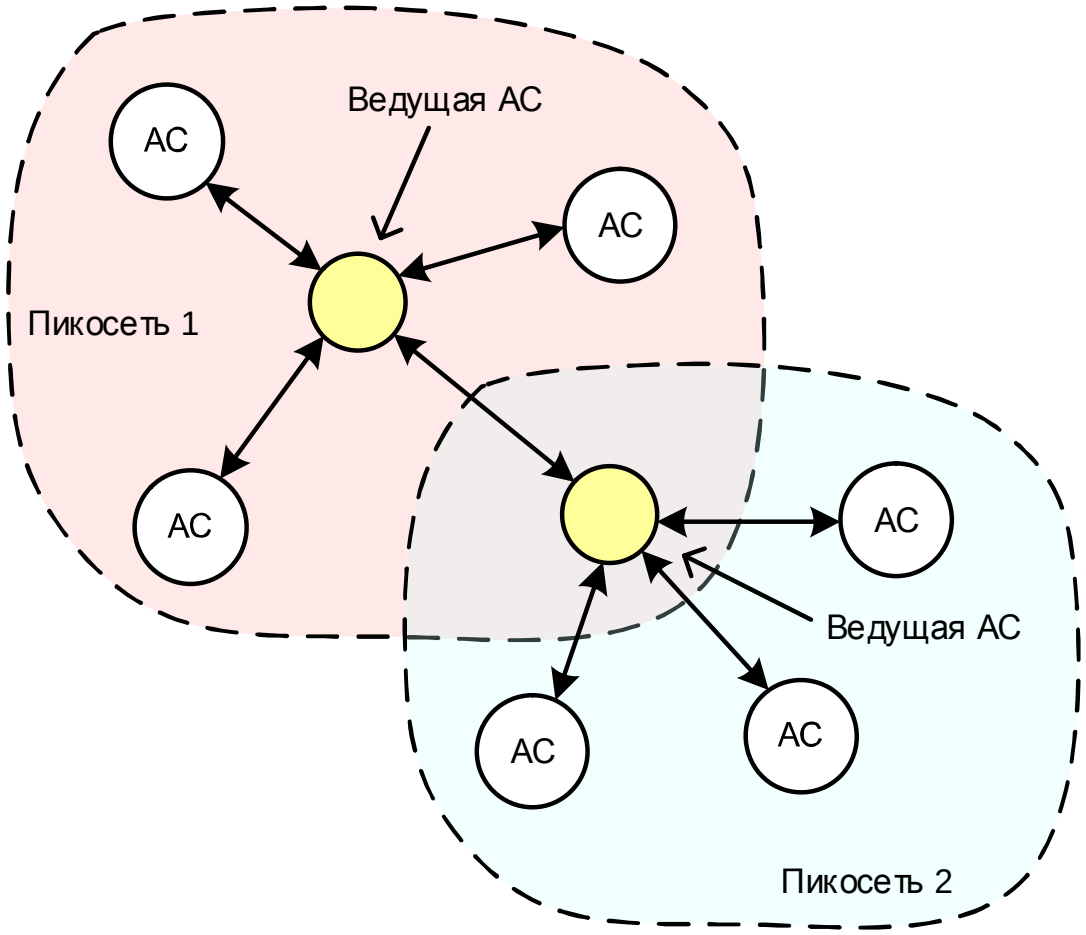
# Топология сети Bluetooth (IEEE 802.15.1)



# История создания группы Bluetooth SIG

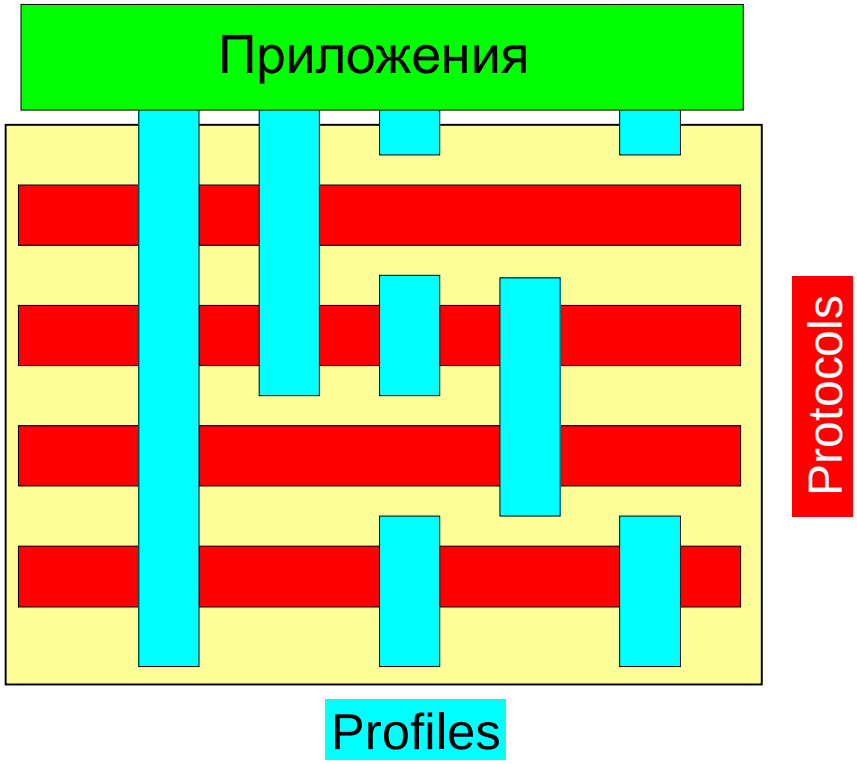
Февраль 1998: Создание группы Bluetooth SIG компаниями Ericsson, IBM, Intel, Nokia, Toshiba
Июль 1999: публикация 1.0a спецификации (более 1500 страниц)
Декабрь 1999: ver. 1.0b
Декабрь 1999: К группе учредителей Bluetooth SIG присоединились компании 3Com, Lucent, Microsoft, Motorola
Март 2001: ver. 1.1
Август 2001: Более 2500 компаний, использующих BT в своих разработках

Спецификации Bluetooth представляют собой наборы документов общим объемом более 1500 страниц. Базовая часть спецификации отражает построение ядра *(Core)* Bluetooth - физического и канального уровня, образующих транспортную платформу доставки сообщений.

