Беспроводные системы ПД

Лекция 02
Технология Wi-Fi (семейство IEEE 802.11)

Wi-Fi — торговая марка организации Wi-Fi Alliance для локальных беспроводных сетей WLAN на базе спецификаций семейства IEEE 802.11. Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity — «беспроводное качество») понимают целое семейство стандартов передачи цифровых потоков данных по радиоканалам. Любое оборудование, соответствующее одному из стандартов семиейства IEEE 802.11, может быть протестировано в Wi-Fi Alliance и получить соответствующий сертификат и право нанесения логотипа Wi-Fi.

Wi-Fi Alliance или — объединение крупнейших производителей компьютерной техники и беспроводных устройств, работающих по технологии Wi-Fi. Альянс разрабатывает семейство стандартов 802.11 и методы построения WLAN. Основан в 1999 компаниями 3Com, Aironet (Cisco), Harris Semiconductor (Intersil), Lucent (Agere), Nokia и Symbol Technologies как альянс **WECA (Wireless Ethernet Compatibility Alliance)**. В 2000 переименован в Wi-Fi Alliance. На сегодняшний день альянс объединяет около 600 компаний, работающих в области беспроводных технологий.

IEEE 802.11 — набор стандартов связи для коммуникации в WLAN в частотных диапазонах 0,9; 2,4; 3,6 и 5 ГГц.

Список стандартов (частично)

При описании стандарта в скобках указан год его принятия. Скорость указана брутто, т. е. с учетом служебного трафика. Как правило, в самых идеальных условиях полезная скорость передачи данных по Wi-Fi не превышает 50% канальной.

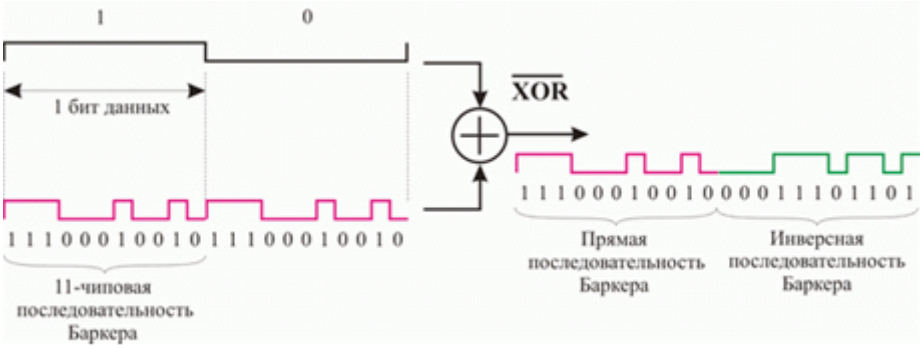
- **802.11** — изначальный 1 Мбит/с и 2 Мбит/с, 2,4 ГГц и ИК стандарт (1997).
- **802.11a** — 54 Мбит/с, 5 ГГц стандарт (1999, выход продуктов в 2001).
- **802.11b** — улучшения к 802.11 для поддержки 5,5 и 11 Мбит/с, 2,4 ГГц (1999).
- **802.11g** — 54 Мбит/с, 2,4 ГГц стандарт (обратно совместим с **b**) (2003).
- **802.11n** — увеличение скорости передачи данных (600 Мбит/с). 2,4 или 5 ГГц. Обратно совместим с **802.11a/b/g** (сентябрь 2009).
- **802.11u** — взаимодействие с не-802 сетями (например, сотовыми).
- **802.11v** — управление беспроводными сетями.
- **802.11y** — дополнительный стандарт связи, работающий на частотах 3,65–3,70 ГГц. Обеспечивает скорость до 54 Мбит/с на расстоянии до 5000 м на открытом пространстве.
- **802.11ac** — Скорость передачи данных — до 6,77 Гбит/с для устройств, имеющих 8 антенн. (январь 2014).

- **802.11ad** — новый стандарт с дополнительным диапазоном 60 ГГц (частота не требует лицензирования). Скорость передачи данных — до 7 Гбит/с.
- **802.11ah** — стандарт, предназначенный для работы в диапазоне ~900 МГц. Предполагается, что он позволит обеспечить скорость до 40 Мбит/с. Основное назначение — интернет-вещей. (2007). В 2016 Wi-Fi Alliance анонсировал расширение стандарта, получившее название Wi-Fi HaLow.

Первый стандарт 802.11 предусматривал два типа среды передачи: радиочастота 2,4 ГГц и инфракрасный диапазон 850–950 нм. ИК-устройства не были широко распространены и в будущем развития не получили. В диапазоне 2,4 ГГц было предусмотрено два способа расширения спектра:

- методом скачкообразного изменения частоты (FHSS)
- методом прямой последовательности (DSSS).

В первом случае все сети используют одну и ту же полосу частот, но с различными алгоритмами перестроения. Во втором случае появляются частотные каналы от 2412 МГц до 2472 МГц с шагом 5 МГц, сохранившиеся по сей день. В качестве расширяющей последовательности используется последовательность Баркера длиной 11 чипов.



***Важно:* Под чипом понимается элементарный символ последовательности.** *Этот термин введен, чтобы не путать его с реальным битом данных.*
При этом максимальная скорость передачи данных (канальная, брутто) составляла от 1 до 2 Мбит/с. Таким образом чиповая скорость составляет 22 Мбит/с. Для передачи сигнала в 802.11 использовалась 2-х и 4-х позиционная манипуляция, при последней за один такт передачи передаются 2 бита (4 уровня сигнала).

На смену 802.11 пришёл **стандарт 802.11b**, в котором скорость передачи данных была увеличена до 5,5; 11 и 22 (опционально) Мбит/с. Увеличение скорости было достигнуто путём уменьшения избыточности помехоустойчивого кодирования с 1/11 до 1/2 и даже 2/3 за счёт внедрения блочных и сверточных кодов. Кроме того, максимальное число ступеней модуляции было увеличено до 8 на символ (3 бита на 1 бод). Ширина канала и используемые частоты не изменились, но при уменьшении избыточности и увеличении глубины модуляции выросли требования к соотношению сигнал/шум. Из-за невозможности увеличения мощности устройств по причине экономии энергии мобильных устройств и законодательных ограничений,пришлось сократить зону обслуживания на новых скоростях. Площадь обслуживания на унаследованных скоростях 1–2 Мбит/с не изменилась. От способа расширения

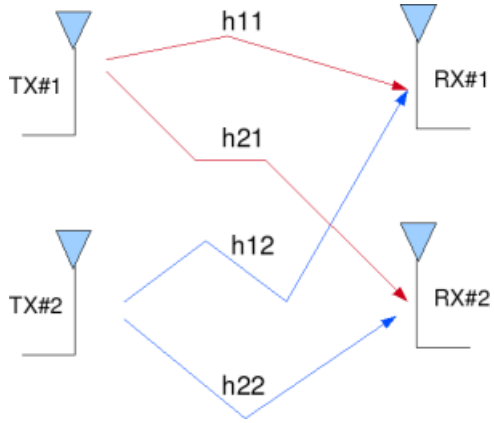
спектра методом скачкообразной перестройки частоты было решено полностью отказаться. Больше в семействе Wi-Fi он не использовался.

