

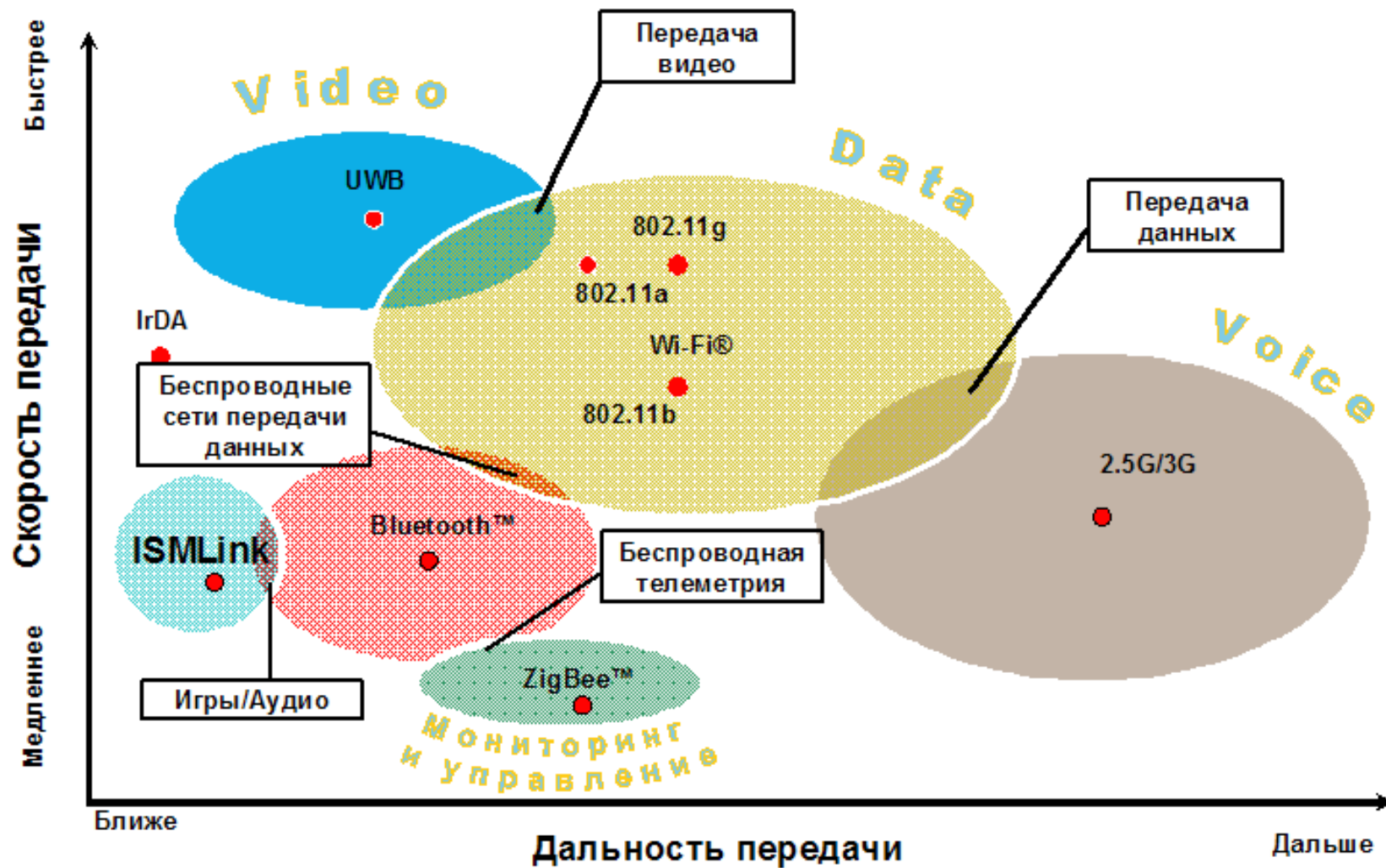
# Семейство стандартов IEEE 802.15

Bluetooth

ZigBee

UWB

# Стандарты беспроводной связи



# Семейство стандартов IEEE 802.15

Семейство стандартов IEEE 802.15 образует беспроводную сеть WPAN (Wireless Personal Area Network), которая обеспечивает беспроводную связь между различного типа устройствами на небольших расстояниях.

Стандарты, которые входят в это семейство - это

Bluetooth (IEEE 802.15.1)

IEEE 802.15.3, ZigBee (IEEE 802.15.4)

UWB (Ultra Wideband) (IEEE 802.15.4a/b).

# Bluetooth

Bluetooth – технология беспроводной передачи данных по радиоканалу между различными типами электронных устройств с целью обеспечения взаимодействия. Разработка этой системы была начата в 1998 г. компаниями Ericsson, IBM, Intel, Nokia, Toshiba, а позднее - группой SIG (Special Interest Group), в которую входят многие фирмы, в том числе корпорации Lucent, Microsoft и другие.

При разработке Bluetooth-интерфейса выдвигались следующие требования:

аппаратура должна быть компактной, недорогой и экономичной, т.е. должна быть способна работать при малых значениях потребляемого тока.

# Методы передачи

Система Bluetooth работает в диапазоне 2.4 - 2.48 ГГц (диапазон ISM – Industry, Science, Medicine - промышленный, научный, медицинский) и предназначена для передачи на дальность от 10 до 100 метров голоса или данных.

Передача голоса возможна по трем каналам со скоростью 64 Кбит/с.

Передача данных возможна с помощью либо

- асимметричного метода, обеспечивающего скорость передачи 721 Кбит/с в одном направлении и 57,6 Кбит/с в другом, либо
- симметричного метода, обеспечивающего одинаковую скорость 432,6 Кбит/с в обоих направлениях.

# Передача данных пакетами

В Bluetooth реализована передача данных пакетами с использованием скачкообразной перестройкой частоты 1600 раз в секунду по псевдослучайному закону или шаблону (pattern), составленному из 79 подчастот (принцип FHSS – Frequency-Hopping Spread Spectrum).

Настройка на один шаблон позволяет использующим Bluetooth устройствам осуществлять обмен данными, в то время как другие устройства будут воспринимать передаваемую информацию как шум.


# Информационная безопасность

Информационная безопасность системы беспроводной передачи данных Bluetooth базируется на использовании:

- частотных шаблонов и необходимости синхронизации процессов приема и передачи данных,
- возможности реализации односторонней или двусторонней аутентификации,
- шифрования передаваемых данных.

Длина ключа шифрования может варьироваться от 8 до 128 бит, что дает возможность регулировать криптостойкость используемого алгоритма шифрования.

Система Bluetooth позволяет объединять в одну беспроводную пикосеть (piconet) от двух до восьми различных электронных устройств, таких как, например, сотовый телефон, беспроводная гарнитура, ноутбук, цифровой фотоаппарат, принтер, клавиатура и др., но общее количество объединяемых устройств (как результат объединения пикосетей) может достигать 71.