Вторая часть документов отражает реализацию *Профилей (Profiles)* - как набора правил взаимодействия с приложением и высокоуровнего протокола доставки сообщений поверх транспортной платформы Bluetooth (L2CAP протокол), реализующих определенные типа услуг.

**WEB ресурс группы Bluetooth SIG -** https://www.bluetooth.com

# Концепция предоставления ТК услуг ВТ устройством



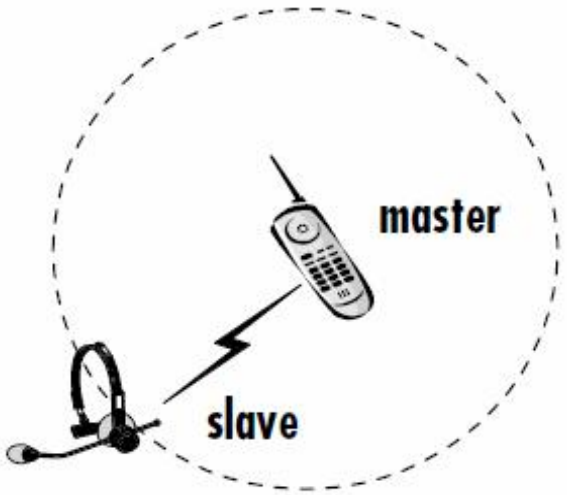

1. Приложениям требуется доставка данных
2. У каждого приложения могут быть свои требования к условиям доставки данных
3. Вид трафика может быть различным:
   -непрерывным (реальный масштаб времени), требующий резервирование пропускной способности КС;
   - пульсирующим (эпизодическим), для передачи данные не в реальном масштабе времени;
   - комбинированным: приложение может генерировать два вида трафика

Профиль BT – перечень правил конфигурации служб и протоколов канального и физического уровней, подходящий для реализации конкретной ТК услуги. Приложение запрашивает у терминала ВТ конкретную услугу, а ВТ актуализирует определенный профиль для реализации запрошенной ТК услуги.

# Профили Bluetooth (ver. 1.2)

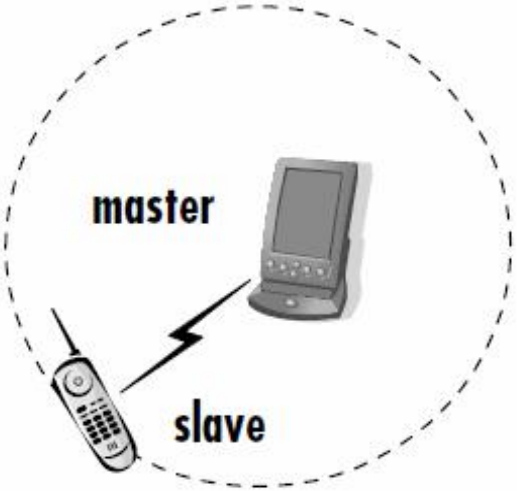
В соответствии со спецификацией Bluetooth (v1.1) определяются 25 поддерживаемых типов приложений (профилей), из которых 13 являются **основными**, а 12 - дополнительными. По существу профили являются регламентациями прикладного уровня, в соответствии с которыми осуществляется конфигурация протоколов и модулей канального и физического уровня BT

**Однопрофильное BT устройство**

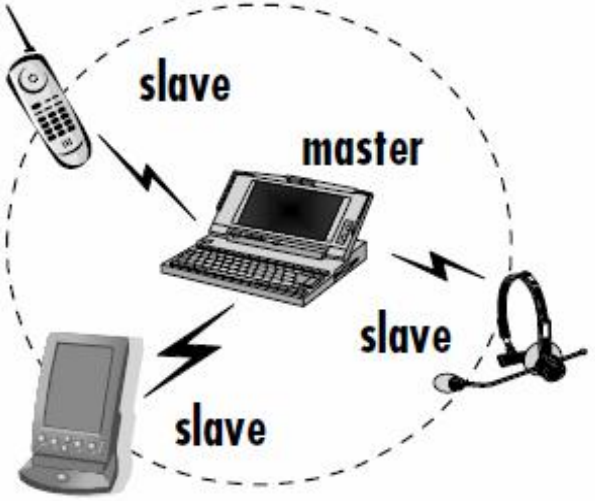



Запрограммированное персональное соединение только с одним устройством

**Многопрофильные BT устройства и сети**




Соединение "точка-точка" с одним устройством любого типа (Ad Hoc)




Соединение "точка-многоточка": организация пикосети из восьми и менее активных устройств

# Профили Bluetooth (ver. 1.2)

## Основные профили

| | Название | *Описание* |
|---|---|---|
| 1 | **GAP** (*Generic Access Profile*) | ***Профиль общего доступа***. Это основной профиль Bluetooth, отвечающий за поддержание связи между устройствами, выявление других доступных профилей, а также за безопасность. Этот профиль должен быть включен во все устройства Bluetooth, так как в него входят функции, необходимые для работы всех основных протоколов Bluetooth |
| 2 | **SDAP** (*Service Discovery Application Profile*) | ***Протокол определения предлагаемых сервисов***. Дает приложению возможность непосредственно обращаться к ресурсам протокола SDP для того, чтобы определять, какие услуги Bluetooth доступны при работе с удаленным устройством |
| 3 | **CTP** (*Cordless Telephony Profile*) | ***Профиль беспроводной телефонии***. Предназначен для мобильных телефонов с поддержкой Bluetooth. Этот профиль поддерживает процедуру организации телефонного соединения, требующую маршрутизацию по телефонной сети общего пользования (ТФОП). При этом телефонное соединение организуется через точку доступа Bluetooth, которая, в свою очередь, подключена к ТФОП |
| 4 | **GOEP** (*Generic Object Exchange Profile*) | Профиль операций клиент-сервер при работе с объектами (обмен данными). Определяет, каким образом терминал Bluetooth использует протокол OBEX |
| 5 | **LAP** (*LAN Access Profile*) | Протокол связи мобильного ПК со стационарной LAN. Предназначен для создания IP-сетей и позволяет создавать небольшие беспроводные сети, объединяющие персональные компьютеры или смарт-телефоны. Он также используется точками доступа для связи с кабельными сетями ЛВС или Internet |
| 6 | **DNP** (*Dial-up Networking Profile*) | Предназначен для компьютеров, связывающихся с сетью Internet через сотовый телефон. Этот профиль включает в себя профиль последовательного порта и протокол PPP |

