WIFI

Стандарты беспроводных локальных сетей

Стандарт	Опубликован	Частота, GHz	Скорость, Мбит/с	Метод расширения спектра	Дальность (в помещении / снаружи), м
802.11 legacy	1997	2.4	2	DSSS, FHSS	20 / 100
802.11a	1999	5	54	OFDM	35 / 120
802.11b	1999	2.4	11	DSSS	38 / 140
802.11g	2003	2.4	54	OFDM, DSSS	38 / 140
802.11n	2009	2.4 и/или 5	450	OFDM	70 / 250

Комитет 802.11 был создан в 1990 году.
В 1991 году NCR/AT&T разработала технологию Wave Lan.
В 1999 был создана международная организация Wireless Ethernet Compatibility Alliance (WECA).

802.11a

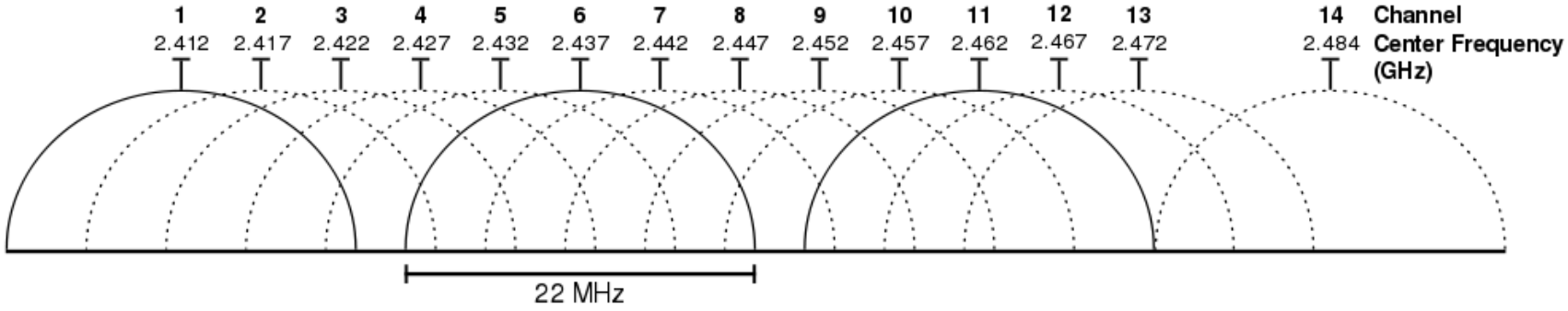
Наименование параметра	Значение параметра	Метод модуляции
Диапазон частот, МГц	5150-5350; 5650-6425	
Метод доступа к среде	Множественный доступ с контролем несущей и предотвращением коллизий	
Метод расширения спектра	OFDM	
Частотный разнос каналов, МГц	20	
Количество поднесущих в канале	52	
Скорости передачи данных по радиоканалу, Мбит/с	6; 9	BPSK
	12; 18	QPSK
	24; 36	16QAM
	48; 54; 108	64QAM
Максимальная мощность излучения передатчика в полосе частот: 5150-5250; 5250-5350 МГц	Не более 20 дБм (100 мВт)	
Максимальная мощность излучения передатчика в полосе частот: 5650-5725; 5725-5825; 5825-6425 МГц	Не более 30 дБм (1 000 мВт)	

Для предотвращения создания помех системам слежения за спутниками связи в Европе используются протоколы Dynamic Frequency Selection (DFS) и Transmit Power Control (TPC)

802.11b

Наименование параметра	Значение параметра	Метод кодирования и модуляции
Диапазон частот, МГц	2400-2483,5	
Метод расширения спектра	DSSS	
План частот	2412+5(n-1), n = 1, 2 ...13	
Скорости передачи данных по радиоканалу, Мбит/с	1	Код Баркера, DBPSK
	2	Код Баркера, DQPSK
	5,5	CCK, DQPSK PBCC, DQPSK
	11	CCK, DQPSK PBCC, DQPSK
	22	PBCC, DQPSK
Максимальная мощность излучения передатчика, дБм	не более 20 (100 мВт)	

Частотный план диапазона 2.4GHz



- При ширине полосы 22 MHz и шаге каналов 5 MHz можно использовать только каждый 4 или 5 канал.
- В России и США: 1, 6 и 11.
- В Европе: 1, 5, 9,13 или 1, 6, 11.
- Канал 14 был введён в Японии и разрешен к использованию в некоторых других странах.