По сравнению с интерфейсом беспроводной связи IEEE 802.11, работающим в том же диапазоне частот – 2,4 ГГц, Bluetooth-система обеспечивает

- меньшую скорость передачи информации
- (721 Кбит/с против 11 Мбит/с в стандарте IEEE 802.11b),
- меньшую дальность и
- меньшее число объединяемых в сеть устройств

(максимально до 71 устройства у Bluetooth, 128 на одну сеть у IEEE 802.11).


Но система Bluetooth может по трем каналам передавать голосовую информацию, а главное, более дешева (в десятки раз), малогабаритна и экономична.





Bluetooth способна осуществлять передачу данных даже при наличии препятствий и не только по принципу «точка–точка», но и по принципу «точка–много точек», что в положительную сторону отличает Bluetooth от технологии беспроводной инфракрасной связи IrDa, которая обеспечивает связь лишь в зоне прямой видимости и только по принципу «точка–точка».


Хотя в Bluetooth предусмотрена криптографическая защита конфиденциальности передаваемых данных, а также процедура аутентификации, предназначенная для защиты от несанкционированного доступа к системе, нарушения информационной безопасности устройств, снабженных Bluetooth, являются реальностью.



Угрозы информационной безопасности сотовых систем связи, реализуемые через Bluetooth-интерфейс:

- 1) проникновение в абонентский аппарат мобильных вирусов и связанные с этим угрозы потери конфиденциальности передаваемой информации, а также целостности, доступности и конфиденциальности информации, хранящейся в абонентском аппарате;
- 2) перехват информации, передаваемой по радиоканалу системы Bluetooth;
- 3) дистанционный перехват управления абонентским аппаратом, позволяющий злоумышленнику осуществлять звонки и/или отсылку SMS и MMS сообщений за счет законного владельца аппарата, изменять настройки аппарата, считывать информацию, хранящуюся в памяти аппарата.

Важной задачей является защита конфиденциальности информации, хранящейся в памяти мобильных устройств.



Виды атак на устройства с поддержкой Bluetooth могут быть классифицированы следующим образом.

1. Bluejacking - атака, использующая способность устройств Bluetooth обнаруживать другие близко расположенные Bluetooth-устройства и посылать на них сообщения, которые отображаются на дисплее атакуемого устройства. Bluejacking может использоваться для рассылки спама и распространения вредоносных программ, а также в хулиганских целях.

2. Bluesnarfing – атака, основанная на несанкционированном соединении с другим Bluetooth-устройством без уведомления его владельца с целью получения доступа к данным, записанным в памяти аппарата, таким как, например, телефонные номера, записи в адресной книге и ежедневнике. На практике доказана возможность осуществления таких соединений, несмотря на использование так называемого «невидимого» режима работы атакуемого Bluetooth-устройства.



Виды атак на устройства с поддержкой Bluetooth.

3. Bluebug – атака, направленная на установление последовательного соединения с атакуемым Bluetooth-устройством с тем, чтобы осуществлять контроль за его службами обмена данными, посылать и получать сообщения, а также производить телефонные звонки с атакованного аппарата.

# Bluetooth (IEEE 802.15.1)

Bluetooth – это беспроводная технология, являющаяся стандартом, который обеспечивает беспроводную передачу данных на небольших расстояниях между мобильными персональными компьютерами, мобильными телефонами и другими устройствами в режиме реального времени как цифровых данных, так и звуковых сигналов.

Стандарт IEEE 802.15.1 базируется на спецификациях Bluetooth v. 1.x. Bluetooth - это недорогой радиointерфейс с низким уровнем энергопотребления (порядком 1 mW).

Сначала дальность действия Bluetooth была в радиусе 10 м, позже увеличилось до 100 м.

Для работы Bluetooth используется так называемый нижний 2,45 ГГц диапазон ISM (industrial, scientific, medical), который предназначен для работы промышленных, научных и медицинских приборов.

# Типы соединения

Протокол Bluetooth поддерживает соединения типа

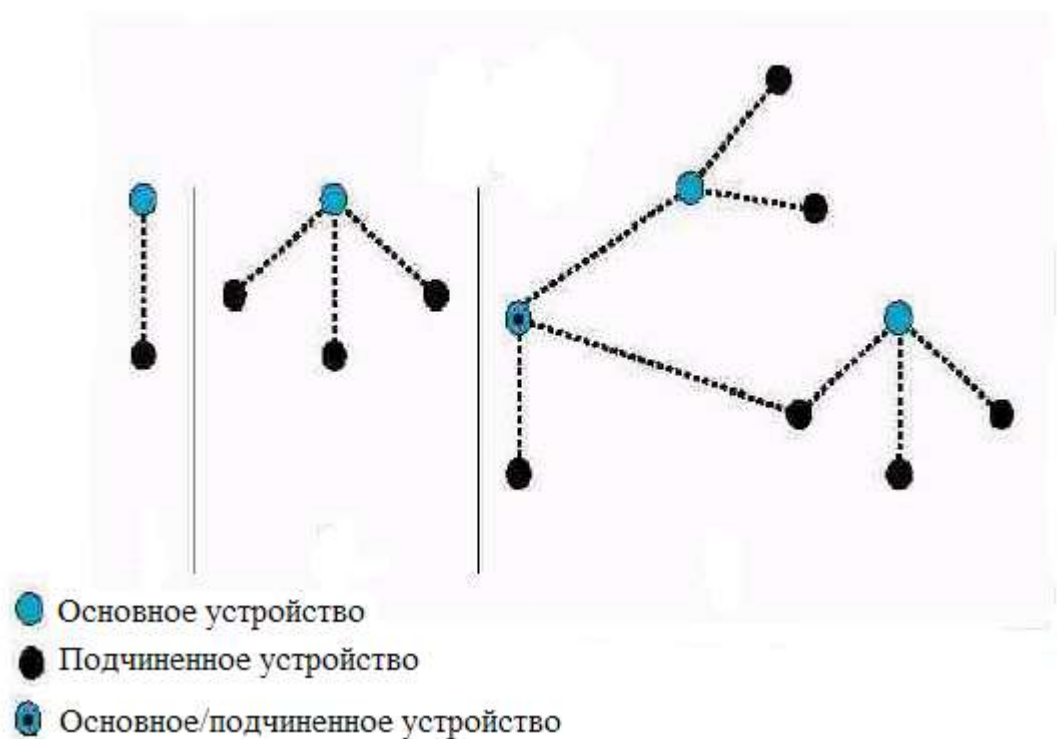
- точка-точка,
- также и соединения типа точка-многоточка.

