11, более известного пользователям по названию Wi-Fi, фактически являющегося брендом, предложенным и продвигаемым организацией Wi-Fi Alliance.

Технология Wi-Fi была создана в 1991 г. NCR Corporation/AT&T (впоследствии Lucent Technologies и Agere Systems) в Ньивегейн, Нидерланды. Название Wi-Fi иногда интерпретируется как аббревиатура английских слов *Wireless Fidelity*, что дословно переводится с английского языка как «беспроводная точность».

В настоящее время разработкой данной технологии занимается рабочая группа 802.11 Комитета по стандартизации Института инженеров

электротехники и электроники IEEE (англ. *Institute of Electrical and Electronics Engineers*). Силами рабочей группы в июне 1997 года была ратифицирована первая спецификация 802.11. Изначально стандарт IEEE 802.11 предполагал возможность передачи данных по радиоканалу на скорости не более 1 Мбит/с (опционально, на скорости 2 Мбит/с) на частоте 2,4 ГГц [1, 2].

Для беспроводных сетей связи на основе стандарта IEEE 802.11 изначально были выделены следующие частотные диапазоны:

1) Радиочастотные:

- 2,401 – 2,483 ГГц;
- 3,657 – 3,700 ГГц;
- 5,150 – 5,905 ГГц;
- 57,00 – 64,80 ГГц.

2) Инфракрасный: 315,571 – 352,697 ТГц.

Каждый стандарт из набора IEEE 802.11a/b/g/n/ac/ad/ax определяет диапазон и полосу частот для организации каналов связи на основе выбранных методов кодирования, модуляции и расширения спектра.

II ТОПОЛОГИИ СЕТЕЙ СТАНДАРТА IEEE 802.11

Абоненты сети IEEE 802.11 могут создавать топологии следующих типов:

- топология с набором независимых базовых служб IBSS (англ. *Independent Basic Service Set*);
- топология с набором базовых служб BSS (англ. *Basic Service Set*);
- топология с расширенным набором служб ESS (англ. *Extended Service Set*).

В первом случае две или более станций взаимодействуют друг с другом, создавая произвольные одноранговые коммуникации между беспроводными сетевыми контроллерами WNIC (англ. *Wireless Network Interface Controller*) отдельных компьютеров (рис. 3.1).

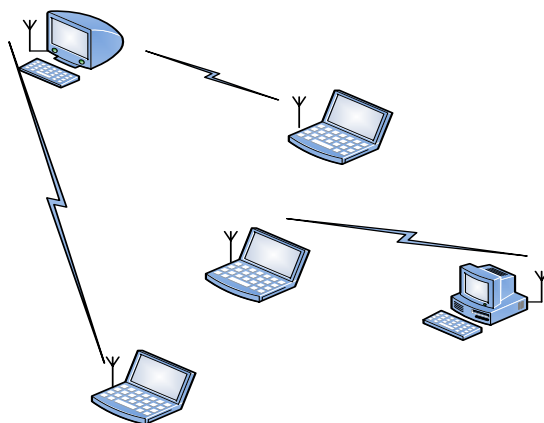


Рис. 3.1. Топология IBSS

Сети такого типа получили название «ad hoc». Они не имеют опорной проводной инфраструктуры, и подключение новых узлов сети происходит «на лету», с некоторой долей непредсказуемости. Беспроводные терминалы в такой сети не просто принимают и отправляют сообщения, но выступают в роли сетевых узлов, которые должны получать доступ к сетевым ресурсам при помощи процедур многостанционного доступа, а также маршрутизировать пакеты и устанавливать их приоритеты.

При применении (инфраструктурной) топологии с базовым набором служб или (рис. 3.2) клиенты (станции) общаются только с точкой доступа AP (англ. *Access Point*), которая и руководит передачей данных между ними (в проводной сети аналогом является топология звезда с концентратором в центре). Точка доступа реализует большинство функций управления передачей данных (доступ к среде, маршрутизация, приоритеты и пр.), при этом беспроводные терминалы осуществляют только простую обработку сигналов.

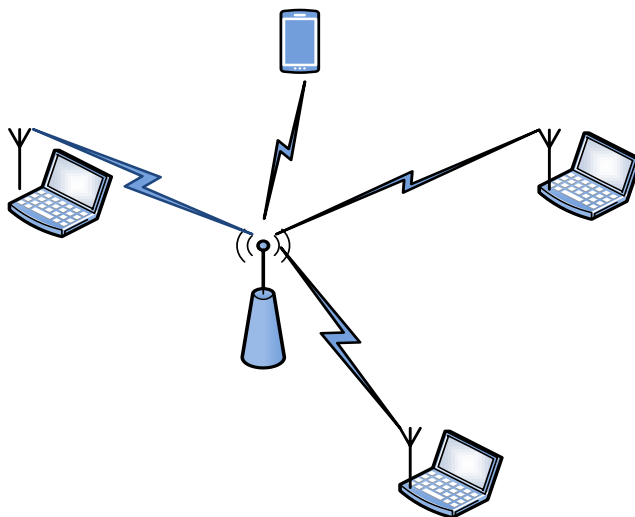


Рис. 3.2. Топология BSS

Топология с расширенным набором служб (рис. 3.3) отражает коммуникации отдельных компьютеров с точкой доступа. Сети с такой топологией называют *структурированными*. WLAN данного типа обладает проводной инфраструктурой, соединяющей её с другими сетями. Радиообмен осуществляется только между точкой(ми) доступа и беспроводными терминалами, т.е. два беспроводных терминала могут взаимодействовать только через соответствующую AP.

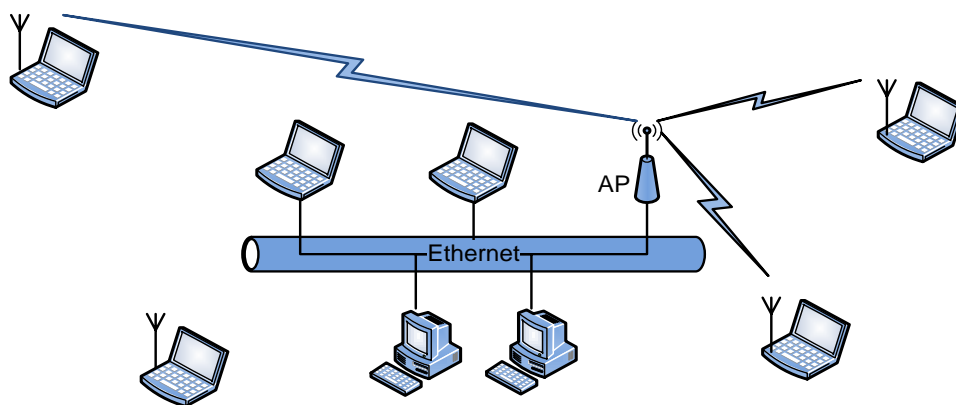


Рис. 3.3. Топология ESS

Такой способ организации позволяет упростить управление доступом к сети и почти полностью избежать коллизий. Однако наличие проводной составляющей ограничивает гибкость использования структурированных сетей.

IBSS легко преобразовать в BSS или ESS, но использовать две топологии одновременно затруднительно, поскольку как одноранговые коммуникации проявляют нестабильность вблизи AP, так и коммуникации структурированной сети могут нарушаться.

III МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ ОТКРЫТЫХ СИСТЕМ OSI И СТАНДАРТЫ IEEE 802.11

Стандарт распространяется на стационарные и мобильные станции и определяет функции физического и канального уровней эталонной модели взаимодействия открытых систем OSI (англ. *Open System Interconnection*). На физическом уровне IEEE 802.11 определяет: диапазон(ы) частот; скорости передачи данных; методы модуляции, кодирования и мультиплексирования. Подуровни канального уровня MAC (англ. *Media Access Control*) и LLC (англ. *Logical Link Control*) определяют метод доступа, адресацию, безопасность передачи и способы проверки корректности данных.

На рис. 3.4 представлено соответствие стандартов IEEE 802.x проводных и беспроводных локальных сетей модели OSI.

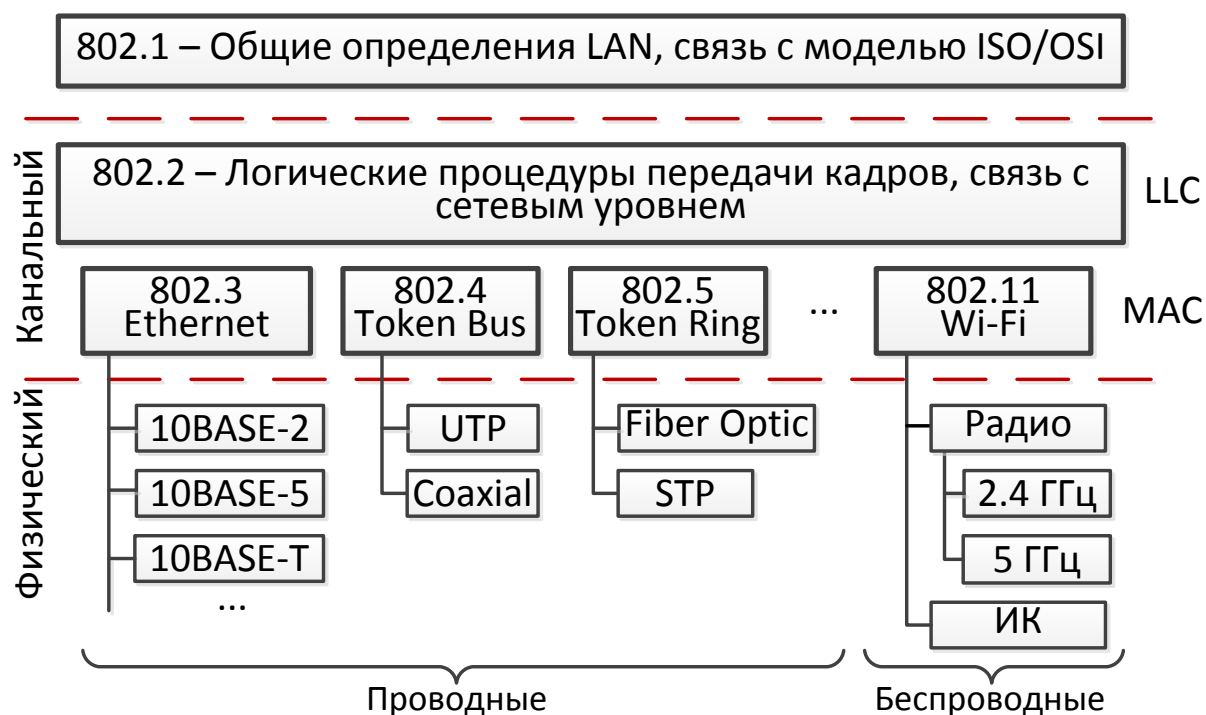


Рис. 3.4. Соответствие уровней стандартов локальных сетей уровням модели OSI

В настоящее время IEEE 802.11 представляет собой набор стандартов, описывающих физический уровень различных технологий WLAN (IEEE 802a/b/g/n/ac/ad/ax), а также принципы безопасности, мобильности и пр.

IV КАНАЛЬНЫЙ УРОВЕНЬ СЕТЕЙ СТАНДАРТА IEEE 802.11

Рассмотрим общие принципы организации сетей Wi-Fi на канальном уровне.

4.1 Методы доступа в беспроводных сетях IEEE 802.11

Стандарт IEEE 802.11 использует разделяемую среду передачи для организации локальной сети. Это означает, что несколько абонентов одновременно не могут вести передачу. Вопросы об использовании среды передачи решаются на MAC-подуровне канального уровня Wi-Fi.

Возможно использование двух методов доступа к среде:

1) *Функция распределённой координации DCF* (англ. *Distributed Coordination Function*) может применяться как в сетях с топологией ad hoc, так и в сетях со инфраструктурной топологией.

2) *Функция точечной координации PCF* (англ. *Point Coordination Function*) применяется только в сетях с базовым или расширенным набором служб.

Обе функции применяются в сетях без поддержки качества обслуживания QoS.

DCF

В основе первого метода лежит алгоритм *множественного доступа с прослушиванием несущей и предотвращением коллизий CSMA/CA* (англ. *Carrier Sense Multiple Access with Collision Avoidance*), опционально в сочетании с алгоритмом PTS/CTS для решения проблемы «скрытого узла».

Алгоритм CSMA/CA напоминает CSMA/CD в сети Ethernet с некоторыми отличиями. Его можно описать следующим образом:

Узел, ожидающий передачи прослушивает несущую частоту, определяя её занятость. После того как узлы определяют, что среда свободна, прежде чем начать передачу они выжидают в течение некоторого промежутка времени.

Этот временной интервал складывается из двух составляющих:

- *обязательный промежуток DIFS* (англ. *DCF Interframe Space*);
- *выбираемый случайным образом промежуток обратного отсчёта* (англ. *Backoff time*).

Backoff time равен целому числу элементарных тайм-слотов (англ. *Slot Time*).

$$\text{Backoff time} = \text{Random}[CW_{min}, CW_{max}] \cdot \text{SlotTime}$$

$$CW_{min} = 31$$

$$CW_{max} = 1023$$

CW (англ. *Contention Window*) – окно конкурентного доступа, каждый узел формирует сам.

Если в течение всего промежутка **DIFS + Backoff time** среда оставалась свободной узел начинает передачу (рис. 3.5).

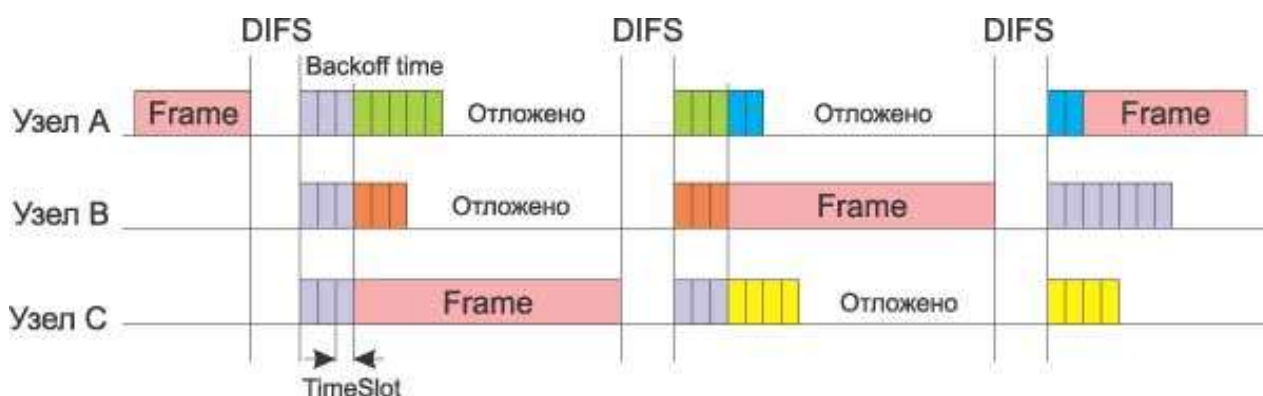


Рис. 3.5. Пример реализации механизма CSMA/CA

После успешной передачи окно CW формируется вновь.

Если же за время ожидания передачу начал другой узел сети, то значение счётчика обратного отсчёта останавливается, и передача данных откладывается.

После того как среда станет свободной, данный узел снова начинает процедуру обратного отсчёта, но уже с меньшим размером окна CW.

Вероятность коллизии можно снизить, увеличивая максимальный размер CW, но при этом растёт задержка, что приводит к уменьшению производительности сети.

Чтобы уменьшить вероятность коллизии применяется следующий алгоритм:

После каждого успешного приёма кадра принимающая сторона через короткий промежуток SIFS (англ. *Short Interframe Space*) подтверждает успешный приём (рис. 3.6.), посылая ответную квитанцию (подтверждение) — кадр ACK (англ. *ACKnowledgement*).

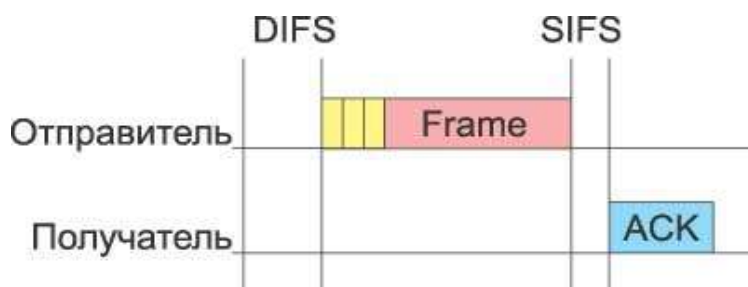


Рис. 3.6. Пример передачи квитанции

Если в процессе передачи данных возникла коллизия, то передающая сторона не получает кадр ACK, свидетельствующий об успешном приёме.