802.11g

Наименование параметра	Значение параметра
Диапазон частот, МГц	2400-2483,5
План частот (центральные частоты каналов, МГц)	2412+5(n-1), n = 1, 13
Методы расширения спектра	DSSS, OFDM
Скорости передачи данных по радиоканалу и модуляции, Мбит/с	1; 2; 5,5; 6; 9; 11; 12; 18; 22; 24; 33; 36; 48; 54; расширения: 108, 140
Методы кодирования	Код Баркера, CCK, PBCC, OFDM, CCK-OFDM
Методы модуляции	DBPSK, DQPSK, BPSK, QPSK, 16-QAM, 64-QAM
Максимальная мощность излучения передатчика	Не более 24 дБм (250 мВт)

Расширения стандарта 802.11g

- Общие подходы
  - Сжатие данных
  - Пакетная передача данных
- Atheros SuperG (108G, Xtreme G, 108 Mbit/s 802.11g)
  - Используется связывание 2 каналов (54+54=108 Мбит/с)
  - Использует только 6-ой канал
  - Статический режим работы используется когда всё оборудование поддерживает SuperG
  - Динамический режим работы позволяет совмещать разное оборужование
  - Возможна работа SuperG через 1 канал
- Connexant Nitro MX Xtreme
  - Декларируется скорость до 140 Мбит/с
  - DirectLink: передача данных между устройствами минуя AP но под её управлением
- 125 High Speed Mode (g+, G Plus, Turbo G, SpeedBooster, 125 M)

802.11n

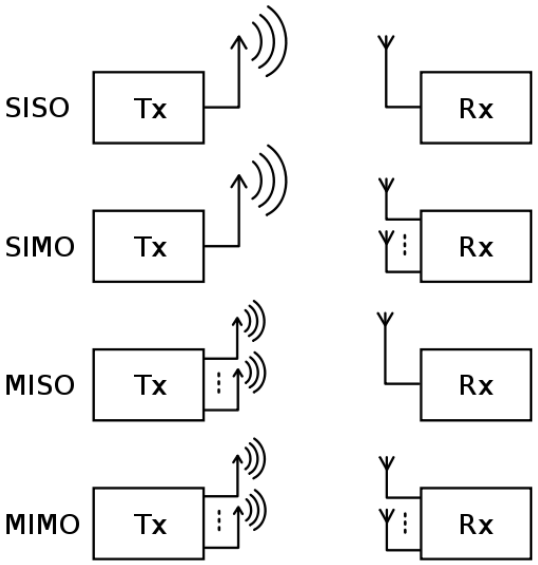
Наименование параметра		Значение параметра
Диапазон частот, МГц		2400-2483,5 и/или 5150-5350, 5650-6425
Метод доступа к среде		Множественный доступ с контролем несущей и предотвращением коллизий
Число потоков MIMO, не менее		Базовая станция — 2
		Абонентская станция — 1
Число потоков MIMO, не более		4
Метод расширения спектра		OFDM
Частотный разнос каналов, МГц		20 и/или 40
Количество поднесущих в канале		56 (при ширине канала 20 МГц)
Максимальная мощность передатчика, работающего в диапазоне, МГц	2400-2483,5	Не более 24 дБм (250 мВт)
	5150-5250, 5150-5250, 5250-5350	Не более 20 дБм (100 мВт)
	5650-5725, 5725-5825	Не более 30 дБм (1000 мВт)

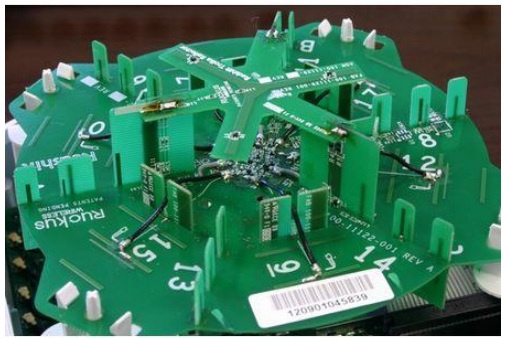
Режимы работы оборудования:

- Режим предыдущих версий / Legacy: a, b, g без n
- Смешанный режим / Mixed: a, b, g и частичная поддержка n
- Высокоскоростной режим / High Throughput (HT): только n