Два устройства или более, которые используют один и тот же канал образуют пикосеть (piconet). Одно из устройств работает как основное (мастер) (master), а остальные – как подчиненные (slave) устройства. В одной пикосети может быть до восьми активных подчиненных устройств, при этом остальные подчиненные устройства находятся в состоянии "парковки", которые синхронизированны с основным устройством. На расстоянии 10 м может существовать до 10 пикосетей.

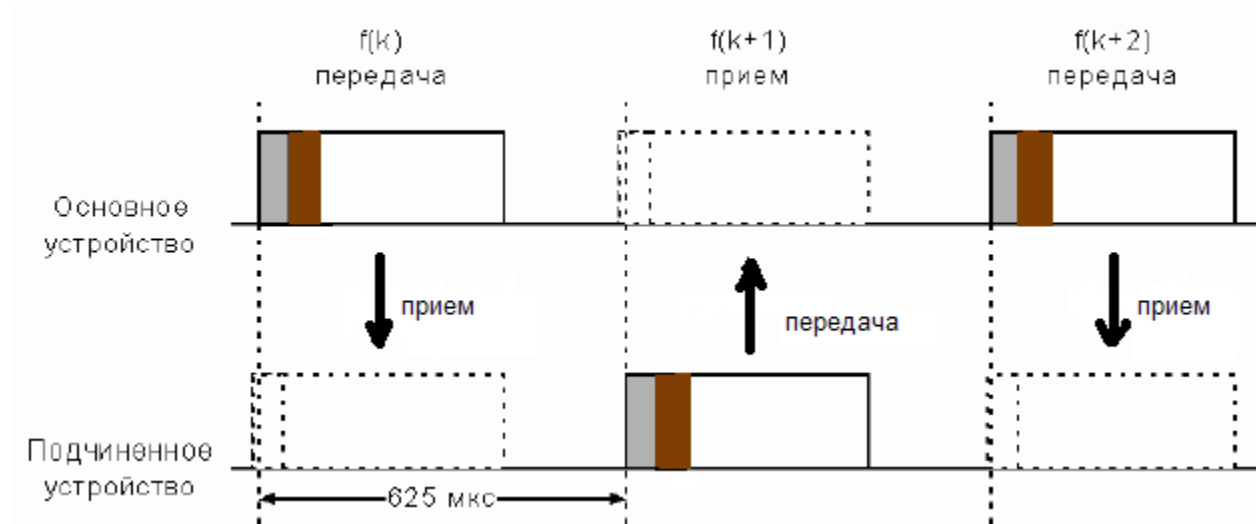
“Распределенную сеть” (scatternet) образуют взаимодействующие пикосети.

В каждой пикосети действует только одно основное устройство, но подчиненные устройства могут входить в различные пикосети. Помимо этого, основное устройство одной пикосети может быть подчиненным устройством в другой.

# Различные виды пикосети Bluetooth



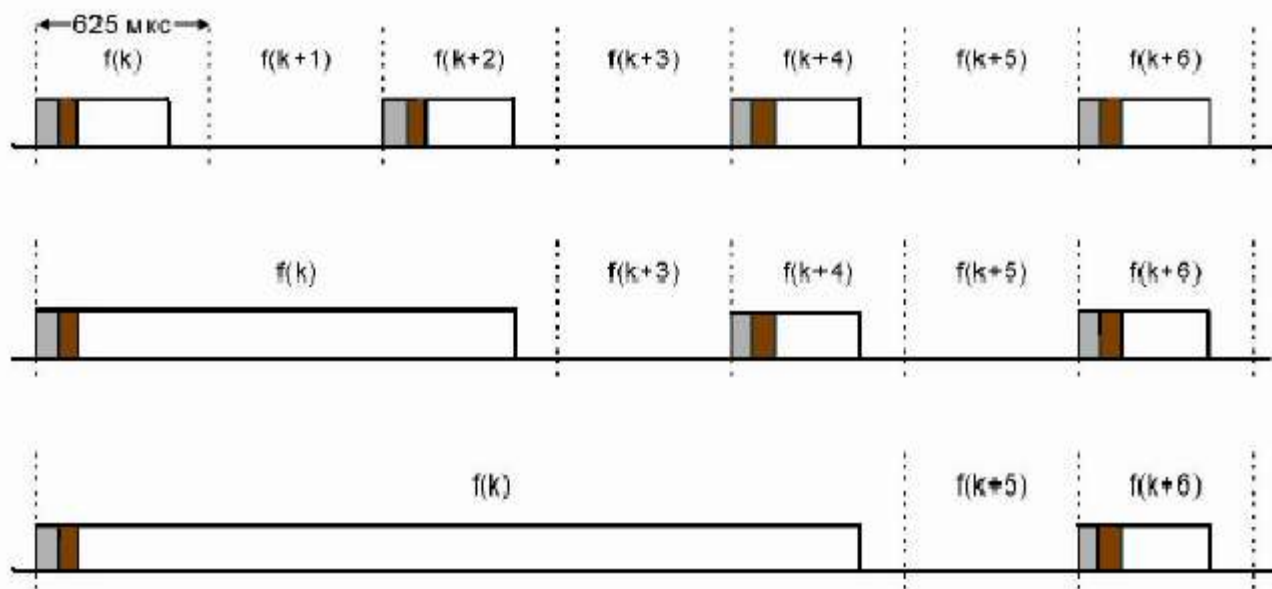
# Передача данных Bluetooth



В стандарте Bluetooth предусмотрена дуплексная передача на основе разделения времени (Time Division Duplexing - TDD).

Основное устройство передает пакеты в нечетные временные сегменты, а подчиненное устройство – в четные.





Пакеты в зависимости от длины могут занимать до пяти временных сегментов. При этом частота канала не меняется до окончания передачи пакета.




Протокол Bluetooth может поддерживать

- асинхронный канал данных,
- до трех синхронных (с постоянной скоростью) голосовых каналов
- или канал с одновременной асинхронной передачей данных и синхронной передачей голоса.


Скорость каждого голосового канала – 64 Кбит/с в каждом направлении,

асинхронного в асимметричном режиме – до 723,2 Кбит/с в прямом и 57,6 кбит/с в обратном направлениях

или до 433,9 Кбит/с в каждом направлении в симметричном режиме.



Синхронное соединение (SCO – Synchronous Connection Oriented) возможно только в режиме точка-точка. Такой вид связи применяется для передачи информации, чувствительной к задержкам – например, голоса. Основное устройство поддерживает до трех синхронных соединений, подчиненное – до трех синхронных соединений с одним основным устройством или до двух – с разными основными устройствами. При синхронном соединении основное устройство резервирует временные сегменты, следующие через так называемые SCO-интервалы. Даже если пакет принят с ошибкой, повторно при синхронном соединении он не передается.



При асинхронной связи (ACL – Asynchronous Connection Less) используются временные сегменты, не зарезервированные для синхронного соединения.