Следующее увеличение скорости до 54 Мбит/с было реализовано в стандарте **802.11a** (начал разрабатываться раньше, чем 802.11b, но финальная версия была выпущена позже, стандарты 802.11b и 802.11a не совместимы). Увеличение скорости в основном было достигнуто за счёт увеличения глубины модуляции до 64 уровней на символ (6 бит на 1 бод). Кроме того, была радикально пересмотрена радиочастотная часть: расширение спектра методом прямой последовательности было заменено на расширение спектра методом разделения последовательного сигнала на параллельные ортогональные поденсущие (OFDM). Использование параллельной передачи на 48 подканалах позволило снизить межсимвольную интерференцию за счёт увеличения длительности отдельных символов. Передача данных осуществлялась в диапазоне 5 ГГц. При этом ширина одного канала составляет 20 МГц. В отличие от стандартов 802.11 и 802.11b, даже частичное перекрытие этой полосы может привести к ошибкам передачи. В диапазоне 5 ГГц расстояние между каналами составляет именно 20 МГц.

Стандарт 802.11g был утверждён в октябре 2002 года. Он стал компиляцией 802.11a и 802.11b в диапазоне 2,4 ГГц: в нём поддерживались скорости обоих стандартов. Этот стандарт предусматривает использование диапазона частот 2,4 ГГц, обеспечивая скорость соединения до 54 Мбит/с (при модуляции OFDM) и гарантируя обратную совместимость со стандартом 802.11b, для чего он поддерживает также режим модуляции DSSS (скорость при этом 11 Мбит/с).

В **стандарте 802.11n** (в обоих диапазонах 2,4 и 5 ГГц) скорость была увеличена до 72 Мбит/с за счёт уменьшения защитных интервалов между передаваемыми символами. Для увеличения пропускной способности можно было объединить два канала по 20 МГц и получить 150 Мбит/с. При этом в диапазоне 2,4 ГГц может поместиться всего один расширенный канал в 40 МГц. Также, согласно стандарту, если в диапазоне 2,4 ГГц на котором используется канал удвоенной ширины появляется устройство, работающее на канале стандартной ширины, то устройство 802.11n обязано перейти на работу с каналом стандартной ширины. Соответственно, использовать каналы по 40 МГц рекомендуется только в диапазоне 5 ГГц. Для сосуществования каналов шириной 20/40 МГц точка доступа стандарта 802.11n должна переходить на другой канал или переключаться на использование канала шириной в 20 МГц, если соседняя точка доступа начинает передачу в одной из половин канала 40 МГц. Главным недостатком широких каналов является большее влияние на них помех и, соответственно, меньшее расстояние передачи данных. Существует также обратная модификация каналов производителями — уменьшение их ширины до 5 или 10 МГц, что позволяет увеличить дальность передачи ценой меньшей скорости.

Ещё одним способом повышения скорости стала технология MIMO: использование нескольких приёмопередатчиков, работающих на одной и той же частоте. Разделение каналов происходит за счёт пространственного разнесения антенн и математических операций над сигналом, принятым на разные антенны: он будет различаться в силу многолучевого распространения радиоволн. Стандарт 802.11n поддерживает MIMO 4x4:4 (четыре независимых канала) и обеспечивает скорость до 600 Мбит/с.



Однако данная технология требует высокого качества изготовления радио части устройств. Кроме того, данные скорости принципиально не реализуемы на мобильных терминалах (основной целевой группе стандарта Wi-Fi): наличие 4-х антенн на достаточном разнесении не может быть реализовано в малогабаритных устройствах как по соображениям отсутствия места, так и из-за отсутствия достаточного на 4 приёмопередатчика энергии.

В большинстве случаев скорость 600 Мбит/с является не более, чем маркетинговой уловкой и нереализуема на практике, так как фактически её можно добиться только между стационарными точками доступа, установленными в пределах одной комнаты при хорошем соотношении сигнал/шум.

Стандарт 802.11ac предусматривает максимальную скорость до 6,93 Гбит/с, однако фактически такая скорость ещё не достигнута ни на одном оборудовании, представленном на рынке. Увеличение скорости достигнуто за счёт увеличения полосы пропускания до 80 и даже до 160 МГц. Такая полоса не может быть предоставлена в диапазоне 2,4 ГГц, поэтому стандарт 802.11ac функционирует только в диапазоне 5 ГГц. Ещё один фактор увеличения скорости – увеличение глубины модуляции до 256 уровней на символ (8 бит на 1 бод) Такая глубина модуляции может быть получена только вблизи точки из-за повышенных требований к соотношению сигнал/шум. Указанные улучшения позволили добиться увеличения скорости до 867 Мбит/с. Остальное увеличение получено за счёт потоков MIMO 8x8:8. 867x8=6,93 Гбит/с. Технология MIMO была усовершенствована: впервые в стандарте Wi-Fi информация в одной сети может передаваться двум абонентам одновременно с использованием различных пространственных потоков.

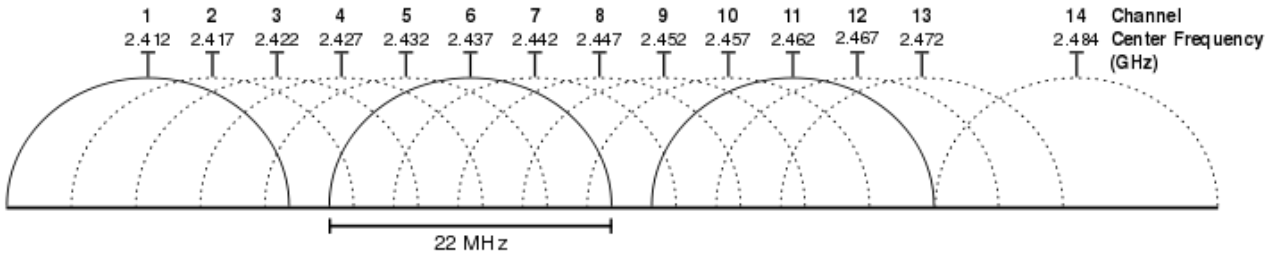
Частотная сетка 802.11

Как было указано ранее, сети 802.11 работают в частотных диапазонах 0,9; 2,4; 3,6 и 5 ГГц. Каждый из этих диапазонов разделяется на ряд поддиапазонов, или каналов. В разных странах существуют свои ограничения по использованию частотных диапазонов, поэтому и число доступных для нелицензированного использования каналов в каждой стране различно. В РФ для нелицензированного использования на сегодня разрешены каналы из диапазонов 2,4 и 5 ГГц.