## Основные профили

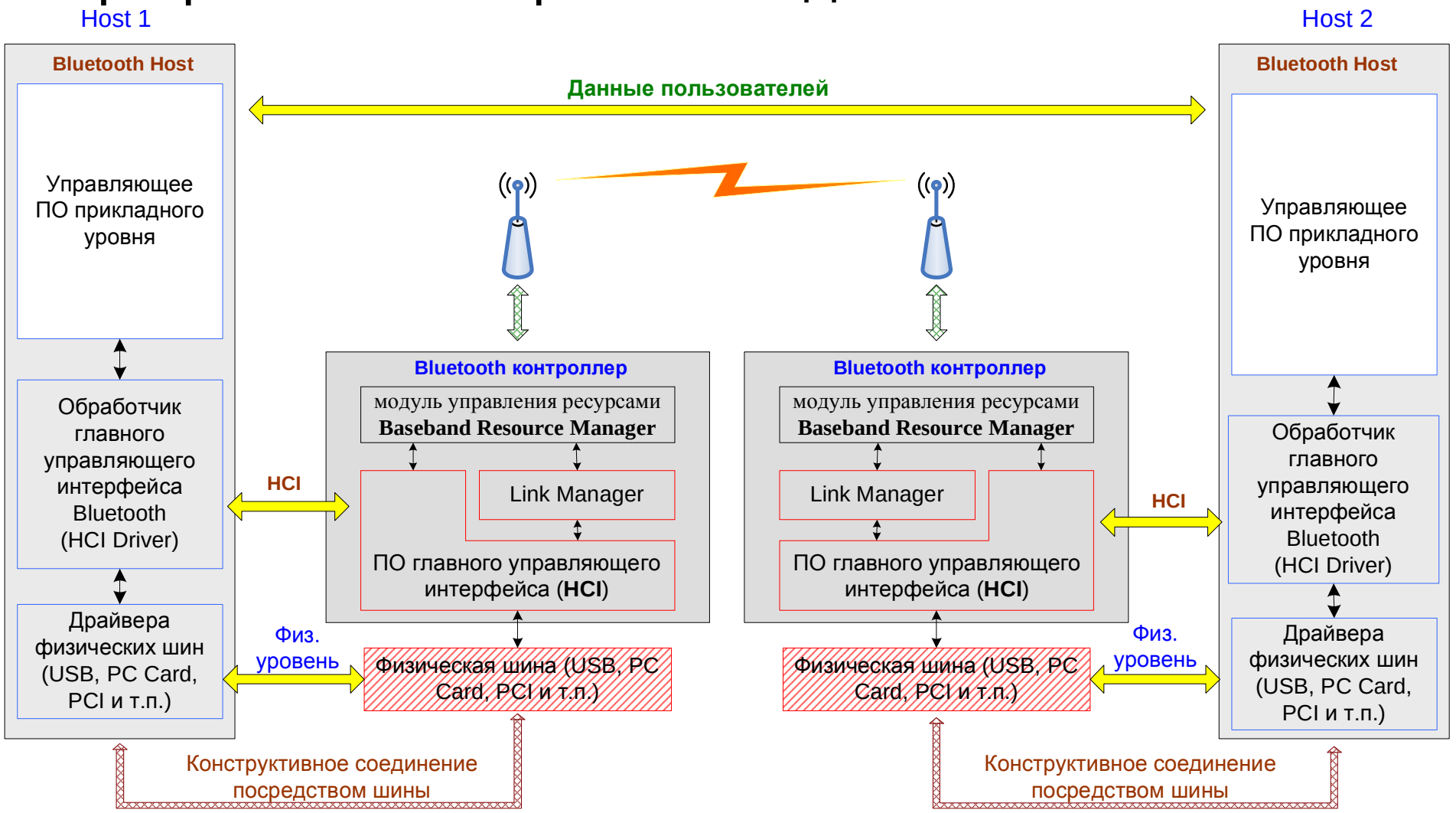
| | | |
|---|---|---|
| 7 | **FP** (*Fax Profile*) | Протокол связи факса с мобильным телефоном. Он позволяет мобильному телефону эмулировать факс-модем при соединении через Bluetooth с ноутбуком, имеющим программное обеспечение поддержки факса |
| 8 | **SPP** (*Serial Port Profile*) | Профиль для работы с последовательным портом. Он обеспечивает эмуляцию интерфейса RS-232 или USB и используется многими профилями более высокого уровня |
| 9 | **IP** (*Intercom Profile*) | Этот профиль, базирующийся на протоколе TCS, обеспечивает двустороннюю голосовую связь между устройствами Bluetooth. Он рассчитан на прямое взаимодействие двух устройств, расположенных в зоне взаимной досягаемости, и не поддерживает звонки, требующие маршрутизации по телефонной сети общего пользования |
| 10 | **HS** (*Headset Profile*) | Протокол связи устройства hands-free с мобильным телефоном. Определяет способ, посредством которого обеспечивается беспроводное соединение устройства с гарнитурой, оснащенной динамиками и микрофоном. Профилем используются команды AT, первоначально разработанные для управления модемами |
| 11 | **OPP** (*Object Push Profile*) | Протокол пересылки простых объектов. Управляет обменом электронными визитками в формате vCard |
| 12 | **FTP** (*File Transfer Profile*) | Профиль, реализующий протокол пересылки файлов. Позволяет устройству получать доступ к данным, хранящимся на другом устройстве, аналогично протоколу ftp |
| 13 | **SP** (*Synchronization Profile*) | Протокол синхронизации PDA с другим ПК. Обеспечивает синхронизацию данных, хранящихся на различных устройствах |

