ETU "LETI"
SAINT PETERSBURG ELECTROTECHNICAL UNIVERSITY

ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Беспроводные технологии

Классификация беспроводных сетей

NFC
RFID

Bluetooth
ZigBee
Z-Wave
ANT

802.11a/b/g/n/…

Wi-SUN
ZigBee-NAN

4G/5G

	PAN	LAN	MAN	WAN
Стандарты	Bluetooth	IEEE 802.11 a/g/n	802.16 MMDS,LMDS	GPRS,CDMA, 3-5G
Скорость	< 48 Мбит/с	54-300 Мбит/с	40Мбит/с- 1 Гбит/с	10-25 Гбит/с
Диапазон	Короткий	Средний	Длинный	Длинный
Область применения	Точка- Точка	Сеть	Доступ последней мили	Мобильные устройства

Стандарт IEEE 802.11

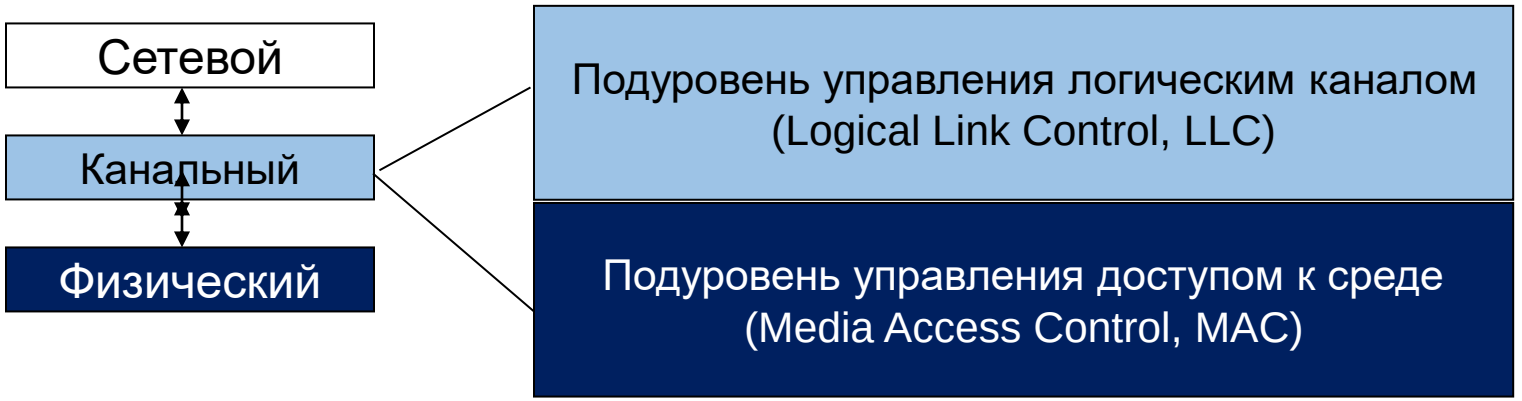
IEEE 802.11 — набор стандартов связи для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 0,9; 2,4; 3,6; 5 и 60 ГГц.

IEEE определяет четыре основных стандарта WLAN 802.11: 802.11a, 802.11b, 802.11g и 802.11n.

	802.11a	802.11b	802.11g	802.11n
Год принятия	1999	1999	2003	2009
Скорость	54 Мбит/с	11 Мбит/с	54 Мбит/с	До 600 Мбит/с
Полоса частот	5 ГГц	2.4 ГГц	2,4 ГГц	2,4-2,5 или 5 ГГц
Количество каналов	23	3	3	9

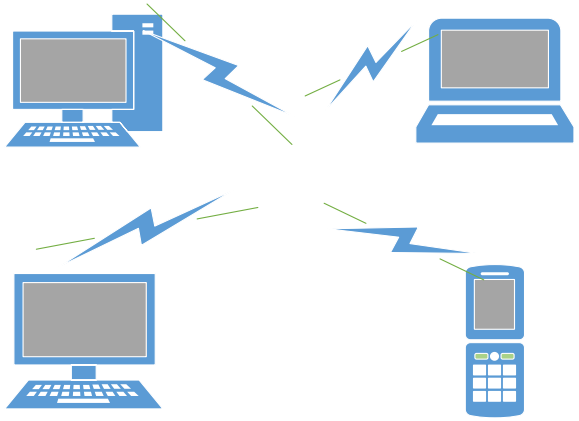
Канальный уровень

- Физический уровень – способ передачи сигналов
- 6 стандартов IEEE серии 802.11 используют электромагнитное излучение:
  - 2,4 ГГц – 802.11b, 802.11g, 802.11n
  - 5 ГГц – 802.11a, 802.11n, 802.11ac
  - не требуют лицензирования
  - наличие помех и коллизий.
- **Уровень MAC** – способ доступа к общей среде выполняет следующие функции: доступ к разделяемой среде; обеспечение перехода станции между базовыми станциями; обеспечение безопасности передачи данных.
- **Уровень LLC** – передача данных



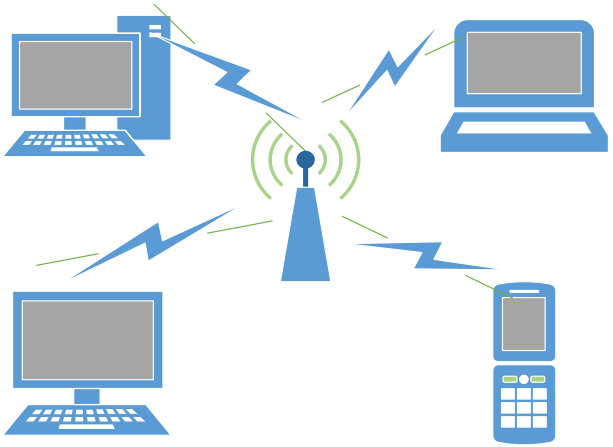
Топология

1. Независимые базовые зоны обслуживания (Сети Ad-hoc)



Проблема: увеличение вероятности коллизий, поскольку в случае одновременной передачи сигналов станциями A и C, эти станции не могут зафиксировать возникновение коллизии.

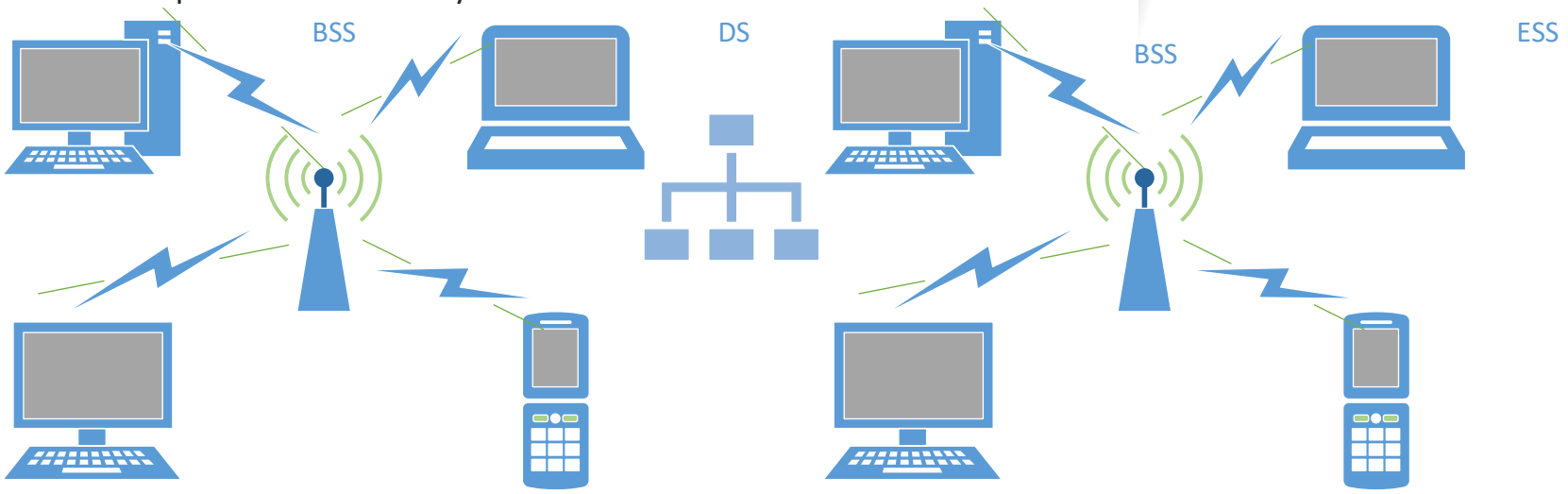
2. Базовый набора служб (Basic Service Set, BSS)



Возможность подключения достаточно большого количества пользователей, более высокая помехоустойчивость . Точка доступа может работать как по прямому назначению, так и в составе проводной сети и служить в качестве моста между проводным и беспроводным сегментами сети.

Топология

3. Расширенные зоны обслуживания

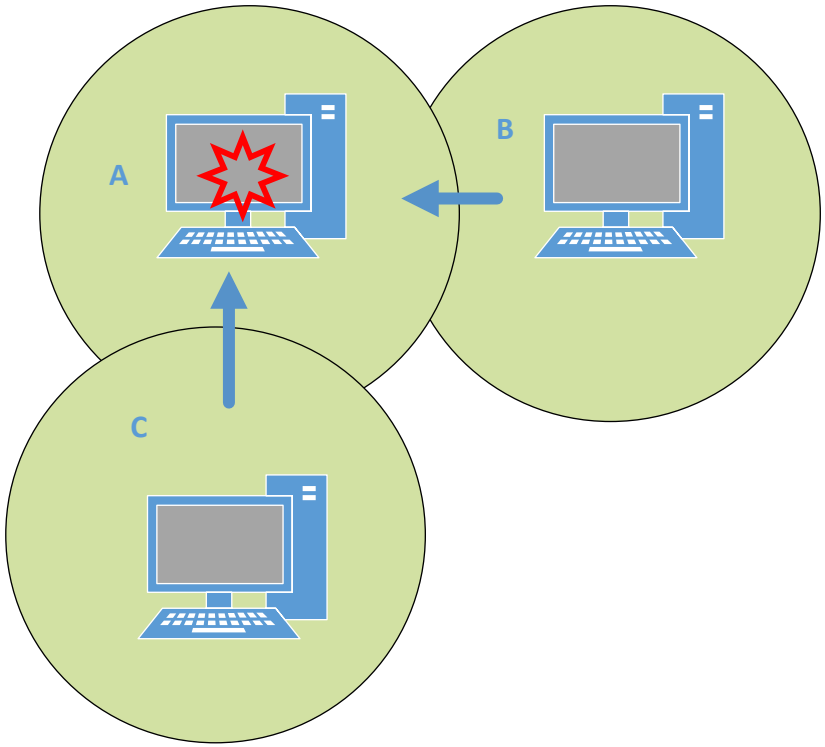


Сеть с базовым набором услуг (Basic Service Set - BSS) – конструктивная единица сети, состоит из нескольких станций, реализующих протокол MAC. Соединяется с распределительной системой (Distribution System - DS) через точку доступа или кабельное соединение.