В этом случае размер CW-окна для передающего узла увеличивается почти вдвое.

Если для первой передачи размер окна равен **31*слот**, для второй попытки передачи он составляет **63*слот**, для третьей — **127*слот**, для четвертой — **255*слот**, для пятой — **511*слот**, для всех последующих — **1023*слот**.

Кроме того, необходимо учитывать размер кадра. Если делать кадры большими, то при возникновении коллизии придётся повторно передавать большой объем данных, что опять приводит к снижению производительности.

Если делать кадры маленькими, то объем служебной информации будет превышать объем полезной информации и снижать производительность сети.

Контроль несущей

Известны два механизма прослушивания несущей:

- физическое (на физическом уровне модели OSI);
- виртуальное (на канальном уровне – подуровня MAC).

Физическое прослушивание осуществляется на беспроводном интерфейсе устройства и определяется измерением мощности сигнала других устройств.

Физический механизм признаёт среду свободной, если уровень сигнала на антенне меньше заданного значения.

Виртуальный контроль основан на передаче информации о длительности резервирования среды. Такая информация содержится в заголовке кадра данных или в управляющем кадре RTS/CTS.

Устройства могут определять сколько времени канал будет занят.

Алгоритм RTS/CTS

Данный механизм опционально доступен устройствам Wi-Fi и предназначен для решения проблемы скрытого узла (рис. 3.7).

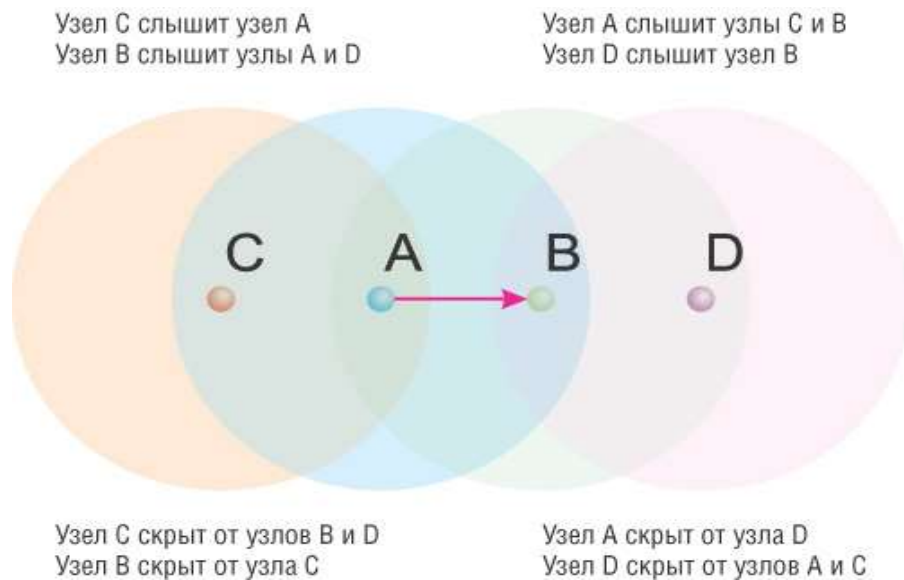


Рис. 3.7. Иллюстрация проблемы скрытого узла

1) Каждый узел сети, перед тем как послать данные в эфир, сначала отправляет специальное короткое сообщение, которое называется «Готов к передаче» RTS (англ. *Ready To Send*).

RTS-сообщение содержит информацию о продолжительности предстоящей передачи и об адресате и доступно всем узлам в сети (если только они не скрыты от отправителя).

2) Приём сообщения RTS позволяет другим узлам задержать передачу на время, равное объявленной в RTS длительности сообщения.

3) Приёмная станция, получив сигнал RTS, отвечает посылкой сигнала «Готов к приёму» CTS (англ. *Clear To Send*), свидетельствующего о готовности станции к приёму информации.

4) После этого передающая станция посылает пакет данных, а приёмная станция должна ответить кадром ACK, подтверждающим безошибочный приём (рис. 3.8).

Данный алгоритм помогает решить проблему «скрытого узла», возникающую, когда целевой узел расположен вне зоны досягаемости узла-отправителя. В этом случае, не получив ответный пакет CTS, узел-отправитель повторяет посылку пакета RTS через случайное время задержки.

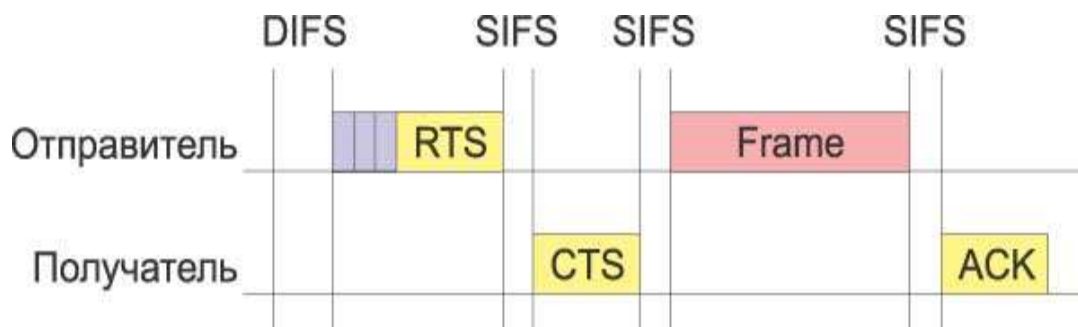


Рис. 3.8. Пример обмена кадрами в механизме RTS/CTS

Алгоритм RTS/CTS предоставляет возможность справиться с проблемой возникновения коллизий, которая не решается посредством рассмотренного базового способа организации коллективного доступа в DCF.

У алгоритма RTS/CTS имеются свои подводные камни, которые в определенных ситуациях могут приводить к снижению эффективности использования среды передачи данных. Например, в некоторых ситуациях возможно такое явление, как распространение эффекта ложных блокировок узлов, что в конечном счёте может привести к ступору сети (рис. 3.9).

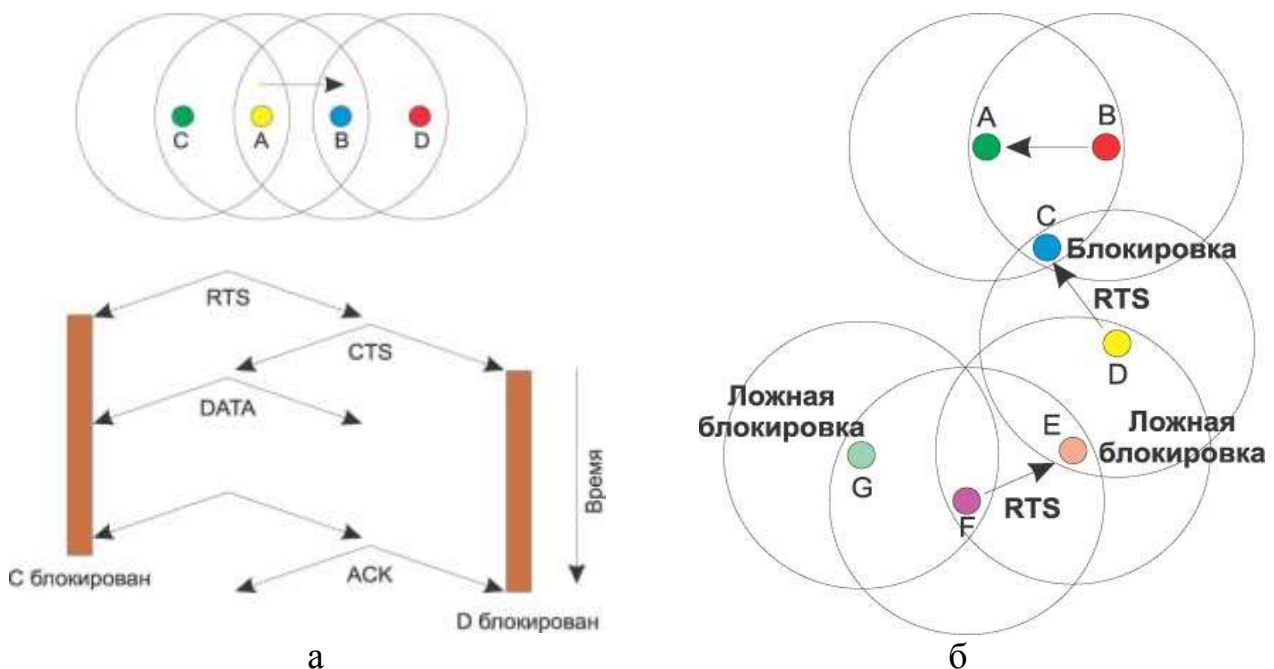


Рис. 3.9. Пример реализации механизма RTS/CTS: а) – нормальная ситуация; б) – ситуация с ложными блокировками

PCF

Функция PCF является опциональной и применяется только в режиме инфраструктуры.

Точка доступа выступает в качестве центра координации. Режимы DCF и PCF объединяются в так называемом суперфрейме, который образуется из PCF-промежутка бесконкурентного доступа к среде, называемого CFP (англ.

Contention-Free Period), и следующего за ним DCF-промежутка CP (англ. *Contention Period*) конкурентного доступа к среде (рис. 3.10).

Длительность CP-промежутка должна быть достаточной для того, чтобы обеспечить возможность передать хотя бы один кадр с использованием DCF-механизма.

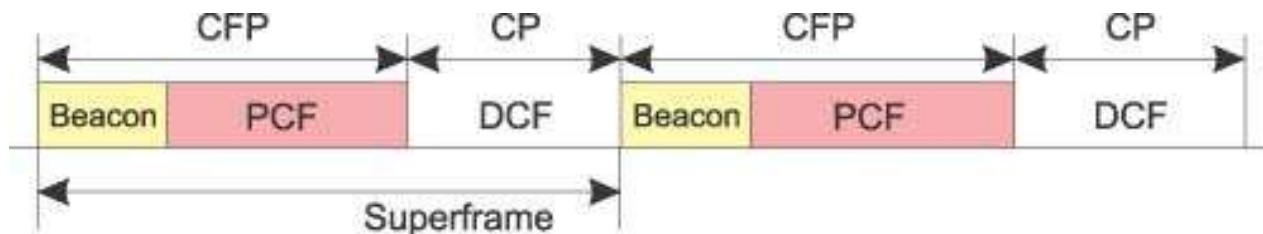


Рис. 3.10. Суперфрейм PCF

Во время режима PCF точка доступа опрашивает все узлы сети о кадрах, которые стоят в очереди на передачу, посылая им служебные кадры CF_POLL (кадры опроса).

Опрашиваемые узлы в ответ на получение кадров CF_POLL посылают подтверждение CF_ACK. Если подтверждения не получено, то точка доступа переходит к опросу следующего узла (рис. 3.11).

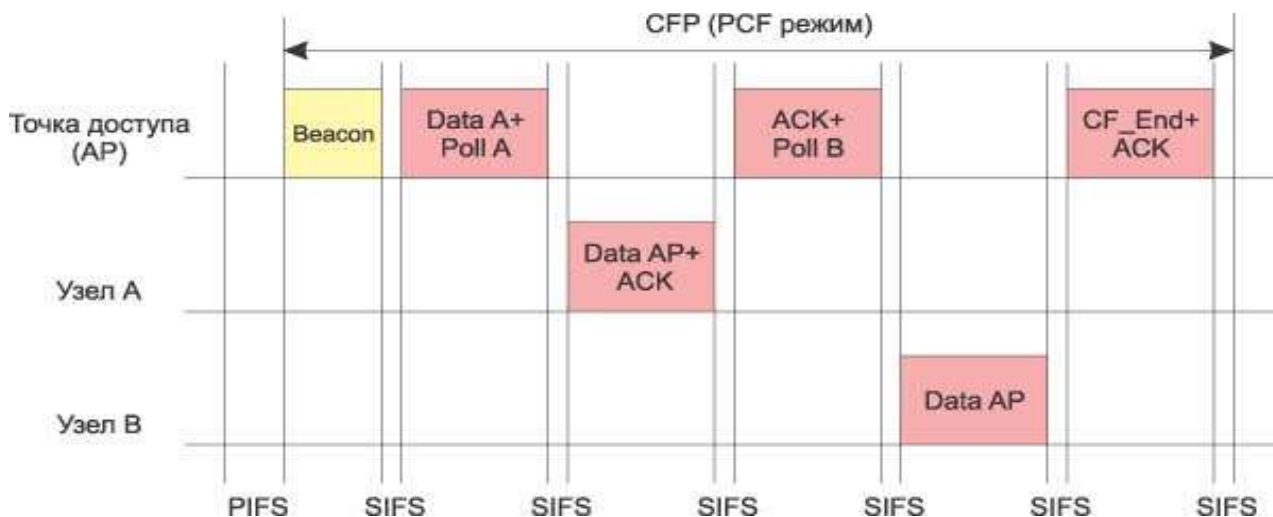


Рис. 3.11. Опрос узлов в режиме PCF

Узлы, ответившие согласием, помещаются в опросный лист в соответствии с его приоритетом, а затем поочерёдно получают право на передачу однократно за период.

Допускаются следующие типы кадров во время режима PCF:

- DATA – кадр данных;
- CF_ACK – кадр подтверждения;
- CF_POLL – кадр опроса;
- DATA+CF_ACK – комбинированный кадр данных и подтверждения;
- DATA+CF_POLL – комбинированный кадр данных и опроса;
- DATA+CF_ACK+CF_POLL – комбинированный кадр данных, подтверждения и опроса;

– CF_ACK+CF_POLL – комбинированный кадр подтверждения и опроса.

Когда центр координации (AP) пытается получить доступ к среде, то он ожидает (как и все узлы) окончания текущей передачи и, поскольку для него определяется минимальный режим ожидания, первым получает доступ к среде.

Промежуток ожидания, определяемый для центра координации, называется PIFS (англ. *PCF Interframe Space*).

Во время периода CP узлы осуществляют передачу в соответствии с алгоритмом DCF. PCF позволяет управлять QoS через приоритеты, но не поддерживает классы трафика TC (англ. *Traffic Classes*).

4.2 Обновлённые методы доступа в беспроводных сетях IEEE 802.11e

Для наилучшего обеспечения QoS в 2005 г вышел стандарт IEEE 802.11e, в котором определены расширенные функции доступа к распределённой среде передачи данных, позволяющие учитывать приоритеты и дифференциацию трафика.

Расширенная функция распределённой координации EDCF

На уровне MAC в стандарте IEEE 802.11e предусматривается расширение функции распределённой координации EDCF (англ. *Enhanced DCF*).

В случае реализации механизма EDCF рассматриваются различные категории трафика TC (англ. *Traffic Categories*), которые отличаются друг от друга степенью приоритета относительно доступа к среде передачи данных.

Механизм доступа к среде остаётся таким же, как и в случае DCF.

Каждый узел сети, убедившись, что среда свободна, прежде чем начать передачу, выжидает в течение промежутка времени AIFS (англ. *Arbitration Interframe Space*), после чего приступает к процедуре обратного отсчёта (рис. 3.12).

Длительность промежутка обратного отсчёта определяется как случайное целое число тайм-слотов из диапазона [1, CW(TC)+1], где CW(TC) – размер окна для трафика заданной категории.

В случае возникновения коллизии во время передачи значение нового окна вычисляется по формуле:

$$newCW[TC] = (oldCW[TC]+1) \cdot PF[TC] - 1$$

где PF — это постоянная масштабирования окна, значение которой зависит от категории трафика.