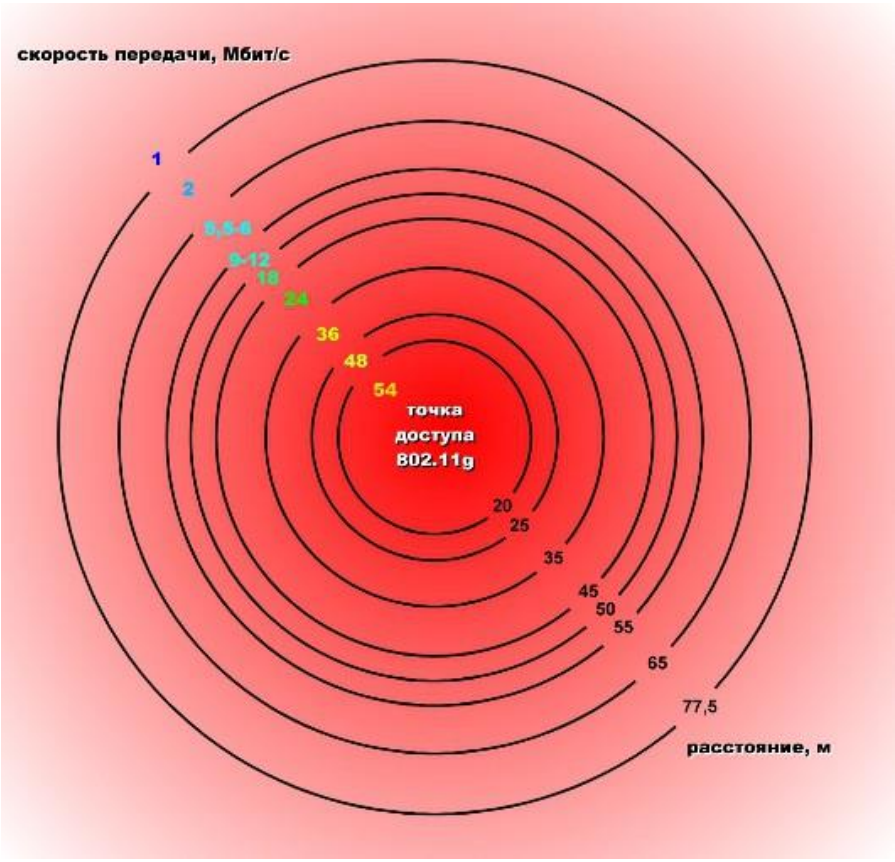
MIMO

- Использование нескольких передающих антенн
  - Формирование диаграммы направленности передатчика
  - Пространственно-временные блоковые коды
  - Субсимвольный временной сдвиг
  - Выбор антенны
- Использование информации от нескольких приёмных антенн
  - Сложение принимаемых сигналов для повышения коэффициента сигнал/шум
- Одновременное применение нескольких передающих и принимающих антенн
  - Пространственное мультиплексирование