Сеть с расширенным набором услуг (Extended Service Set - EES) – состоит из нескольких BSS объединенных распределительной системой DSS.

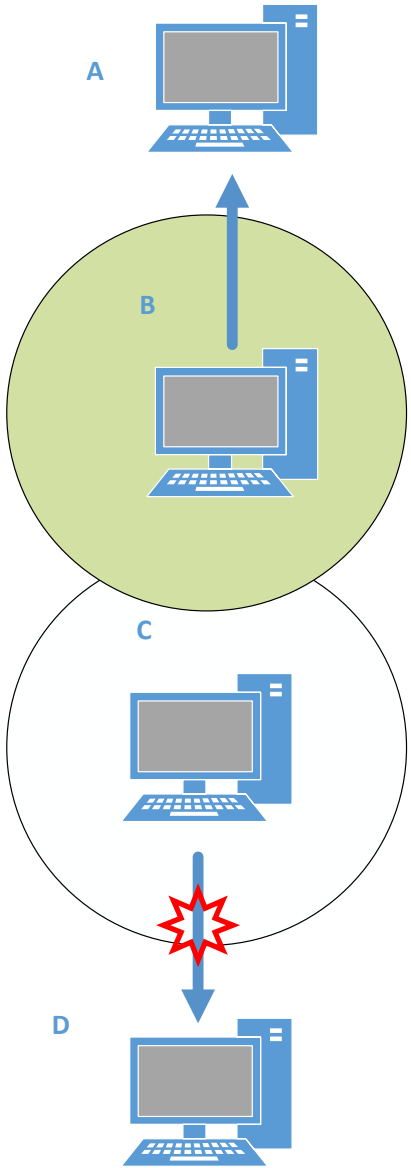
Служба распределенной системы (Distributed System Service - DSS) – служба, обеспечивающая передачу пакетов между станциями, которые не могут взаимодействовать непосредственно. DSS образуется базовыми станциями и распределительной системой DS. DS может быть основана на проводной или беспроводной среде.

Проблемы «засвеченной» станции



1. Хост B планирует осуществить передачу данных A, контроль канала показал, что он свободен.
2. В этот же момент времени хост C тоже решил передать данные хосту A, поскольку зона действия беспроводной среды C свободна.
3. Однако когда эти данные дошли до компьютера A, они столкнулись с теми данными, которые передавал хост B, произошла коллизия и хост A не может принять данные, не от одного хоста.

Проблемы скрытой станции



Хост D находится вне зоны действия передатчика хоста B, поэтому хост C может смело передавать данные хосту D, однако сам хост C находится в зоне действия передатчика хоста B, поэтому он считает, что среда занята и ждет когда хост B закончит передачу.

Проблемы передачи в среде Wi-Fi

- Передаваемый сигнал намного мощнее принимаемого
- Проблемы «скрытой» и «засвеченной» станции
- Сигнал о коллизии может не дойти до всех компьютеров
- При отсутствии подтверждения кадр пересылается повторно

- Коллизия в Wi-Fi обходится очень дорого:
  - Обнаруживается по отсутствию подтверждения
  - Временные затраты: передача кадра, тайм-аут ожидания подтверждения

Режимы коллективного доступа к среде

Для борьбы с этим, 802.11 использует типа коллективного доступа к среде передачи данных:

- функция распределенной координации (Distributed Coordination Function, DCF)
- функция централизованной координации (Point Coordination function, PCF).

Протокол Multiple Access with Collision Avoidance (MACA)

- Может использоваться в Wi-Fi (не обязательно)
- Применяется в основном в произвольном режиме (Ad-hoc)

Режимы коллективного доступа к среде. Режим DCF

DCF – подуровень для эпизодического обмена равноправных станций – каждая станция может захватить среду. Эта функция основана на методе коллективного доступа с обнаружением несущей и механизмом избегания коллизий (Carrier Sense Multiple Access/Collision Avoidance, CSMA/CA):

1. Каждый хост, прежде чем начать передачу, «прослушивает» среду, пытаясь обнаружить несущий сигнал, и только при условии, что среда свободна, может начать передачу данных.

2. Если среда занята, то хост устанавливает таймер ожидания = время резервации канала (время, необходимое на полную передачу сообщения) + время передачи кадра + короткий межкадровый интервал + время передачи подтверждения. После этого повторяется попытка передачи кадра.

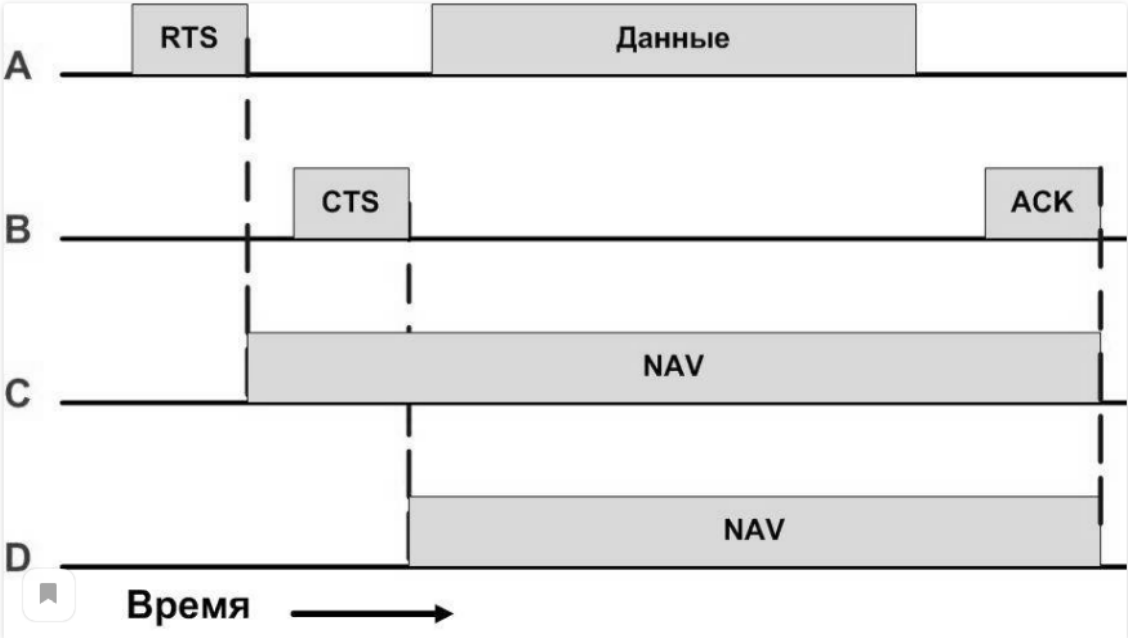
3. Если получатель принял кадр неискаженным, то он подтверждает получение, посылая служебный кадр ACK - квитанцию о доставке.

4. Если передающая станция не получила пакет ACK, то предполагается, что произошла коллизия, и через случайный промежуток времени кадр передаётся снова.

Недостаток: конфликтный принцип, асинхронная передача.

Режимы коллективного доступа к среде. Режим DCF.

1. A посылает B кадр RTS, запрашивая разрешение на передачу.
2. B подтверждает возможность передачи кадром CTS (+размер сообщения).
3. A запускает таймер ACK и начинает передачу данных.
4. В случае корректного приема, B генерирует кадр АСК, сообщающий станции A о конце передачи. Если интервал времени таймера на станции A истекает прежде, чем получен АСК, весь алгоритм работы протокола повторяется с самого начала. Механизм выставления NAV удерживает станции от передачи.



Режимы коллективного доступа к среде. Режим DCF

Проблемы беспроводных сетей:

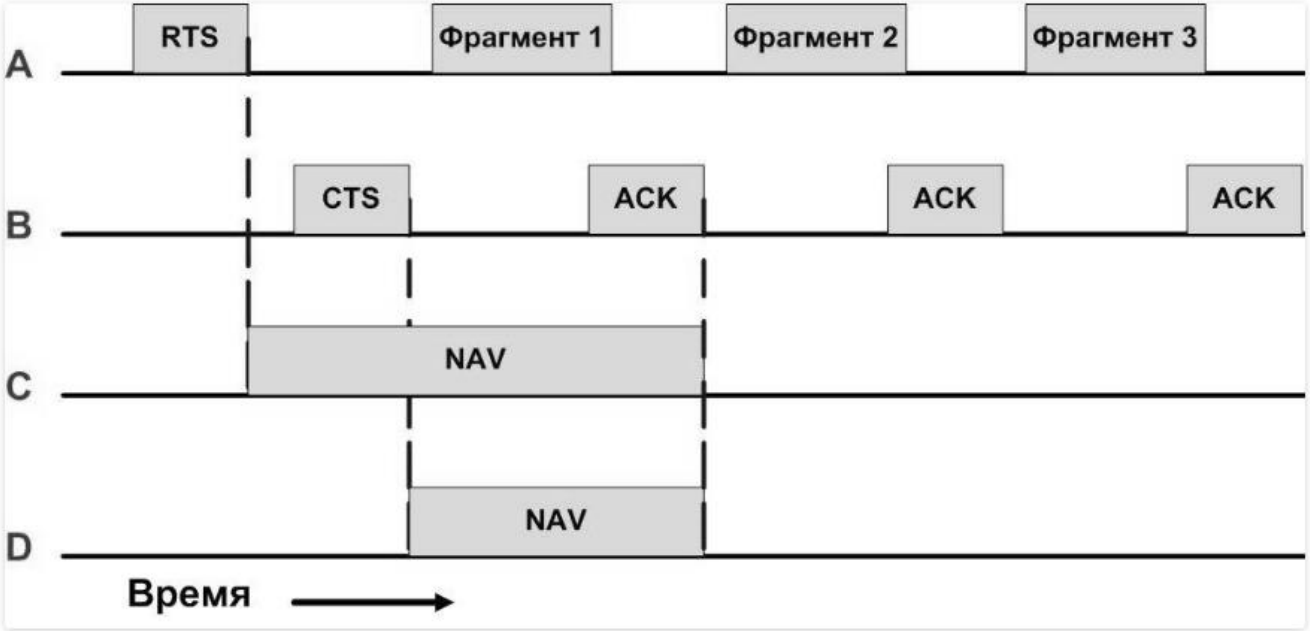
- Наличие коллизий
- Шум
- Низкая надежность канала связи.
- В результате вероятность корректной передачи кадра уменьшается пропорционально увеличению его длины.
- *Фрагментация* повышает надежность передачи путем принудительной повторной пересылки коротких отрезков кадров, в которых произошла ошибка, а не кадров целиком.
- Недостаток – уменьшение пропускной способности сети