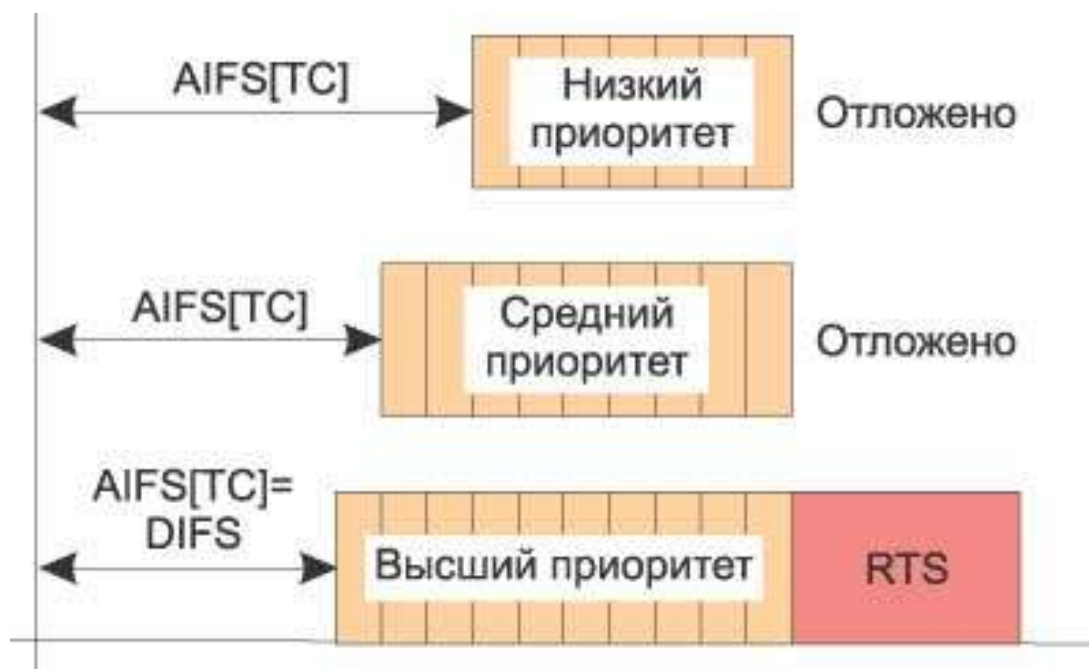


Рис. 3.12. Пример реализации механизма EDCF

Гибридная функция координации HCF

Аналогично тому, как EDCF является развитием механизма DCF, HCF является развитием централизованной функции координации PCF. И если PCF был реализован поверх DCF, то HCF реализуется поверх EDCF.

Точка доступа является центром гибридной координации или гибридным координатором (HC) и управляет коллективным доступом всех узлов сети к среде передачи данных, для чего опрашивает все узлы сети, внесённые в её список (list), и на основании этого опроса организует передачу данных между всеми узлами сети.

В сетях с механизмом HCF в течение определенного промежутка времени CFP реализуется механизм бесконкурентного доступа, когда доступ к среде контролируется точкой доступа, затем следует промежуток конкурентного доступа CP с механизмом EDCF. Чередующиеся режимы бесконкурентного и конкурентного доступа образуют суперфрейм (рис. 3.13).

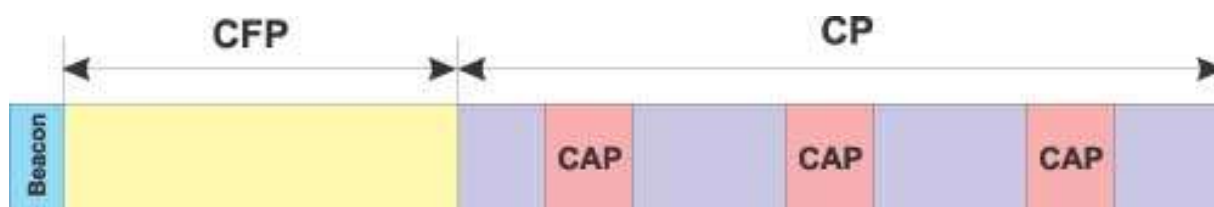


Рис. 3.13. Суперфрейм механизма HCF

В отличие от рассмотренного выше метода EDCF, в период конкурентного доступа CP на основе механизма HCF точка доступа также может получать внеочередной доступ к среде, образуя так называемые периоды CAP (англ. *Controlled Access Periods*).

Для опроса узлов сети НС использует служебные кадры QoS CF_POLL, а узлы отвечают на запросы кадрами подтверждениями QoS CF_ACK.

Точка доступа может передавать:

- кадры данных (QoS DATA);
- комбинированные кадры опроса и данных (QoS DATA+CF_POLL);
- комбинированные кадры опроса и подтверждения (QoS CF_ACK+CF_POLL);
- комбинированные кадры опроса, подтверждения и данных (QoS DATA+CF_ACK+CF_POLL).

Узлы сети могут помимо кадров данных совмещать кадры подтверждения с передачей данных (DATA + CF_ACK).

V ФОРМАТ КАДРА IEEE 802.11

В IEEE 802.11 определено три типа кадров:

- **информационный** (англ. *data frame*) – для передачи полезной информации;
- **контрольный** (англ. *control frame*) – для управления доступом к среде;
- **управляющий** (англ. *management frame*) – для обмена служебной информацией.

Формат кадра одинаковый для всех типов кадра, но содержание и применение полей будет различаться (рис. 3.14). Кадр IEEE 802.11 содержит заголовок (англ. *MAC Header*), тело (англ. *Frame Body*) и контрольную сумму FCS (англ. *Frame Check Sequence*). Максимальная длина кадра составляет 2348 байт.

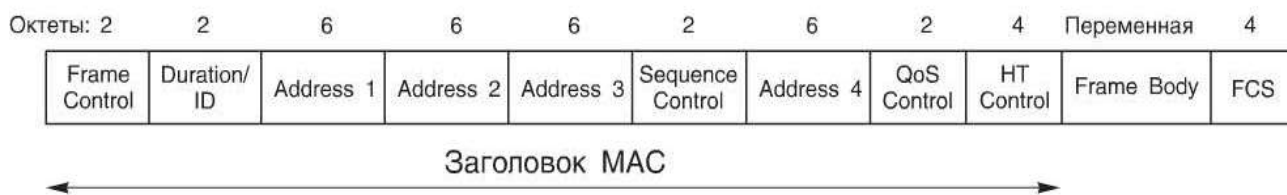


Рис. 3.14. Формат кадра Wi-Fi

Поля общего формата кадра

– **Управление кадром** (англ. *Frame Control*). Указывается тип кадра и предоставляется управляющая информация (рис. 3.15).

– **Идентификатор длительности/соединения** (англ. *Duration ID*). 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** (англ. *Address 1 – Address 4*). Число и значение полей адреса зависит от контекста. Возможны следующие типы адреса: *источника*,

назначения, передающей станции, принимающей станции. Поле адреса получателя присутствует во всех беспроводных кадрах. Поле адреса передатчика присутствует во всех кадрах, кроме кадров подтверждения и CTS.

- **Управление очередностью** (англ. *Sequence Control*). Содержит 4-битовое подполе номера фрагмента, используемое для фрагментации и повторной сборки, и 12-битовый порядковый номер, используемый для нумерации кадров, передаваемых между приёмником и передатчиком.

- **Контроль QoS** (англ. *QoS Control*). Состоит из нескольких подполей, содержит идентификатор трафика TID (англ. *Traffic Indicator*) и приоритет пользователя. Существует восемь пользовательских приоритетов, разделённых на четыре класса трафика.

- **Контроль высокой пропускной способности** (англ. HT Control). Используется для передачи характеристик PHY и MAC.

- **Тело кадра** (англ. *Frame Body*). Содержит модуль данных протокола LLC или управляющую информацию MAC.

- **Контрольная последовательность кадра** (англ. *Frame Control Sequence*). 32-битовая проверка чётности с избыточностью.

Управление кадром (Frame Control)

Номер бита	B0	B1	B2	B3	B4	B7	B8	B9	B10	B11	B12	B13	B14	B15
	Protocol Version		Type		Subtype		To DS	From DS	More Fragments	Retry	Power Management	More Data	Protected Frame	Order
Длина в битах	2		2		4		1	1	1	1	1	1	1	1

Рис. 3.15. Поле Управление кадром

- **Версия протокола** (англ. *Protocol Version*). Версия 802.11, текущая версия – 0.

- **Тип** (англ. *Type*). Определяет тип кадра: *контроль*, *управление* или *данные*.

- **Подтип** (англ. *Subtype*). Дальнейшая идентификация функций кадра.

- **К DS** (англ. *To DS*). Координационная функция MAC присваивает этому биту значение 1, если кадр предназначен распределительной системе (англ. *Distribution System*).

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

- **Большие фрагменты** (англ. *More Fragments*). Установлен в 1, если за данным фрагментом следует ещё несколько.

- **Повтор** (англ. *Retry*). Принимает значение 1, если данный кадр является повторной передачей предыдущего.

- **Управление мощностью** (англ. *Power Management*). Принимает значение 1, если передающая станция находится в режиме ожидания.

– **Больше данных** (англ. *More Data*). Указывает, что станция передала не все данные. Каждый блок данных может передаваться как один кадр или как группа фрагментов в нескольких кадрах.

– **Защищённый кадр** (англ. *Protected Frame*). Принимает значение 1, если реализован алгоритм конфиденциальности (криптографический алгоритм) содержимого поля Тело кадра.

– **Порядок** (англ. *Order*). Принимает значение 1, если используется услуга строгого упорядочения, указывающая адресату, что кадры должны обрабатываться строго по порядку.

Контрольные кадры

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

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

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

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

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

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

6) **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. Этими кадрами являются:

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

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

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

4) **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:

1) **Запрос ассоциации**. Посылается станцией к точке доступа с целью запроса ассоциации с данной сетью с базовым набором услуг BSS (англ. *Basic Service Set*). Кадр включает информацию о возможностях, например, будет ли использоваться шифрование, или способна ли станция отвечать при опросе.

2) **Ответ на запрос ассоциации**. Возвращается точкой доступа и указывает, что запрос ассоциации принят.

3) **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.

4) **Ответ на запрос повторной ассоциации**. Возвращается точкой доступа и указывает, что запрос повторной ассоциации принят.

5) **Пробный запрос**. Используется станцией для получения информации от другой станции или точки доступа. Кадр используется для локализации BSS стандарта IEEE 802.11.

6) **Ответ на пробный запрос**. Отклик на пробный запрос.

7) **Сигнальный кадр**. Передаётся периодически, позволяет мобильным станциям локализовать и идентифицировать BSS.

8) **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.

9) **Разрыв ассоциации.** Используется станцией для аннулирования ассоциации.

10) **Аутентификация.** Для аутентификации станций используются множественные кадры.

11) **Отмена аутентификации.** Передаётся для прекращения безопасного соединения.

VI НАБОР СТАНДАРТОВ IEEE 802.11a/b/g/n/ac/ad

В 1997 г была ратифицирована первая спецификация 802.11. Изначально стандарт IEEE 802.11 предполагал возможность передачи данных по радиоканалу на скорости не более 1 Мбит/с и, опционально, на скорости 2 Мбит/с в инфракрасном и 2.4 ГГц диапазонах.

6.1 Технические характеристики стандарта IEEE 802.11

Исходный стандарт 802.11 определяет три метода передачи на физическом уровне:

- передача в диапазоне **инфракрасных волн**;
- технология расширения спектра путём **скачкообразной перестройки частоты** (FH-SS) в диапазоне 2,4 ГГц;
- технология широкополосной модуляции с **расширением спектра методом прямой последовательности** (DS-SS) в диапазоне 2,4 ГГц.

Технические характеристики стандарта сведены в таблицу 3.1.

Таблица 3.1. Основные характеристики канала в IEEE 802.11

Диапазон частот	Радиоканал	Модуляция	Кодовая последовательность	Скорость передачи, Мбит/с	Количество бит на символ
2.4 ГГц	FH-SS	2 GFSK	–	1	1
		4 GFSK	–	2	2
	DS-SS	DBPSK	11-чиповый код Баркера	1	1
		DQPSK	11-чиповый код Баркера	2	2
ИК-диапазон	–	16-PPM	–	1	1
		4-PPM	–	2	2

Передача в инфракрасном диапазоне с длиной волны 850-950 нм предполагает применение в качестве генератора полупроводникового лазерного диода или светодиода LED (англ. *Light-Emitting Diode*). Поскольку инфракрасное излучение практически не проникает через препятствия, зона покрытия WLAN на его основе ограничивается расстоянием прямой видимости.

Поддерживаются две скорости передачи данных – 1 и 2 Мбит/с. На скорости 1 Мбит/с поток данных разбивается на квартеты, каждый из которых затем во время модуляции кодируется одним из 16-ти символов. На скорости 2 Мбит/с поток данных делится на битовые пары, каждая из которых модулируется одним из четырёх символов.

Устройства Wi-Fi со скачкообразной перестройкой частоты делят полосу частот от 2,401 до 2,483 ГГц на 79 неперекрывающихся каналов шириной 1 МГц. Частотные скачки происходят не реже 2.5 раз в секунду между 6-ю каналами шириной 1 МГц, таким образом, расширяя спектр до 6 МГц. Чтобы минимизировать число коллизий между перекрывающимися зонами покрытия определяют 3 набора последовательностей частот каждая длиной 26.

DS-SS в стандарте IEEE 802.11 делит полосу частот на некоторое число перекрывающихся каналов (в разных странах от 11 до 14, в России – 13), полосой 22 МГц. Каждый из каналов отстоит от соседнего на 5 МГц. Таким образом, доступными оказываются три неперекрывающихся канала: 1, 6, 11 (рис. 3.16). В каждый передаваемый информационный бит (логический 0 или 1) встраивается 11-чиповая последовательность Баркера. Ширина спектра преобразованного сигнала будет в 11 раз больше ширины спектра первоначального сигнала. Чиповые последовательности, встраиваемые в информационные биты, называют *шумоподобными последовательностями* (PN-sequence), а результирующий сигнал *шумоподобным* (англ. pseudo-noise) сигналом.

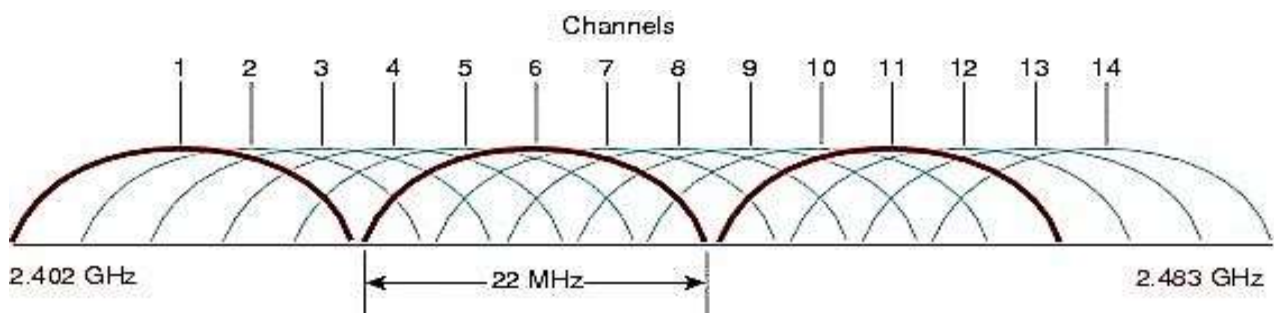


Рис. 3.16. Распределение частот DS-SS

6.2 Технические характеристики стандарта IEEE 802.11a

Для повышения скорости передачи рабочей группой IEEE 802.11 были разработаны сразу два стандарта IEEE 802.11a и IEEE 802.11b, вышедшие в 1999 г.

Характеристики IEEE 802.11a сведены в таблицу 3.2.

Таблица 3.2. Основные характеристики канала в IEEE 802.11a

Диапазон	Радиоканал	Модуляция	Свёрточное кодирование	Скорость передачи,	Кол-во бит на символ в	Кол-во бит в
----------	------------	-----------	------------------------	--------------------	------------------------	--------------

частот			e	Мбит/с	одном подканале	OFDM символе
5 ГГц	OFDM	BPSK	1/2	6	1	24
		BPSK	3/4	9	1	36
		QPSK	1/2	12	2	48
		QPSK	3/4	18	2	72
		16-QAM	1/2	24	4	96
		16-QAM	3/4	36	4	144
		64-QAM	2/3	48	6	192
		64-QAM	3/4	54	6	216

В стандарте используется технология *OFDM* (англ. *Orthogonal Frequency Division Multiplexing*) – ортогональное мультиплексирование с разделением по частоте полосы 20 МГц, которая позволяет достичь скорости 54 Мбит/с. Частотный диапазон делится на 52 поднесущие, каждая шириной 312.5 кГц, по которым одновременно передаются данные. При этом 4 поднесущих выделены на управление, для передачи используются остальные 48.