- ***Диапазон 2,4 ГГц***

Диапазон 2,4 ГГц используется в стандартах 802.11b/g/n. Это часть так называемого ISM диапазона, отведенного в большинстве стран для гражданских целей (ISM – Industrial, Science, Medicine). Помимо 802.11b/g/n в этом диапазоне работают технологии Bluetooth и ZigBee.

Диапазон 2,4 ГГц содержит всего 14 перекрывающихся каналов шириной 22 МГц каждый. Для стандарта 802.11g и более поздних ширина каждого канала установлена равной 20 МГц. Суммарно они занимают полосу частот от 2,401 ГГц до 2,495 ГГц.



В зависимости от законодательства страны, разрешенными для использования могут быть только некоторые из каналов. В России и на Украине разрешено использовать каналы 1–13, в Японии все 14. Во Франции и Испании разрешено использовать только 4 канала (2,457–2,472 ГГц — 10–13 каналы).

В РФ частотный диапазон 2,4 ГГц регламентируется следующими документами

1. Решение ГКРЧ от 7 мая 2007 г. № 07-20-03-001 «О выделении полос радиочастот устройствам малого радиуса действия»
2. Решение ГКРЧ от 20 ноября 2014 г. № 14-29-01 «О внесении изменений в решение ГКРЧ от 7 мая 2007 г. № 07-20-03-001 «О выделении полос радиочастот устройствам малого радиуса действия»

Если рассмотреть разрешенный в РФ диапазон, то в нем одновременно доступны всего 3 неперекрывающихся 22 МГц канала, например 1, 6 и 11. Точки доступа, работающие на неперекрывающихся каналах не создают друг другу помех. При работе в стандарте 802.11g/n, где используются каналы 20 МГц, одновременно доступно 4 неперекрывающихся канала — 1, 5, 9 и 13. Учитывая, что оборудование 802.11b используется очень редко, имеет смысл ориентироваться именно на эти каналы.

Для оценки ситуации в эфире используются такие программы, как inSSIDer или LinSSID. Они позволяют проверить на каких каналах работают точки доступа, в зоне действия которых находится ноутбук-измеритель и выбрать канал для работы вновь устанавливаемой точки доступа.

- ***Диапазон 5 ГГц***

Диапазон 5 ГГц используется в стандартах 802.11a/n/ac. При этом, в РФ используются только технологии 802.11n/ac.

Диапазон 5 ГГц разделен на четыре поддиапазона.

1. **UNII-1:** 5150–5250 МГц (доступно 4 частотных канала).
2. **UNII-2:** 5250–5350 МГц (доступно 4 частотных канала).
3. **UNII-2 Extended:** 5470–5725 МГц (доступно 11 частотных каналов).
4. **UNII-3:** 5725–5825 МГц (доступно 4 частотных канала).

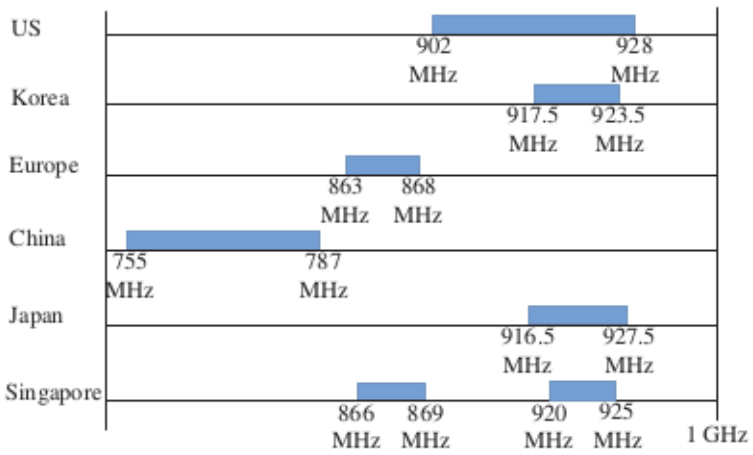
Ширина каждого канала установлена равной 20 МГц.

Номер канала	Частота, МГц	Номер канала	Частота, МГц	Номер канала	Частота, МГц	Номер канала	Частота, МГц
Поддиапазон UNII-1							
36	5180	40	5200	44	5220	48	5240
Поддиапазон UNII-2							
52	5260	56	5280	60	5300	64	5320
Поддиапазон UNII-2 Extended							
100	5500	112	5560	124	5620	136	5680
104	5520	116	5580	128	5640	140	5700
108	5540	120	5600	132	5660		
Поддиапазон UNII-3							
149	5745	153	5765	157	5785	161	5805

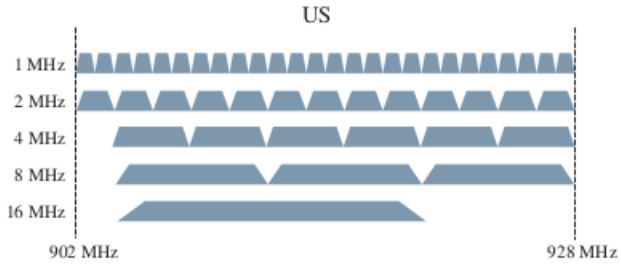
На территории РФ в диапазоне 5 ГГц для нелицензированного использования внутри помещений разрешены каналы с 36 по 64. При этом, оборудование, работающее в диапазоне 5250–5350 МГц должно быть зарегистрировано в установленном в РФ порядке. Регламентируется теми же решениями ГКРЧ, что и диапазон 2,4 ГГц.

- ***<u>Диапазон 0,9 ГГц</u>***

Диапазон 0,9 ГГц или, так называемый субгигагерцовый диапазон, применяется в стандарте 802.11ah. Во многих странах этот частотный диапазон является нелицензируемым. На территории РФ частоты 900 МГц частично отданы сотовым операторам.



Субгигагерцовый диапазон в разных странах исторически широко используется для различных радиотехнологий, поэтому в спец. 802.11ah предложены различные диапазоны для разных стран.