Фрагментация кадров в Wi-Fi

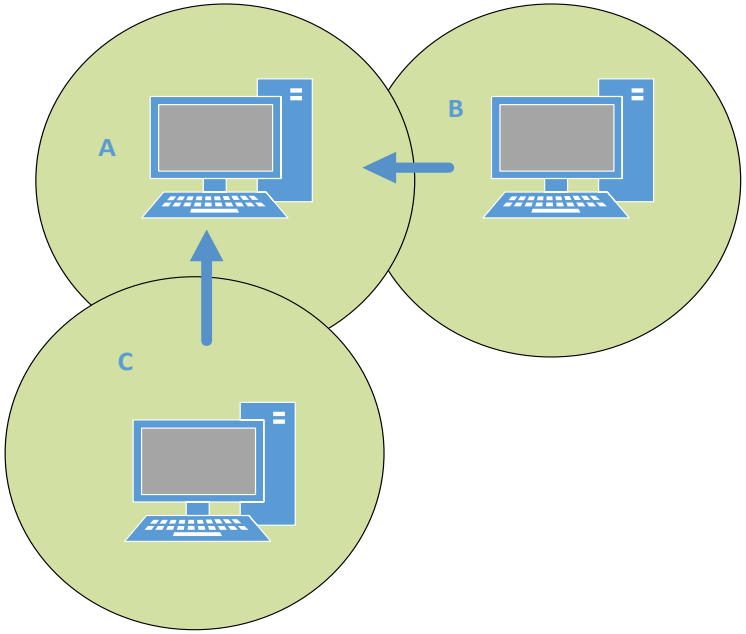
- Флаг MF в поле «Управление кадром»
  - More Fragments (еще фрагменты)
  - Признак использования фрагментации
  - Фрагменты большого кадра передаются с установленным флагом MF
  - Последний фрагмент передается без этого флага
- Поле «Управление очередностью» кадра уровня MAC
  - Sequence Control (управление последовательностью/очередностью)
  - Номер фрагмента

Режимы коллективного доступа к среде. Режим DCF

- 1. Осуществляется разбиение кадров на небольшие отрезки, каждый из которых содержит собственную контрольную сумму.
- 2. Фрагменты нумеруются и подтверждаются индивидуально с использованием протокола с ожиданием и передаются по сети.
- 3. Подтверждение принудительной повторной пересылки коротких отрезков кадров, в которых произошла ошибка, а не кадров целиком
- 4. Механизм выставления NAV удерживает станции от передачи.



Решение проблемы скрытой станции



1. *Хост B* инициирует передачу данных с хостом B сообщением RTS и
2. *Хост A в* ответ передает управляющее сообщение CTS и это сообщение получает не только *хост B*, но и *C*, который находятся вне зоны действия передатчика *компьютера B*.
3. *Хост C* понимает, что сейчас *B,* сигнал от которого он не видит, будет передавать данные размером 1500 байт, поэтому он ждет когда передача закончиться.

Режимы коллективного доступа к среде. Режим PCF

Интервалы коллективного доступа:

- пересылка приоритетного трафика (Short IFS)
- PIFS – D(CF)IFS – процедура организации приоритетного синхротрафика
- DIFS – процедура организации неприоритетного асинхронного трафика

Приоритеты

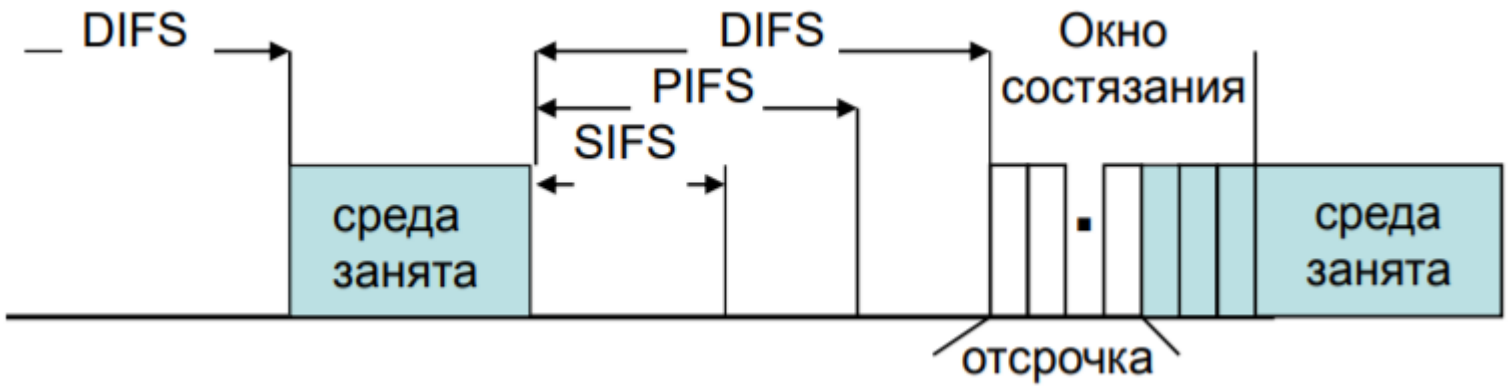
- Межкадровый интервал SIFS имеет наименьшее значение, он служит для первоочередного захвата среды ответными CTS-кадрами или квитанциями, которые продолжают или завершают уже начавшуюся передачу кадра.
- Значение межкадрового интервала PIFS больше, чем SIFS, но меньше, чем DIFS. Промежутком времени между завершением PIFS и DIFS пользуется арбитр среды. В этом промежутке он может передать специальный кадр, который говорит всем станциям, что начинается контролируемый период.

Захват среды возможен, когда среда свободна в течение времени, равного или большего, чем DIFS.

Режимы коллективного доступа к среде. Режим PCF

Механизм PCF является опциональным и применяется в сетях с точкой доступа, выступающей в виде центра координации (Point Coordinator, PC)

1. Каждый хост может работать в режиме PCF, для этого он должен подписаться на эту услугу при присоединении к сети.
2. Координатор циклически опрашивает станции с приоритетным трафиком используя процедуру опроса, для реализации права хостов на использование среды, направляя им специальный кадр.
3. Хост, получив такой кадр, подтверждает прием специального кадра и одновременно передает данные к адресату в интервале SIFS-PIFS.
4. При отсутствии подтверждения координатор опрашивает следующую станцию в интервале PIFS-DIFS.
5. После его окончания арбитр передает соответствующий кадр и начинается неконтролируемый период.



Формат кадра Wi-Fi уровня MAC

2 байта	2 байта	6 байт	6 байт	6 байт	2 байта	6 байт	0-2304 байт	4 байта
Управление кадром	Длительность	Адрес 1	Адрес 2	Адрес 3	Управление очередностью	Адрес 4	Тело кадра	Контрольная сумма

2 бита	2 бита	4 бита	1 бит	1 бит	1 бит	1 бит	1 бит	1 бит	1 бит	1 бит
Версия протокола	Тип	Подтип	To DS	From DS	MR	RT	Power Mgmt	MD	Protection Frame	Order

Управление питанием

Стандарт IEEE 802.11 PSM

- Режимы работы станции: активный и спящий
- В спящем режиме станция не принимает и не передает данные
- Точка доступа записывает кадры для «спящей» станции в буфер
- «Спящая» станция регулярно просыпается и читает все кадры от точки доступа
- Передавать кадры станция может в любое время

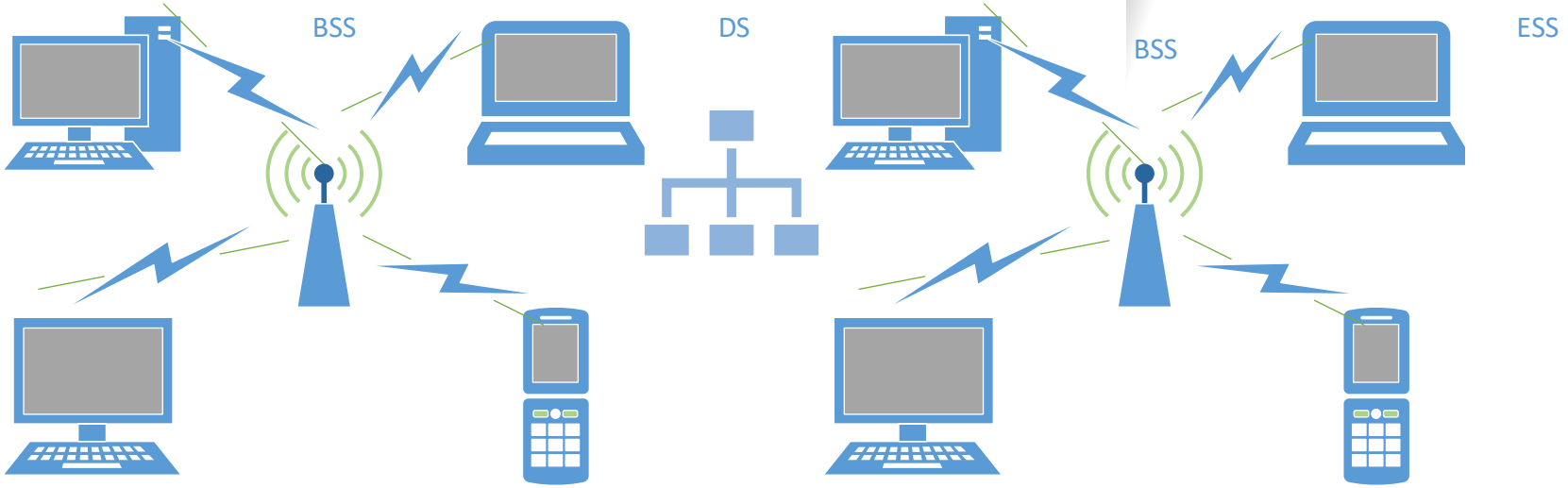
Флаг PM

- Power Management (управление питанием)
- Показывает, в каком режиме находится станция

Флаг MD

- More Data (больше данных)
- Сигнализирует, что есть еще кадры для получения

Адреса в кадре Wi-Fi



To DS	From DS	Адрес 1	Адрес 2	Адрес 3	Адрес 4
0	0	RA/DA	TA/SA	BSSID	n/a
0	1	RA/DA	TA/BSSID	SA	n/a
1	0	RA/BSSID	TA/SA	DA	n/a
1	1	RA	TA	DA	SA