## дополнительные профили

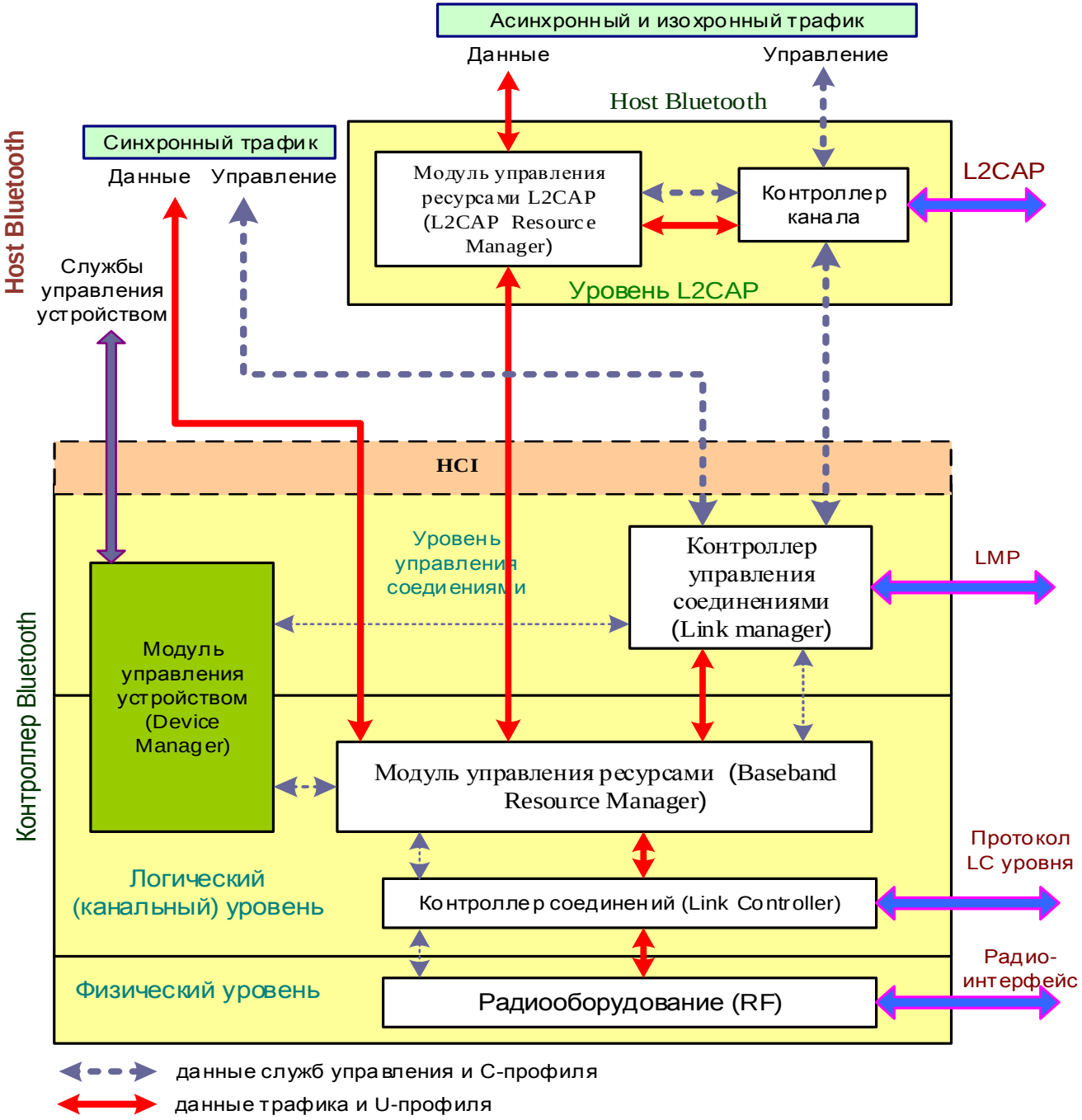
| | | |
|---|---|---|
| 1 | **ESDP** (*Extended Service Discovery Profile*) | Профиль для реализации процедур Plug and Play |
| 2 | **A2DR** (*Advanced Audio Distribution Profile*) | Усовершенствованный профиль рассылки аудио данных |
| 3 | **AVRCD** (*Audio Video Remote Control Profile*) | Аудио-видео профиль удаленного управления |
| 4 | **BIP** (*Basic Imaging Profile*) | Базовый профиль работы с изображением |
| 5 | **BPP** (*Basic Printing Profile*) | Базовый профиль для печати |
| 6 | **CIP** (*Common ISDN Access Profile*) | Общий профиль доступа к ISDN |
| 7 | **GAVDP** (*Generic Audio Video Distribution Profile*) | Общий профиль рассылки аудио и видео данных |
| 8 | **HFR** (*Hands-Free Profile*) | Профиль для ведения переговоров по громкой связи (hands-free) |
| 9 | **HCRP** (*Hardcopy Cable Replacement Profile*) | Протокол замены приборного связного кабеля |
| 10 | **HID** (*Human Interface Device Profile*) | Профиль для реализации интерфейса с человеком |
| 11 | **PAN** (*Personal Area Networking*) | Протокол формирования персональной сети |
| 12 | **SAP** (*SIM Access Profile*) | Протокол доступа к SIM |