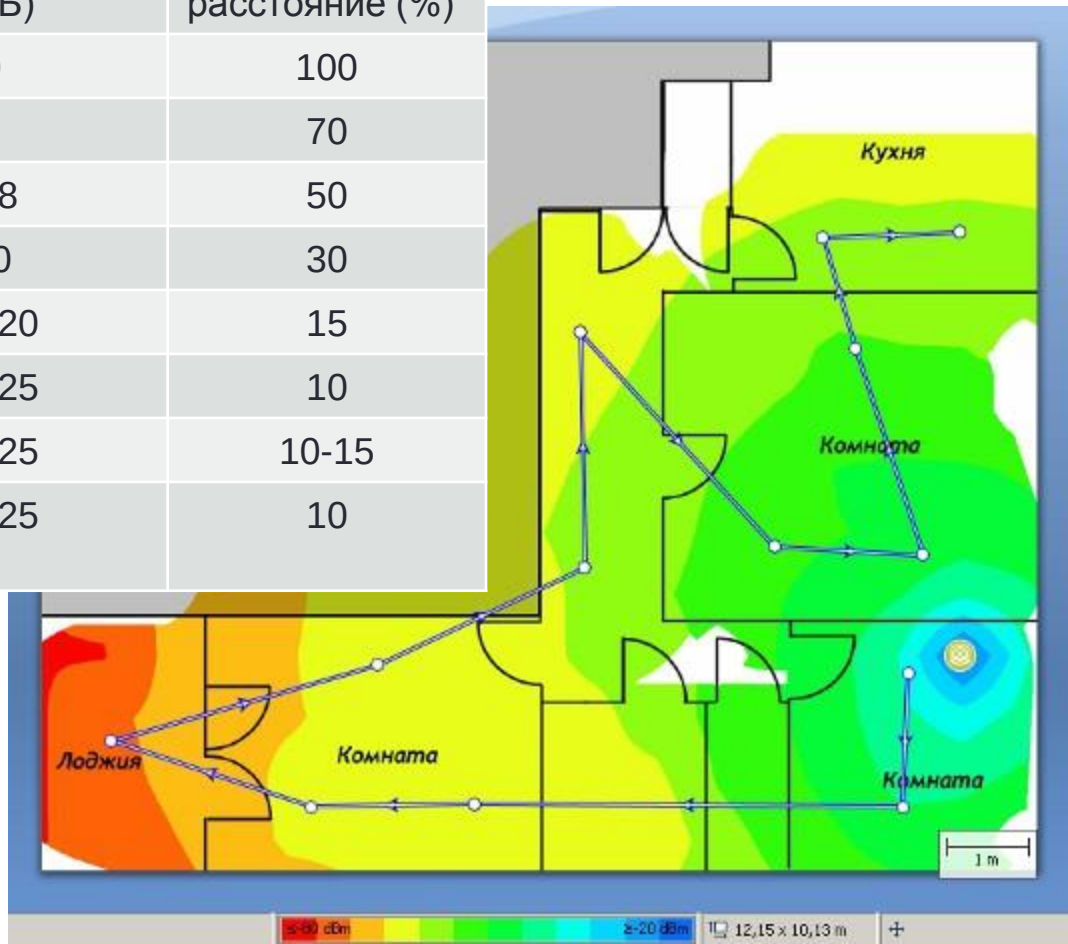
Скорость передачи в сетях WiFi



Зависимость теоретической скорости передачи в сети WiFi от расстояния на открытом пространстве (по данным фирмы TrendNet).

Распространение сигнала WiFi в реальных условиях

Потеря эффективности сигнала WiFi (по данным фирмы Zyxel)		
Препятствие	Дополнительные потери (дБ)	Эффективное расстояние (%)
Открытое пространство	0	100
Окно без тонировки	3	70
Окно с тонировкой	5-8	50
Деревянная стена	10	30
Межкомнатная стена 15 см	15-20	15
Несущая стена 30 см	20-25	10
Бетонный пол/потолок	15-25	10-15
Монолитное ж.б. перекрытие	20-25	10



Реальное распределение мощности роутера WiFi в 3-х комнатной квартире. По статье Ю. Ревич, dgl.ru

Режимы работы сетей WiFi

- Infrastructure
  - Сеть управляется точкой доступа
- Ad hoc
  - Не используется точка доступа
  - Для подключения достаточно знать SSID и номер канала
  - Нельзя соединить мостом с другими сетями
  - Может быть снижена скорость работы

Формат кадра 802.11

- Frame control
  - **Protocol Version (2 бита):** Версия протокола, сейчас 0
  - **Type (2 бита):** Тип кадра: Control, Data или Management
  - **Sub Type (4 бита):** Уточнение типа кадра.
  - **ToDS и FromDS (по 1 биту):** Направление передачи пакета для пакетов данных.
  - **More Fragments (1 бит):** Используется при фрагментации.
  - **Retry (1 бит):** Устанавливается для кадров, посылаемых повторно.
  - **Power Management (1 бит):** Устанавливается в 1 если отправитель перейдёт в режим энергосбережения после передачи.
  - **More Data (1 бит):** Сообщает что есть ещё пакеты и не надо уходить в режим энергосбережения.
  - **WEP (1 бит):** Устанавливается в 1 если пакет не был зашифрован или расшифрован.
  - **Order (1 бит):** Устанавливается в 1 при передаче кадров в режиме строгого порядка.
- Duration ID
  - Duration,
  - Contention-Free Period (CFP)
  - Association ID (AID).
- MAC адреса.
- Sequence Control
  - Номер фрагмента (4 бита)
  - Последовательный номер кадра (12 бит)
- Quality of Service (2 байта) расширение 802.11e.
- Данные от 0 до 2304 байт
- Frame Check Sequence (FCS) (4 байта) – Контрольная сумма

Типы кадров 802.11

- Кадры управления / Control frames
  - Acknowledgement (ACK) frame.
  - Request to Send (RTS) frame.
  - Request to Request to Send (RRTS) frame.
  - Clear to Send (CTS) frame.

- Кадры данных / Data frame используются для передачи данных протоколов более высокого уровня

Типы кадров 802.11

- Кадры обслуживания / Management frames
  - Authentication frame: используются для аутентификации станции и AP.
    - При открытой аутентификации станция посылает запрос AP, AP отвечает приёмом или отклонением
    - При использовании ключей станция посылает запрос, AP отвечает кадром со случайными данными, станция шифрует эти данные и передает обратно AP, AP сверяет зашифрованные данные со своим вариантом.
  - Association request frame: Запрос станции о подключении к сети.
  - Association response frame: Ответ на запрос о подключении.
  - Beacon frame: Периодически посылается AP, содержит SSID и другие данные.
  - Deauthentication frame: Посылается станцией, которая хочет закрыть соединение.
  - Disassociation frame: Посылается станцией, которая хочет закрыть соединение.
  - Probe request frame: Запрос информации одной станции о другой (поддерживаемые скорости и т.п.).
  - Probe response frame: Ответ на запрос.
  - Reassociation request frame: Запрос на переход к новой AP.
  - Reassociation response frame: Подтверждение перехода к новой AP.