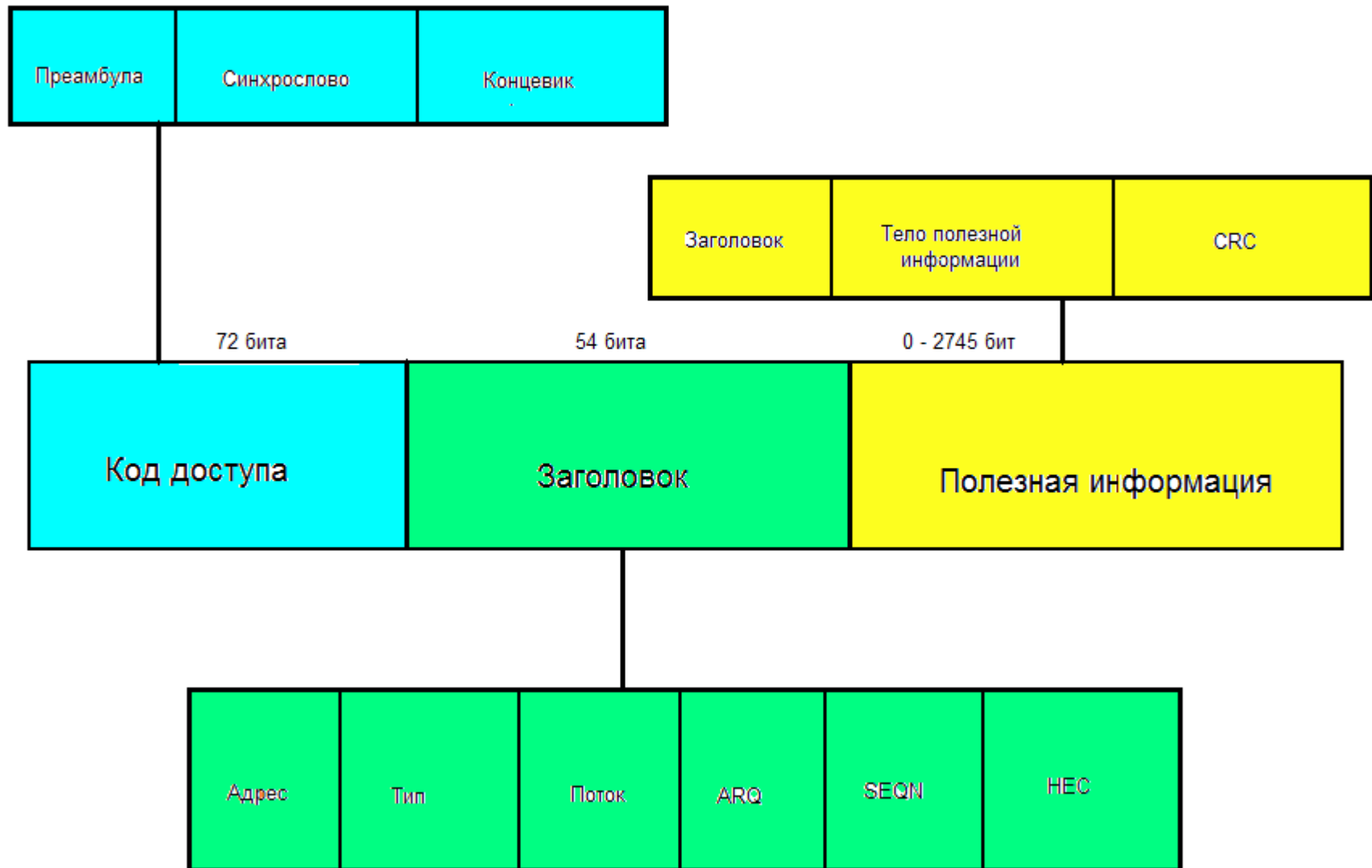
Асинхронное соединение возможно между основным и всеми активными подчиненными устройствами в пикосети (точка - многоточка).


Основное и подчиненное устройства могут поддерживать только одно асинхронное соединение.

Поскольку в пикосети может быть несколько подчиненных устройств, конкретное подчиненное устройство отправляет пакет основному, только если в предыдущем временном интервале на его адрес пришел пакет от основного устройства. Если в адресном поле ACL-пакета адрес не указан, пакет считается “широковещательным” – его могут принимать все устройства.

Асинхронное соединение позволяет повторно передавать пакеты, принятые с ошибками.

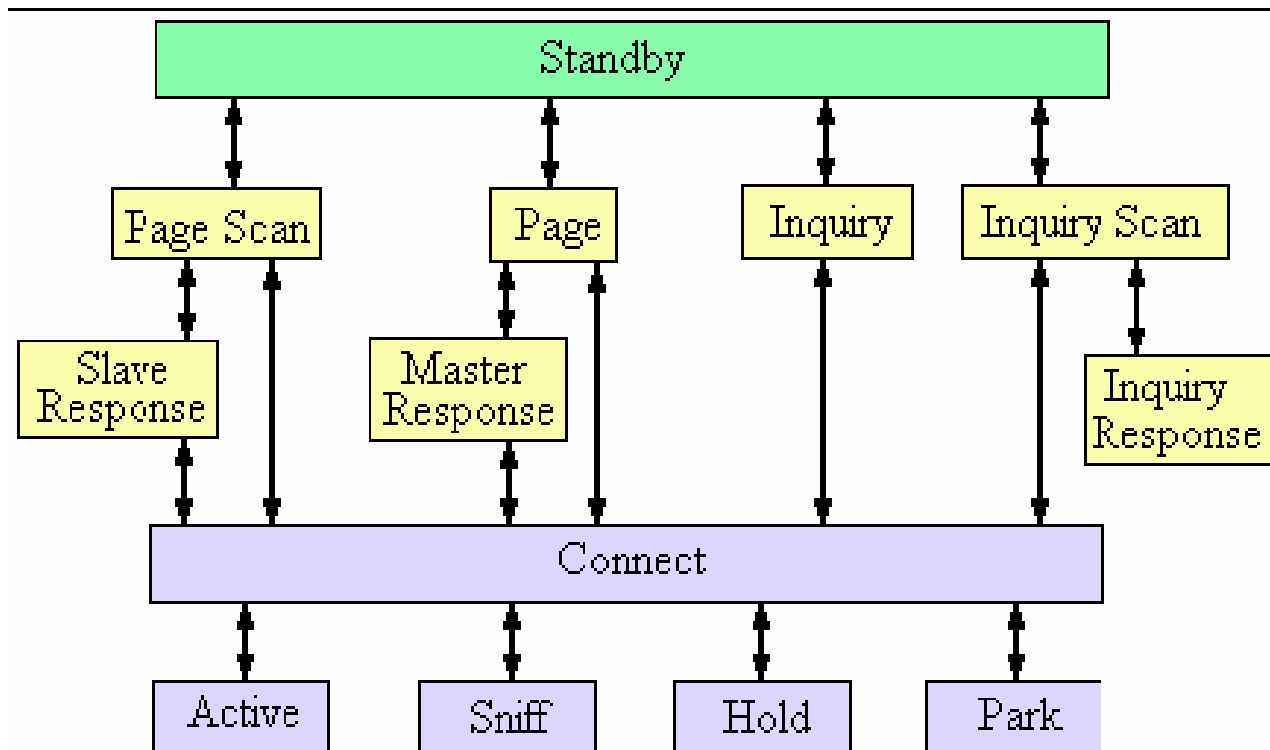
# Структура пакета





Стандартный пакет Bluetooth содержит код доступа длиной 72 бита, 54-битный заголовок и информационное поле длиной не более 2745 бит. Пакеты могут быть различных типов. Так, пакет может состоять только из кода доступа (в этом случае его длина равна 68 битам) или кода доступа и заголовка.