# Иерархическая модель Bluetooth (BT)

# Программно-аппаратная модель системы Bluetooth



# Архитектура системы стандарта Bluetooth

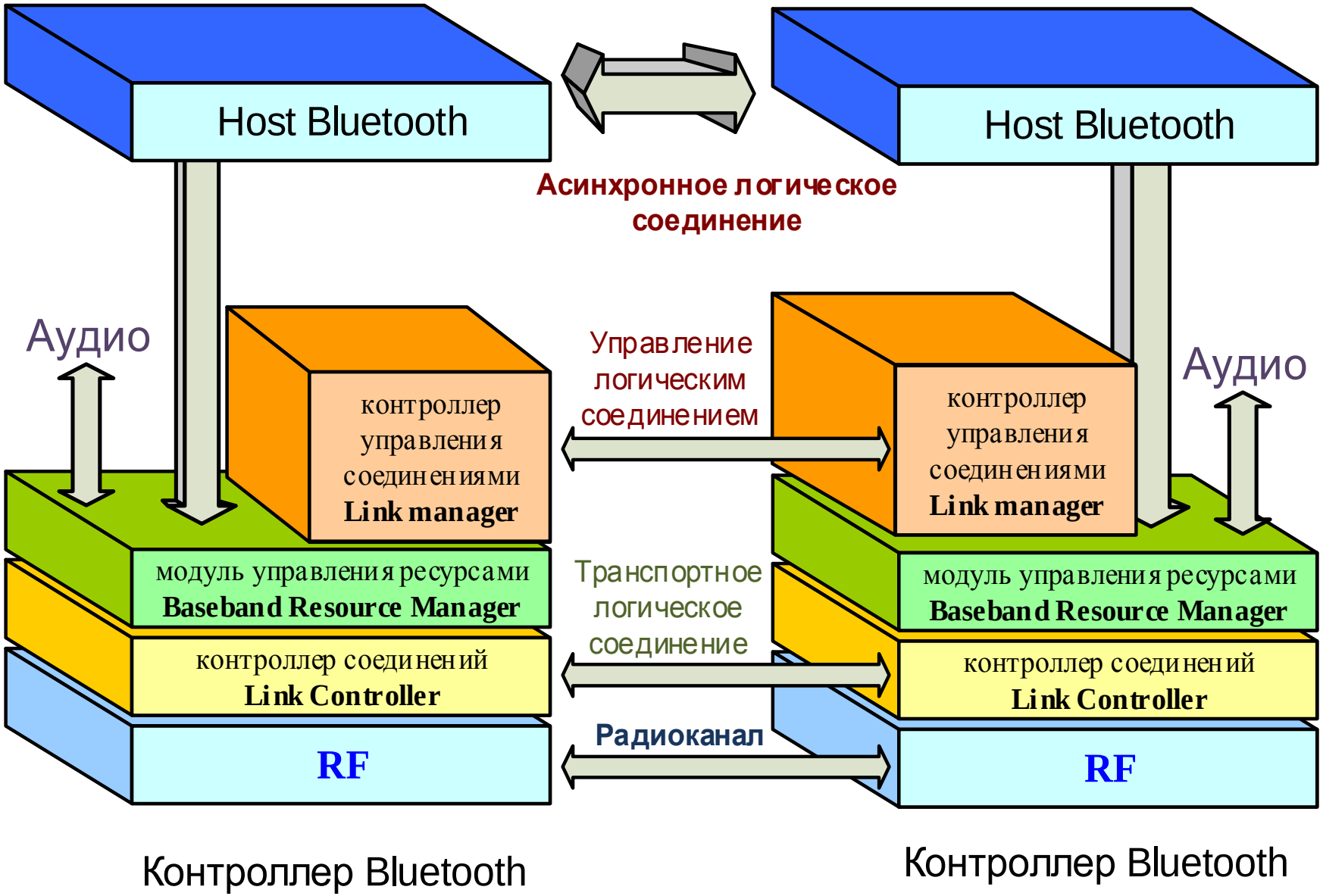



**HCI** - *Host Controller Interface*

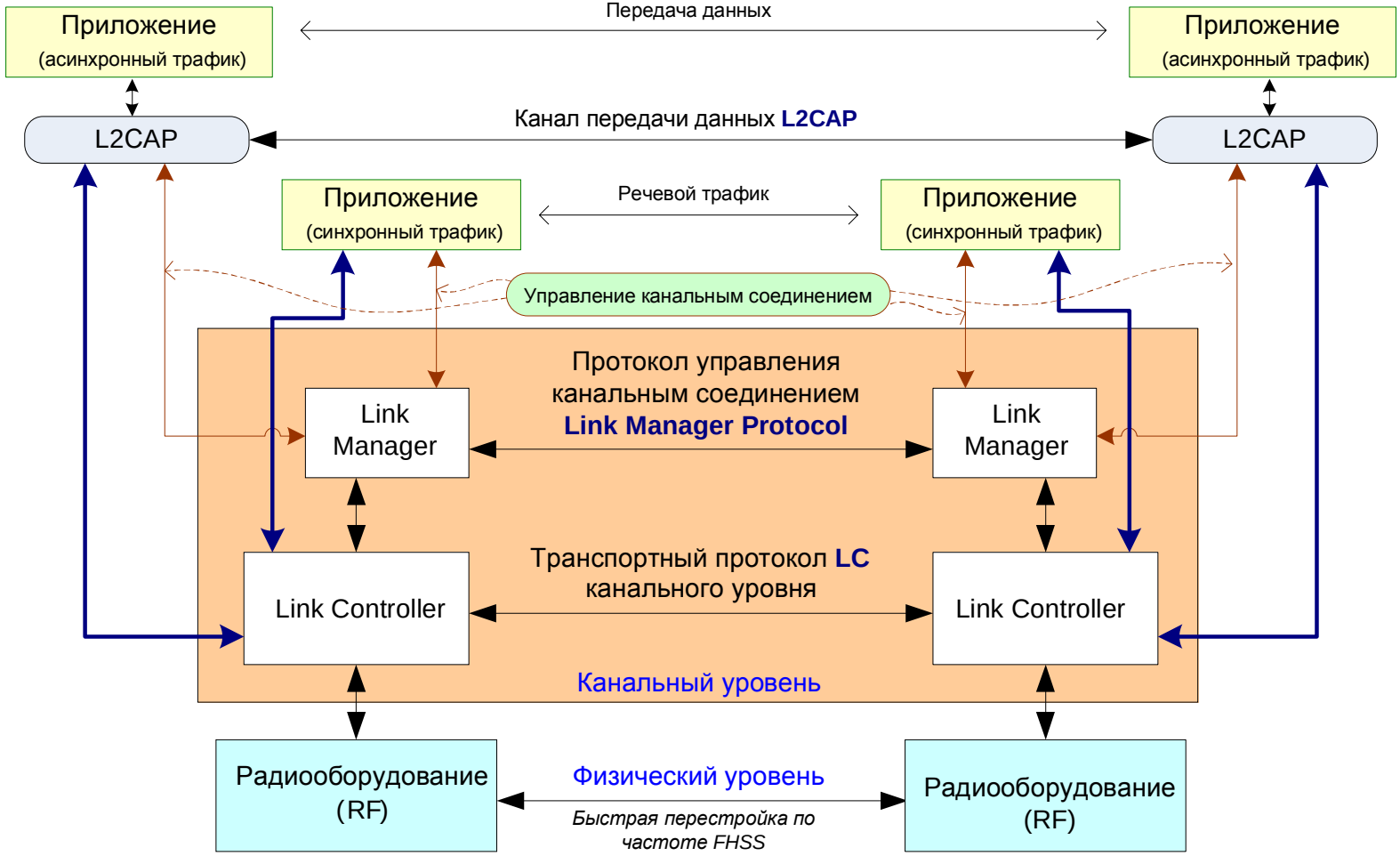
**L2CAP** - *Logical Link Control and Adaptation Protocol*

**Host Bluetooth –** высокоуровневый контроллер, управляющий услугами канальных соединений; используется только для асинхронного трафика