Радиус зоны действия сети – до 50 м.

Стандарт IEEE 802.11a несовместим по частоте и технологии физического уровня с оригинальным стандартом IEEE 802.11.

6.3 Технические характеристики стандарта IEEE 802.11b

IEEE 802.11b использует технологию DS-SS и имеет обратную совместимость с DS-SS версией оригинального стандарта. Характеристики радиоканала IEEE 802.11b приведены таблице 3.3.

Таблица 3.3. Основные характеристики канала в IEEE 802.11b

Диапазон частот	Радиоканал	Модуляция	Кодовая последовательность	Скорость передачи, Мбит/с	Количество бит на символ
2.4 ГГц	DS-SS	DBPSK	11-чип Баркера	1	1
		DQPSK	11-чип Баркера	2	2
		DBPSK	8-чип CCK	5.5	4
		DQPSK	8-чип CCK	11	8

Для достижения скоростей 5.5 и 11 Мбит/с применяются комплементарные коды CCK (англ. *Complementary Code Keying*), представляющие собой 8-чиповые последовательности комплексных чисел из набора: 1, -1, j, -j, 1+j, 1-j, -1+j, -1-j. Сумма их автокорреляционных функций для любого циклического сдвига, отличного от нуля, всегда равна нулю. Каждый элемент CCK-последовательности представляет собой комплексное число, значение которого определяется по довольно сложному алгоритму. Всего существует 64 набора возможных CCK-последовательностей, причем выбор каждой из них определяется последовательностью входных бит. Для однозначного выбора одной CCK-последовательности требуется знать шесть входных бит.

Радиус зоны действия сети – до 100 м.

6.4 Технические характеристики стандарта IEEE 802.11g

Данный стандарт работает в диапазоне частот 2.4 ГГц и совместим с устройствами IEEE 802.11b, но несовместим с IEEE 802.11a.

Заметим, что в реализацию стандарта добавлено двоичное пакетное сверточное кодирование PBCC (англ. *Packet Binary Convolutional Code*) со скоростями кодирования $\frac{1}{2}$ или $\frac{2}{3}$. Кроме того, в стандарте IEEE 802.11g использованы технологии обоих предыдущих стандартов DS-SS и OFDM. Для повышения скорости возможно применение технологии OFDM в сочетании с комплементарными кодами.

Характеристики канала можно видеть в таблице 3.4.

Таблица 3.4. Основные характеристики канала в IEEE 802.11g

Диапазон частот	Радиоканал	Модуляция	Кодирование	Опционально	Скорость передачи, Мбит/с
2.4 ГГц	DS-SS	DBPSK	Код Баркера		1
		DQPSK	Код Баркера		2
		DBPSK	ССК	PBCC $\frac{1}{2}$	5.5
	OFDM	BPSK	–	-	6
	OFDM	BPSK	–	ССК	9
	DS-SS	DQPSK	ССК	PBCC $\frac{2}{3}$	11
	OFDM	QPSK	–	ССК	12
	OFDM	QPSK	–	ССК	18
	DS-SS	8-PSK	PBCC $\frac{1}{2}$		22
	OFDM	16-QAM	–	ССК	24
	DS-SS	8-PSK	PBCC $\frac{2}{3}$		33
	OFDM	16-QAM	–	ССК	36
	OFDM	64-QAM	–	ССК	48
	OFDM	64-QAM	–	ССК	54

Дальность действия сети – до 40 м. внутри помещений и до 300 м. снаружи.

6.5 Технические характеристики стандарта IEEE 802.11n

Стандарт IEEE 802.11n (теперь **Wi-Fi 4**) для сетей Wi-Fi был утвержден 11 сентября 2009 г. IEEE 802.11n разрешает работу в двух диапазонах частот – 2.4 ГГц и 5 ГГц и имеет обратную совместимость со всеми ранее

утвержденными стандартами. Теоретически возможная скорость передачи достигает 600 Мбит/с при использовании следующих возможностей:

1) Применение сдвоенных каналов с полосой частот 40 МГц в диапазоне 5 ГГц вместо 20 МГц в диапазоне 2.4 ГГц.

2) OFDM мультиплексирование с 57-ю (в полосе 20 МГц) или 114-ю (в полосе 40 МГц) поднесущими.

3) Укороченный циклический префикс CP – 400 нс вместо стандартных 800 нс.

4) Применение технологии MIMO (англ. *Multiple Input Multiple Output*) размерностью от 1×1 до 4×4.

Примеры характеристик канала для IEEE 802.11n приведены в таблице 3.5.

Таблица 3.5. Основные характеристики канала в IEEE 802.11n

Полоса, МГц	Модуляция	Скорость кодирования	MCS* индекс	Количество информационных потоков	Циклический префикс, нс	Скорость передачи, Мбит/с
20	BPSK	$\frac{1}{2}$	0	1	800	6.5
	QPSK	$\frac{1}{2}$	1	1	800	13.0
	QPSK	$\frac{3}{4}$	2	1	800	19.5
	16-QAM	$\frac{1}{2}$	3	1	800	26.0
	16-QAM	$\frac{3}{4}$	4	1	800	39.0
	64-QAM	$\frac{2}{3}$	5	1	800	52.0
	64-QAM	$\frac{3}{4}$	6	1	800	58.5
	64-QAM	$\frac{5}{6}$	7	1	800	65.0
	BPSK	$\frac{1}{2}$	0	1	400	7.2
	QPSK	$\frac{1}{2}$	1	1	400	14.4
	QPSK	$\frac{3}{4}$	2	1	400	21.7
	16-QAM	$\frac{1}{2}$	3	1	400	28.9
	16-QAM	$\frac{3}{4}$	4	1	400	43.3
	64-QAM	$\frac{2}{3}$	5	1	400	57.8
	64-QAM	$\frac{3}{4}$	6	1	400	65.0
	64-QAM	$\frac{5}{6}$	7	1	400	72.2
	BPSK	$\frac{1}{2}$	8	2	800	13.0
	⋮					
40						
	BPSK	$\frac{1}{2}$	24	4	800	54.0

Полоса, МГц	Модуляция	Скорость кодирования	MCS* индекс	Количество информационных поток	Циклический префикс, нс	Скорость передачи, Мбит/с
	QPSK	$\frac{1}{2}$	25	4	800	108.0
	QPSK	$\frac{3}{4}$	26	4	800	162.0
	16-QAM	$\frac{1}{2}$	27	4	800	216.0
	16-QAM	$\frac{3}{4}$	28	4	800	324.0
	64-QAM	$\frac{2}{3}$	29	4	800	432.0
	64-QAM	$\frac{3}{4}$	30	4	800	486.0
	64-QAM	$\frac{5}{6}$	31	4	800	540.0
	BPSK	$\frac{1}{2}$	24	4	400	60.0
	QPSK	$\frac{1}{2}$	25	4	400	120.0
	QPSK	$\frac{3}{4}$	26	4	400	180.0
	16-QAM	$\frac{1}{2}$	27	4	400	240.0
	16-QAM	$\frac{3}{4}$	28	4	400	360.0
	64-QAM	$\frac{2}{3}$	29	4	400	480.0
	64-QAM	$\frac{3}{4}$	30	4	400	540.0
	64-QAM	$\frac{5}{6}$	31	4	400	600.0

* – Схема модуляции и кодирования (англ. *Modulation&Coding Scheme*).

Дальность действия сети – до 5 км.

6.6 Технические характеристики стандарта IEEE 802.11ac

Принятие финальной версии спецификации 802.11ac (он же **W-Fi 5**) состоялось в январе 2014 г. Хотя этот стандарт предполагает полный переход в более эффективный для передачи диапазон 5 ГГц, в течение нескольких лет выпускаемые устройства будут поддерживать обратную совместимость со старыми стандартами и два диапазона частот (2.4 ГГц и 5 ГГц). Максимально достижимая скорость передачи – 6.9 Гбит/с.

В основе данного стандарта лежат те же принципы, что и в основе IEEE 802.11n (OFDM, MIMO, сдвоенные полосы частот, укороченный CP). Значительный прирост скорости в IEEE 802.11ac получен за счет нескольких изменений:

1) Увеличение ширины канала. Если в IEEE 802.11n были применены сдвоенные каналы 40 МГц, то в IEEE 802.11ac ширина полосы составляет 80 МГц (по умолчанию) и 160 МГц.

2) В IEEE 802.11ac применяется технология MIMO, как и в IEEE 802.11n. Но, если в последнем максимальная размерность MIMO составляет 4×4 (параллельно могут передаваться четыре информационных потока), то IEEE 802.11ac может использовать MIMO размерностью до 8×8 . Если передача одного информационного потока в полосе 160 МГц происходит со скоростью 866 Мбит/с, то восемь потоков повышают скорость в 8 раз до 6.9 Гбит/с.

Кроме вышесказанного стандарт IEEE 802.11ac имеет несколько особенностей.

Сети Wi-Fi предыдущих стандартов предусматривают поочередное обслуживание подключенных клиентов. В каждый момент времени только одно устройство может получать и отправлять данных, тогда как другие ожидают своей очереди. Увеличение числа подключенных к одной сети клиентов приводит к росту времени ожидания обслуживания, появлению задержек и снижению эффективности использования сетевых ресурсов. В IEEE 802.11ac применяется технология MU-MIMO (англ. *Multi User MIMO*), которая обеспечивает возможность одновременной передачи информации группам клиентов (рис. 3.17). В результате общая пропускная способность беспроводной сети увеличивается в несколько раз.

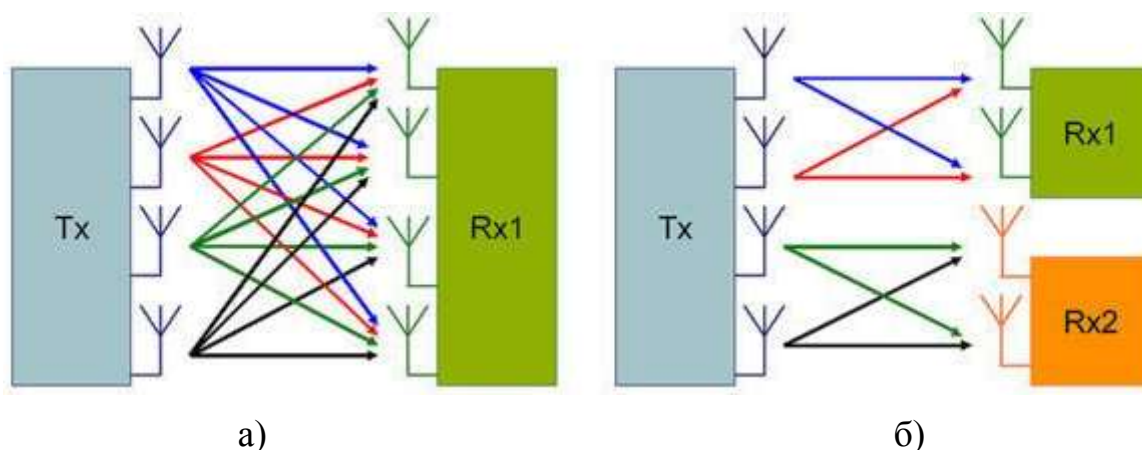


Рис. 3.17. SU-MIMO и MU-MIMO 4×4 : а) – 1 пользователь, 4 потока; б) – 2 пользователя по 2 потока

Одной из сильных сторон устройств стандарта IEEE 802.11ac является экономное расходование энергии. По сравнению с более ранними устройствами экономия может достигать 6 раз.

Ещё одно преимущество стандарта IEEE 802.11ac – технология **Beamforming** (формирование луча), основанная на применении антенн MIMO. Эта технология эффективно борется с падением мощности сигнала на приеме из-за многолучевого распространения. В обычном режиме передающая антенна с круговой диаграммой направленности распространяет сигнал равномерно во все стороны, и множество отраженных копий сигнала приходят в точку приема со сдвигом фазы, уменьшая суммарную мощность. При использовании Beamforming передатчик приблизительно определяет местоположение

приемника и, руководствуясь этой информацией, формирует направленный сигнал с помощью нескольких антенн (рис. 3.18).



Рис. 3.18. Технологии Wi-Fi сетей: а) – с обычной антенной; б) – с технологией beamforming

Beamforming улучшает распространение сигнала не только на открытой территории, но и в помещениях (прохождение сквозь стены, перегородки, мебель и другие препятствия), а также в условиях городской застройки.

6.7 Технические характеристики стандарта IEEE 802.11ad

Технологии IEEE 802.11ad и IEEE 802.11ac развивались одновременно, и главная цель у них одна – преодоление гигабитного барьера скорости. Максимально достижимая скорость в беспроводных сетях на основе этих стандартов одинакова – 6.9 Гбит/с. Главным их отличием является рабочая частота, которая определяет особенности этих стандартов. Для IEEE 802.11ad она составляет 60 ГГц вместо 5 ГГц.

Недостатком данного стандарта можно считать тот факт, что на пути распространения сигнала не должно быть стен и других серьезных препятствий. Радиус покрытия составляет несколько метров (максимально 10 метров).

VII ДОПОЛНИТЕЛЬНЫЕ СТАНДАРТЫ IEEE 802.11

Кроме рассмотренных выше основных стандартов 802.11a, b, g, n, существует ряд вспомогательных, описывающих сервисные функции различных Wi-Fi-изделий:

– **802.11d** предназначен для адаптации различных Wi-Fi-устройств к специфическим условиям страны. Как уже упоминалось выше, конкретные диапазоны частот для каждого отдельно взятого государства определяются внутри самой страны и могут различаться в зависимости от географического положения. Стандарт IEEE 802.11d позволяет регулировать полосы частот в

устройствах разных производителей с помощью специальных опций, введенных в протоколы управления доступом к среде передачи.

- **802.11e** описывает классы качества QoS для приложений, обеспечивающих передачу аудио- и видеофайлов. Изменения, введенные на уровне MAC-протоколов 802.11e, регламентируют качество одновременной передачи звука и изображения для беспроводных аудио- и видеосистем.

- **802.11f** унифицирует параметры Wi-Fi-точек доступа различных производителей. Стандарт позволяет пользователю работать с разными сетями при перемещении между зонами действия отдельных сетей.

- **802.11h** является необходимым требованием ETSI, предъявляемым к оборудованию, допущенному для эксплуатации на территории стран Европейского Союза. В большинстве европейских стран наземные станции слежения за метеорологическими спутниками и спутниками связи, а также радары военного назначения работают в диапазонах, близких к 5 МГц. Для предотвращения конфликтных ситуаций стандарт 802.11h вводит обязательный для использования в Европе механизм автоматического сброса мощности на частотах 5 ГГц для бытовых устройств Wi-Fi при попадании их в зону действия изделий 802.11 специального и военного назначения. Например, все Wi-Fi-оборудование, выпускаемое французской фирмой ACKSYS, проходит обязательную европейскую сертификацию на соответствие стандарту 802.11h.

- **802.11i**. В первых вариантах стандартов 802.11 для обеспечения безопасности сетей Wi-Fi использовался алгоритм WEP (англ. *Wired Equivalent Privacy*). Предполагалось, что этот метод может обеспечить конфиденциальность и защиту передаваемых данных авторизованных пользователей беспроводной сети от прослушивания. Однако, как выяснилось, эту защиту можно взломать всего за несколько минут. Поэтому в стандарте 802.11i были разработаны новые методы защиты сетей Wi-Fi, реализованные как на физическом, так и программном уровнях. В настоящее время для организации системы безопасности в сетях 802.11 рекомендуется использовать алгоритмы WPA (англ. *Wi-Fi Protected Access*). Они также обеспечивают совместимость между беспроводными устройствами различных стандартов и различных модификаций. Протоколы WPA используют усовершенствованную схему шифрования RC4 и метод обязательной аутентификации с использованием EAP. Устойчивость и безопасность современных сетей Wi-Fi определяется протоколами проверки конфиденциальности и шифрования данных (RSNA, TKIP, CCMP, AES).

- **802.11k** был разработан, чтобы улучшить распределение трафика между абонентами внутри сети. В беспроводной локальной сети абонентское устройство обычно соединяется с той точкой доступа, которая обеспечивает наиболее сильный сигнал. Это может привести к перегрузке сети, если к одной точке доступа будут стремиться подключиться сразу много абонентов. Для контроля подобных ситуаций в стандарте 802.11k предложен механизм, ограничивающий количество абонентов, подключаемых к одной точке доступа,

и подсоединяющий новых абонентов к другой точке, несмотря на более слабый сигнал от неё. В этом случае полная пропускная способность сети увеличивается благодаря более эффективному использованию ресурсов.