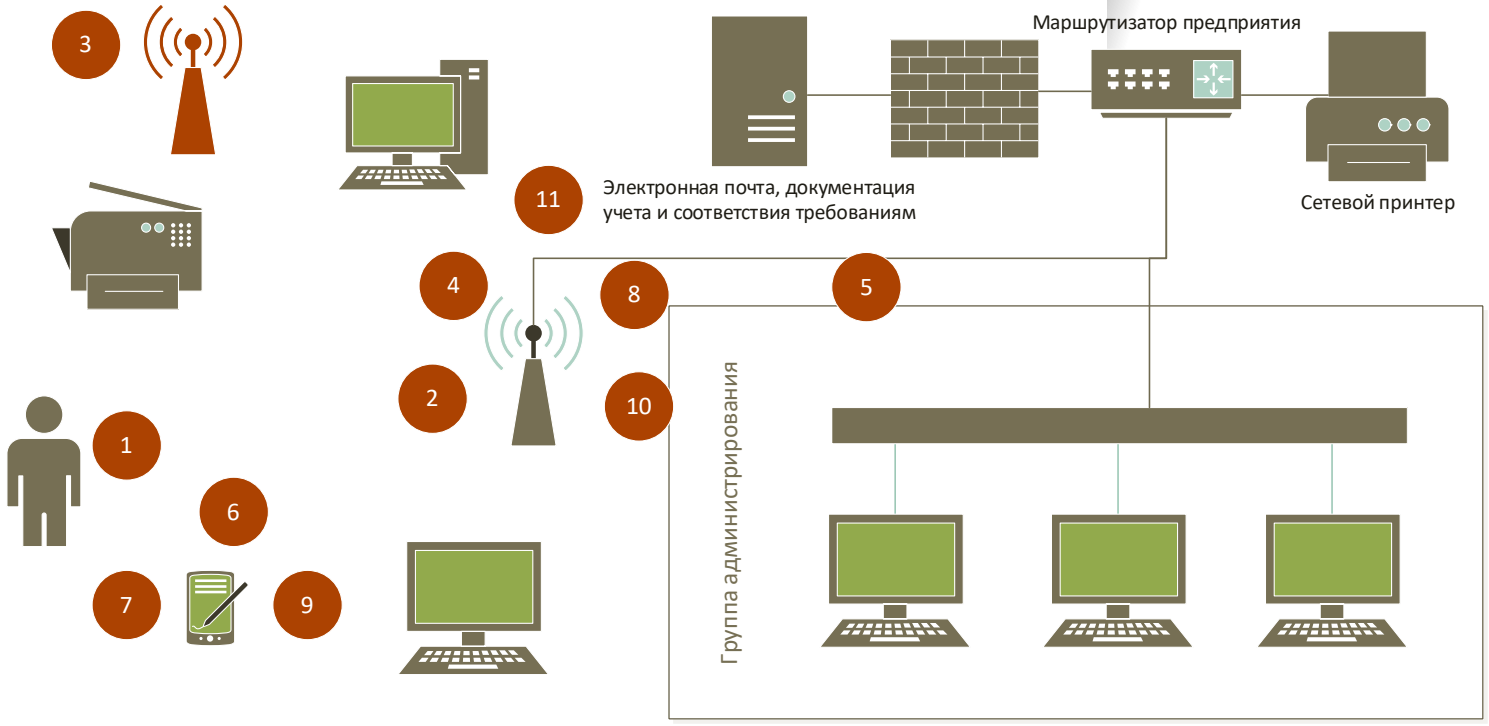
- RA – Receiver address
- TA – Transmitter address
- DA – Destination address
- SA - Source address
- BSSID – идентификатор сети

Нормативно-правовая база

ГОСТ Р ИСО/МЭК 27033-1-2011. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции.
ГОСТ Р 59162-2020. Национальный стандарт Российской Федерации.

Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 6. Обеспечение информационной безопасности при использовании беспроводных IP-сетей.

Вопросы безопасности



1	Несанкционированный доступ	5	Неправильная маршрутизация	9	Незащищенная начальная загрузка
2	Анализ пакетов	6	Перехват IMSI	10	Взлом методов шифрования и ключей
3	Фальшивая точка доступа	7	Отслеживание оборудования пользователя	11	Доступ в нерабочее время
4	Ddos	8	Принудительная передача данных	12	Использование механизма WPS

Вопросы безопасности

Атаки напрямую на сеть:

- *анализ пакетов*

- реализация атаки Ddos - злоумышленник создает устройство, заполняющее весь спектр на частоте 2.4 Ггц помехами и нелегальным трафиком. При этом достаточно трудно доказать сам факт проведения DDos атаки на физическом уровне в беспроводной сети.

Организация поддельных точек доступа -задача сводится к «созданию» двойника сети, к которой у потенциальной жертвы может быть сконфигурирован доступ (как с зашитой, так и без). Также, при наличии рядом легитимной точки доступа, злоумышленник может попытаться ее «погасить», чтобы перенаправить клиентов на свою точку доступа.

Вероятность реализации повышается, если:

- Используются протоколы WEP/PEP
- У пользователя настроено автоматическое подключение к сети

Вопросы безопасности

Избыточное покрытие сети

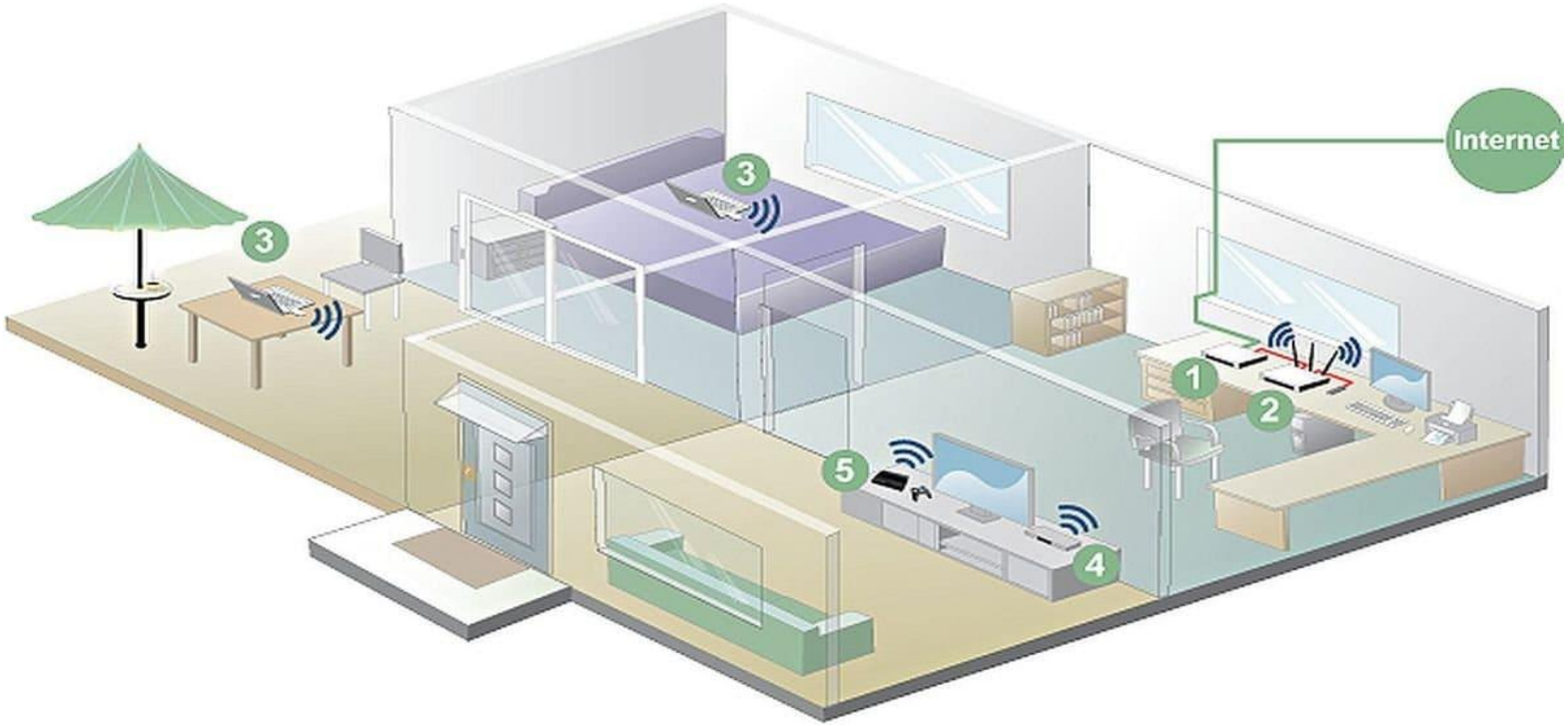
-доступность за пределами контролируемой зоны

- оценка диаграмм направленности сети

Рекомендации:

-снижение мощности сигнала

-перемещение оборудование (центр, другие помещения)



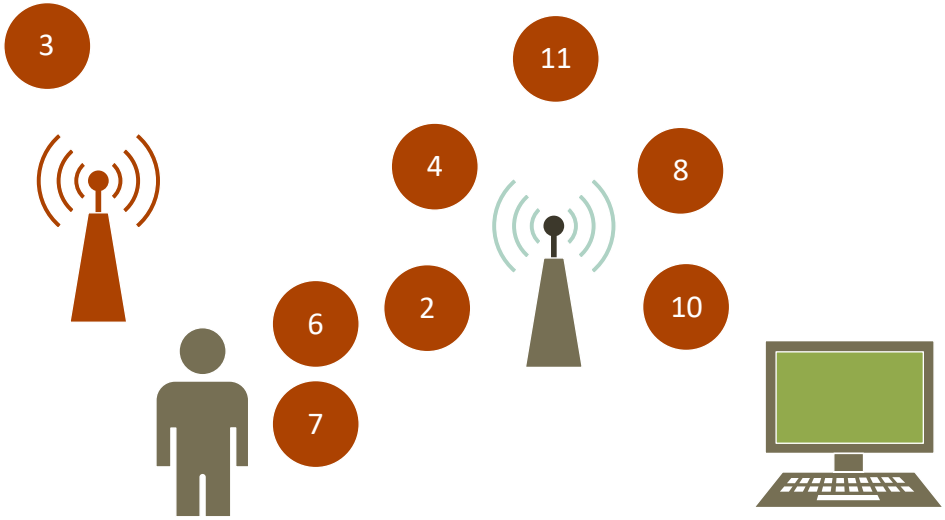
Вопросы безопасности

- **Проблемы идентификатора беспроводной ЛВС.** Идентификатор SSID регулярно передается точками радиодоступа в специальных фреймах Beacon. По нему атакующий может определить SSID с помощью анализатора трафика, например Sniffer Pro Wireless.