# Иерархическая модель Bluetooth

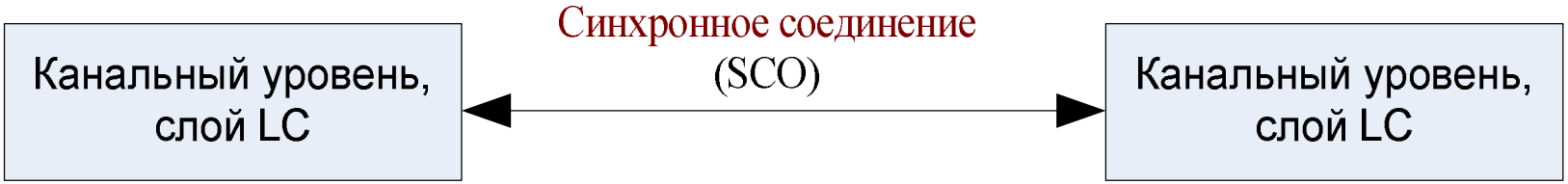


На канальном уровне предоставляются два различных способа логического соединения - синхронный, ориентированный на соединение (*Synchronous Connection-Oriented* - **SCO**), и асинхронный без установления соединения (*Asynchronous Connection-Less* - **ACL**). Синхронное соединение требует постоянного резервирования части канального ресурса, асинхронное соединение получает радиоресурс при необходимости доставки сообщений.

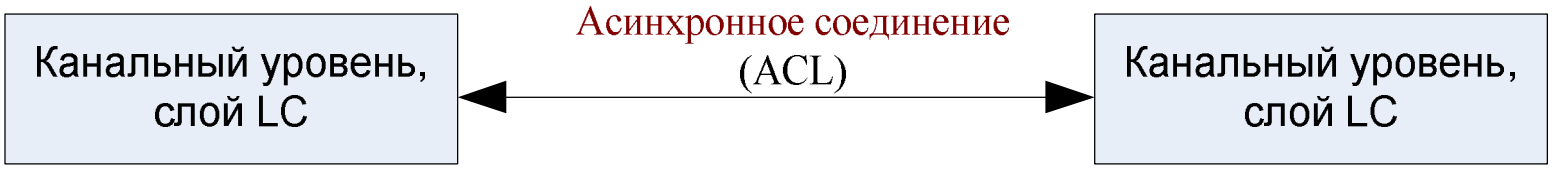


# Логические и транспортные (L2) соединения Bluetooth

# Транспортные каналы подуровня LC




**Синхронное подключение** (SCO) с установлением соединения используется для передачи изохронного трафика, как правило, чувствительного к задержкам. Это подключение реализует тип соединения «точка-точка». Каждое соединение подобного типа требует **обязательного резервирования физических каналов** в прямом и обратном направлениях. При этом запрос повторной передачи пакетов в случае ошибочного приема, как правило, не используется.



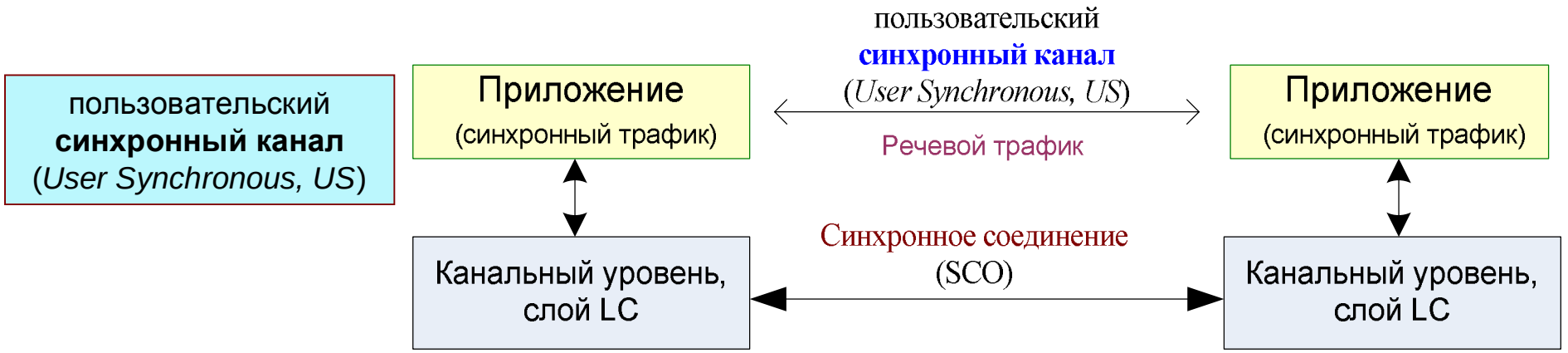

**Асинхронные подключения** (ACL) без установления соединения реализуют доставку пакетов по схеме «точка-многоточка» между ведущим устройством и остальными терминалами пикосети. Ведущее устройство Bluetooth может связываться с любым из ведомых устройств пикосети по каналам, не занятым под SCO. Инициатором обмена в этом режиме выступает всегда ведущее устройство. Ведомое устройство имеет право на передачу пакета только тогда, когда получает адресованный ему запрос от ведущего устройства. Для большинства типов пакетов, используемых в режиме ACL, предусматривается повторная передача в случае обнаружения ошибки приема.