Выделенная полоса частот разбивается на каналы по 1 МГц, которые могут объединяться в более широкие каналы 2, 4, 8 и 16 МГц для увеличения скорости передачи данных. Здесь работает тот же принцип, что и в протоколе 802.11n.

Для примера приведено распределение каналов в диапазоне 902–928 МГц, используемом в США. В зависимости от выделенной полосы частот и особенностей законодательства максимальная полоса пропускания объединенных каналов в разных странах может отличаться.

- Южная Корея — 4 МГц
- Европа — 2 МГц
- Китай — 8 МГц
- Япония — 1 МГц
- Сингапур — 4 МГц

Для передачи данных в каналах технология 802.11ah использует те же принципы, что и 802.11ac. Для работы в каналах шириной 2, 4, 8 и 16 МГц используется модуляция OFDM с числом несущих, аналогичным каналам 20, 40, 80 и 160 МГц в 802.11ac. Например, в 2 МГц канале используется 64 поднесущих OFDM, из которым 52 используются для передачи данных. В каждом из каналов может быть использована одна из 10 кодовых схем MCS 0–9.

MCS	Модуля-ция	Скорость кода	MCS	Модуля-ция	Скорость кода	MCS	Модуля-ция	Скорость кода
0	BPSK	1/2	4	16-QAM	3/4	8	256-QAM	3/4
1	QPSK	1/2	5	64-QAM	2/3	9	256-QAM	5/6
2	QPSK	3/4	6	64-QAM	3/4			
3	16-QAM	1/2	7	64-QAM	5/6			

В каналах 1 МГц используется OFDM с 24 поднесущими и схема кодирования MCS 10, представляющая собой MCS 0 с двукратным повторением передаваемых данных, что обеспечивает большую дальность при той же помехоустойчивости.

- ***Диапазон 3,6 ГГц***

Диапазон 3,6 ГГц применяется в стандарте 802.11y. В нем применяются каналы 5, 10 и 20 МГц.

Канал	Частота (МГц)	5 МГц	10 МГц	20 МГц	Канал	Частота (МГц)	5 МГц	10 МГц	20 МГц
131	3657,5	Да	Нет	Нет	135	3677,5	Да	Нет	Нет
132	3662,5	Да	Нет	Нет	136	3682,5	Да	Нет	Нет
132	3660,0	Нет	Да	Нет	136	3680,0	Нет	Да	Нет

133	3667,5	Да	Нет	Нет	137	3687,5	Да	Нет	Нет
133	3565,0	Нет	Нет	Да	137	3685,0	Нет	Нет	Да
134	3672,5	Да	Нет	Нет	138	3689,5	Да	Нет	Нет
134	3670,0	Нет	Да	Нет	138	3690,0	Нет	Да	Нет

Принцип работы

Обычно схема Wi-Fi сети содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка (Ad-hoc), когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передаёт свой идентификатор сети SSID (Service set identification) с помощью специальных сигнальных кадров-маяков на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с — наименьшая скорость передачи данных для Wi-Fi. Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID приёмник может выбирать между ними на основании данных об уровне сигнала, согласно принятым кадрам-маякам.

По способу объединения ТД в единую систему можно выделить:

- Автономные ТД (самостоятельные, децентрализованные, умные)
- ТД под управлением контроллера («легковесные», централизованные)
- Бесконтроллерные, но не автономные (управляемые без контроллера)

В случае *автономной архитектуры* сеть строится как набор несвязанных ТД, каждая из которых конфигурируется и обслуживается независимо. Поэтому сложность обслуживания сети, построенной подобным образом, растет линейно с ростом количества устройств. Обычно такие сети содержат не более 3–5 ТД.
Существуют исключения, которые облегчают создание более масштабных сетей, например, технология кластеризации ТД. Такое решение предлагает Cisco в линейке ТД для малого бизнеса (Cisco WAP 321, WAP 121). Но такая архитектура в любом случае не имеет полноценного управления радиоресурсами, т. к. нет единого центра. Все сводится к упрощению задачи конфигурирования сети.
Развитием автономной архитектуры явились *псевдо-централизованные решения*, в которых в относительно небольшой группе ТД одна точка выделяется как контроллер группы. По сути такой мини-контроллер может выполнять многие функции полноценного контроллера сети Wi-Fi. Однако процессор ТД имеет ограниченную производительность и масштабирование таких решений невелико. Подобные решения и ТД предлагает, например, компания Aruba (Aruba Instant).

В случае *централизованной архитектуры* сети Wi-Fi полное управление инфраструктурой сети радиодоступа выполняется контроллером сети WLAN. Например, у Cisco подобная архитектура называется CUWN (Cisco Unified Wireless Network). Контроллер в централизованном решении сети стандарта Wi-Fi управляет загрузкой/изменением ПО, изменениями конфигурации, RRM (динамическое управление радиоресурсами), управляет связью с внешними серверами (AAA, DHCP,

LDAP и т. п.), управляет аутентификацией пользователей, управляет профилями качества обслуживания QoS. Контроллеры могут объединяться в группы для обеспечения бесшовного роуминга клиентов между различными точками доступа в зоне покрытия.

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

- Со статическими настройками радиоканалов
- С динамическими (адаптивными) настройками радиоканалов
- Со «слоистой» или многослойной структурой радиоканалов

Ad-hoc-сеть (беспроводная динамическая/самоорганизующаяся сеть) — децентрализованная беспроводная сеть, не имеющая постоянной структуры. Клиентские устройства соединяются «на лету», образуя собой сеть. Каждый узел сети пытается переслать данные, предназначенные другим узлам. При этом определение того, какому узлу пересылать данные, производится динамически, на основании связности сети.

Построение сети

При проектировании беспроводной сети в помещениях применяют различные подходы, которые почти всегда содержат несколько этапов.

1. Оценка количества точек доступа в зависимости от предполагаемого числа пользователей Wi-Fi и услуг, которые должны быть им предоставлены.
2. Размещение точек доступа на план-схеме помещения с учетом его размеров, материалов, из которых изготовлены стены и мебель, а также размещения пользователей.

Одним из самых простых способов определения количества точек доступа является задание фиксированного количества пользователей на точку. Например, существует рекомендация использовать одну точку доступа на 20 пользователей при отсутствии шифрования и одну точку на 15 пользователей при использовании какого-либо шифрования. Такой подход очень прост, но имеет ряд недостатков. Во-первых, такое количество точек доступа может оказаться избыточным, что приведет к лишним тратам как на само беспроводное оборудование, так и на организацию его размещения (электропитание, подключение к проводной локальной сети). Во-вторых, при большом количестве точек доступа, размещённых в одном помещении, рассчитанном на большое число пользователей (например, конференц-зал или лекторий), они могут мешать друг другу и их потребуется разносить по разным каналам, что может быть сложным при использовании диапазона 2,4 ГГц (например, если используется технология 802.11g).