Wired Equivalent Privacy (WEP)

- WEP - Исходный вариант шифрования пакетов WiFi
  - Использовал RC4 для шифрования и CRC32 для контроля ошибок или вставки посторонних пакетов
  - Ключи RC4 не должны повторяться при передаче, поэтому они дополнялись 24-битной псеводслучайной последовательностью Initialization Vector / IV
  - Последовательность оказалось слишком короткой, что позволило дешифровать ключи

WiFi Proteced Access (WPA)

- Temporal Key Integrity Protocol (TKIP)
  - Использована более сложная функция смешивания ключа и IV
  - Использована более сложная контрольная сумма
  - В данный момент тоже сломан
- Wi-Fi Protected Access (WPA)
  - В исходном варианте использовала TKIP
  - WPA-Personal (WPA-PSK): использует ключ, имеющийся у AP и станции
  - WPA-Enterprise (WPA-802.1X, WPA): использует протокол EAP и сервер аутентификации
- Wi-Fi Protected Access II (WPA2)
  - CCMP – протокол шифрования на основе AES

Extensible Authentication Protocol (EAP)

- Стандарт, определяющий инфраструктуру аутентификации, определен в RFC 3748 и RFC 5247
- В данный момент определено порядка 40 методов аутентификации
- Требования к методам EAP применяемых в беспроводных сетях определены в RFC 4017
- EAP-TLS [RFC 2716]

  Аутентификация на основе ассиметричной криптографии с применением инфраструктуры публичных ключей
- EAP-TTLS [RFC 5281],

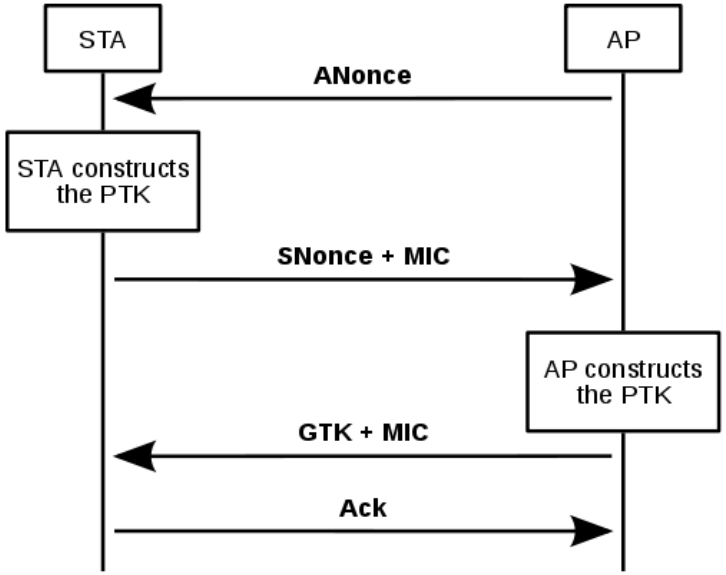
  Расширение EAP-TLS, клиенту не обязательно иметь подписанный публичный ключ
- PEAP

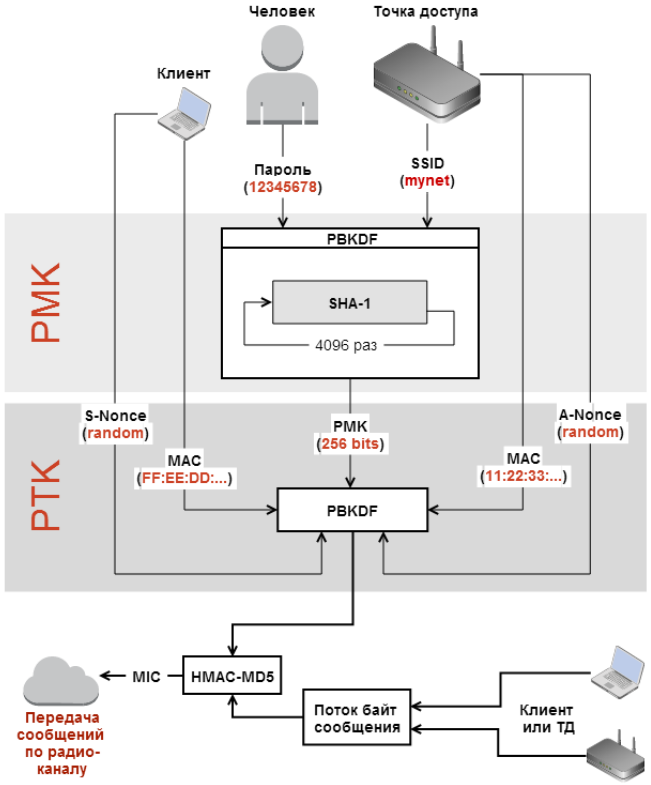
  Передача EAP через зашифрованный канал
- EAP-SIM [RFC 4186]