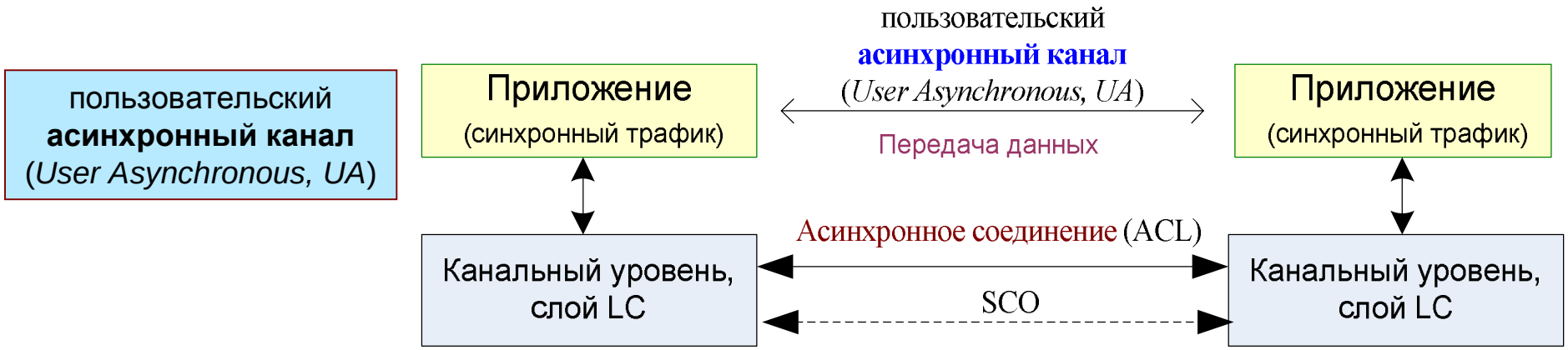
# Пользовательские логические каналы

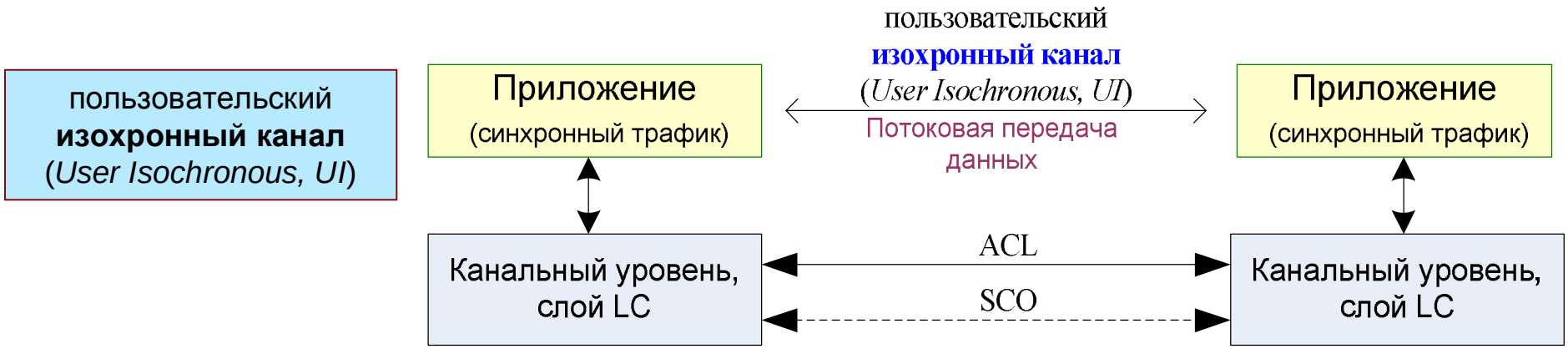
Транспортные соединения канального уровня используются для образования пользовательских логических каналов.

В рамках транспортного соединения подуровня LC реализуются следующие пользовательские логические каналы передачи данных:

- пользовательский **асинхронный канал** (*User Asynchronous, UA*) переносит асинхронные данные пользователя по каналу ACL или по синхронному каналу SCO в составе пакетов DV;
- пользовательский **изохронный канал** (*User Isochronous, UI*) переносит непрерывные данные пользователя по каналу ACL, но может также переносить эти данные в пакетах DV по каналу SCO. Синхронизация для поддержки непрерывности потока данных обеспечивается на сетевом уровне;
- пользовательский **синхронный канал** (*User Synchronous, US*) переносит синхронные данные пользователя по каналу SCO.




пользовательский
асинхронный канал
(User Asynchronous, UA)
Приложение
(синхронный трафик)
пользовательский
асинхронный канал
(User Asynchronous, UA)
Передача данных
Приложение
(синхронный трафик)
Асинхронное соединение (ACL)
Канальный уровень,
слой LC
SCO
Канальный уровень,
слой LC


пользовательский
изохронный канал
(User Isochronous, UI)
Приложение
(синхронный трафик)
пользовательский
изохронный канал
(User Isochronous, UI)
Потоковая передача
данных
Приложение
(синхронный трафик)
ACL
Канальный уровень,
слой LC
SCO
Канальный уровень,
слой LC