Второй способ исходит из требований по уровню сигнала. Например, считается, что для доступа в Интернет (электронная почта и веб-серфинг) достаточно обеспечить на всей территории помещения уровень сигнала не хуже, чем −(68–70) дБм. Такой подход как правило требует применения специализированного программного обеспечения для предварительного расчета, либо использования измерений на месте, когда предполагаемая к использованию точка доступа размещается в разных местах

помещения, и производится измерение ее сигнала на возможных точках размещения пользователей. Как правило этот способ предлагает заниженное число точек доступа, благодаря чему на практике построенная сеть может не справиться с нагрузкой. К тому же, полное покрытие помещения может оказаться не нужным в том случае, когда пользователи компактно размещаются в одной части помещения, а другая часть помещения не используется.

Третий способ предварительного определения количества точек доступа исходит из требований по скорости доступа в зависимости от необходимых пользователям услуг. В результате таких расчетов может получиться некоторое усредненное количество точек доступа. Однако вопрос неравномерности размещения пользователей также необходимо учитывать на этапе размещения точек доступа на план-схеме помещения.
При проведении планирования необходимо также провести энергетический расчет и составить частотный план, чтобы размещенные в помещении точки доступа не влияли друг на друга, а их сигнал не выходил за границы помещения и не влиял на беспроводные сети, расположенные снаружи помещения.

Влияние препятствий на зону покрытия сети 802.11

При размещении точек доступа очень важно определить, из каких материалов сделаны стены, перекрытия, конструкционные элементы и мебель в помещении, и уже с учетом этого проводить размещение оборудования и выбор антенн, которые будут использоваться вместе с точками доступа.
Например, одной из распространенных ошибок при размещении точек доступа, является установка точки с всенаправленной (омни) антенной возле металлической или железобетонной стены или конструкции. В этом случае металлическая поверхность будет отражать сигнал. Диаграмма направленности антенны изменится став направленной. Вдобавок возникнет мощное многолучевое распространение (multipath), так как половина излучаемой мощности будет уходить к металлической стене/поверхности и, отражаясь обратно, создаст интерференцию своему же полезному излучению. Другим примером может являться размещение точки возле емкостей и труб в водой, которая интенсивно поглощает высокочастотное излучение (особенно в частотном спектре 2,4 ГГц).

Основным методом решения является вынесение точек доступа с внутренними антеннами (или самих внешних антенн) за пределы преград, обеспечивая беспрепятственное излучение с учетом диаграммы направленности антенн.

Также необходимо учитывать, что уровень сигнала убывает пропорционально квадрату расстояния, потому скорость быстро падает естественным путем по мере удаления от точки доступа.

Модель OSI

Wi-Fi охватывает первые два уровня модели OSI, каждый из которых разделен на два подуровня.

2. Канальный	Подуровень LLC
	Подуровень MAC
1. Физический	Подуровень PLCP
	Подуровень PMD

Физический уровень:

1. PLCP (Physical Layer Convergence Protocol) — выполняет процедуру отображения PDU уровня MAC во фрейм, соответствующий версии протокола и используемому типу разделения каналов. Также на этом подуровне выполняются передача, обнаружение несущей и прием сигнала;
2. PMD (Physical Medium Dependent) — "подуровень, зависящий от среды передачи". Он различен для разных скоростей передачи и разных стандартов из серии 802.11. Подуровень PMD обеспечивает данные и сервис для подуровня PLCP и функции радиопередачи и приема, результатом которых является поток данных, информация о времени, параметры приема.

Основным рабочим состоянием уровней PLCP является обнаружение несущей и оценка незанятости канала. Для выполнения передачи PLCP переключает PMD из режима "прием" в режим "передача" и посылает элемент данных PPDU (PLCP Data Unit).

Второй уровень (Data Link):

1. LLC (Logical Link Control) — идентичен для всех сетей платформы 802.
2. MAC (Media Access Control) — идентичен для всех сетей платформы 802.11.

Метод доступа к сети

Для доступа к общей разделяемой среде передачи используется метод доступа **CSMA/CA — «Carrier Sense Multiple Access With Collision Avoidance»** («Carrier sensing multiple access with collision avoidance») — «множественный доступ с контролем несущей и избеганием коллизий» («многостанционный доступ с контролем несущей и предотвращением конфликтов»).

Для предотвращения коллизий используется следующая последовательность действий:

- используется схема прослушивания несущей волны
- станция, которая собирается начать передачу, посылает jam signal (сигнал преднамеренной помехи)
- после продолжительного ожидания всех станций, которые могут послать jam signal, станция начинает передачу кадра
- если во время передачи станция обнаруживает jam signal от другой станции, она останавливает передачу на отрезок времени случайной длины и затем повторяет попытку

В 802.11 для реализации CSMA/CA используются кадры Request to Send (запрос на отправку) и Clear to Send (готовность к отправке).

Функция RTS/CTS является опциональной и разработана для уменьшения количества коллизий при пересылке кадров, когда присутствуют скрытые устройства с Wi-Fi, имеющие ассоциацию с той же точкой доступа (пример: в зоне покрытия точки доступа есть капитальная стена и два смартфона с двух сторон «слышат» эту точку, но «не слышат» друг друга). Мобильные устройства отправляют RTS кадр (играет роль jam-сигнала) к другому устройству, как первую фазу в двухшаговом процессе, необходимом до отправки кадра данных. Мобильное устройство (или точка доступа) с WiFi отвечает на кадр RTS кадром CTS, подтверждая тем самым для запрашивающего устройства чистоту канала для отправки кадра данных. Кадр CTS включает параметр времени, на которое все другие устройства в сети не должны передавать какие-либо кадры в течении периода, который требуется запрашивающему устройству на передачу его кадра. Данная функция минимизирует коллизии даже при наличии скрытых устройств.

Кадры Request to Send и Clear to Send относятся к так называемым кадрам контроля.

Фреймы сети 802.11

Стандарт 802.11 определяет три типа кадров:
1. Кадры управления (Management frames),
2. Кадры контроля (Control frames),
3. Кадры данных (Data frames).

Каждый кадр имеет контрольное поле, которое определяет версию протокола 802.11, тип кадра и различные индикаторы (например: WPA включен, управление энергосбережением активно и т. п.). Дополнительно к этому все кадры содержат MAC-адреса источника и получателя, номер кадра в последовательности, тело кадра и контрольную сумму. Кадры 802.11 инкапсулируют пакеты верхних уровней модели OSI.

