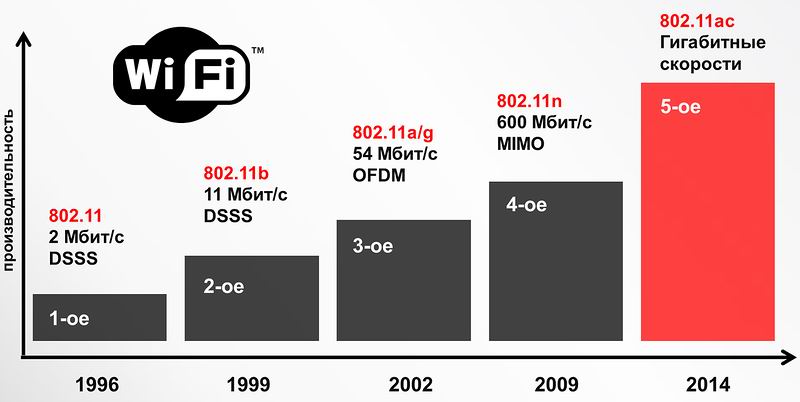
1. Основные стандарты Wi-Fi (набор стандартов 802.11).

* IEEE 802.11 – базовый стандарт для сетей Wi-Fi, который определяет набор протоколов для самых низких скоростей передачи данных
* **IEEE 802.11b** – описывает б**о**льшие скорости передачи и вводит больше технологических ограничений.
* **IEEE 802.11a** – описывает значительно более высокие скорости передачи (transfer) чем 802.11b. Используются частотные каналы в частотном спектре 5GHz. Протокол Не совместим с 802.11b.
* • **802.11d**. Для адаптации различных устройств стандарта WiFi к специфическим условиям страны. Внутри регуляторного поля каждого государства диапазоны часто различаются и могут быть отличны даже в в зависимости от географического положения.
* • **802.11e**. Описывает классы качества QoS для передачи различных медиафайлов и, в целом различного медиаконтента. Адаптация МАС-уровня для 802.11e, определяет качество, например, одновременной передачи звука и изображения.
* • **802.11f**. Направлен на унификацию параметров Точек Доступа стандарта Wi-Fi различных производителей. Стандарт позволяет пользователю работать с разными сетями при перемещении между зонами действия отдельных сетей.
* • **802.11h**. Используется для предотвращения создания проблем метеорологическим и военным радарам путем динамического снижения излучаемой мощности Wi-Fi оборудованием или динамический переход на другой частотный канал при обнаружении триггерного сигнала (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).
* **802.11i**. В первых вариантах стандартов WiFi 802.11 для обеспечения безопасности сетей Wi-Fi использовался алгоритм WEP.

2. Сравнение стандартов беспроводной передачи данных.



3. Принцип организации Wi-Fi.

Wi-Fi- это современная беспроводная технология соединения компьютеров в локальную сеть м подключения их к интернет. Обычно схема wifi сети содержит не меннее одного клиента. Адаптер представляет собой устройство, которое подключается через слот расширения PCI, USB, compactflsh. Wi-Fi адаптер выполняет ту же функцию, что и сетевая карта в проводной сети.

Доступ к сети обеспечивается путем передачи широокоформатных сигналов через эфир. Точка доступа передает свой индентификатр сети (ssid) с помощью специальных сигнальных пакетов на скорости 0,1 Мбит\с кждые 100мс.

4. Классификация беспроводной сети Wi-Fi

**- Точка доступа** (Access Point, или сокращенно AP) является наиболее распространенным типом соединения. Используется дома или в офисах в виде сочетания беспроводной точки доступа и маршрутизатора.

**- Соединение точка-точка** (Point to Point, P2P) используется для беспроводной связи двух маршрутизаторов, когда нужно объединить две локальные сети или два ПК.

**- Соединение точка-мультиточка** (Point to Multipoint, P2MP) использует один мощный передатчик, который транслирует сигнал Wi-Fi множеству пользователей.