- **Уязвимость аутентификации по MAC-адресу.** При аутентификации по MAC-адресу, атакующий может обмануть метод аутентификации путем подмены своего MAC-адреса легитимным. Подмена MAC-адреса возможна в беспроводных адаптерах, допускающих использование локально администрируемых MAC-адресов. Злоумышленник может воспользоваться анализатором трафика протокола IEEE 802.11 для выявления MAC-адресов легитимных абонентов.

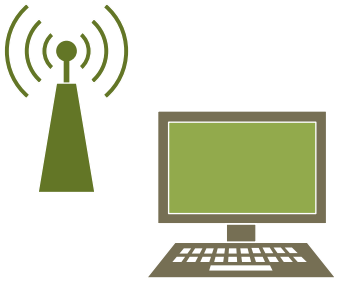
- **Уязвимость открытой аутентификации.** Открытая аутентификация не позволяет определять легитимность пользователя, в связи с этим рекомендуется использовать WEP. Или использовать методы аутентификации более высокого уровня.

Механизм реализации удаленного доступа



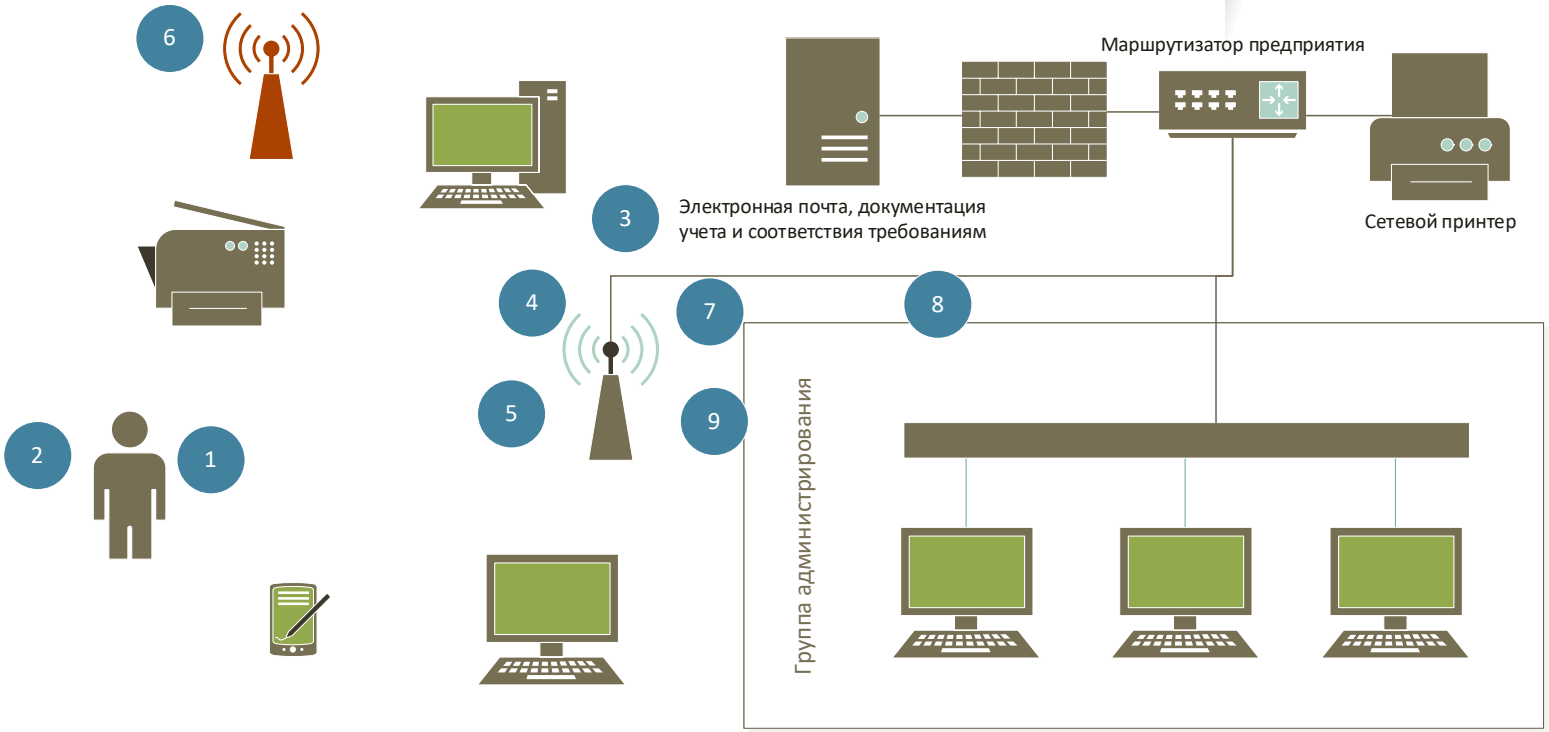
1. Сценарий проникновения через фальшивую точку доступа
2. Сценарий проникновение через гостевой доступ
3. Сценарий перебора пароля по словарю

Использование механизма WPS



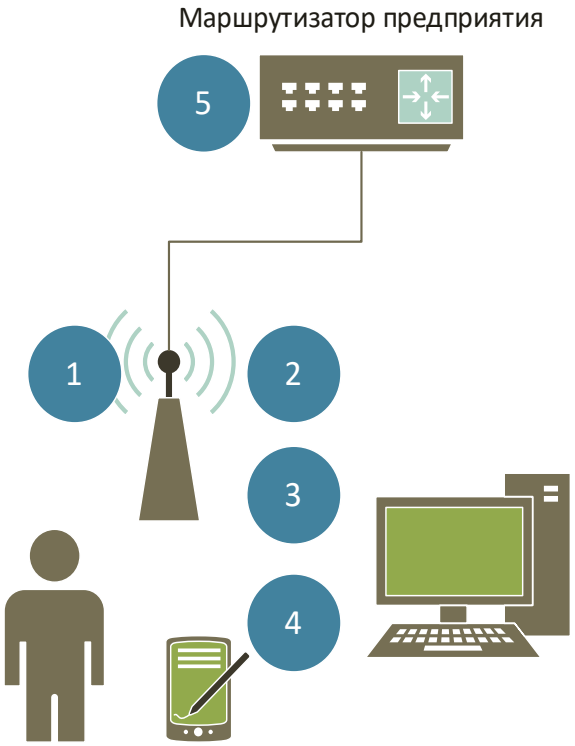
- Использование механизма WPS
- Получение доступа к беспроводной сети
- Развитие атаки

Механизмы обеспечения безопасности



1	Режим изоляции гостевого входа точки доступа	5	Безопасные методы аутнтификации	9	Обновление ПО
2	Запрет на использование гостевого доступа	6	Выявление несанкционированных точек	10	Основные механизмы и средства безопасности беспроводных сетей ориентированы, как правило, на защиту канального уровня. Защита на более высоких уровнях сетевой модели реализуется на базе типичных для проводных сетевых КС механизмах
3	Использование надежных механизмов шифрования	7	Управление доступом		
4	Сегментирование сети	8	Межсетевое экранирование		

Обеспечение безопасности на основании сервисов Wi-Fi



Подключение компьютера к точке доступа

1. Использование идентификатор беспроводной локальной сети (Service Set Identifier - SSID)

Аутентификация

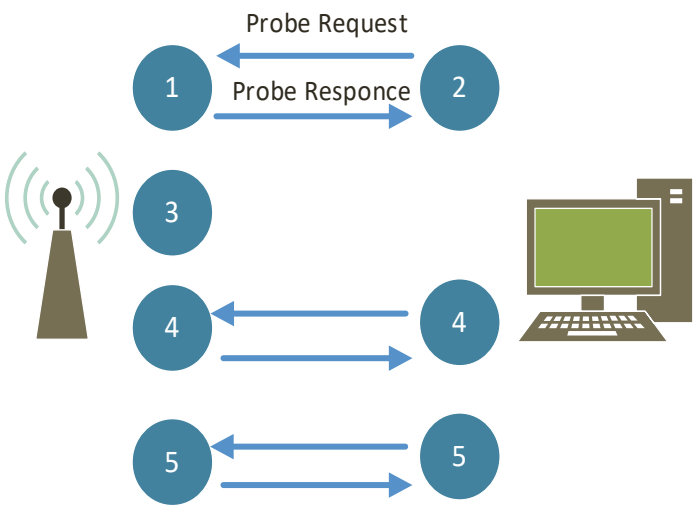
2. Контроль за подключением к точке доступа на основе MAC-адресов и имени сети
3. Шифрование на основе протокола WEP (RC4)/ WPA (AES)
4. Проверка права передачи данных

Ассоциация

Доставка данных

6. Шифрование на основе протокола WEP (RC4)/ WPA (AES).
7. Контроль за доступом к среде передачи

Принципы аутентификации

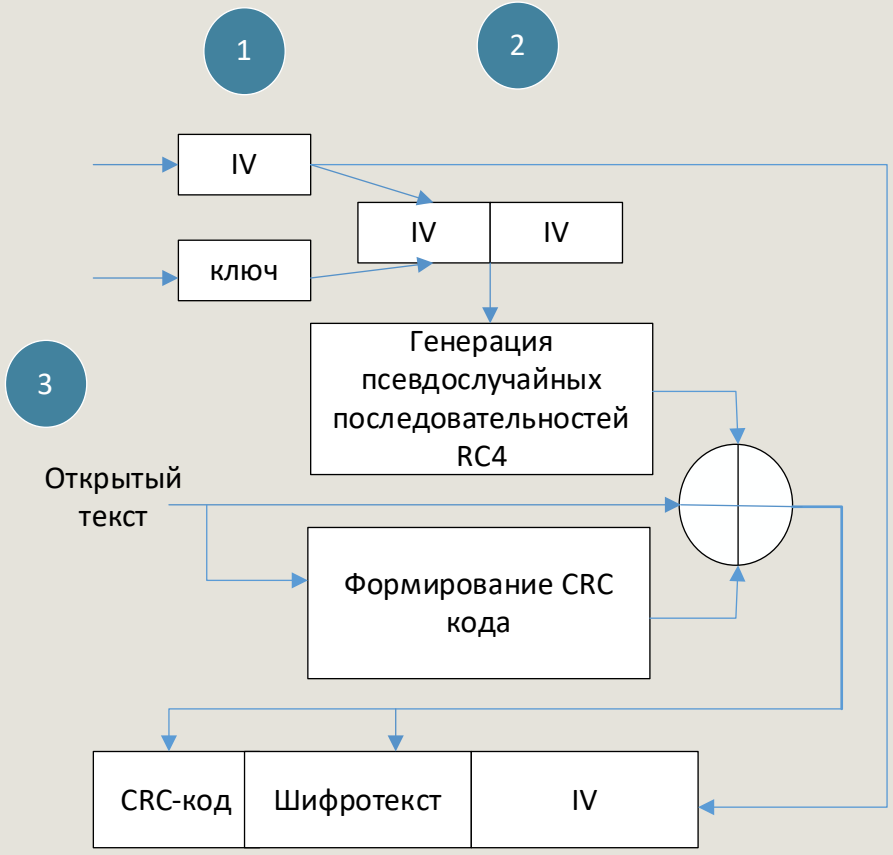


Подключение компьютера к точке доступа

1. Поиск точек радиодоступа в своей зоне радиовидимости с помощью управляющих фреймов Probe Request
2. Каждая точка радиодоступа, удовлетворяющая параметрам, отвечает фреймом Probe Response, содержащим синхронизирующую информацию и данные о текущей загрузке точки радиодоступа.
3. Каждая точка радиодоступа из находящихся в зоне радиовидимости абонента, удовлетворяющая запрашиваемым во фрейме Probe Request параметрам, отвечает фреймом Probe Response, содержащим синхронизирующую информацию и данные о текущей загрузке точки радиодоступа.
4. Аутентификация абонента по его MAC-адресу. При аутентификации по MAC-адресу происходит сравнение MAC-адреса абонента либо с хранящимся локально списком разрешенных адресов легитимных абонентов
5. Фаза ассоциирования