  Аутентификация с помощью SIM-карты

Обмен ключами

- Pairwise Master Key (PMK) – разделяемый секретный ключ = hash(пароль, ESSID)
- Pairwise Transit Key (PTK)=hash(PMK Anonce Snonce APmac STAmac)

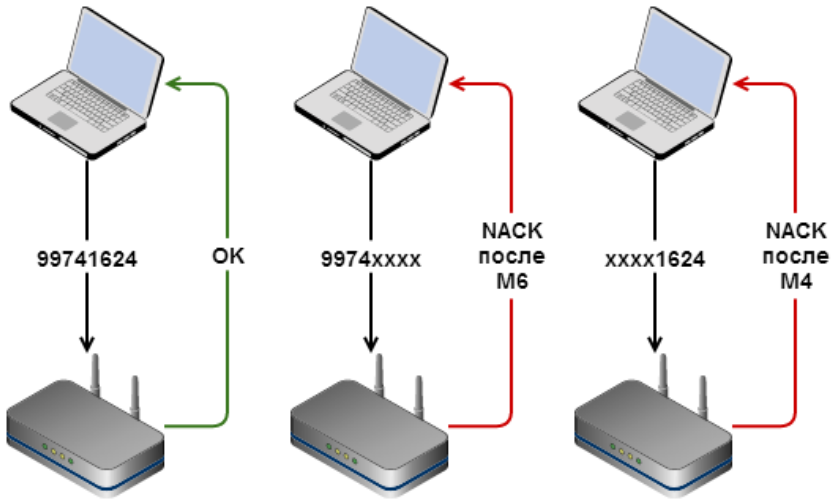




WPS (QSS)

Технология предназначенная для упрощения подключения к точке доступа.

- WPS позволяет подключиться по 8-символьному коду, состоящему из цифр (PIN).
- Из-за ошибки в стандарте для подключения достаточно угадать 4 цифры..
  - Достаточно10000 попыток.
  - В секунду можно отправлять 10-50 запросов.
  - Ключ можно подобрать за 3 – 15 часов.
- В некоторых устройствах есть ограничение на число попыток входа.
  - Хорошо, если есть на половине моделей роутеров.
  - Даже если оно есть, PIN можно подобрать за неделю



Сокрытие имени сети (ESSID)

- Для подключения к сети надо указывать имя сети (ESSID).
- Во время работы для идентификации сети используется MAC-адрес точки доступа (BSSID).
- AP «открытой сети» передаёт маячок со своим ESSID 10 раз в секунду.
- AP «закрытой сети» передаёт маячки с пустым ESSID (или не передаёт ничего, пока нет клиентов).
- При подключении клиент в любом случае передаёт ESSID.
  - Можно заставить клиента переподключиться, отправив специально сформированный кадр.
  - Можно просто подождать подключения клиента.

ESSID и автоподключение к сети

- Передача ESSID нужна, чтобы работала функция «всегда подключаться к этой сети»:
  - AP передаёт маячки с именем сети;
  - клиентский компьютер видит известную ему сеть и подключается к ней.

- Автотподключение к сети может использоваться для перехвата данных:
  - злоумышленник передаёт со своей AP маячок, с именем известной компьютеру/телефону сети (может передавать много разных имён);
  - компьютер/телефон автоматически подключается к AP злоумышленника;
  - злоумышленник передаёт траффик в интернет, получая к нему доступ.

- Выводы:
  - Не стоит включать автоподключение к общественным сетям (все злоумышленники знают, как зовут сети Дом.ru, Макдональдса и т.п.).
  - Если Вы опасаетесь адресных атак, автоподключение не стоит включать вообще.

Атака на WPA перебором

- Математически доказано, что корректно выполненный 4-х фазный хэндшейк WPA позволяет сторонам безопасно проверить знание пароля друг другом и установить ключ шифрования сессии.
- Алгоритм «взлома» сети WPA:
  1. вычислить главный ключ сети (PMK):
     1. имя сети ESSID – известно;
     2. пароль – пробовать все по очереди (из словаря, и т.п.)
  2. вычислить PTK, нужны:
     1. PMK, MAC-адреса – известны;
     2. nonce-строки – необходимо перехватить начало соединения;
  3. вычислить и сравнить MIC, если не совпали goto 1.
- Каждая итерация требует 8192 вычислений SHA-1, который в 3 раза медленнее MD5.
- Вычисленный ключ даст возможность дешифровать данные только конкретной сессии конкретного клиента.