– **802.11m**. В рамках IEEE 802.11 существует рабочая группа TASK GROUP, занимающаяся исправлением ошибок и ответами на запросы и замечания, которые любой человек может отправить в IEEE. Эти поправки и исправления суммируются в отдельном документе с общим названием 802.11m. Первый выпуск 802.11m был в 2007 г, следующий выпуск исправлений, дополнений и поправок ко всем редакциям 802.11 – в 2011 г.

– **802.11p** регулирует взаимодействие Wi-Fi-оборудования, движущегося со скоростью до 200 км/ч мимо неподвижных точек доступа, удалённых на расстояние до 1 км. Он входит в состав стандарта WAVE (англ. *Wireless Access in Vehicular Environ*) и является своего рода интерфейсом для связи с IEEE 1609. Стандарты WAVE определяют архитектуру и дополнительный набор служебных функций и интерфейсов, которые обеспечивают безопасный механизм радиосвязи между движущимися транспортными средствами. Эти стандарты разработаны для таких приложений, как, например, организация дорожного движения, контроль безопасности движения, автоматизированный сбор платежей, навигация и маршрутизация транспортных средств и др.

– **802.11r** регламентирует быстрый автоматический роуминг Wi-Fi-устройств при переходе из зоны действия одной точки доступа к зоне охвата другой. Этот стандарт ориентирован в основном на интернет-телефонию и на мобильные телефоны с поддержкой Wi-Fi. До появления этого стандарта при движении абонент часто терял связь с одной точкой доступа, был вынужден искать другую и заново выполнять процедуру подключения. Устройства с поддержкой 802.11r могут регистрироваться заранее с соседними точками доступа и выполнять процесс переподключения в автоматическом режиме. Таким образом значительно уменьшается время, когда абонент не доступен в сетях Wi-Fi.

– **802.11s** разработан для топологии многоузловых или ячеистых сетей (англ. *Wireless Mesh Network*), где любое устройство может служить как маршрутизатором, так и точкой доступа. Если ближайшая точка доступа перегружена, данные перенаправляются к ближайшему незагруженному узлу. При этом пакет данных передаётся от одного узла к другому, пока не достигнет конечного места назначения. В данном стандарте введены новые протоколы на уровнях MAC и PHY, которые поддерживают широковещательную и многоадресную передачу, а также одноадресную поставку по самоконфигурирующейся системе точек доступа Wi-Fi. С этой целью в стандарте введён четырёхадресный формат кадра. Проект получил внутреннее название SEE-MESH и в настоящее время находится в стадии разработки (в основном работы по этому проекту ведёт немецкая компания Riedel Communications).

– **802.11t.** Этот документ представляет собой набор методик, рекомендованных IEEE для тестирования сетей 802.11: способы измерений и обработки результатов, требования, предъявляемые к испытательному оборудованию.

– **802.11u.** Предназначен для регулирования взаимодействия сетей Wi-Fi с внешними сетями. Стандарт должен определять протоколы доступа, протоколы приоритета и запрета на работу с внешними сетями. В настоящее время стандарт находится на этапах оценки и утверждения проекта.

– **802.11v.** В стандарте должны быть разработаны поправки, направленные на совершенствование систем управления сетями IEEE 802.11. Модернизация на MAC- и PHY-уровнях должна позволить централизовать и упорядочить конфигурацию клиентских устройств, соединённых с сетью. Находится в стадии разработки.

– **802.11y.** Дополнительный стандарт связи для диапазона частот 3,65-3,70 ГГц. Предназначен для устройств последнего поколения, работающих с внешними антеннами на скоростях до 54 Мбит/с на расстоянии до 5 км на открытом пространстве. Стандарт полностью не завершён.

– **802.11w.** Разработан с целью улучшения защиты и безопасности уровня управления доступом к среде передачи данных (MAC). Протоколы стандарта структурируют систему контроля целостности данных, подлинности их источника, запрета несанкционированного воспроизведения и копирования, конфиденциальности данных и других средств защиты. В стандарте введена защита фрейма управления, а дополнительные меры безопасности позволяют нейтрализовать внешние атаки, такие, как, например, DoS. Кроме того, эти меры обеспечат безопасность для наиболее уязвимой сетевой информации, которая будет передаваться по сетям с поддержкой IEEE 802.11r, k, y. В настоящее время стандарт ещё не завершён.

VIII БЕЗОПАСНОСТЬ В СЕТЯХ WI-FI. СТАНДАРТ IEEE 802.11i

В 2000 г. стало понятно, что необходимо уделить повышенное внимание проблеме безопасности беспроводных локальных сетей. Организацией IEEE была создана рабочая группа 802.11i, которая занялась решением этой проблемы. Результатом стал принятый в 2004 г. стандарт IEEE 802.11i, улучшающий безопасность Wi-Fi.

Защита беспроводной сети заключается в обеспечении аутентификации, шифрования и проверки целостности данных.

8.1 Механизм безопасности WEP

Изначально безопасность соединения Wi-Fi обеспечивалась с помощью технологии WEP – безопасность, эквивалентная проводной сети (англ. *Wired Equivalent Privacy*). Механизм WEP предлагает два вида аутентификации: открытая система и распределенный ключ, не предоставляющие должного уровня защиты. Для проверки корректности данных применяется вычисление 32-х разрядной контрольной суммы CRC (англ. *Cyclic Redundancy Check*). В основе WEP шифрования лежит поточный шифр RC4, выбранный из-за своей высокой скорости работы и возможности использования переменной длины ключа. Из-за множества уязвимостей, как в механизмах аутентификации, так и шифрования, механизм WEP в настоящее время почти не используется.

8.2 Механизмы безопасности WPA и WPA2, стандарт IEEE 802.11i

Заменой WEP стал разработанный в 2003 г. промежуточный механизм WPA (англ. *Wi-Fi Protected Access*). Спецификации WPA обеспечения безопасности конфиденциальности и целостности данных включают в себя следующие компоненты:

- стандарт IEEE 802.1x, на основе которого осуществляется аутентификация абонентов;
- алгоритм шифрования TKIP (англ. *Temporal Key Integrity Protocol*);
- механизм проверки целостности сообщений MIC (англ. *Message Integrity Check*).

Средства в составе стандарта IEEE 802.1x

Стандарт IEEE 802.1x использует следующие протоколы и средства:

- EAP (англ. *Extensible Authentication Protocol*) – протокол расширенной аутентификации пользователей или удаленных устройств;
- TLS (англ. *Transport Layer Security*) – протокол защиты транспортного уровня, который обеспечивает целостность передачи данных между сервером и клиентом, а также их взаимную аутентификацию;
- RADIUS (англ. *Remote Authentication Dial-In User Server*) – сервер аутентификации удаленных клиентов.

Протокол EAP

На основе EAP реализовано более 100 методов, принятых в качестве официальных механизмов аутентификации в стандартах WPA и WPA2. EAP используется для выбора метода аутентификации, передачи ключей и обработки этих ключей подключаемыми модулями – *методами EAP*.

Рассмотрим некоторые из этих методов:

- **EAP-MD5** – это обязательный уровень EAP, который должен присутствовать во всех реализациях стандарта 802.1x, именно он был разработан первым. Он дублирует протокол CHAP.

Протокол аутентификации обменом рукопожатием CHAP (англ. *Challenge Handshake Authentication Protocol*) основан на резюме сообщения (англ. *message digest*), которое вычисляется с помощью алгоритма MD5:

- клиент отправляет серверу своё имя;
- сервер отвечает набором случайных символов;
- клиент, используя алгоритм MD5, вычисляет резюме сообщения (содержание случайной строки и пароль пользователя являются входными параметрами вычисления) и отправляет обратно ответ;
- сервер проделывает те же действия. Получив от клиента резюме сообщения, сервер сравнивает результаты и принимает решение об аутентификации.

- **EAP-TLS** (*EAP-Transport Layer Security* – протокол защиты транспортного уровня) поддерживает взаимную аутентификацию на базе сертификатов.

- **EAP-LEAP** (*Lightweight EAP* – облегченный EAP) – это запатентованный компанией Cisco вариант EAP, основанный на применении паролей, который реализован в точках доступа и беспроводных клиентских картах Cisco.

- **EAP-TTLS** (*Tunneled Transport Layer Security EAP* – туннельный протокол защиты транспортного уровня EAP), разработанный компанией Certicom and Funk Software. Сертификат требуется от сервера, а не от клиента.

EAP-TTLS поддерживает также ряд устаревших методов аутентификации: PAP, CHAP, MS-CHAP, MS-CHAPv2 и EAP-MD5.

- **PEAP** (защищенный EAP), основанный на тех же принципах, что и EAP-TTLS, но 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 программном обеспечении точек доступа D-link и в Windows XP SP2.

- **EAP-SIM** и **EAP-AKA** для аутентификации на базе SIM и USIM. В основном предназначены для аутентификации в сетях GSM, а не в беспроводных сетях 802.11.

- **EAP-PSK** (*EAP-Pre-Shared Key* – заранее известный ключ), метод определенный в RFC 4764, использующий для взаимной аутентификации и обмена сессионным ключом заранее оговоренный ключ. Метод разработан для работы в незащищенных сетях, таких как IEEE 802.11, и в случае успешной аутентификации обеспечивается защищенное двустороннее соединение между клиентом и точкой доступа.

Протокол TLS

TLS разработан как развитие протокола SSL (англ. *Secure Sockets Layer* – уровень защищенных сокетов).

Протокол TLS предназначен для обеспечения криптографическими средствами аутентификации отправителя (клиента) – адресата (сервера),

контроля целостности и шифрования данных информационного обмена. Для аутентификации на основе сертификатов TLS применяет асимметричное шифрование, для конфиденциальности данных – симметричное шифрование, а для сохранения целостности сообщений – коды аутентичности сообщений (англ. *Message Authentication Code*).

RADIUS-сервер

RADIUS (англ. *Remote Authentication in Dial-In User Service*) – протокол для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах. RADIUS-сервер интегрирован с абонентской базой данных (зарегистрированных пользователей) и является частью биллинговой политики сети. Механизм WPA-PSK (WPA2-PSK) использует упрощенный алгоритм аутентификации (по паролю) без использования RADIUS-сервера.

Для осуществления аутентификации архитектура IEEE 802.1x включает в себя следующие логические элементы:

- **Клиент** (англ. *Supplicant*) – программное обеспечение удаленного абонента (ноутбука, телефона, планшета и т.п.), которому требуется аутентификация для доступа к сети.
- **Аутентификатор** (англ. *Authenticator*) – программное обеспечение точки радиодоступа, которое запрашивает аутентификацию.
- **Сервер аутентификации** (англ. *Authentication Server*) – программное обеспечение RADIUS-сервера, осуществляющее аутентификацию.

Обобщенный процесс аутентификации с использованием RADIUS-сервера отображен на рис. 3.19.

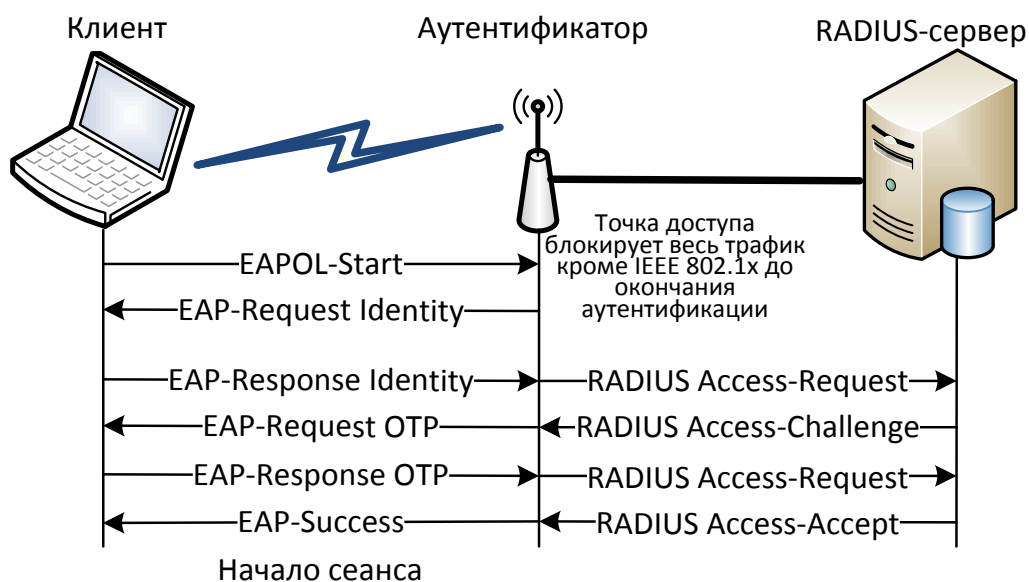


Рис. 3.19. Процесс аутентификации абонента беспроводной сети с использованием RADIUS-сервера

До тех пор пока Клиент не аутентифицирован, он может поддерживать только протокол EAPOL (англ. *EAP Encapsulation Over LAN*) для передачи EAP-сообщений. Сообщение EAPOL-start инициирует процесс аутентификации. Аутентификатор запрашивает Идентификатор (англ. *Identity*) Клиента, который затем передает Серверу. В запросе Аутентификатора содержится информация о выбранном методе EAP.

Затем сервер запрашивает через Аутентификатор единовременный пароль OTP (англ. *One-Time Password*) Клиента, который представляет собой 64-битовое сообщение MD5. После проверки OTP Сервер разрешает/запрещает доступ устройству.

Для перехода в неавторизованное состояние клиент посылает сообщение EAPOL-logoff.

Алгоритм шифрования TKIP. Механизм MIC

Протокол целостности временного ключа TKIP использует для шифрования тот же алгоритм RC4, что и WEP. В основе алгоритма RC4 лежит генератор псевдослучайных битов, на вход которого подается ключ переменной длины. Размер ключа в TKIP увеличен с 40 до 128 бит, кроме того для шифрования каждого передаваемого пакета генерируется новый ключ.

Сервер аутентификации, используя протокол IEEE 802.1x, генерирует уникальный базовый ключ для безопасного соединения. TKIP передает сгенерированный ключ абоненту и точке доступа, а затем динамически генерирует ключи для шифрования пакетов передаваемых данных.

Другим важным механизмом является проверка целостности сообщений методом контрольной суммы MIC. MIC служит для предотвращения перехвата пакетов данных, содержание которых может быть изменено, а модифицированный пакет вновь передан по сети. Для вычисления контрольной суммы используется мощная математическая функция, как на передающей, так и на приемной стороне. Приемник сравнивает вычисленный результат с полученным по сети, и, если они не совпадают, данные считаются ложными и пакет отбрасывается.

Отличие WPA2 от WPA

Механизм WPA2 определяется стандартом IEEE 802.11i и призван заменить WPA, поскольку предоставляет абонентам Wi-Fi сетей более сильную защиту.

WPA2 задействует новый метод шифрования CCMP (англ. *Counter-Mode with CBC-MAC Protocol*), основанный на более мощном, чем RC4, алгоритме шифрования AES (англ. *Advanced Encryption Standard*). AES представляет собой симметричный алгоритм блочного шифрования секретным ключом с размером блока 128 бит и фиксированным размером ключа 128/192/256 бит.

С 2006 г. поддержка WPA2 является обязательной для всех сертифицированных устройств Wi-Fi.

IX МОБИЛЬНОСТЬ В СЕТЯХ WI-FI. ОБЗОР СТАНДАРТОВ IEEE 802.11r/k

Мобильность абонентов в сетях Wi-Fi поддерживается *механизмом быстрого переключения FT* (англ. *Fast Basic Service Set (BSS) Transition*), определенным стандартом **IEEE 802.11r** (2008 г.).

Цель FT – уменьшить время потери соединения между станцией (абонентским устройством) и сетью при переключении от одной точки доступа к другой. Протоколы FT входят в состав механизма переподключения и применимы только к абонентским устройствам и только внутри одной инфраструктуры ESS (в домене одного вендора). Протоколы FT определяют обмен информацией между станцией и точкой доступа в течение подключения или последующего переподключения.

Стандартом определены два протокола:

- ***FT Protocol*** используется, когда станции не требуется запрос ресурсов перед переходом в «целевой» AP;
- ***FT Resource Request Protocol*** используется для предварительного запроса ресурсов при переходе.