Кадры управления (Management Frames)

Кадры управления 802.11 позволяют устанавливать и поддерживать соединения в сети стандарта WiFi.

Пользовательские устройства могут работать в двух режимах поиска сети:
1. Режим *Пассивного сканирования* (Passive Scanning) — прослушивание эфира.
Медленный режим, т. к. пользовательское устройство должно последовательно прослушивать все частотные каналы поддерживаемого диапазона для выявления кадров-маяков точек доступа.
2. Режим *Активного сканирования* (Active Scanning) — активная отправка запросов в эфир.

Устройство посылает кадры типа Probe Request по всем частотным каналам в поддерживаемом диапазоне часто с указанием искомого SSID сети (direct probe request) или без SSID (null probe request). Активное сканирование значительно повышает динамику работы с сетью и позволяет обеспечить быстрый роуминг, но при этом создает дополнительную нагрузку на сеть.

Всего стандарт 802.11 определяет 14 типов кадров управления:
1. Association request,
2. Association response,
3. Reassociation request,
4. Reassociation response,
5. Probe request,
6. Probe response,
7. Beacon,
8. ATIM (Announcement traffica indication mesage),
9. Disassiciation,
10. Authentication,
11. Deauthentication,
12. Action,
13. Action No Ack,
14. Timing advertisement

Кадр аутентификации (Authentication frame)

В стандарте IEEE 802.11 требуется выполнить два обязательных последовательных шага до начала пересылки трафика: аутентификация и ассоциация.

Аутентификация в сети 802.11 — это процесс в ходе которого точка доступа разрешает или отвергает идентификационные данные от конечного устройства (при наличии в сети AAA-сервера ТД может перенаправлять эти запросы на него). Конечное устройство начинает процесс путем отправки кадра аутентификации, содержащего его идентификационную информацию, к точке доступа. При открытой аутентификации, радиокарта конечного устройства отправляет кадр аутентификации и ТД отвечает кадром аутентифкации, означающим подтверждение (или отказ). В случае схем аутентифкации с ключом конечное устройство отправляет начальный кадр аутентификации и ТД отвечает кадром аутентифкации, содержащим специальную тестовую последовательность (challenge text). Конечное устройство должно далее отправить обратно зашифрованную версию тестовой последовательности (шифруется своим ключем) в кадре аутентификации. ТД проверяет корректность ключа и отвечает пользовательскому устройству фреймом аутентификации, содержащим результат аутентификации.

Кадр деаутентификации (Deauthentication frame)

Пользовательское устройство отправляет кадр деаутентификации к другому устройству, если хочет прервать безопасное соединение. Фрейм деаутентификации это уведомление, а не запрос. При получении кадра деаутентификации ни одна принимающая сторона не может отказаться его выполнить, за исключением случая

когда включен режим защиты кадров (802.11w: MFP или Management Frame Protection) и не удалось успешно выполнить контроль от подделки кадра MIC (Message Integrity Check). Если кадр уведомления деаутентификации не услышан на другом конце, то правила управления на MAC-уровне позволяют трактовать такое состояние как потерю коммуникаций.

Кадр запроса на ассоциацию (Association request frame)

Ассоциация 802.11 указывает ТД выделить и занять ресурсы для заданной новой сессии и синхронизироваться с радиокартой устройства пользователя. Радиокарта пользовательского устройства начинает процесс ассоциации путем отправки кадра запроса на ассоциацию к точке доступа. Этот кадр содержит информацию о радиокарте устройства пользователя (например, поддерживаемые скорости передачи данных и т. п.) и SSID сети WLAN, с которой устройство хочет быть ассоциировано. После получения запроса на ассоциацию точка доступа решает вопрос по ассоциированию с радиокартой и, если принято положительное решение, резервирует область памяти и формирует идентификатор сессии AID (Association Identifier) для данной радиокарты.

Кадр ответа на запрос ассоциации (Association response frame)

ТД отправляет кадр ответа на запрос ассоциации, который содержит уведомление о подтверждении или отказе на запрос радиокарты об ассоциации. Если точка доступа подтверждает ассоциацию пользовательского устройства, то кадр ответа включает информацию о данной ассоциации, например идентификатор ассоциации и поддерживаемые скорости передачи данных. Если результат ответа положителен, то радиокарта пользовательского устройства может использовать данную ТД для взаимодействия с другими радиокартами на других пользовательских устройствах в сети.

Кадр повторного запроса ассоциации (Reassociation request frame)

Если мобильное устройство пользователя выполняет роуминг от текущей ТД к другой ТД, которая имеет больший уровень сигнала, определяемого по кадру-маяку, то радиокарта мобильного устройства будет отправлять кадр повторного запроса на ассоциацию к новой ТД. Новая ТД затем координирует пересылку данных, которые могут все ещё находиться в буфере предыдущей ТД и ожидать передачи на данное мобильное устройство.

Кадр ответа на повторный запрос ассоциации (Reassociation response frame)

ТД отправляет кадр ответа на повторный запрос ассоциации, который содержит сообщение подтверждения или отказа для радиокарты мобильного устройства, запрашивающего ассоциацию с сетью. Подобно процессу ассоциации фрейм включает информацию относительно ассоциации, как, например, идентификатор сессии ассоциации и поддерживаемые скорости передачи данных.

Кадр остановки ассоциации (Disassociation frame)

Мобильное устройство отправляет кадр остановки ассоциации другому устройству, если оно хочет закончить ассоциацию. Например, радиокарта, которая была выключена правильным образом, может отправить кадр остановки ассоциации для того чтобы известить точку доступа, что данное устройсто выключается.

Кадр-маяк (Beacon frame)

Это один из наиболее важных кадров управления. ТД периодически отправляет маяки для анонсирования своего присутствия и предоставления необходимой информации (SSID, частотный канал, временные маркеры для синхронизации устройств по времени, поддерживаемые скорости, возможности обеспечения QoS и т. п.) всем устройствам в зоне ее покрытия. Радиокарты пользовательских устройств периодически сканируют все каналы 802.11 и слушают маяки, как основу для выбора лучшей ТД для ассоциации. Пользовательские устройства обычно не посылают маяки, за исключением ситуации, когда выполняется процедура участия в одноранговом соединении типа Ad-hoc.

Кадр пробы (Probe request frame)

Мобильные устройства с Wi-Fi отправляют пробу, чтобы получить информацию от другого устройства. Например радиокарта мобильного устройства отправлет пробу, чтобы определить какие точки доступа находятся внутри зоны покрытия.

Кадр ответ на пробу (Probe response frame)

Ответ на пробу содержит информацию о функциональности, поддерживаемых скоростях передачи данных и т. п.