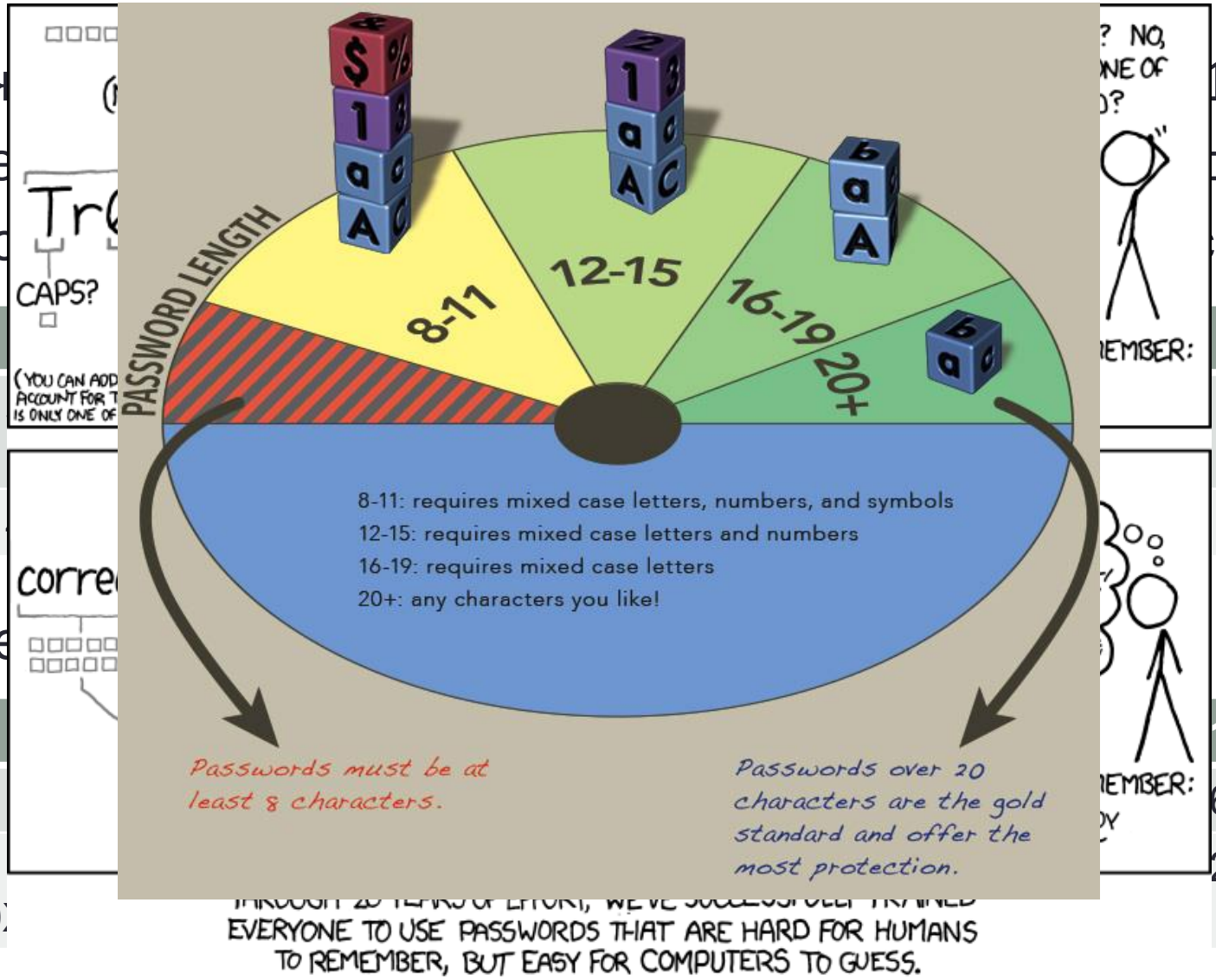
Устойчивость WPA к подбору пароля

- Каж
- Inte
- Ско

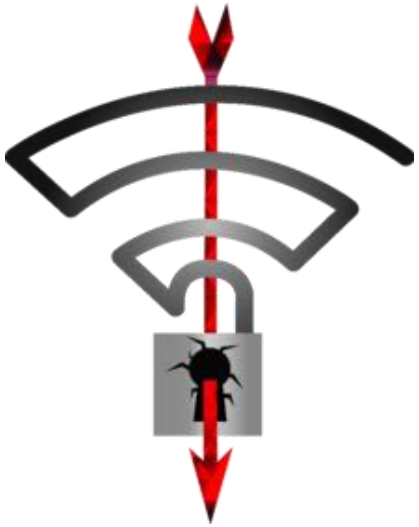
675MX	295X*2
11	203*2

- Вре

Пароль	12 букв
i7	675 лет
8 штук AMD290	2.1 года



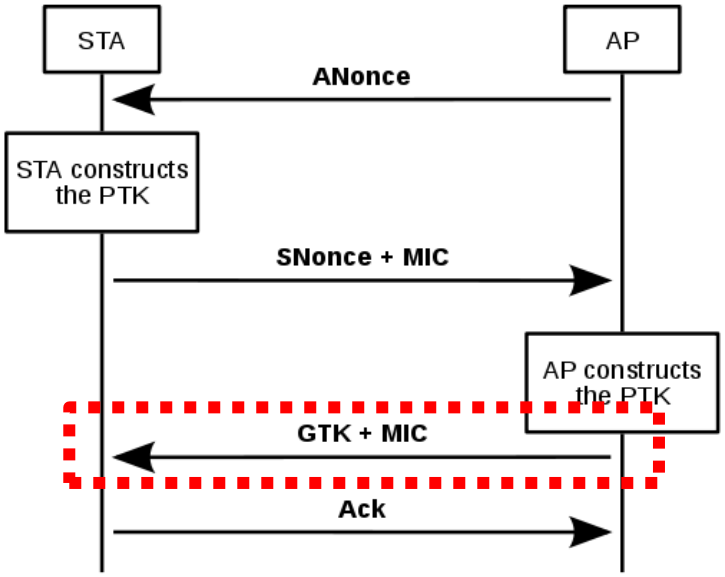
Key Reinstallation Attack KRACK



- В 2016 году Mathy Vanhoef обнаружил подозрительную строку в WiFi драйверах OpenBSD.
- В июле 2017 года о уязвимости были предупреждены производители ОС и оборудования.
- 16 октября 2017 года информация об уязвимости была опубликована для широкой публики.

- Уязвимость позволяет дешифровать данные, передаваемые через WiFi
- В случае использования методов шифрования TKIP или GCMP уязвимость позволяет вставлять произвольные данные в соединение.

Как работает KRACK



- Так как пакеты могут теряться, точка доступа по стандарту может отправлять третье сообщение несколько раз.
- Получив повторное сообщение клиент заново переустанавливает пароль и сбрасывает счётчики отправленных и принятых данных (nonce).
- Атакующий может подслушать и воспроизвести это сообщение, что приведёт к повторному использованию клиентом одного и того же пароля с одними и теми же значениями nonce на новых данных.
- Это делает возможным дешифровку ключа сессии по пакетам с известными данными (или, например, с английским текстом).
- Не позволяет восстановить пароль.

KRACK на Android и Linux

- Примечание в стандарте WiFi рекомендует стирать в памяти пароль, после того, как он был использован.
  - Это вообще-то была хорошая идея.