Переключение станции от текущей к целевой точке доступа может выполняться двумя методами:

- ***по воздуху*** (англ. *Over-the-Air*) – станция взаимодействует непосредственно с целевой точкой доступа, используя алгоритм аутентификации;
- ***через распределённую систему*** (англ. *Over-the-Distribution System (DS)*) – станция взаимодействует с целевой точкой доступа через текущую AP, которая выступает конвертером кадров между ними.

При перемещении абонентское устройство непрерывно сканирует радиосреду на предмет наилучших параметров канала, и подключается (переключается) к той точке доступа, которая в данный момент их обеспечивает (рис. 3.20).

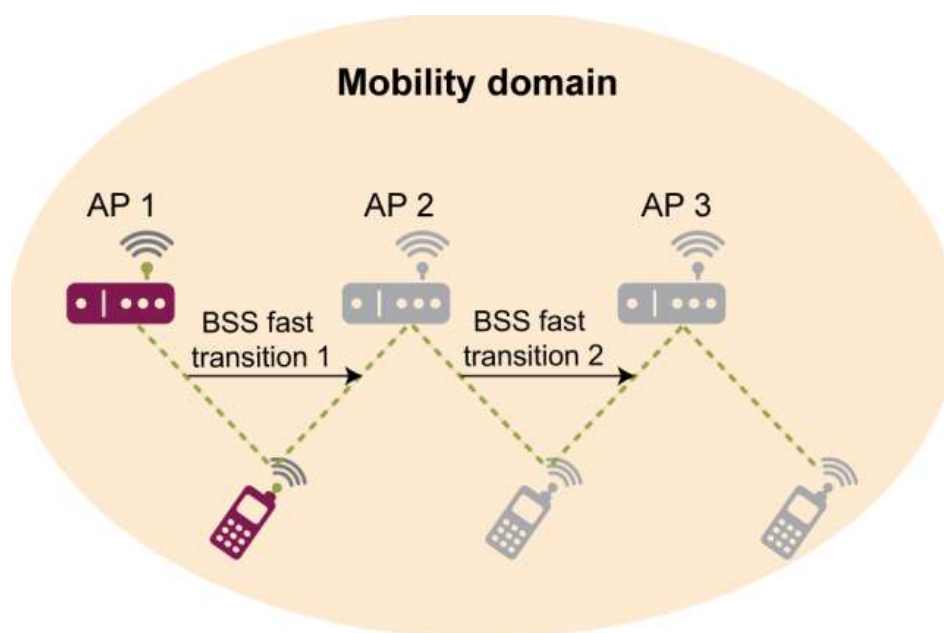


Рис. 3.20. Механизм быстрого переключения

Стандарт **IEEE 802.11k** (2008 г.) определяет количественные измерения сигнала текущей и соседних точек доступа таким образом, чтобы мобильная станция могла принять обоснованное решение переключиться с одной AP на другую.

Таким образом, стандарт IEEE 802.11r обеспечивает абонентское устройство стандартным методом быстрого переключения между точками доступа, с тем, чтобы свести к минимуму время роуминга.

X КАЧЕСТВО ОБСЛУЖИВАНИЯ В СЕТЯХ WI-FI. СТАНДАРТ IEEE 802.11E

Для некоторых приложений Wi-Fi сети, таких как передача голоса по IP VoIP (англ. *Voice over IP*) или потоковое видео, имеют большое значение параметры качества обслуживания (QoS), например, задержка и ее джиттер или потери пакетов. Для этих приложений должна быть реализована возможность приоритезации трафика, которая определена в стандарте **IEEE 802.11e**.

Стандарт IEEE 802.11e (2005 г.) вносит ряд поправок, касающихся QoS для функций MAC-подуровня канального уровня WLAN. В систему вводится идентификатор QoS, которым помечаются пакеты приложений, в разной степени чувствительных к задержке, джиттеру или потерям.

Сетевому трафику может быть назначен один из восьми уровней приоритета (0-7), в зависимости от его срочности. Например, сообщения электронной почты допускают значительно большую задержку по сравнению с мультимедийными приложениями.

В стандарте определены четыре категории доступа АС (англ. *Access Categories*), одна из которых присваивается пакету перед отправкой (таблица 3.6).

Таблица 3.6. Соответствие категорий доступа классам приоритета трафика

Приоритет	Категория доступа	Назначение
0	0	Best Effort
1	0	Background
2	0	Background
3	1	Video Probe
4	2	Video
5	2	Video
6	3	Voice
7	3	Voice

Функции MAC-уровня для доступа к разделяемой среде передаче DCF и PCF, описанные в разделе 4.1, стандарт IEEE 802.11e заменяет *гибридной функцией координации* HCF (англ. *Hybrid Coordination Function*), в которой DCF соответствует метод доступа EDCA (англ. *Enhanced Distributed Channel Access*), а PCF – HCCA (англ. *HCF Controlled Channel Access*), которые работают с учетом классов приоритета трафика TC (англ. *Traffic Classes*).

EDCA

EDCA реализует конкурентный механизм доступа к среде, поэтому не дает гарантии QoS. Приоритезация трафика осуществляется в данном методе с помощью регулирования длительности промежутков времени DIFS. Вместо DIFS определен *арбитражный межкадровый промежуток* AIFS (англ. *Arbitration Inter Frame Space*), длительность которого тем меньше, чем выше приоритет пакета. Таким образом, более срочный трафик имеет шанс быть переданным с меньшей задержкой. Преимуществами данного метода являются легкость его настройки и простота применения.

HCCA

Метод HCCA очень схож с PCF и реализуется на основе опроса станций о готовности их к передаче, при этом, чем выше приоритет передаваемой информации, тем выше эта станция окажется в опросном листе, и тем больший промежуток времени будет выделен ей для передачи. При этом задержка низкоприоритетного трафика может достигать значительных размеров. Данный механизм сложнее в использовании, чем описанный выше EDCA, но позволяет тонкую настройку TC и обеспечивает гарантированные параметры QoS. Для более подробной информации см. раздел 4.2.

XI VOICE ENTERPRISE

Передача голоса в корпоративной сети Wi-Fi предъявляет дополнительные требования к параметрам QoS (на всем протяжении сеанса связи должны поддерживаться низкие значения задержки, джиттера задержки и потерь), а также к производительности передачи голосовой информации в реальных условиях, т.е. в общем потоке с трафиком других приложений.

Wi-Fi *сертификация Voice Enterprise* основана на соответствии системы следующим стандартам и сертификациям:

1) **Базовая сертификация физического уровня**, а именно 802.11a, b, g, n или ac. Wi-Fi сертификация Voice Enterprise не зависит от физического уровня и допускается любая комбинация перечисленных выше радиointерфейсов.

2) **WMM** (англ. *Wi-Fi MultiMedia*) – сертификация Wi-Fi Alliance, основанная на стандарте IEEE 802.11e, задает приоритезацию трафика.

3) **WMM-AC** (англ. *WMM Admission Control*) – дополнительная сертификация для управления полосой пропускания улучшает производительность Wi-Fi сети в режиме реального времени для передачи голоса и видео. Точка доступа оценивает кадр запроса от клиентского устройства на соответствие условиям нагрузки сети и пропускной способности канала. Если точка доступа может удовлетворить запрос, она разрешает клиенту передачу потока трафика. В противном случае запрос будет отклонен и клиент должен принять решение либо отложить передачу, либо переключиться к другой точке доступа, либо ограничить скорость информационного потока.

4) **Стандарт IEEE 802.11r** определяет бесшовный и быстрый роуминг FT (англ. *Fast Basic Service Set (BSS) Transition*) – переключение от одной точки доступа к другой, без которого невозможно обеспечить качество звонка мобильного абонента в Wi-Fi сети. При этом время, затрачиваемое на переключение, должно быть менее 20 мс.

5) **WPA2-Enterprise** – сертификация на основе стандарта IEEE 802e (см. раздел 10), определяющая безопасность информации в Wi-Fi сети. Сертификация поддерживает пользователей WPA2, удаленную аутентификацию с использованием RADIUS-сервера и различных EAP методов.

6) **WMM-PS** (англ. *WMM Power Saving*) – сертификация, оптимизирующая порядок обмена данными клиента с точками доступа для большей энергоэффективности.

Сертификация предполагает следующие виды тестирования оборудования:

1) Тестирование на соблюдение протоколов:

- **Radio Resource Measurement:** элементы 802.11k. Обязательно для инфраструктуры и клиентов.

- **Fast BSS transition:** элементы 802.11r. Обязательно для инфраструктуры и клиентов.
 - **Wireless network management:** 802.11v BSS Transition Management Опционально для инфраструктуры и клиентов.
- 2) Соответствие требованиям производительности (Обязательно для инфраструктуры и клиентов.).
- **Задержка** (включая части роуминга): менее 50 мс в одну сторону.
 - **Джиттер:** менее 50 мс.
 - **Потеря пакетов:** менее 1%.
 - **Последовательно потерянных пакетов:** не более трех.

Поддерживающие Voice Enterprise продукты предназначены для работы в корпоративной среде, с «тяжёлым» гетерогенным трафиком и жёсткими требованиями к производительности, безопасности и мобильности. Сертификации подлежат как точки доступа, так и абонентские устройства.

Таким образом, программа сертификации Voice Enterprise поддерживает передачу голоса в корпоративной сети, опираясь на функциональные возможности других программ сертификации, в том числе WPA2-Enterprise для обеспечения безопасности, WMM QoS WMM-Admission Control для поддержания передачи на должном уровне качества обслуживания, а также WMM-Power Save для энергосбережения.

XII WI-FI 6 VS WI-FI 5, WI-FI 6E

12.1 Поколения Wi-Fi

Wi-Fi 5 (802.11ac) и Wi-Fi 6 (802.11ax) – два разных поколения одной технологии.

Отвечающая за разработку стандартов Wi-Fi организация Wi-Fi Alliance помимо стандартных технических названий (802.11ac, 802.11ax и так далее) с недавних пор начала присваивать стандартам Wi-Fi более понятное и простое цифровое обозначение (рис. 3.21).

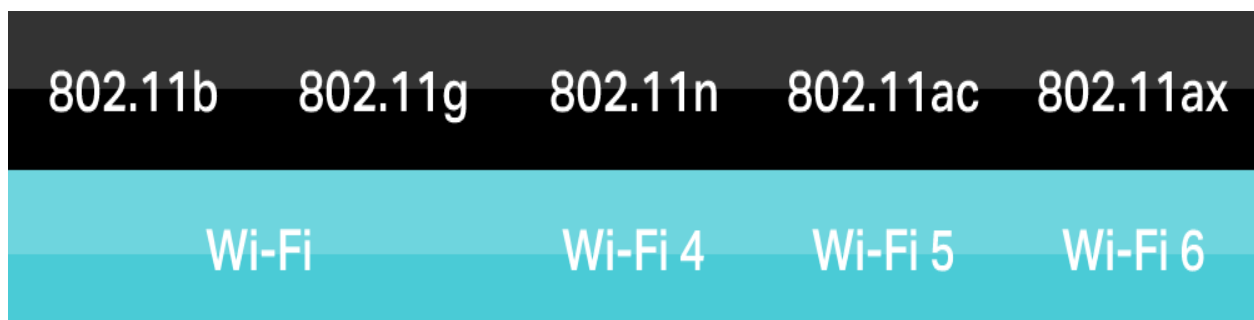


Рис. 3.21. Поколения и стандарты Wi-Fi

Wi-Fi 6 поддерживает технологии OFDMA, 1024-QAM, MU-MIMO для входящего и исходящего трафика, Target Wake Time и BSS Coloring, WPA3.

Wi-Fi 6 обеспечивает более высокую скорость и эффективность, а также улучшенное качество работы в условиях высокой плотности клиентов.

12.2 Соотношение скоростей Wi-Fi

Максимальная номинальная скорость Wi-Fi 6 увеличена до 9,6 Гбит/с, что примерно на 40 % выше, чем скорость Wi-Fi 5 (рис. 3.22).

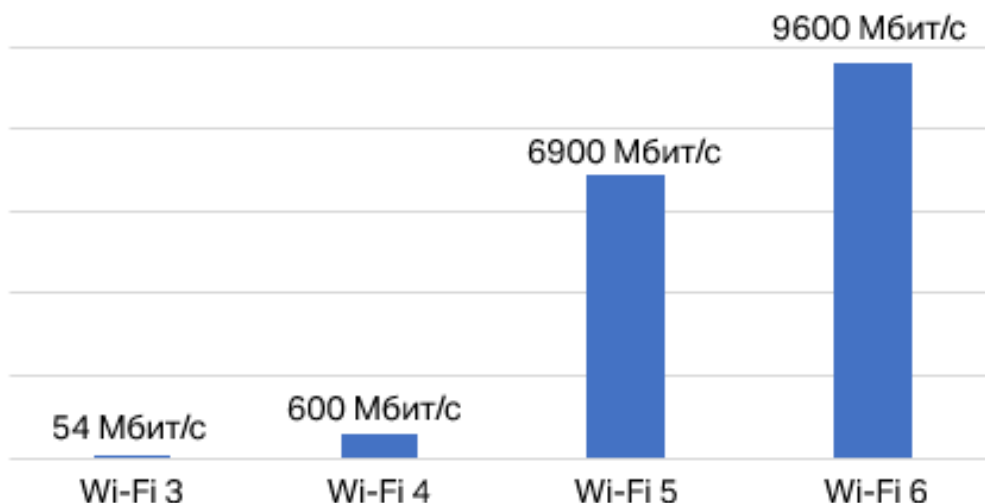


Рис. 3.22. Соотношение скоростей Wi-Fi

Скорость передачи данных Wi-Fi 5 составляет до 6.9 Гбит/с. Он использует 256-QAM механизм модуляции сигнала и имеет максимальную ширину канала 80 МГц.

В Wi-Fi 6 скорость передачи может достигать 9.6 Гбит/с в зависимости от конкретной модели. Продвинутый механизм модуляции сигнала (1024-QAM) и более широкие каналы (до 160 МГц) позволяют Wi-Fi 6 обеспечивать более быстрый и эффективный поток данных даже в условиях высокой загруженности сети.

12.3 Модуляция в Wi-Fi

В 1024-QAM увеличена длина каждого символа кодировки с 8 бит (в 256-QAM на стандарте Wi-Fi 5) до 10 бит, что повышает скорость передачи данных и эффективность использования спектра примерно на 25%, т.к. в каждый пакет будет помещаться больше данных (рис. 3.23-3.24).

Это позволяет использовать приложения, требовательные к пропускной способности, например, VR.