# Работа Bluetooth



Есть два основных состояния для устройств Bluetooth: Соединение (Connection) и Режим ожидания (Standby). Предусмотрено семь субсостояний, которые используются для добавления клиента или подключения к пикосети: page, page scan, inquiry, inquiry scan, master response, slave response и inquiry response.

# Протоколы Bluetooth.

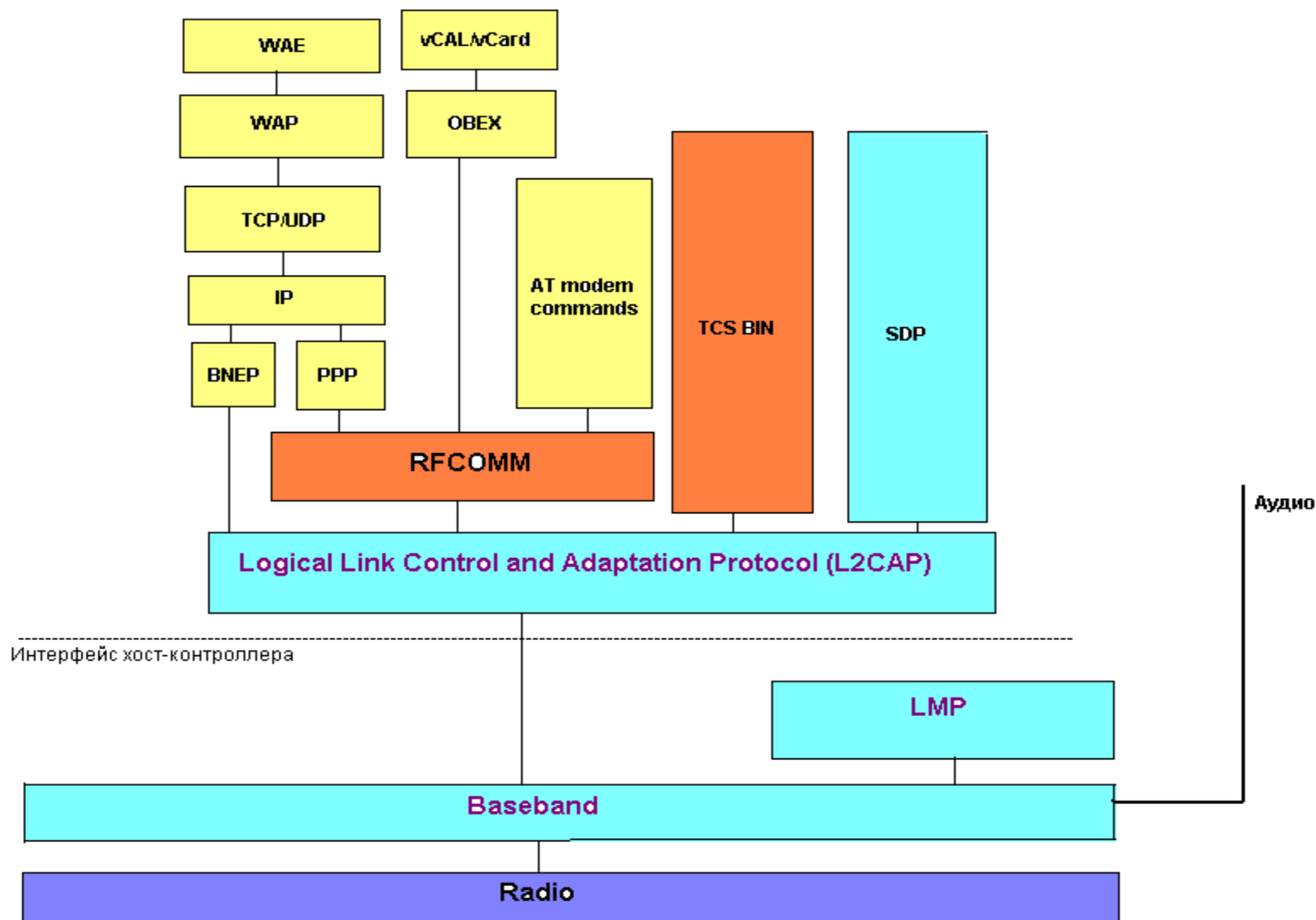
При работе устройств Bluetooth используются специфические протоколы для Bluetooth и общие, которые используются в различных телекоммуникационных системах. Все они образуют стек протоколов Bluetooth.

Все эти протоколы можно разделить на 4 слоя:

1. Корневые протоколы.
2. Протокол замены кабеля
3. Протокол управления телефонией
4. Заимствованные протоколы



# Стек протоколов Bluetooth



# Профили Bluetooth


Специальная рабочая группа Bluetooth SIG определила различные модели использования, каждая из которых сопровождается профилем.

Профили определяют протоколы и функции, которые поддерживают определенные модели использования. Если устройства от различных производителей соответствуют одному профилю, определенному в спецификации Bluetooth, они смогут взаимодействовать.

Четыре общих профиля применяются для различных моделей использования. Это

- профиль общего доступа,
- профиль последовательного порта,
- профиль приложения обнаружения услуг и
- профиль общего обмена объектами.

Остальные профили применяются непосредственно для определенных моделей использования.