5. Преимущества и недостатки сети Wi-Fi

* Позволяет развернуть сеть без прокладки кабеля. Например, в исторических зданиях.
* Позволяет иметь доступ к мобильным устройствам
* Wi-Fi устройства широко распространены на рынке и гарантируется совместимость оборудования с поддержкой wifi

6. Архитектура, компоненты сети Wi-Fi.

При построении беспроводной сети используются два типа архитектуры сети: распределенная (WDS) и централизованная. Для организации распределённой сети необходимо установить точки доступа AP. AP объединяют в одном устройстве функциональность сетевого контроллера и радиотрансивера, т.е. может работать как на приём, так и на передачу. WDS технология позволяет AP устанавливать беспроводное соединение не только с беспроводными клиентами, но и между собой. Соединения WDS основываются на MAC-адресах и используют специальный тип кадров, в которых задействованы все четыре поля для MAC-адресов, определённые стандартом 802.11, вместо трех, как при обычной передаче данных между точкой доступа и клиентом.

Компоненты сети Wi-Fi

a) контроллер Wi-Fi, который выполняет функцию управления, отвечает за безопасность сети, мониторинг, распределение нагрузки между точками доступа, обеспечивает бесшовное покрытия, реализацию гостевого доступа и т. д. WiFi контроллеры используются в основном на коммерческих предприятиях, в сетях провайдеров.

b) роутер, или как его ещё называют маршрутизатор - это специализированный сетевой компьютер, имеющий два или более сетевых интерфейса.

Он пересылает пакеты данных между различными сегментами сети, Wi-Fi адаптерами. Роутер может связывать разнородные сети различных архитектур. Фактически роутер совмещает в себе АР и маршрутизатор и, кроме функции беспроводной ретрансляции трафика, роутер умеет:

- маршрутизировать пакеты данных между различными сетями и подсетями.

- присваивать IP-адреса компьютерам и другим устройствам, которые к нему подключены.

- обеспечивать сетевую защиту.

- ограничивать скорость трафика, а также многое другое.

c) Wi-Fi адаптер - это специальное устройство, которое способно принимать и отсылать пакеты данных по широкополосной радиосвязи.

7. Типы и разновидности соединений.

По способу объединения точек доступа в единую систему

- Автономные точки доступа (называются также самостоятельыне, умные)

- Точки лоступа, работающие под управлением контроллера (называются централизованные)

- автономные

По способу организации и управления радиоканалами можно выделить беспроводные локальные сети

- со статическими настройками радиоканалов

- С динамическими настройками радиоканалов

- со слоистой или многослойной структорой радиоканлов

8. Безопасность сети Wi-Fi (основные методы и протоколы защиты).

Принято считать, что безопасности беспроводных сетей угрожают:

* нарушение физической целостности сети;
* подслушивание трафика;
* вторжение в сеть.

В беспроводном оборудовании стандарта IEEE 802.11 предусмотрены специальные меры защиты от нарушения целостности сети: расширение спектра сигнала в варианте DSSS или FHSS.

В беспроводных сетях для снижения вероятности несанкционированного доступа предусмотрен контроль доступа по MAC-адресам устройств и тот же самый WEP.

 9. Протокол шифрования WEP (принцип шифрования, основные уязвимости).  
  
Принцип шифрования  
  
Основан на алгоритме RC4, который реализован в виде симметричного потокового шифрования.  
  
Генерируется ключевой поток, с помощью специальной функции, и этот ключевой поток суммируется с потоком данных по модулю два.  
  
Дешифрация – генерация этого же потока и зашифрованного потока по модулю два, тем самым получая исходные данные.  
  
Существует 2 вида шифрования: потоковое и блочное.  
  
Потоковое – побитовое сложение по модулю 2. Длина ключа равна длине кодируемого сообщения.  
  
Блочное – Исходное сообщение разбивается на блоки, и каждый блок отдельно складывается побитово с ключом  
  
Данные в виды шифрования используют метод электронной книги (ECB). Это значит что одно и то же исходное сообщение – всегда одно и то же зашифрованное сообщение на выходе.  
  
Это недостаток, который исправляют с помощью вектора инициализации и обратной связи.  
  