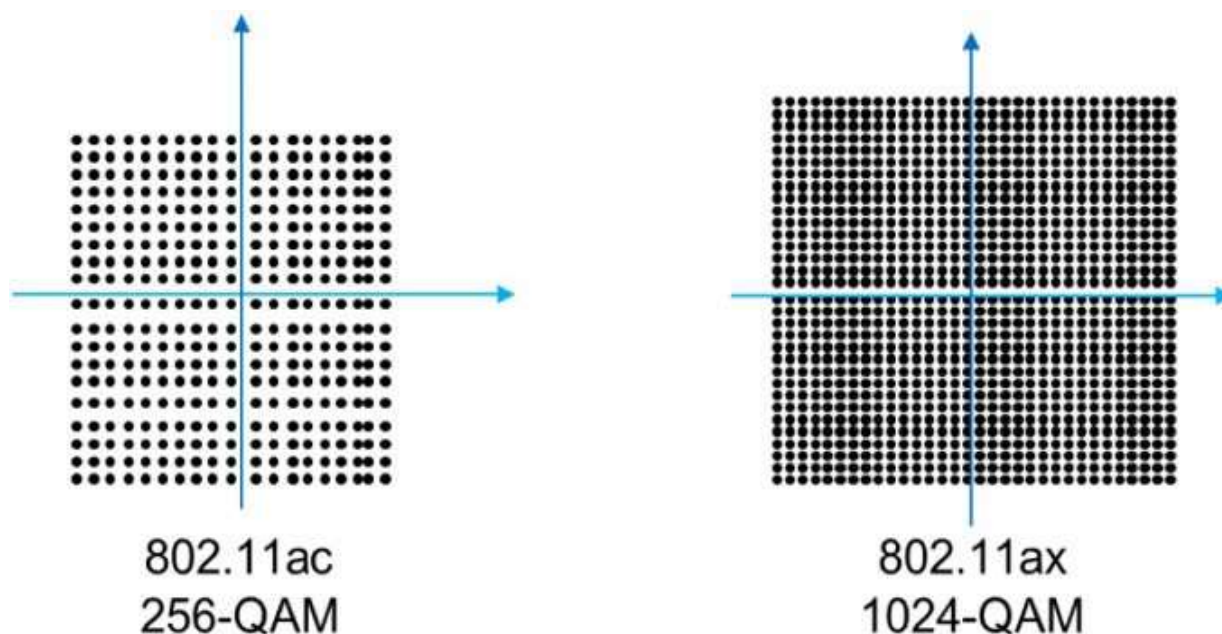


Рис. 3.23. Сигнальное созвездие модуляции в Wi-Fi

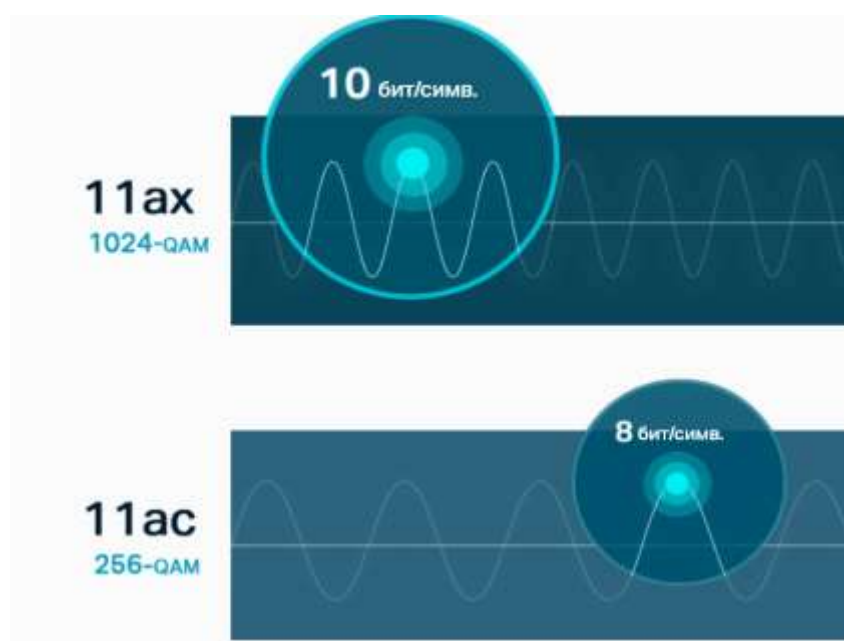


Рис. 3.24. Длина символа модуляции в Wi-Fi

Данное улучшение работает только в условиях, где уровень сигнала высокий, а шум низкий. Например, уровень мощности приёма сигнала, необходимый для декодирования кадра с модуляцией 1024-QAM 5/6 для канала 80 МГц, должен быть не ниже -45 дБм, а достичь этого можно только в случае, если приёмник и передатчик находятся на близком расстоянии друг от друга.

12.4 Диапазоны частот в Wi-Fi

Если разработчики стандарта IEEE 802.11ac (Wi-Fi 5) решили полностью отказаться от привычного Wi-Fi диапазона 2.4 ГГц с переходом в полосу 5 ГГц для повышения скорости передачи, связанного с большей шириной канала, и

увеличения количества каналов с сокращением межканальных помех, то IEEE 802.11ax возвращает двухдиапазонный режим – 2,4 и 5 ГГц для обратной совместимости стандартов и устройств, работающих на разных частотах (табл. 3.7, рис. 3.25).

Таблица 3.7. Диапазоны частот и ширина полосы канала

Стандарт	Wi-Fi 5	Wi-Fi 6
Диапазон(ы) частот, ГГц	5	2,4 и 5
Максимальная ширина полосы, МГц	80	160

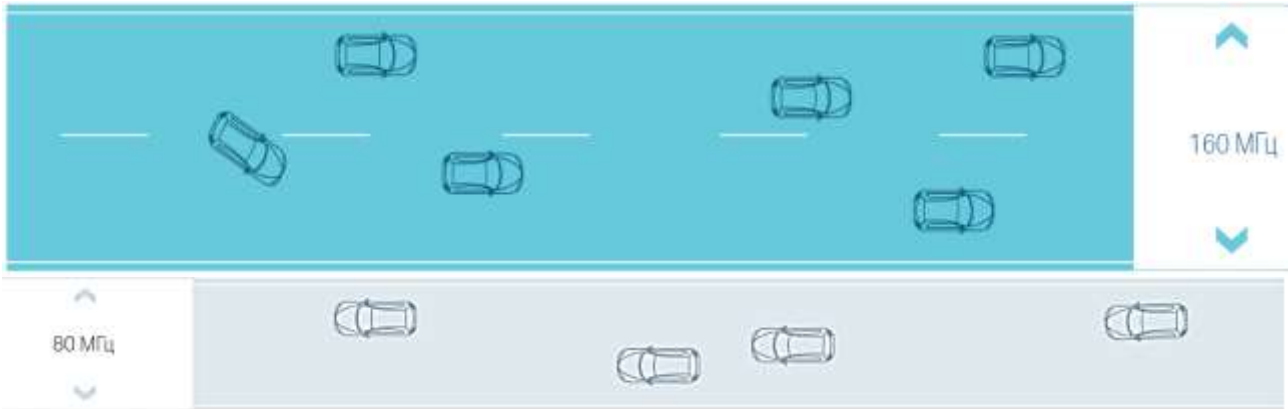


Рис. 3.25. Соответствие пропускной способности канала ширине полосы

12.5 OFDMA

OFDMA (Orthogonal Frequency Division Multiple Access) – множественный доступ с ортогональным разделением частот.

С увеличением числа клиентских устройств производительность сети падает из-за передачи большого числа коротких пакетов и как результат – большего количества задержек и коллизий.

OFDMA делит спектр на ресурсные единицы и распределяет их сразу между несколькими пользователями (рис. 3.26-3.27).



Рис. 3.26. Распределение ресурсов в разных версиях Wi-Fi

В Wi-Fi 5 количество поднесущих – 256 или 512, в Wi-Fi 6 это значение достигает 1024 и даже 2048, что способствует увеличению покрытия сети, и, соответственно, скорости передачи на 11%.

В 802.11ax поддерживается три типа циклического префикса:

- 0,8 мкс – для обеспечения обратной совместимости стандартов;
- 1,6 мкс – для повышения эффективности передачи внутри и вне помещения в восходящем направлении при MU-MIMO/OFDMA;
- 3,2 мкс – для повышения надёжности при передаче вне помещения в восходящем направлении при MU-MIMO/OFDMA.

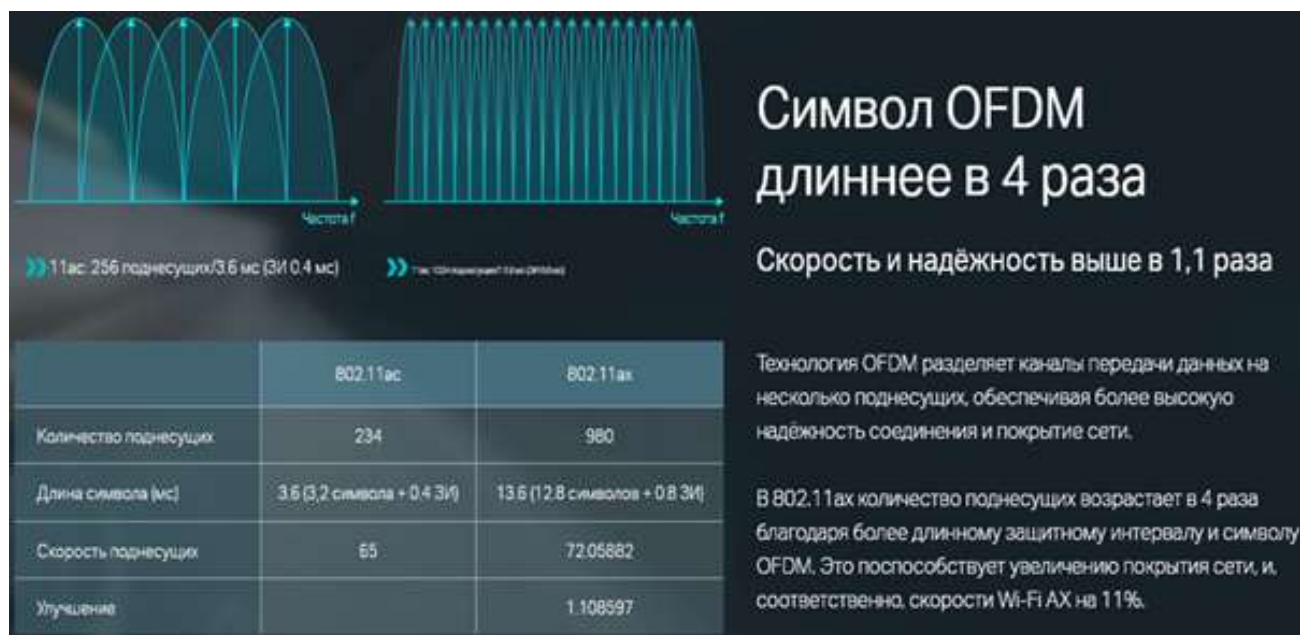


Рис. 3.27. Характеристики IEEE 802.11ac и IEEE 802.11ax (ширина канала 80 МГц)

12.6 MIMO

Антенны — ещё одна важная вещь для сравнения Wi-Fi 6 и Wi-Fi 5. В стандартных маршрутизаторах переменного тока одновременно может передавать только одно устройство, но с технологией MU-MIMO (многопользовательский множественный вход – множественный выход, англ. Multi-User Multiple Input – Multiple Output) несколько устройств могут обмениваться данными с маршрутизатором одновременно (рис. 3.28).

В стандарте Wi-Fi 5 используется 4 x 4 MU-MIMO. Это означает, что он имеет 4 пространственных потока и может обмениваться данными максимум с четырьмя устройствами одновременно. Опционально в Wi-Fi 5 количество пространственных потоков может быть увеличено до 8.

В стандарте Wi-Fi 6 используется 8 x 8 MU-MIMO. Это означает, что он имеет 8 пространственных потоков и может обмениваться данными максимум с восемью устройствами одновременно. Особенно это важно для мест массового скопления людей.

Wi-Fi 5 поддерживает MU-MIMO в нисходящем (англ. *Downlink*) канале, а Wi-Fi 6 поддерживает MU-MIMO в обоих направлениях.



Рис. 3.28. Пространственно-временное кодирование

12.7 Формирование луча (beamforming)

Формирование луча – одно из важных свойств Wi-Fi 6. Это не новая, а улучшенная функция для повышения производительности новой технологии Wi-Fi, которая опционально присутствовала в Wi-Fi 5.

Beamforming – это функция, с помощью которой маршрутизатор определяет получателя и отправляет данные направленно (рис. 3.29).

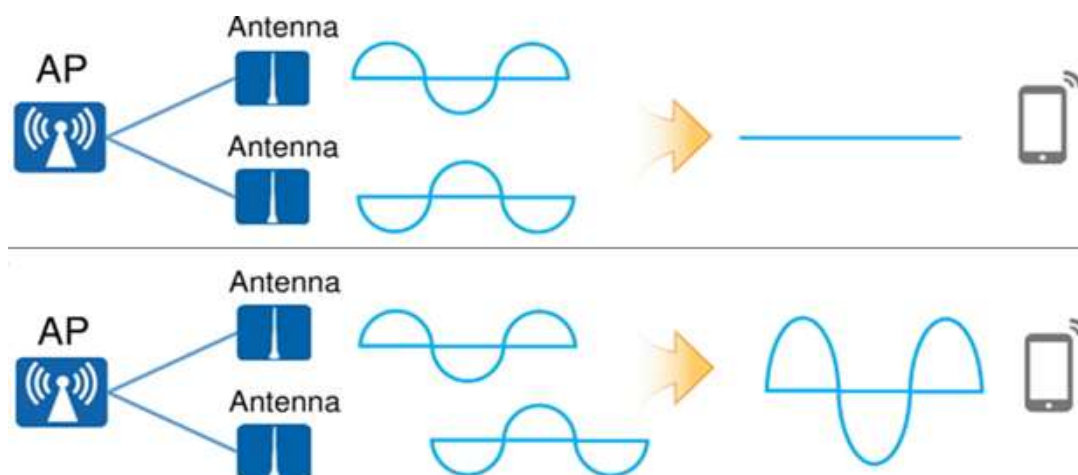


Рис. 3.29. Beamforming

12.8 Протоколы безопасности

Безопасность очень важна в сетях связи. Это справедливо и для беспроводных сетей Wi-Fi.

Для обеспечения безопасности используются различные протоколы. Wi-Fi 5 поддерживает протоколы WPA и WPA 2 для защиты беспроводного соединения. В последние годы WPA 2 был наиболее часто используемым протоколом безопасности беспроводной локальной сети, но с развитием технологий уязвимости WPA 2 увеличиваются. Для решения проблем уязвимости был разработан протокол и выпущен в 2018 г. WPA 3, который рекомендуется к применению в стандарте Wi-Fi 6. Причём Wi-Fi 6 поддерживает протоколы WPA, WPA 2 и WPA 3 одновременно.

В протоколе WPA 3 реализованы следующие новые функции для личного и для корпоративного использования:

- **индивидуальное шифрование данных.** При входе в публичную сеть WPA 3 регистрирует новое устройство способом, не подразумевающим использование общего пароля. В WPA 3 используется протокол DPP (англ. *Device Provisioning Protocol*) для сетей Wi-Fi, позволяющий пользователям использовать теги NFC или QR-коды для подключения устройств к сети. Кроме того, для обеспечения безопасности WPA 3 используется шифрование GCMP-256 вместо применявшегося ранее 128-битного шифрования.

- **протокол SAE** (одновременная аутентификация равных, англ. *Simultaneous Authentication of Equals*). Этот протокол используется для создания безопасного «рукопожатия», при котором сетевое устройство подключается к беспроводной точке доступа, и оба устройства обмениваются данными для проверки аутентификации и подключения. Даже если пароль пользователя недостаточно надёжный, WPA 3 обеспечивает более безопасное взаимодействие по протоколу DPP для сетей Wi-Fi.

- **усиленная защита от атак методом подбора пароля.** Протокол WPA 3 защищает от подбора пароля в автономном режиме. Пользователю позволяет выполнить только одну попытку ввода пароля. Кроме того, необходимо взаимодействовать напрямую с устройством Wi-Fi: при каждой попытке ввода пароля требуется физическое присутствие. В протоколе WPA 2 отсутствует встроенное шифрование и защита данных в публичных открытых сетях, что делает атаки методом подбора пароля серьёзной угрозой.

Две других опции, не зависящих от WPA 3, *улучшенное открытие* (англ. *Enhanced Open*) и *простое соединение* (англ. *Easy Connect*) повышают безопасность сетей Wi-Fi нового типа.

Сети Wi-Fi **Enhanced Open** предоставляют пользователям неавторизованное шифрование данных, что значительно усиливает безопасность. Защита прозрачна для пользователя и основана на шифровании *Opportunistic Wireless Encryption* (OWE), определенного в спецификации Internet Engineering Task Force RFC8110 и спецификации беспроводного шифрования Wi-Fi Alliance, *Opportunistic Wireless Encryption Specification*, которые были разработаны для защиты от пассивного прослушивания. Таким образом, при подключении к открытой сети с защитой WPA 3 весь передаваемый трафик по умолчанию будет шифроваться.

Wi-Fi Alliance разработал простой способ аутентификации Wi-Fi *Easy Connect*. Изначально он сделан для малопроизводительных IoT-устройств, но скорее всего этот способ авторизации понравится и простым пользователям. Подключить устройство к беспроводной сети можно будет путём сканирования его QR-кода.

Wi-Fi Easy Connect позволяет пользователям безопасно добавлять новое устройство в существующую Wi-Fi сеть, используя терминал с более надёжным интерфейсом, например, смартфон или планшет. Это может быть любое устройство, способное сканировать QR-код и запускать протокол *Device Provisioning Protocol (DPP)* разработанный Wi-Fi Alliance.

Выбранное устройство считается конфигуратором, а все остальные устройства являются дочерними для него и используют конфигуратор для подключения к сети.