WEP

Wired Equivalent Privacy (WEP) — алгоритм для обеспечения безопасности сетей Wi-Fi. Используется для обеспечения конфиденциальности и защиты передаваемых данных авторизированных пользователей беспроводной сети от прослушивания.



1

Каждый участник устанавливает у себя общий секретный ключ (в 802.11 предусмотрено наличие до четырех секретных ключей). Размер секретного ключа может быть установлен равным 40 или 104 битам

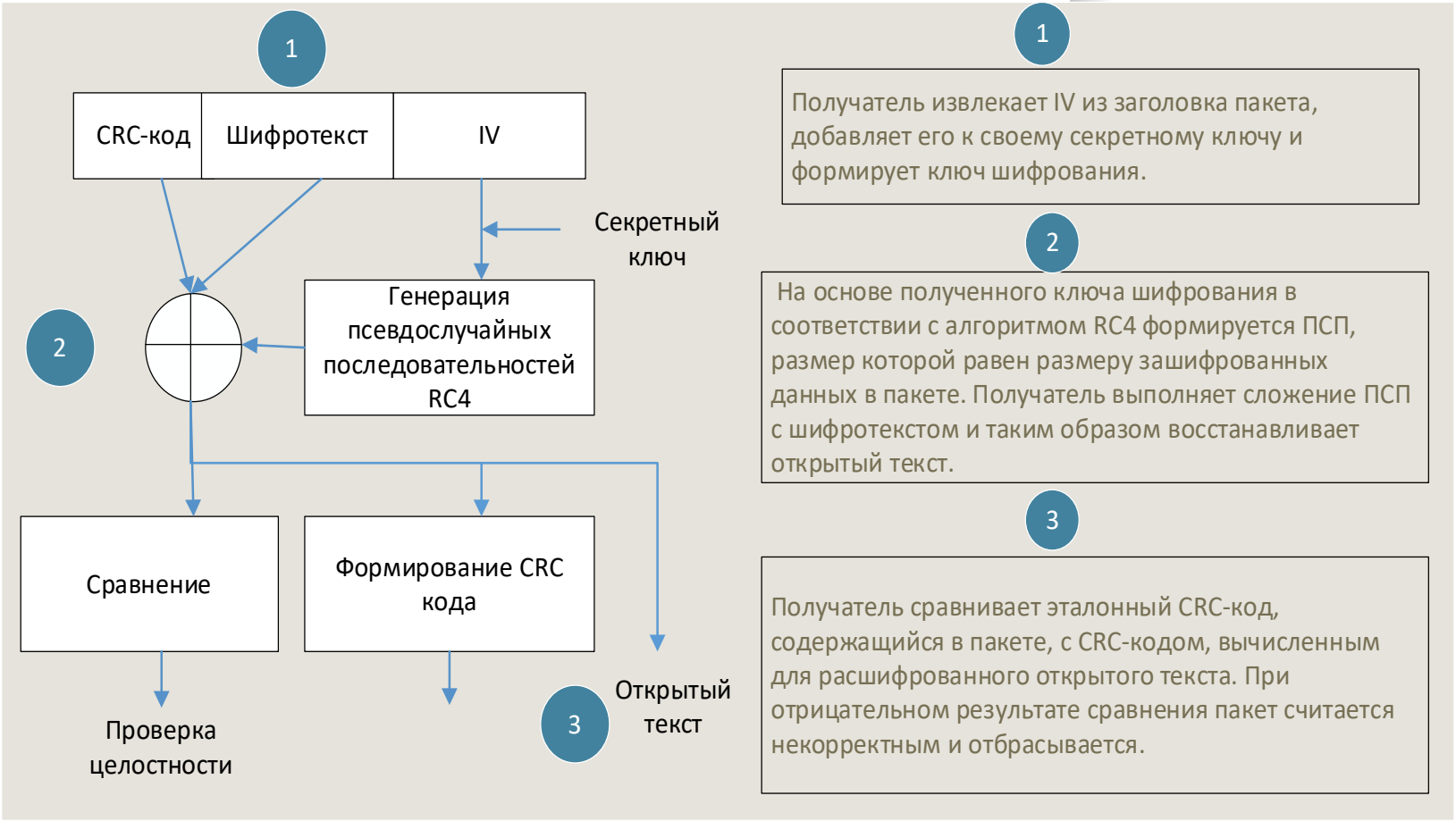
2

Вектор инициализации размером 24 бита, добавляется к секретному ключу со стороны младших байтов и формирует ключ шифрования данного пакета (размером 64 или 128 бит).

3

Использование алгоритма RC4 и полученного ключа шифрования позволяет зашифровать данные с использованием ПСП. Отправитель добавляет IV в соответствующее поле в заголовке пакета и устанавливает битовый флаг, сообщающий об использовании WEP. Пакет отправляется получателю.

WEP

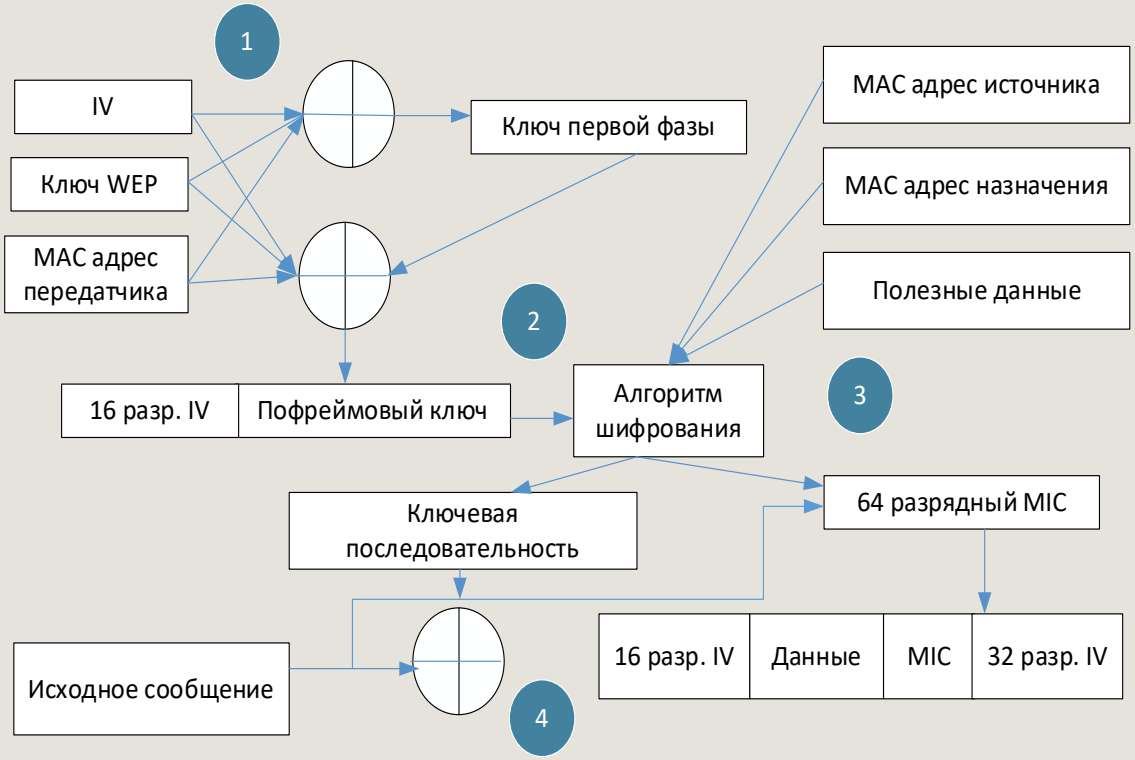


Аутентификация с использованием WEP подвержена атакам человек посередине. Атакующий перехватывает как нешифрованный, так зашифрованный трафик, и формирует ключевую последовательность на основе анализа вектора инициализации

WPA

- WPA (Wi-Fi Protected Access), WPA2 и WPA3 — программы сертификации устройств беспроводной связи, разработанные объединением Wi-Fi Alliance для защиты беспроводной Wi-Fi-сети. Основаны на стандарте IEEE 802.11i-2004.
- Преимущества:
- Обязательная аутентификация с использованием EAP.
- Усовершенствованная схема шифрования RC4
- Система централизованного управления безопасностью, возможность использования в действующих корпоративных политиках безопасности.

WPA



1. Механизм шифрования TKIP осуществляется следующим образом:
2. С помощью алгоритма пофреймового назначения ключей генерируется пофреймовый ключ.
3. Алгоритм MIC генерирует MIC для фрейма в целом.
4. Фрейм фрагментируется в соответствии с установками MAC относительно фрагментации.
5. Фрагменты фрейма шифруются с помощью пофреймового ключа.
6. Осуществляется передача зашифрованных фрагментов.

1

Пофреймовое изменение ключей шифрования. Помимо увеличения 24-разрядный вектор инициализации до 48-разрядного IV, MAC-адрес передатчика и WEP-ключ обрабатываются вместе с помощью двухступенчатой функции перемешивания.