С помощью вектора инициализации изменяют ключевую последовательность при каждой новой отправке сообщения  
  
Обратная связь работает в блочном шифровании: каждый новый блок суммируется по модулю два с зашифрованным предыдущим, а для первого блока генерируется ключ с помощью вектора инициализации.  
  
Основные уязвимости:  
  
Пассивные сетевые атаки:  
  
Некоторые векторы инициализации дают возможность установить побайтовый состав секретного ключа, применяя статистический анализ.  
  
Активные сетевые атаки:  
  
Индуктивное вычисление секретного ключа :  
  
- Повторное использование вектора инициализации:  
  
хакер отправляет жертве различные пакеты данных, и прослушивает его сеть, получая зашифрованные пакеты.  
  
Далее применяет функцию XOR (сложение по модулю 2), воссоздавая вектор инициализации и ключ шифрования.  
  
Такую ключевую последовательность можно будет «вырастить» для любой длины, хакер методом подбора находит нужный новый байт,  
  
ведь на правильную ключевую последовательность, точка доступа в атакуемой сети ответит однозначно.  
  
- Манипуляция битами:   
  
Опирается на уязвимость вектора контроля целостности. Хакер манипулирует битами канального уровня с целью икажения пакетов 3 его уровня.  
  
Алгоритм: Какое то время читает трафик жертвы, далее захватывает пакет, произвольно меняет биты протокола третьего уровня.  
  
Модифицирует вектор контроля целостности. Передает модифицированный фрейм в локальную сеть.  
  
Принимающая сторона проверяет контроль целостности, и анализирует данные протоколоа 3 его уровня, а там моифицированные хакером данные.  
  
Тогда обратно в сеть отправляется зашифрованное сообщение об ошибке. Хакер с помощью данного сообщения вычисляет ключевую последовательность (как в предыдущем случае).  
  
Вычисления вектора целостности сообщения : Исходный фрейм имеет вектор С1. Содается фрейм F2 такой же длины и делается XOR.  
  
Так мы создаем модифицированный фрейм F3. Вычисляется промежуточный вектор C2 для F3. Далее XOR C1 и C2 – получаем C3 – нужный нам вектор целостности.  
  
10. Протокол шифрования WPA (принцип шифрования, основные уяз-  
  
вимости).   
  
Принцип шифрования  
  
Усовершенствованный протокол TKIP вместо RC4  
  
-Пофреймовое изменение ключей шифрования:   
  
Базовый WEP ключ смешивается со старшими 32 разрядами вектора инициализациии MAC адресом передатчика. Получаем ключ первой фазы  
  
Ключ 1 фазы + вектор инициализации + MAC-адрес  
  
Через пофр

 еймовый ключ вычисляется новая ключевая последовательность, и применяется алгоритм RC4. И так для каждого фрейма.  
  
Для контроля целостности сообщения применяется алгоритм MIC. MIC имеет уникальный ключ, который перемешивается с MAC-адресом источника и MAC-приемника,  
  
а также со всей незашифрованной частью фрейма.  
  
Алгоритм TKIP  
  
1. Генерируется пофреймовый ключ как описано выше  
  
2. Генерируется вектор контроля целостности с помощью алгоритма MIC  
  
3. Фрейм шифруется с помощью пофреймового ключа  
  
4. Передача зашифрованного фрейма  
  
Дешифровка сообщения  
  
Уязвимости  
  
11. Протоколы аутентификации в сети Wi-Fi (использующей техноло-  
  
гию 802.11X).   
  
Open system authentication  
  
проверка по MAC(если включена)  
  
проверка WEP ключа (если включена)  
  
Используемые шифры: без шифрования, статический WEP, CKIP.  
  
Open system authentication with eap  
  
Предыдущий вариант аутентификации может использоваться совместно с аутентификацией через протоколы EAP на RADIUS сервере.  
  
Используемые шифры: без шифрования, динамический WEP, CKIP.  
  
Shared system authentication  
  
В этом случае клиент отсылает запрос на соединение к точке доступа. Затем точка доступа отсылает клиенту последовательность,  
  
которую он шифрует и отсылает обратно. Если последовательность зашифрована верно, то аутентификация проходит успешно.  
  