- Библиотека wpa_supplicant версии 2.4 и выше перезаписывает пароль нулями.
  - Используется Linux и Android версии 6 и выше.
- Поэтому, при проведении атаки KRACK эта библиотека устанавливает для соединения пароль, состоящий из одних нулей.
- Перехват и подделка трафика становятся элементарными.

Что позволяет KRACK

		Дешифровка[1]	Подделка[2]	Воспроизведение[3]
4-way	TKIP	клиент → AP	клиент → AP	AP → клиент
	AES-CCMP	клиент → AP		AP → клиент
	GCMP	клиент → AP	клиент → AP	AP → клиент
Fast BSS Transition	TKIP	AP → клиент	AP → клиент	клиент → AP
	AES-CCMP	AP → клиент		клиент → AP
	GCMP	AP → клиент	AP ⇆ клиент	клиент → AP
Group	Любой	AP → клиент		AP → клиент

[1] – позволяет перехватывать и вставлять данные в TCP соединения, например, вставлять злонамеренные скрипты в web-страницы, передаваемые по нешифрованным (http) соединениям.

[2] – позволяет поместить в сеть пакеты, адресованные любым другим устройствам.

[3] - повторная отправка широковещательных пакетов. Можно использовать для подрыва работоспособности TLS, DNSSEC, Kerberos, Bitcoin… .

Защита от KRACK

- Протокол WPA2 [может быть] изменён без потери обратной совместимости.
- Что надо исправлять:
  - Точки доступа, которые поддерживают Fast BSS Transition handshake (802.11r) - в основном точки доступа для корпоративного использования.
  - Точки доступа, которые могут работать в режиме WiFi клиента (ретрансляторы).
  - Всё оборудование, выступающее в роли WiFi клиентов.
- Можно исправить точку доступа так, чтобы она не допускала атаку на незащищенных клиентов, пока они подключены к ней.