2

Получение пофреймового ключа

3

Использование контроля целостности сообщения (MIC) устраняет проведение атак с использованием поддельных фреймов и манипуляции битами. Для этого MIC формируются уникальный ключ, отличающийся от ключа, используемого для шифрования фреймов данных, перемешивается с назначенным MAC-адресом и исходным MAC-адресом фрейма, а также со всей незашифрованной частью фрейма

Сравнение технологий

Технология	Статический WEP	Динамический WEP	WPA	WPA 2 (Enterprise)	WPA 3
Год принятия	1999	1999	2003	2004	2018
Аутентификация	Общий ключ	EAP	EAP или общий ключ	EAP или общий ключ	Технология SEA
Целостность	32-bit Integrity Check Value (ICV)	32-bit ICV	64-bit Message Integrity Code (MIC)	CRT/CBC-MAC (Counter mode Cipher Block Chaining Auth Code — CCM) Part of AES	SHA, BIP-GMAC-256
Шифрование	Статический ключ 40 бит	Сессионный ключ	129	CCMP (AES) 40 бит	CCMP (AES) 128 бит, 198 бит

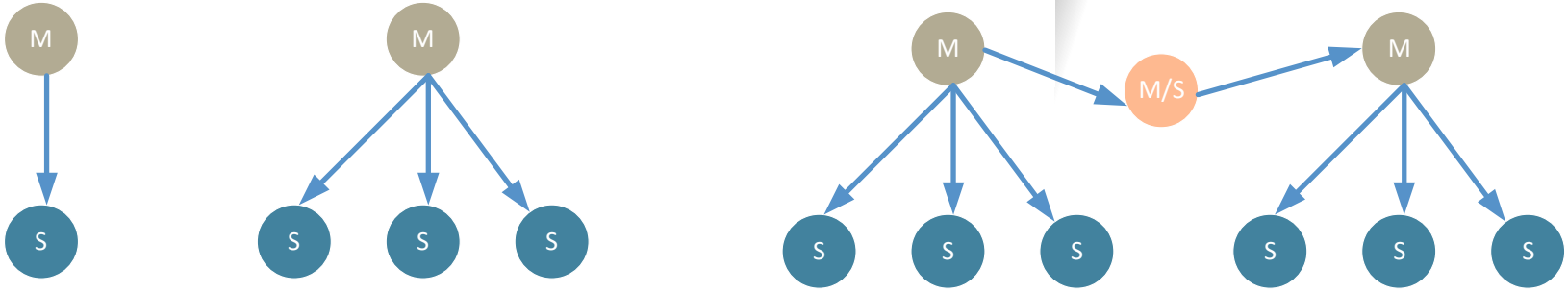
Сравнение технологий

Технология	Статический WEP	Динамический WEP	WPA	WPA 2 (Enterprise)	WPA 3
Распределение ключей	Однократное, вручную	Сегмент Pair-wise Master Key (PMK)	Производное от PMK	Производное от PMK	Производное от PMK
Вектор инициализации	Текст, 24 бита	Текст, 24 бита	Расширенный вектор, 65 бит	48-бит номер пакета (PN)	48-битный вектор инициализации
Алгоритм шифрования	RC4	RC4	RC4	AES	AES
Длина ключа, бит	64/128	64/128	128	до 256	до 256
Требуемая инфраструктура	Нет	RADIUS	RADIUS	RADIUS	RADIUS

Bluetooth

- Bluetooth — производственная спецификация беспроводных персональных сетей WPAN.
- Bluetooth обеспечивает обмен информацией между оконечными пользовательскими устройствами, такими как персональные компьютеры, мобильные телефоны, принтеры, цифровые фотоаппараты, устройства ввода, наушники, гарнитуры на радиочастоте для ближней связи. Протокол Bluetooth относится к физическому уровню модели OSI и в настоящее время определяется спецификацией IEEE 802.15.1.

Топология



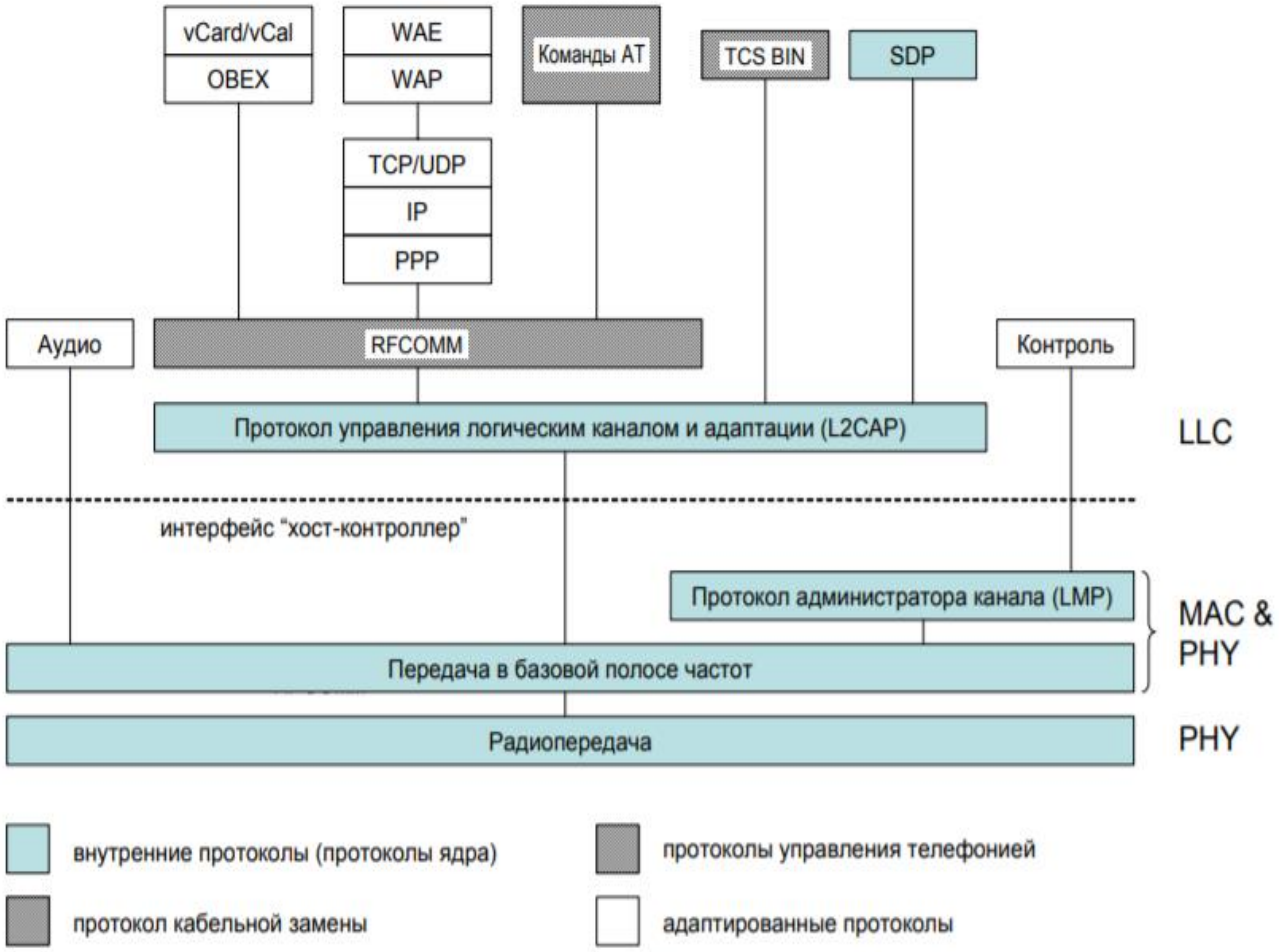
пикосеть типа точка-точка (с одним ведомым устройством)

пикосеть типа звезда (до 7 ведомых устройств)

рассеянная сеть

- **Пикосеть:**
- •в одной пикосети существует только одно ведущее устройство, все остальные – подчинённые;
- •максимальное количество устройств одной пикосети, одновременно участвующих в передаче информации, –не более 8
- •в каждый момент времени обмен данными может идти только между двумя устройствами в одном направлении
- **Рассеянная сеть:**
- •образуется путём перекрытия отдельных пикосетей
- •каждое устройство одной пикосети может входить в другую пикосеть как в качестве подчинённого, так и в качестве ведущего

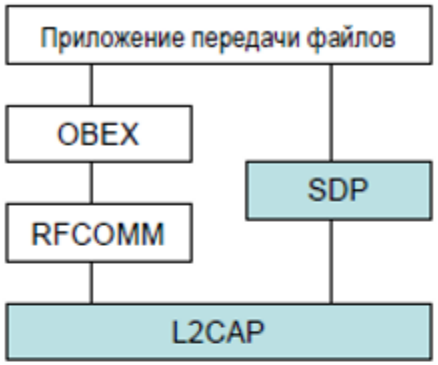
Стек протоколов Bluetooth



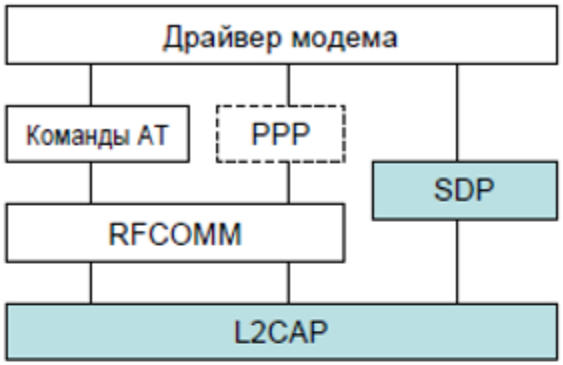
Профили

- Hands-Free Profile (HFP) — используется для соединения беспроводной гарнитуры и телефона, передаёт монозвук в одном канале.
- Human Interface Device Profile (HID) — обеспечивает поддержку устройств с HID (Human Interface Device), таких как мыши, джойстики, клавиатуры и пр. Использует медленный канал, работает на пониженной мощности.