Профиль общего доступа (Generic Access Profile)

Профиль приложения обнаружения услуг (Service Discovery Application Profile)

Профиль беспроводной телефонии (Cordless Telephony Profile)

Профиль внутренней связи (Intercom Profile)

Профиль последовательного порта (Serial Port Profile)

Профиль гарнитуры (Headset Profile)

Профиль коммутируемого выхода на сеть (Dial-up Networking Profile)

Профиль факса (Fax Profile)

Профиль доступа к локальной сети (LAN Access Profile)

Профиль общего обмена объектами (Generic Object Exchange Profile)

Профиль помещения объекта в стек (Object Push Profile)

Профиль передачи файла (File Transfer Profile)

Профиль синхронизации (Synchronization Profile)

# Основные конкуренты

## IrDA

IrDA (Infrared Data Association) – это стандарт инфракрасного интерфейса, который составляет альтернативу для Bluetooth в области беспроводных устройств. Преимуществами IrDA являются:

- дешевле, чем Bluetooth
- скорость передачи данных выше, чем у Bluetooth. У IrDA – 4 Мбит/с, а у Bluetooth – 1 Мбит/с


К недостаткам можно отнести:

- расстояние, на которое можно передать данные относительно мало – 1м
- ограниченное только до соединения точка-точка
- порты устройств должны находиться в прямой видимости друг от друга
- не все устройства поддерживают стандарт (несовместимость между некоторыми продуктами)

# Основные конкуренты

## **UWB (Ultra-Wideband Radio)**

Это сверхширокополосные технологии радиосвязи, которые работают по тому же принципу, что и радары: посылаются короткие импульсы в большой частотной области. К преимуществам можно отнести также отнести малое энергопотребление и невысокую стоимость



IEEE 802.15.4a/b — стандарт так называемой технологии UWB (Ultra Wideband), основанной на передаче множества закодированных импульсов негармонической формы очень малой мощности (0,05 мВт) и малой длительности в широком диапазоне частот (от 3,1 до 10,6 ГГц). Передача данных на расстояниях до 5 метров осуществляется со скоростью от 400 до 500 Мбит/с. Тип модуляции: OFDM, QPSK.


При помощи UWB-технологии можно создавать специальные сети, в которых несколько сверхширокополосных устройств смогут поддерживать связь между любыми узлами. Короткие сигналы UWB сравнительно устойчивы к многолучевому затуханию, возникающему при отражении волны от стен, потолка, зданий, транспортных средств. Высокоскоростные UWB-устройства хорошо подходят для работы с видеопотоками и приложениями, требующими быстрой пересылки данных. Низкоскоростное UWB-оборудование может применяться для отслеживания местоположения на местности владельцев беспроводных устройств и различных объектов.

# ZigBee

Стандарт IEEE 802.15.4 [IEEE ] является самым новым в серии беспроводных (принят в октябре 2003 г.). На его основе ZigBee Alliance ([www.zigbee.org](http://www.zigbee.org)) разработал спецификацию протоколов сетевого и прикладного уровня, которые анонсировал в декабре 2004 года под названием "ZigBee" [ZigBee].

Прикладные профили ориентированы, в частности, на автоматизацию зданий, промышленный мониторинг, вентиляцию и кондиционирование, работу с датчиками. Спецификация ZigBee описывает построение сети, вопросы безопасности, прикладное программное обеспечение.

Основной областью применения ZigBee/IEEE 802.15.4 является передача информации от движущихся и вращающихся частей механизмов (конвейеров, роботов), промышленные системы управления и мониторинга, беспроводные сети датчиков, отслеживание маршрутов движения и местоположения имущества и инвентаря, "интеллектуальное" сельское хозяйство, системы охраны.



В отличие от других беспроводных технологий, где ставится задача обеспечить высокую скорость передачи, большую дальность или высокое качество обслуживания, ZigBee/IEEE 802.15.4 создавался изначально по критериям малой дальности действия, низкой цены, низкой потребляемой мощности, низкой скорости передачи и малых габаритов. Эти свойства идеально соответствуют требованиям к большинству промышленных датчиков. Поэтому ZigBee часто отождествляют с промышленными беспроводными сенсорными сетями WSN (Wireless Sensor Network) [Нас А., Shen, Low, Gutierrez, Jiang, Bonivento]. Устройства ZigBee используются в применениях, где Bluetooth оказывается слишком дорогим, и не требуется высокая скорость передачи.

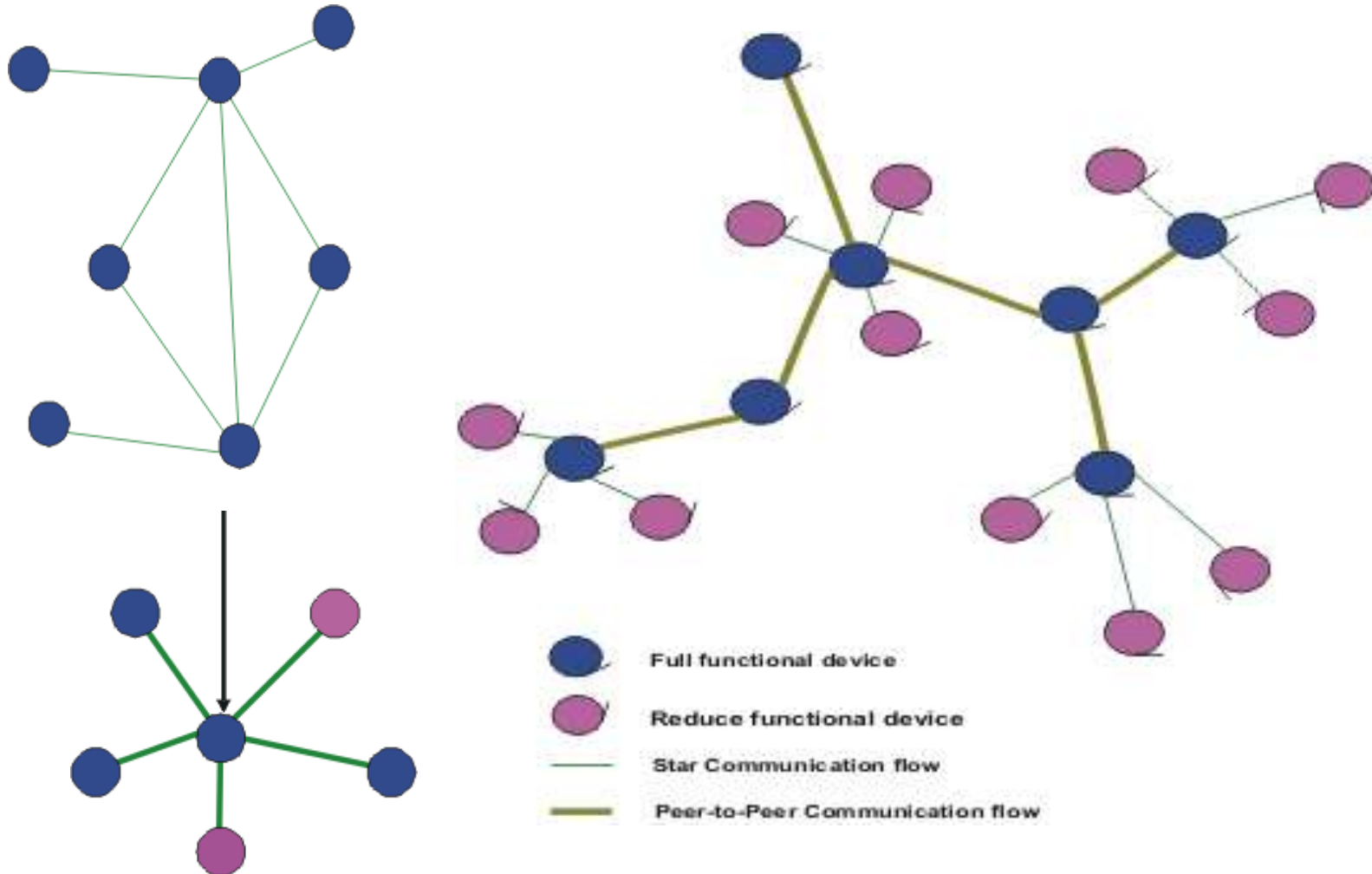
ZigBee, как и Bluetooth, использует нелицензируемый [Решение] диапазон 2,4 ГГц. Стандарт предусматривает также использование частот 868 МГц в Европе и 915 МГц в США. Максимальная скорость передачи составляет 250 кбит/с в диапазоне 2,4 ГГц. Диапазон 2,4 ГГц разделен на 11...26 каналов шириной по 5 МГц каждый.