Кадры Контроля Wi-Fi (Control Frames)

Кадры контроля 802.11 помогают в доставке кадров данных между станциями и между станциями и ТД. Всего стандарт 802.11 определяет 9 типов кадров контроля:
1. PS-Poll (Power Save Poll),
2. RTS (Request to Send),
3. CTS (Clear to Send),
4. ACK (Acknolegement),
5. CF-End (Contention Free-End),
6. CF-End + CF-ACK,
7. Block ACK Request (BlockAckReq),
8. Block ACK (BlockAck),
9. Control wrapper.

Кадр подтверждения (Acknowledgement (ACK) frame)

После получения кадра данных устройство-получатель запускает процесс проверки кадра на ошибки. Если ошибок не обнаружено, то устройство-получатель отправит

кадр подтверждения к устройству-отправителю. Если устройство-отправитель не получило кадр подтверждения после определенного периода времени, то отправитель должен посылает кадр заново (в сети 802.11 все кадры данных unicast должны быть подтверждены, иначе устройство-отправитель будет посылать их заново, снижая производительность системы).

Кадры Данных (Data Frames)

Стандарт WiFi IEEE 802.11 определяет 15 типов фреймов данных:

1. Data frame (простой фрейм данных),

Простой кадр данных это наиболее распространенный тип кадров данных.
Необходимо отметить, что существует кадр специальной нулевой функции (Null function frame), который используется пользовательскими устройствами для информирования ТД об изменениях статуса режима сохранения энергии (Power Save). Когда пользовательское устройство решает выйти из частотного канала для проведения активного сканирования, то устройство должно отправить такой фрейм нулевой функции с битом управления энергией (Power Management), выставленным в 1. После получения такого фрейма ТД должна буферизовать все, что поступает в адрес этого клиента. Когда клиентское устройство возвращается на свой частотный канал, оно должно снова отправить кадр нулевой функции с битом управления энергией, выставленным в 0. После этого точка доступа передаёт все буферизированные ранее данные клиенту.

2. Null function (без данных),
3. Data + CF-ACK (для режима Point Coordination Function),

В режиме Point Coordination Function (PCF) ТД посылает «сигнальные» фреймы через постоянные промежутки времени (обычно 0.1 секунды). Между этими фреймами, PCF определяет два периода: Contention Free Period (CFP) и Contention Period (CP). В CP используется режим Distributed Coordination Function (DCF), основанный на CSMA/CA. А в CFP ТД посылает Contention Free — Poll (CF-Poll) пакеты каждой станции по одному за раз, чтобы дать им право посылать пакеты.

4. Data + CF Poll (PCF only),
5. Data + CF-ACK + CF-Poll (PCF only),
6. CF-ACK (без данных) (PCF only),
7. CF-Poll (без данных) (PCF only),
8. CF-ACK + CF-Poll (без данных) (PCF only),
9. QoS Data (для режима Hybrid Coordination Function),

HCF работает во многом схоже с PCF: интервалы между сигнальными фреймами делятся на два периода, CFP и CP. Во время CFP, Hybrid Coordinator (HC) контролирует доступ в эфир. Во время CP, все станции функционируют по EDCF (DCF с приоретизацией трафика). Главное различие от PCF заключается в том, что присутствуют Traffic Classes (TC). Также HC может координировать трафик любым выбранным им способом (а не только циклически). Кроме того станции дают

информацию о длине их очередей для каждого TC. HC может использовать эту информацию для того, чтобы дать одной станции больший приоритет. Другое отличие заключается в том, что станциям дается Transmit Opportunity (TXOP): они могут посылать несколько пакетов друг за другом, в выделенный им период времени выбранный HC.

10. QoS Null (без данных) (HCF),
11. QoS Data + CF-ACK (HCF),
12. QoS Data + CF-Poll (HCF),
13. QoS Data + CF-ACK + CF-Poll (HCF),
14. QoS CF-Poll (без данных) (HCF),
15. QoS CF-ACK + CF-Poll (без данных) (HCF).

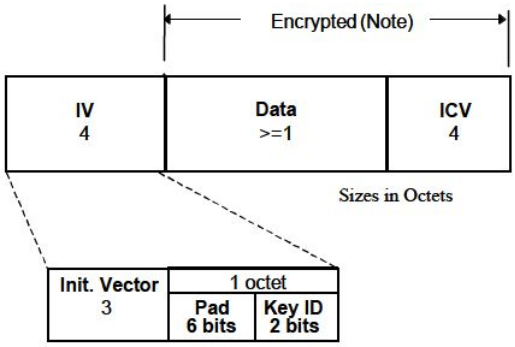
Безопасность в 802.11

Для обеспечения безопасности в сетях Wi-Fi, т. е. для защиты передаваемых данных авторизированных пользователей беспроводной сети от прослушивания и невозможности подключения к сети неавторизованных пользователей используются два основных алгоритма — WEP и WPA.

Wired Equivalent Privacy (WEP)

Существует две основные разновидности WEP: WEP-40 (WEP-64), одобренная IEEE в 1997, и WEP-104 (WEP-128), вышедшая в 2001. Эти версии различаются только длиной ключа. Некоторые производители предлагают реализации WEP с большей длиной ключа — WEP-152 и WEP-256. В настоящее время WEP является устаревшей технологией, так как ее взлом хорошо отработан и может быть осуществлен за малое время. Тем не менее, она продолжает широко использоваться. WEP часто неправильно называют Wireless Encryption Protocol.

Для шифрования в WEP используется поточный шифр RC4. Для подсчета контрольных сумм используется CRC32.



Кадр WEP включает в себя следующие поля:
Незашифрованная часть:

1. Вектор инициализации (Init. Vector, IV) (24 бита)
2. Пустое место (Padding) (6 бит)
3. Идентификатор ключа (Key ID) (2 бита)

Зашифрованная часть:

4. Данные
5. Контрольная сумма (32 бита)

В WEP-40 (WEP-64) используется 40-битный ключ, который вместе с 24-битным вектором инициализации (IV) образует ключ шифрования RC4. 40-битный ключ может быть введен как строка из 10 шестнадцатеричных цифр или как 5 символов

ASCII (8 бит/символ), однако, ограничение символов ASCII только печатаемыми символами значительно снижает пространство возможных ключей.

104-битный ключ в WEP-104 (WEP-128) представляется либо как 26 шестнадцатеричных цифр, либо как 13 символов ASCII. В совокупности с IV он образует 128-битный ключ для RC4.

WEP-152 и WEP-256 работают полностью аналогично. Отличается только длина ключа — 128 + 24 = 152 и 232 + 24 = 256, соответственно.