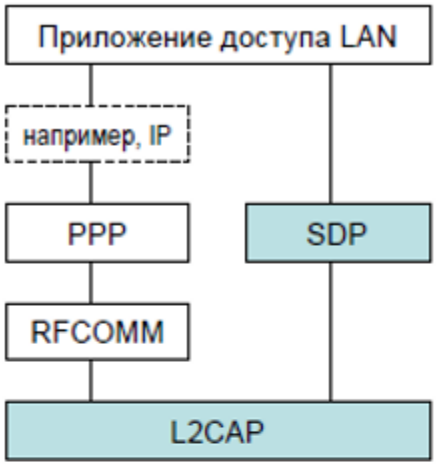
Модели использования



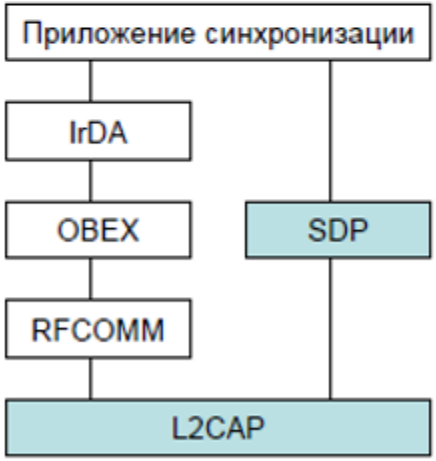
Передача файлов



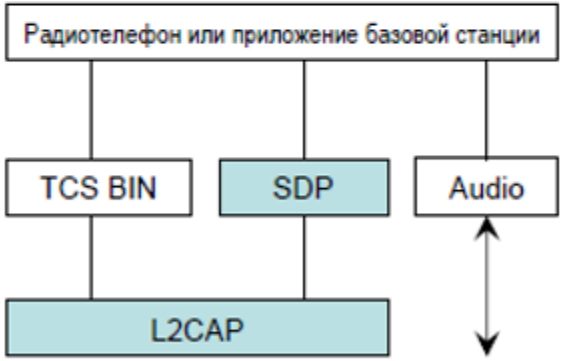
Мост Internet



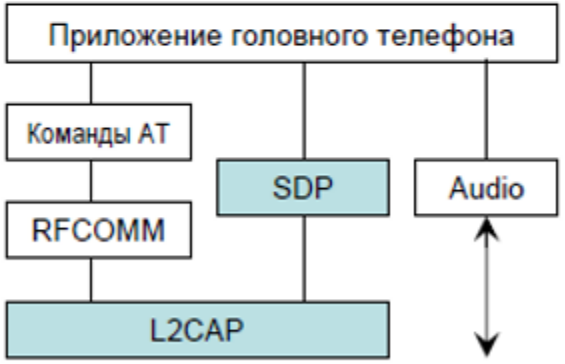
Доступ к локальной сети



Синхронизация

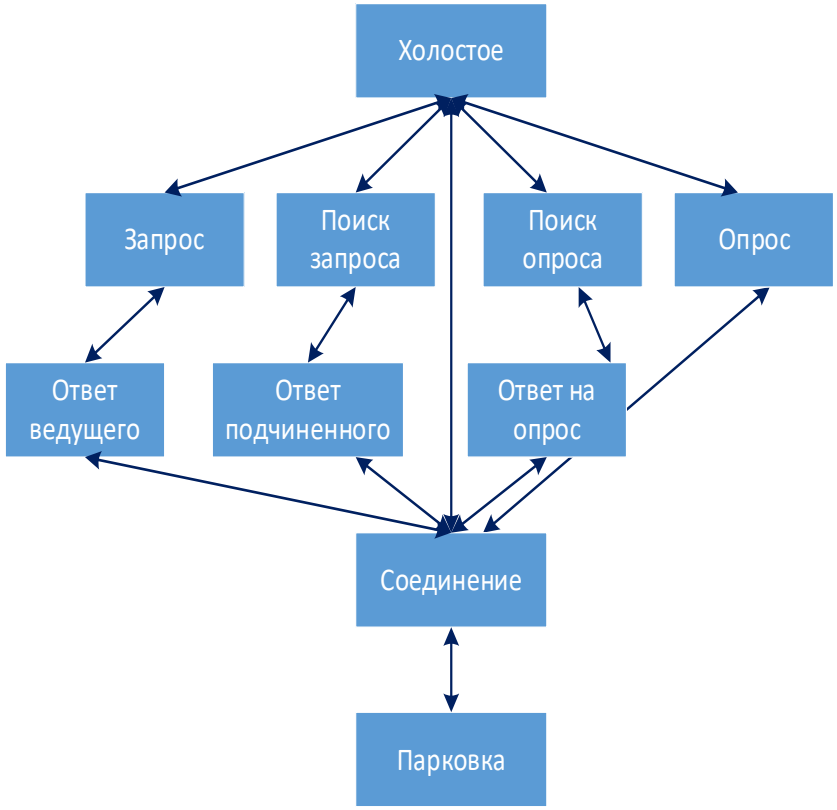


Телефон "три в одном"



Головной телефон

Механизм соединения. Состояния Bluetooth



Основные состояния:

•*холостое состояние* – низкое энергопотребление, работают только часы устройства

•*состояние соединения* – устройство подключено к пикосети

•*состояние парковки* – состояние подчинённого устройства, от которого не требуется участия в работе пикосети, но которое должно оставаться её частью

Промежуточные состояния:

•*опрос* – определение устройством наличия других устройств в пределах его досягаемости

•*поиск опроса* – ожидание устройством опроса

•*ответ на опрос* – устройство, получившее опрос, отвечает на него

•*запрос* – посылается одним устройством другому для установления с ним соединения (запрашивающее устройство становится ведущим, запрашиваемое – подчинённым)

•*поиск запроса* – устройство ожидает запрос

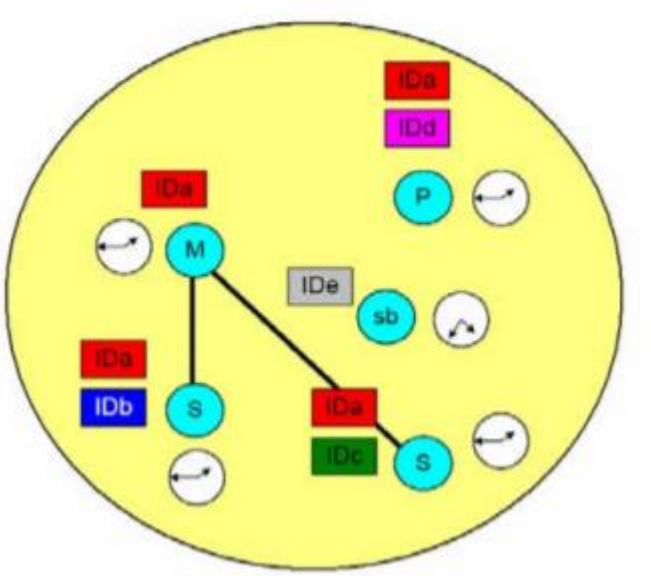
•*ответ подчинённого устройства* – подчинённое устройство отвечает на запрос ведущего

•*ответ ведущего устройства* – ведущее устройство отвечает подчинённому после получения от него ответа на запрос

Механизм соединения [6]

Все подчинённые устройства пикосети имеют:

- одинаковую последовательность перестройки частоты, определяемую адресом IDa ведущего устройства M (FDMA)
- временную синхронизацию с ведущим устройством (TDD, TDMA)
- код доступа к каналу, определяемый адресом ведущего устройства IDa (CDMA)



последовательность перестройки частоты + значение часов ведущего устройства + код доступа к каналу = физический канал пикосети

sb - холостое состояние (standby)

P - парковка

S - подчинённое устройство

Атаки

- *Атака человек по середине*
- Атака BIAS позволяет устанавливать с атакуемым устройством безопасное Bluetooth-соединение в обход механизма аутентификации.
- *Атаки на ключи*
- Компонент CTKD используется для согласования и настройки ключей аутентификации при сопряжении двух устройств с поддержкой Bluetooth. Он работает путем настройки двух разных наборов ключей аутентификации для стандартов Bluetooth Low Energy (BLE) и Basic Rate/Enhanced Data Rate (BR/EDR). Роль CTKD состоит в том, чтобы подготовить ключи и позволить сопряженным устройствам решить, какую версию стандарта Bluetooth они хотят использовать.
- *Атаки на алгоритм шифрования*
- Спецификации BR/EDR (Basic Rate/Enhanced Data Rate) позволяют взломать зашифрованные сообщения по Bluetooth. Для этого злоумышленнику нужно просто зайти в зону покрытия устройств. Уязвимость содержалась в возможности Bluetooth-устройств самостоятельно назначать длину ключа для шифрования информации.

Атаки

- *Атака человек по середине*
- Атака BIAS позволяет устанавливать с атакуемым устройством безопасное Bluetooth-соединение в обход механизма аутентификации.
- *Атаки на ключи*
- Компонент CTKD используется для согласования и настройки ключей аутентификации при сопряжении двух устройств с поддержкой Bluetooth. Он работает путем настройки двух разных наборов ключей аутентификации для стандартов Bluetooth Low Energy (BLE) и Basic Rate/Enhanced Data Rate (BR/EDR). Роль CTKD состоит в том, чтобы подготовить ключи и позволить сопряженным устройствам решить, какую версию стандарта Bluetooth они хотят использовать.
- *Атаки на алгоритм шифрования*
- Спецификации BR/EDR (Basic Rate/Enhanced Data Rate) позволяют взломать зашифрованные сообщения по Bluetooth. Для этого злоумышленнику нужно просто зайти в зону покрытия устройств. Уязвимость содержалась в возможности Bluetooth-устройств самостоятельно назначать длину ключа для шифрования информации.

Обеспечение безопасности [8]

Характеристика	Bluetooth BR/EDR	
	До версии 4.1	Версия 4.1 и новее
Физические радио каналы	79 каналов с шагом в 1 МГц	
Обнаружение / соединение	Опрос (inquiry) / разбиение (paging)	
Конфиденциальность адреса устройства	Отсутствует	
Максимальная скорость данных	1-3 Мбит/с	
Алгоритм сопряжения	До версии 2.1: E21/E22/SAFER+ Версия 2.1-4.0: Elliptic Curve P-192, HMAC-SHA-256	P-256 Elliptic Curve, HMAC-SHA-256
Алгоритм аутентификации устройства	E1/SAFER	HMAC-SHA-256
Алгоритм шифрования	E0/SAFER+	AES-CCM
Стандартный радиус действия	30 метров	
Максимальная выходная мощность	100 мВ (20 дБ)	

Литература

1. ГОСТ Р ИСО/МЭК 27033-1-2011. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции.
2. ГОСТ Р 59162-2020. Национальный стандарт Российской Федерации.
3. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 6. Обеспечение информационной безопасности при использовании беспроводных IP-сетей.
4. Варлатая С. К., Рогова О. С., Юрьев Д. Р. Анализ методов защиты беспроводной сети Wi-Fi от известных способов взлома злоумышленником // Молодой ученый. — 2015. — №1. — С. 36-37.
5. Протоколы беспроводной передачи данных https://intuit.ru/studies/courses/1004/202/lecture/5250?page=3
6. Лекция 1. Обзор архитектуры Bluetooth Версия 2.0 + EDR https://wl.unn.ru/materials/courses/wlnet/Lect/6_Lect_1.pdf
7. Интернет-энциклопедия https://ru.wikipedia.org/wiki/Bluetooth
8. Эксплуатация достоверного Bluetooth-соединения https://www.securitylab.ru/analytics/495788.php