Основная особенность технологии ZigBee заключается в том, что она при относительно невысоком энергопотреблении поддерживает не только простые топологии беспроводной связи («точка-точка» и «звезда»), но и сложные беспроводные сети с ячеистой топологией с ретрансляцией и маршрутизацией сообщений.



# Примеры топологий сети Zigbee

P2P



Звезда

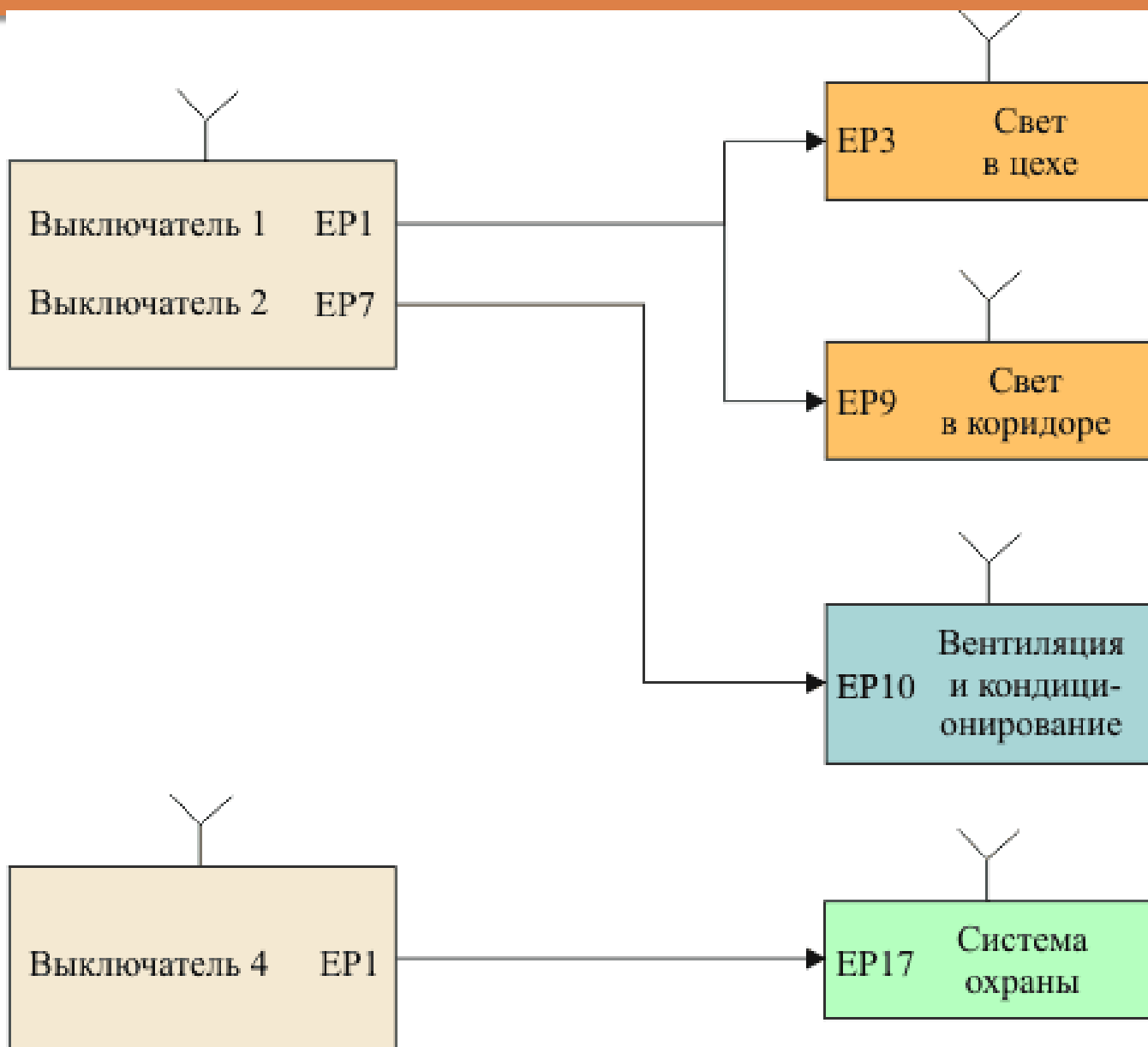
# Устройства ZigBee

Существуют три различных типа устройств ZigBee.