Внимание! В этом варианте защита слабее, чем в случае Open System!  
  
Используемые шифры: без шифрования, динамический WEP, CKIP.  
  
WI-FI protected access (wpa)  
  
Существуют два варианта аутентификации: с помощью RADIUS сервера (WPA-Enterprise) и с помощью предустановленного ключа (WPA-PSK).  
  
Используемые шифры: TKIP[стандарт], AES-CCMP [расширение], WEP[в качестве обратной совместимости].  
  
WI-FI protected access2 (wpa2, 801.111)  
  
Также как и в WPA, в WPA2 есть два варианта аутентификации WPA2-Enterprise с аутентификацией на RADIUS сервере и WPA2-PSK с предустановленным ключом.  
  
Используемые шифры: AES-CCMP [стандарт], TKIP [в качестве обратной совместимости].  
  
12. Коды обнаружения ошибок  
  
Позволяют легко обнаружить ошибку. Используются в протоколах, где есть схема ARQ. В кратце, с каждым пакетом передается его контрольная сумма.  
  
Приемник также вычисляет контрольную сумму пакета, и если они не совпали, значит есть ошибка.  
  
Алгоритмы: контроль по паритету, вертикальный и горизонтальный контроль по паритету. Циклический избыточный контроль(CRC).  
  
13. Коды с коррекцией ошибок   
  
Для коррекции ошибок необходимо знать минимальное расстояние Хэмминга – минимальное число битовых разрядов,  
  
в которых отличается любая пара разрешенных кодов. Коды хэмминга, это блочные коды без памяти.  
  
Для схем контроля по паритету расстояние хэмминга равно 2, и при таком расстоянии коды хэмминга могут только обнаруживать ошибки.  
  
Коды Хэмминга с минимальным расстоянием Хэмминга = 3 гарантированно исправляют 1 ошибку  
  
Коды Рида — Соломона — недвоичные циклические коды, позволяющие исправлять ошибки в блоках данных  
  
14. Протоколы с автоматическим запросом повторной передачи  
  
Протоколы, использующие запросы ARQ.  
  
- Запрос ARQ с остановками - передатчик требует подтверждения приема от приемника по каждому пакету  
  
- Непрерывный запрос ARQ с возвратом - при ошибочном пакете данных передатчику посылается ARQ пакет (возврат),  
  
указывающий на ошибочный блок данных, с которого передатчик повторит отправку.  
  
- Непрерывный запрос ARQ c выборочным повторением. Повторно передаются только ошибочные пакеты.  
  
В основном это протоколы семейства TCP  
  
15. Выбор Wi-Fi роутера (основные параметры).  
  
- Скорость подключения  
  
- Стандарт - 802.11b/g/n или 802.11ac. Так как 802.11ac обладает высокой помехозащищенностью,  
  
то покупать роутер с его поддержкой есть смысл в том случае,  
  
если рядом очень много других Wi-Fi устройств.  
  
- Радиус действия  
  
- Мощность передатчика  
  
- Многие бюджетные роутеры имеют мощность передатчика около 17 дБм или даже меньше,

 чего обычно достаточно для того, чтобы более-менее уверенно "пробить" лишь 2 стены  
  
- Чувствительность приемника:Большинство массовых моделей Wi-Fi роутеров имеют значение чувствительности  
  
90 дБм на скорости 1 Мбит/с при 8% PER, но предпочтительными являются более низкие значения (-92, -94, -98)  
  
- Количество и тип антенн  
  
- Стабильность работы и прошивка.  
  
16. Основные угрозы безопасности Wi-Fi.  
  
- нарушение физической целостности сети:  
  
случайные или преднамеренные помехи в радиоканале: природные явления, СВЧ-печи, специальные генераторы помех  
  
Для защиты от них используются DSSS(ослабление помех в среднем в 10 раз) и  
  
FHSS - передача пакетов на другой частоте  
  
- подслушивание трафика:  
  
прослушивание трафика с помощью специальных программ. FHSS часично помогает. и Алгоритмы шифрования  
  
- вторжение в сеть