Пользователь устанавливает безопасное соединение с дочерним устройством, сканируя его QR-код. Это запускает протокол DPP и автоматически предоставляет ключи, необходимые для доступа к сети.

Easy Connect обеспечивает простоту и гибкость сетей Wi-Fi:

- снимает необходимость запоминать и вводить пароли при подключении новых устройств;
- упрощает настройку и подключение устройств с помощью QR-кода;
- позволяет подключать к Wi-Fi сети устройства с отсутствующим пользовательским интерфейсом (датчики умных домов и элементы IoT);
- Easy Connect не связан с WPA3 поэтому его смогут использовать устройства, поддерживающие как WPA2, так и WPA3;
- позволяет заменять точку доступа без необходимости повторной регистрации всех устройств;

Таким образом, три слагаемых WPA3, Enhanced Open и Easy Connect в сумме равны безопасности беспроводной сети.

12.9 BSS-КОЛОРИРОВАНИЕ

BSS Coloring – это новая функция Wi-Fi 6. Она не используется в Wi-Fi 5. С помощью этого метода можно предотвратить радиосигналы, исходящие от перекрывающихся BSS (англ. *Base Service Station*).

BSS Coloring повышает эффективность OFDMA технологии при подключении в людных местах.

Помехи от соседних беспроводных сетей могут негативно влиять на качество сигнала Wi-Fi. BSS Color помечает каждый пакет данных определённым идентификатором, как бы «подкрашивая» пакеты, принадлежащие разным сетям, разными цветами, даже когда они передаются в одном канале (рис. 3.30). Таким образом, каждый абонент принимает, благодаря «раскраске», только предназначенные ему пакеты (роутер не тратит время на расшифровку чужих пакетов). Это максимально снижает задержки при передаче данных, а также интерференцию (коллизии) от соседних беспроводных сетей.



Рис. 3.30. Колорирование: а – сеть без раскраски, все устройства используют канал; б – раскрашенная сеть передача в канале только внутри одного цвета

Для людных мест и помещений эта функция особенно важна (рис. 3.31).



Рис. 3.31. Колорирование внутри помещений

12.10 ЭНЕРГОСБЕРЕЖЕНИЕ

Технология **планировщик времени пробуждения** TWT (англ. *Target Wake Time*) позволяет роутеру «договариваться» с подключёнными гаджетами о частоте коммуникации, чтобы сократить энергопотребление и продлить срок службы их аккумуляторов (рис. 3.32).

Функция Target Wake Time (TWT) позволяет устройствам определять, когда и как часто они должны пробуждаться для передачи данных.

Таким образом, с помощью этой функции ограничивается активность устройств, во время которой происходит наибольшее потребление всего заряда батареи. Это обеспечивает более продолжительное время автономной работы конечных устройств.

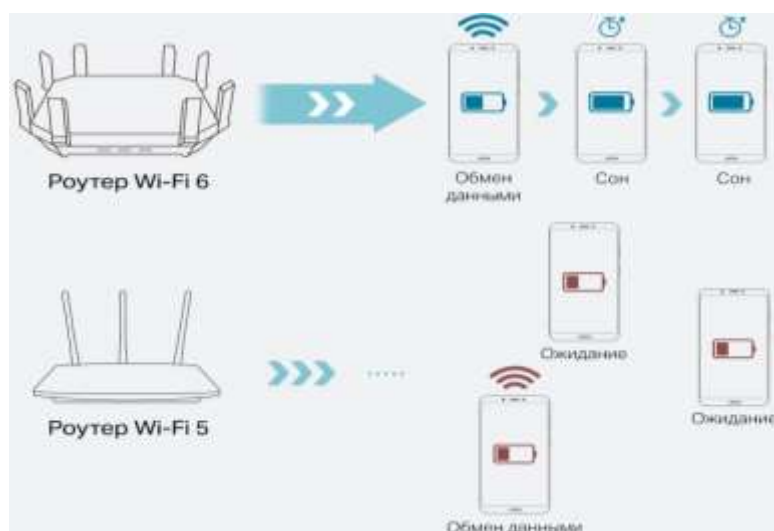


Рис. 3.32. Планировщик времени пробуждения в Wi-Fi 6

12.11 ЭФФЕКТИВНОСТЬ WI-FI 6

Ключевое преимущество шестого поколения Wi-Fi — производительность в условиях высокой плотности клиентов (например, в офисах, торговых центрах, на стадионах).

Несмотря на то, что номинальный прирост скорости по сравнению с Wi-Fi 5 составляет около 40 %, общая пропускная способность всей сети увеличена до 300 %, а задержка — снижена на 75 %.

А отличие от предыдущих стандартов, Wi-Fi 6 также обеспечивает Wi-Fi на высокой скорости для большого числа одновременно подключённых клиентских устройств (рис. 3.33).

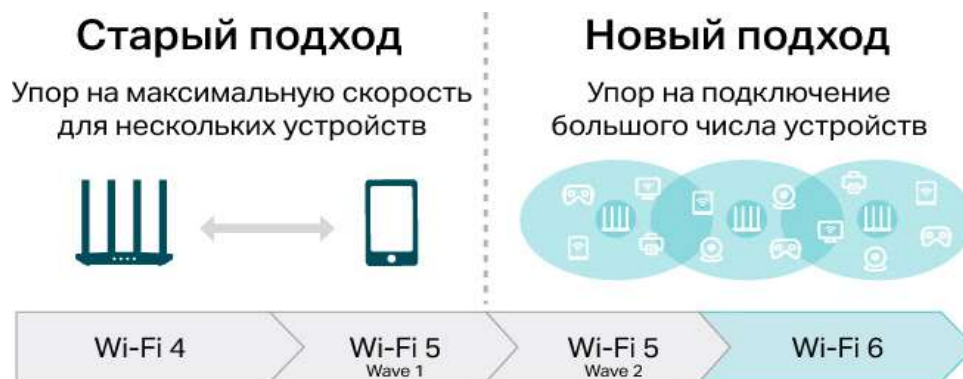


Рис. 3.33. Эффективность Wi-Fi 6

XIII Wi-Fi 6E

Wi-Fi 6E использует те же технологии стандарта IEEE 802.11ax, что и Wi-Fi 6 для беспроводного подключения, но расширяет его возможности до нового диапазона Wi-Fi, называемого 6 ГГц, обеспечивая большую ёмкость, более

широкие каналы и меньшие помехи. Буква Е в названии технологии означает «Extended».

Наибольшее преимущество Wi-Fi 6Е перед Wi-Fi 6 заключается в наличии доступных для использования дополнительных 1200 МГц полосы пропускания. Чем больше диапазон частот, тем больше каналов может использовать Wi-Fi.

Wi-Fi 6Е имеет в своём распоряжении до 14 дополнительных каналов шириной 80 МГц или 7 дополнительных каналов 160 МГц (рис. 3.34).

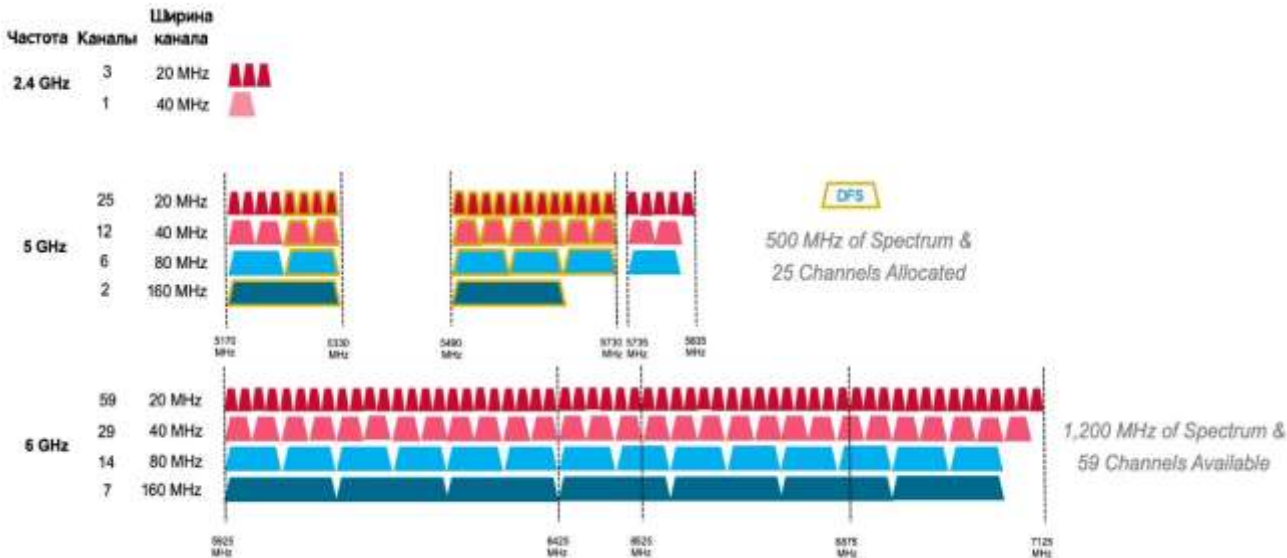


Рис. 3.34. Распределение каналов в стандартах Wi-Fi 5, Wi-Fi 6 и Wi-Fi 6Е

С другой стороны, как у всех новых, «неустоявшихся» технологий, у Wi-Fi 6Е есть недостаток, который он таится в том самом диапазоне 6 ГГц. Этот спектр использует более короткие длины волн, которые подходят для быстрой передачи данных, но испытывают трудности с преодолением больших расстояний и сильнее подвержены помехам от физических препятствий, например, толстых стен зданий.

Вероятно, проблема будет решаться с помощью создания устойчивых ячеистых сетей, состоящих из основного маршрутизатора и нескольких устройств-ретрансляторов. Иными словами, один роутер будет распределять сигнал в сети через несколько передатчиков.

XIV ИТОГ

Основные различия характеристик стандартов Wi-Fi заключены в таблицу 3.8.

Таблица 3.8. Характеристики стандартов IEEE 802.11/a/b/g/n/ac/ax

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

8 января 2024 года официально выпущен стандарт Wi-Fi 7 (IEEE 802.11be), который представляет собой гигантский шаг вперёд: теоретическая пропускная способность вырастет с 9,6 Гбит/с (Wi-Fi 6) до фантастических 46 Гбит/с.

Основные улучшения в стандарте Wi-Fi 7:

- четырёхкратное увеличение пропускной способности: Wi-Fi 7 – это беспроводной стандарт будущего, о чем говорит его пропускная способность в 46 Гбит/с (это в 4,8 раза выше, чем у стандарта Wi-Fi 6);
- в 100 раз лучше латентность в худшем сценарии: латентность Wi-Fi 7 будет в целых сто раз лучше по сравнению с латентностью Wi-Fi 6 в худшей ситуации. Кроме того, латентность в приложениях дополненной/виртуальной реальности улучшена вплоть до пятнадцатикратной величины.
- увеличенная емкость сети: каналы связи шириной 320 МГц и технология MLO делают сети Wi-Fi 7 в пять раз более емкими по сравнению с Wi-Fi 6.
- повышенная стабильность: благодаря тому, что цифровые устройства могут использовать много разных частотных диапазонов и каналов связи, Wi-Fi 7 помогает устранить помехи и тем самым поднять стабильность сетевого подключения.

Сравнительные характеристики стандартов Wi-Fi 5, 6, 6E, 7 представлены в таблице 3.9.

Таблица 3.9. Сравнительные характеристики стандартов Wi-Fi 5, 6, 6E, 7

	WiFi 5	WiFi 6	WiFi 6E	WiFi 7
Дата выхода	2013	2019	2021	2024
Стандарт IEEE	802.11ac	802.11ax	802.11ax	802.11be
Макс. скорость	3.5 Гб/с	9.6 Гб/с	9.6 Гб/с	46 Гб/с
Диапазоны	5 ГГц	2.4 ГГц, 5 ГГц	2.4 ГГц, 5 ГГц, 6 ГГц	2.4 ГГц, 5 ГГц, 6 ГГц
Размер каналов связи	до 160 МГц	до 160 МГц	до 160 МГц	до 320 МГц
Модуляция	256-QAM OFDM	1024-QAM OFDMA	1024-QAM OFDMA	4096-QAM OFDMA
MIMO	4×4 MIMO DL MIMO	8×8 UL/DL MU-MIMO	8×8 UL/DL MU-MIMO	16×16 UL/DL MU-MIMO

Время не стоит на месте и новые технологии уже не за горами.

СПИСОК СОКРАЩЕНИЙ

AC	Access Categories
AIFS	Arbitration Inter Frame Space
AP	Access Point
CCK	Complementary Code Keying
CCMP	Counter-Mode with CBC-MAC Protocol
CFP	Contention Free Period
CP	Contention Period
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
DCF	Distributed Coordination Function
DIFS	DCF Interframe Space
DS	Distribution System
EAP-LEAP	Extensible Authentication Protocol - Lightweight EAP
EAPOL	EAP Encapsulation Over LAN
EAP-PSK	EAP - Pre-Shared Key
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol - Tunneled TLS
EDCA	Enhanced Distributed Channel Access
ESS	Extended Service Set
FT	Fast Basic Service Set Transition
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function
IBSS	Independent Basic Service Set
LED	Light-Emitting Diode
LLC	Logical Link Control
MAC	Media Access Control
MCS	Modulation & Coding Scheme
MD5	Message Digest 5
MIC	Message Integrity Check
MIMO	Multiple Input Multiple Output

MU-MIMO	Multi User MIMO
OSI	Open System Interconnection
OTP	One-Time Password
PBCC	Packet Binary Convolutional Code
PCF	Point Coordination Function
PEAP	Protected Extensible Authentication Protocol
RTS	Ready To Send
SSL	Secure Sockets Layer
SU-MIMO	Single User MIMO
RADIUS	Remote Authentication Dial-In User Server
TC	Traffic Classes
TLS	Transport Layer Security
VoIP	Voice over IP
WMM	Wi-Fi Multimedia
WMM-AC	WMM Admission Control
WMM-PS	WMM Power Saving
WNIC	Wireless Network Interface Controller
WPA	Wi-Fi Protected Access
WPA-PSK	WPA - Pre-Shared Key

ЛИТЕРАТУРА

- 1 Беделл П. Беспроводные технологии / Пер. с англ. – М.: НТ Пресс, 2008. – 441 с.
- 2 Росс Дж. Wi-Fi. Беспроводная сеть / Пер. с англ. – М.: НТ Пресс, 2007. – 320 с.
- 3 Палмер М., Синклер Р.Б. Проектирование и внедрение компьютерных сетей. Учебн. курс. 2-е изд. / Пер. с англ. – СПб.: БХВ-Петербург, 2004. – 752 с.
- 4 Enterprise Mobility 7.3 Design Guide / WLAN RF Design Considerations. [Электронный ресурс] – URL: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob73dg/emob73/ch3_WLAN.html (дата посещения 01.03.2025).
- 5 Сергей Пахомов. Анатомия беспроводных сетей // КомпьютерПресс. 2002. №7. С.167-175.
- 6 What is MIMO. [Электронный ресурс] – URL: <https://www.techtarget.com/searchmobilecomputing/definition/MIMO> (дата посещения 23.02.2025).
- 7 Huang Pi Understanding IEEE 802.11ac VHT Wireless // Electronic Design. 2012. [Электронный ресурс] – URL: <http://electronicdesign.com/communications/understanding-ieee-80211ac-vht-wireless> (дата посещения 25.02.2025).
- 8 Geier E. All about beamforming, the faster Wi-Fi you didn't know you needed // PC World. 2013. [Электронный ресурс] – URL: <http://www.pcworld.com/article/2061907/all-about-beamforming-the-faster-wi-fi-you-didnt-know-you-needed.html> (дата посещения 12.09.2024)
- 9 Бугрименко Д. Проблемы безопасности в беспроводных ЛВС IEEE 802.11и решения Cisco Wireless Security Suite // Cisco Systems, Inc. 1992–2002. – 47 с.
- 10 Фукалов А. Азы протокола WPA2 [Электронный ресурс] – URL: <https://vk.com/@anatolyfukalov-azy-protokola-wpa2> (дата посещения 12.07.2024).
- 11 IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements IEEE // Std 802.11r™-2008.
- 12 802.11e for QoS. [Электронный ресурс] – URL: <http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11e.php> (дата посещения 10.07.2024).
- 13 Wi-Fi CERTIFIED™ Voice-Enterprise // Wi-Fi Alliance® May 2012.