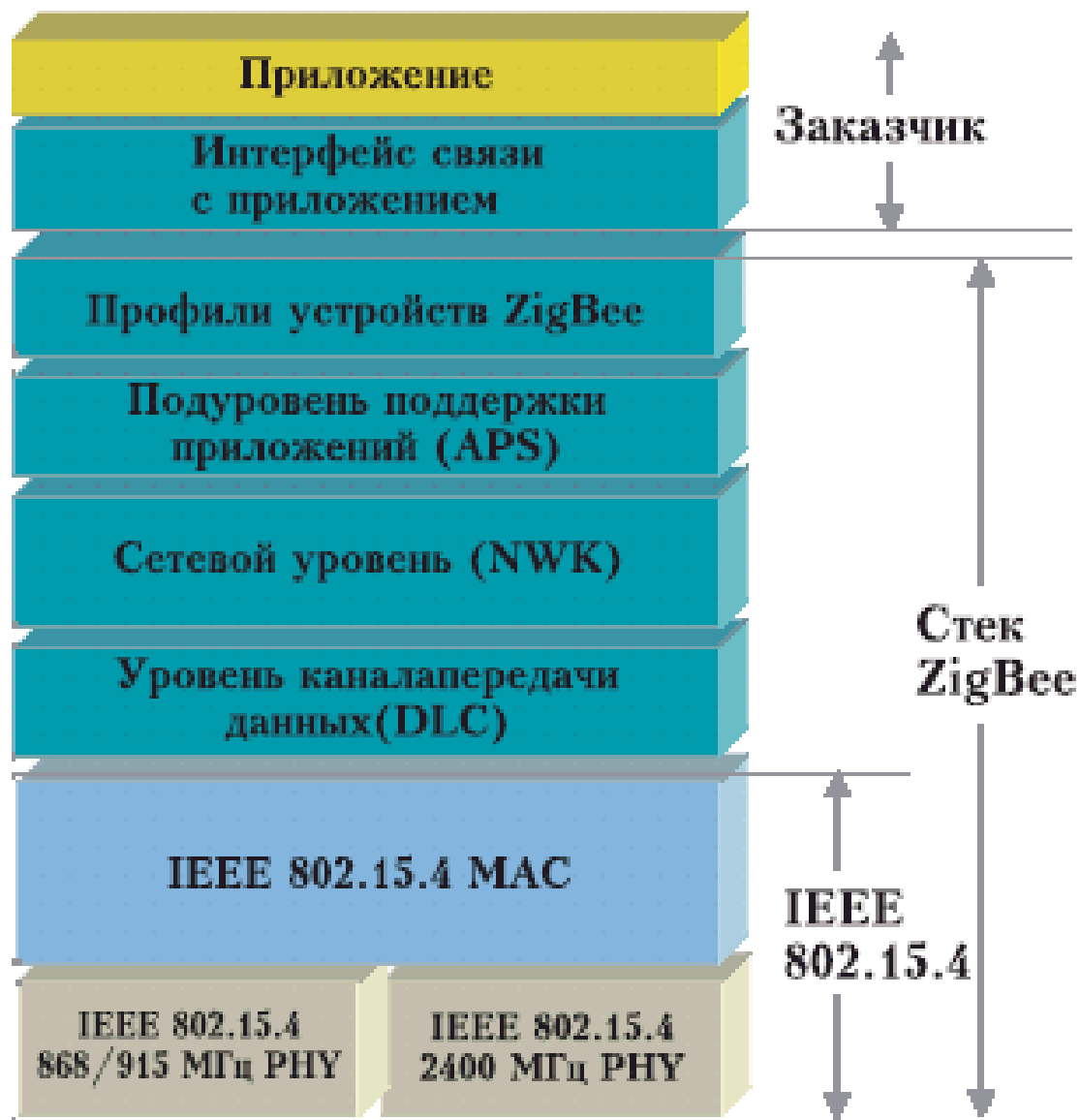
Координатор ZigBee (ZC) — наиболее ответственное устройство, формирует пути древа сети и может связываться с другими сетями. В каждой сети есть один координатор ZigBee. Он и запускает сеть от начала. Он может хранить информацию о сети, включая хранилище секретных паролей производства компании Trust Centre.


Маршрутизатор ZigBee (ZR) — Маршрутизатор может выступать в качестве промежуточного маршрутизатора, передавая данные с других устройств. Он также может запускать функцию приложения.

Конечное устройство ZigBee (ZED) — его функциональная нагруженность позволяет ему обмениваться информацией с материнским узлом (или координатором, или с маршрутизатором), он не может передавать данные с других устройств. Такое отношение позволяет узлу львиную часть времени пребывать в спящем состоянии, что позволяет экономить энергоресурс батарей. ZED требует минимальное количество памяти, и поэтому может быть дешевле в производстве, чем ZR или ZC.



# Стек сетевых уровней Zigbee





Прикладной - Передача сообщений, обнаружение устройств, определение роли устройств

Сетевой - Безопасность, маршрутизация

Канальный (передачи данных) – управляет доступом к радиоканалу

Физический - Радиоканал 2,4 ГГц



## HomeRF

Эта технология разработана для обмена данными между компьютерами и периферийными устройствами в небольших офисах или домах (в радиусе 50 м). Она работает на таких же частотах, как и Bluetooth. С Bluetooth имеется довольно много схожего - цена модулей, потребляемая устройствами мощность. Отличает же их максимальное число узлов в сети - 8 у Bluetooth, 127 у HomeRF, а также скорость изменения частоты тоже разная - 50 раз в секунду у HomeRF, 1600 раз в секунду у Bluetooth.



## IEEE 802.11b

Приложения, которые поддерживают этот стандарт, являются довольно сильными конкурентами для Bluetooth. Некоторые из них также используют скачкообразное изменение частоты при передаче данных. Отличиями являются следующее:

- более высокая скорость – до 11 Мбит/с
- больше радиус передачи данных – 90 м
- больше количество участников – до 127

К минусам можно отнести:

- у Bluetooth меньше потребляемая мощность
- по размерам устройства Bluetooth меньше
- по цене устройства Bluetooth дешевле
- скорость смены частотных каналов у Bluetooth выше: у Bluetooth – 1600 раз в секунду, у приложений, поддерживающих IEEE 802.11b – 2,5 раз в секунду.

# Сравнение стандартов семейства IEEE 802.15

Стандарт	802.15.4 ZigBee			802.15.1 Bluetooth	802.15.3 High Rate WPAN	802.15.4a UWB
Приложения	Мониторинг, управление, сети датчиков, домашняя/промышленная автоматика			Голос, данные, замена кабелей	Потоковое мультимедиа, замена кабелей аудио/ видео систем	
Преимущества	Цена, энергосбережение, размеры сети, выбор частотных диапазонов			Цена, энергосбережение, передача голоса, скачок частот	Высокая скорость, энергосбережение	
Частота	868МГц	915 МГц	2.4 ГГц	2.4 ГГц	2.4 ГГц	3.1 – 10.6 ГГц
Максимальная скорость	20 кбит/с	40 кбит/с	250 кбит/с	1 Мбит/с	22 Мбит/с (доп. 11, 33,44,55 Мбит/с)	110 Мбит/с (10 м), 200 Мбит/с (4м) (доп. 480 Мбит/с)





Стандарт	802.15.4 ZigBee		802.15.1 Bluetooth	802.15.3 High Rate WPAN	802.15.4a UWB
Выходная мощность, ном.	0 dBm (1 мВт)		0 dBm (класс 3) 4 dBm(класс 2) 20 dBm(класс 1)	0 dBm	<100 мВт (110 Мбит/с), <250мВт (200 Мбит/с)
Дальность	10-100 м		10 м (класс 3) 100 м (класс 1)	5-50м	10 м (110 Мбит/с), 4 м (200 Мбит/с)
Чувствительнос	-92 dBm	-85 dBm	-75 dBm	-75 dBm	-
Размер стека	4-32 Кбайт		Более 250 Кбайт	-	
Срок службы батарее	100-1000+дней		1-7 дней	Теоретически более 1000 дней	
Размер сети	65536 (16-битные адреса),  2 <sup>64</sup> (64-битные адреса)		Мастер +7	До 127/хост	