Инкапсуляция данных в кадр WEP:

1. Контрольная сумма от поля «данные» вычисляется по алгоритму CRC32 и добавляется в конец кадра.
2. Данные с контрольной суммой шифруются алгоритмом RC4.
3. Проводится операция XOR над исходным текстом и шифротекстом.
4. В начало кадра добавляется вектор инициализации и идентификатор ключа.

Декапсуляция данных из кадра WEP:

1. К используемому ключу добавляется вектор инициализации.
2. Происходит расшифрование.
3. Проводится операция XOR над полученным текстом и шифротекстом.
4. Проверяется контрольная сумма.

Методы аутентификации WEP

В WEP используется два метода аутентификации:

1. Аутентификация с открытой системой (Open System auth.)
2. Аутентификация с общим ключом (Shared Key auth.)

При открытой системе любой клиент может подключиться к ТД. Процедура аутентификации не производится. Ключ WEP используется только для шифрования трафика.

При аутентификации с общим ключом используется т. н. четырехэтапное рукопожатие:

1. Клиент посылает ТД запрос на аутентификацию.
2. ТД отправляет в ответ некий контрольный текст.
3. Клиент шифрует текст ключом и отправляет обратно.
4. ТД дешифрует полученный шифротекст и сверяет его с оригинальным сообщением, если все верно, то отправляется положительный ответ.

Несмотря на кажущееся увеличение безопасности, метод с общим ключом менее безопасен, поскольку перехват кадров рукопожатия с оригинальным текстом и шифротекстом позволяет упростить процедуру определения ключа. Таким образом, несмотря на то, что при открытой системе к ТД может подключиться любой клиент, для большей безопасности рекомендуется использовать именно этот метод.

Ограничение доступа к ТД может быть осуществлено другими методами, например, списком разрешенных клиентских MAC-адресов.

Wi-Fi Protected Access (WPA и WPA2)

Механизмы WPA и WPA2 одобрены IEEE в 2004. В WPA обеспечена поддержка стандартов 802.1X, а также протокола EAP (Extensible Authentication Protocol — расширяемый протокол аутентификации). Для шифрования в WPA используется усовершенствованный RC4. а в WPA2 поддерживается шифрование AES (Advanced Encryption Standard)с более стойким криптоалгоритмом.

Wi-Fi Alliance даёт следующую формулу для определения WPA, как суммы технологий:

$$WPA = 802.1X + EAP + TKIP + MIC$$

Как упомянуто выше, в стандарте WPA используется Расширяемый протокол аутентификации (EAP) как основа для механизма аутентификации пользователей. Непременным условием аутентификации является предъявление пользователем свидетельства (мандата), подтверждающего его право на доступ в сеть. Для этого пользователь проходит проверку по базе зарегистрированных пользователей. База зарегистрированных пользователей и система проверки в больших сетях, как правило, расположены на специальном сервере (чаще всего RADIUS).

Также WPA имеет упрощённый режим. Он получил название Pre-Shared Key (WPA-PSK или EAP-PSK). При применении режима PSK необходимо ввести один пароль для каждого отдельного узла беспроводной сети (беспроводные маршрутизаторы, точки доступа, мосты, клиентские адаптеры). Если пароли совпадают с записями в базе, пользователь получит разрешение на доступ в сеть.

IEEE 802.1X — стандарт Института инженеров электротехники и электроники, описывающий процесс инкапсуляции данных EAP, передаваемых между запрашивающими устройствами (клиентами), системами, проверяющими подлинность (коммутаторами, точками беспроводного доступа), и серверами проверки подлинности (RADIUS).

Для усиления шифрования используются механизмы TKIP и MIC.

TKIP (Temporal Key Integrity Protocol — протокол целостности временного ключа) отвечает за увеличение размера ключа с 40 до 128 бит, а также за замену одного статического ключа WEP ключами, которые автоматически генерируются и рассылаются сервером аутентификации. Кроме того, в TKIP используется специальная иерархия ключей и методология управления ключами, которая убирает излишнюю предсказуемость, которая использовалась для несанкционированного снятия защиты WEP ключей.

Сервер аутентификации, после получения сертификата от пользователя, использует 802.1X для генерации уникального базового ключа для сеанса связи. TKIP осуществляет передачу сгенерированного ключа пользователю и точке доступа, после чего выстраивает иерархию ключей плюс систему управления. Для этого используется двусторонний ключ для динамической генерации ключей шифрования данных, которые в свою очередь используются для шифрования каждого пакета данных. Подобная иерархия ключей TKIP заменяет один ключ WEP (статический) на 500 миллиардов возможных ключей, которые будут использованы для шифрования данного пакета данных.

Другим важным механизмом является проверка целостности сообщений (Message Integrity Check, MIC). Её используют для предотвращения перехвата пакетов данных, содержание которых может быть изменено, а модифицированный пакет вновь передан по сети. MIC построена на основе мощной математической функции, которая применяется на стороне отправителя и получателя, после чего сравнивается результат. Если проверка показывает на несовпадение результатов вычислений, данные считаются ложными и пакет отбрасывается.

При этом механизмы шифрования, которые используются для WPA и WPA-PSK, являются идентичными. Единственное отличие WPA-PSK состоит в том, что аутентификация производится с использованием пароля, а не по сертификату пользователя.

В WPA2 помимо более надежного шифрования AES вместо TKIP используется CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol — протокол блочного шифрования с кодом аутентичности сообщения (MAC) и режимом сцепления блоков и счётчика) — протокол шифрования 802.11i.

Источники:

1. Wi-Fi. https://ru.wikipedia.org
2. WECA. https://ru.wikipedia.org
3. IEEE 802.11. https://ru.wikipedia.org
4. CSMA/CA. https://ru.wikipedia.org
5. Беспроводная ad-hoc-сеть. https://ru.wikipedia.org
6. WEP. https://ru.wikipedia.org
7. Wired Equivalent Privacy. https://en.wikipedia.org
8. WPA. https://ru.wikipedia.org
9. Материалы с сайта http://www.wi-fi.org
10. Эволюция скорости передачи данных в сетях Wi-Fi. https://habrahabr.ru
11. Кое-что о Wi-Fi. https://habrahabr.ru

12. IEEE 802.11ah: A Long Range 802.11 WLAN at Sub 1 GHz / Weiping Sun, Munhwan Choi and Sunghyun Choi // Journal of ICT Standardization. 2013. Vol. 1. 83–108.
13. Wi-Fi и IEEE 802.11. http://www.bookasutp.ru
14. Типы фреймов сети стандарта IEEE 802.11. http://wi-life.ru