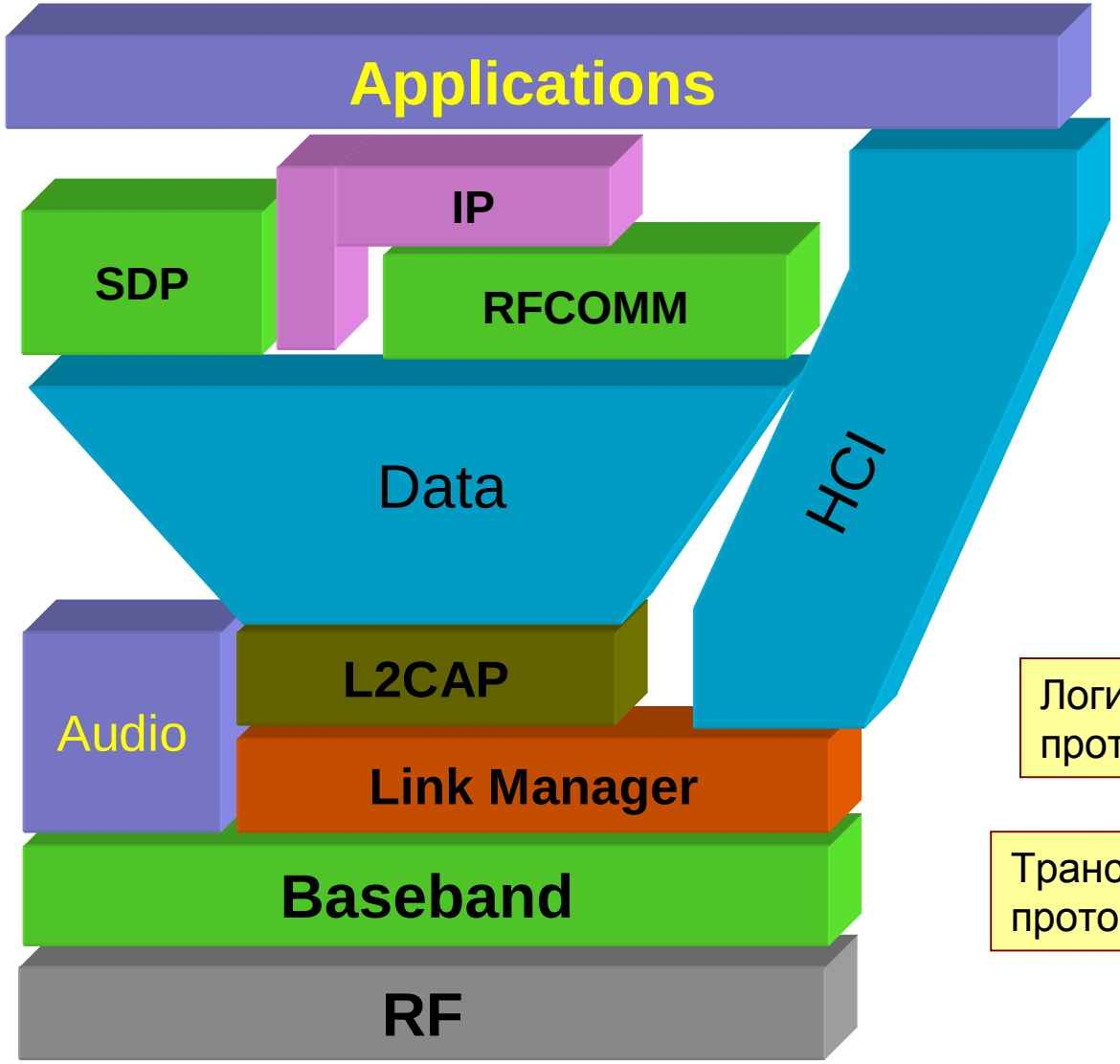
# Стек протоколов BT

Стек протоколов Bluetooth отражает возможность взаимодействия оборудования стандарта Bluetooth с разнообразным оборудованием сетевого и более высоких уровней модели OSI.

При работе устройств Bluetooth используются как специфические протоколы, разработанные специально для Bluetooth, так и общие, используемые в различных телекоммуникационных системах. Все протоколы образуют стек протоколов Bluetooth, который можно условно разделить на четыре группы:

- **корневые протоколы Bluetooth**:
  - транспортный протокол канального уровня LC
  - протокол управления соединениями LMP
  - адаптированный протокол управления логическими связями L2CAP
  - протокол обнаружения услуг SDP;
- протокол замены кабеля RFCOMM;
- протокол управления телефонией TSC и AT-команды;
- заимствованные протоколы: PPP, UDP/TCP/IP, OBEX, WAP, vCARD, vCAL, WAP.

# Иерархия протоколов BT

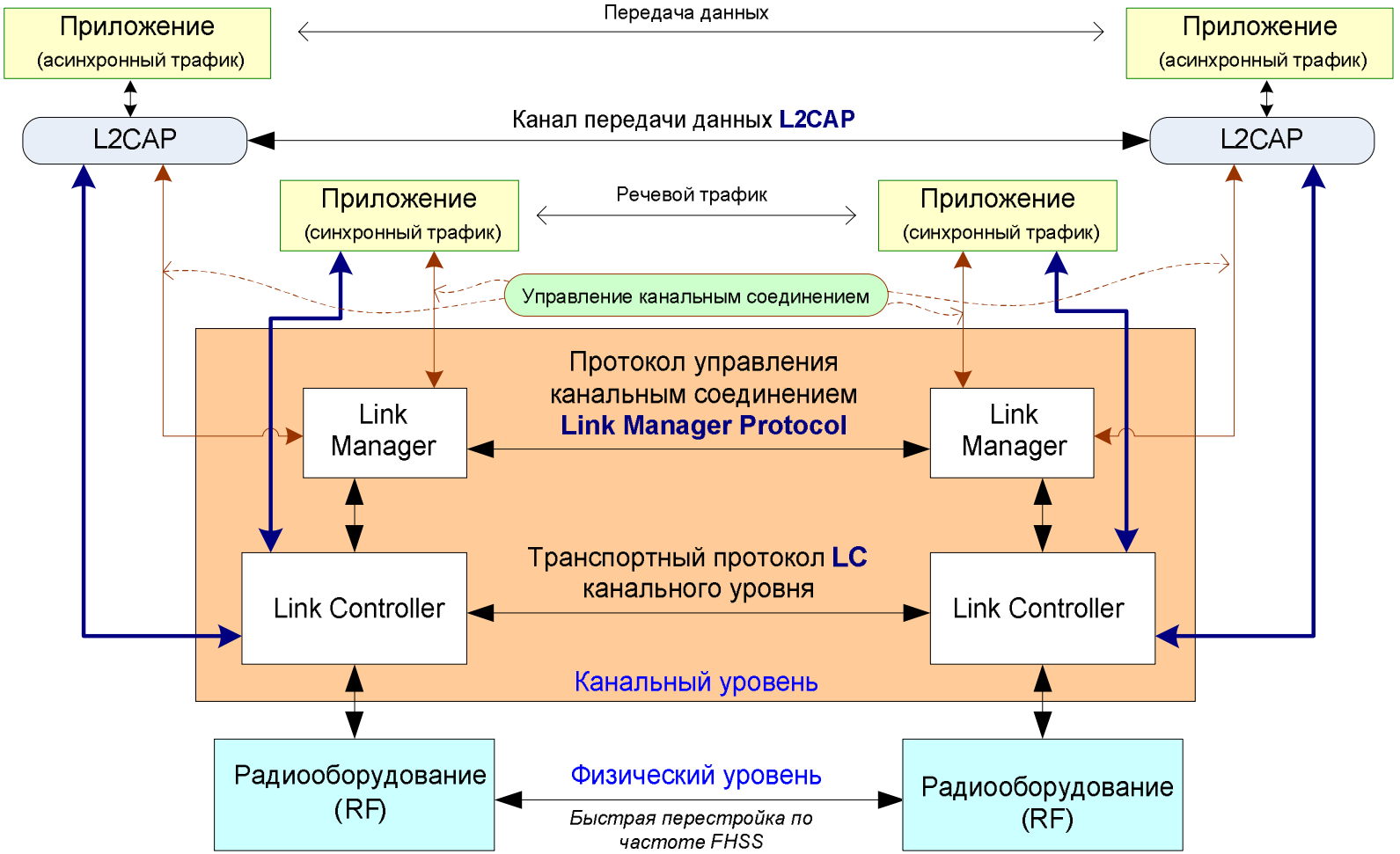



Протоколы приложений BT

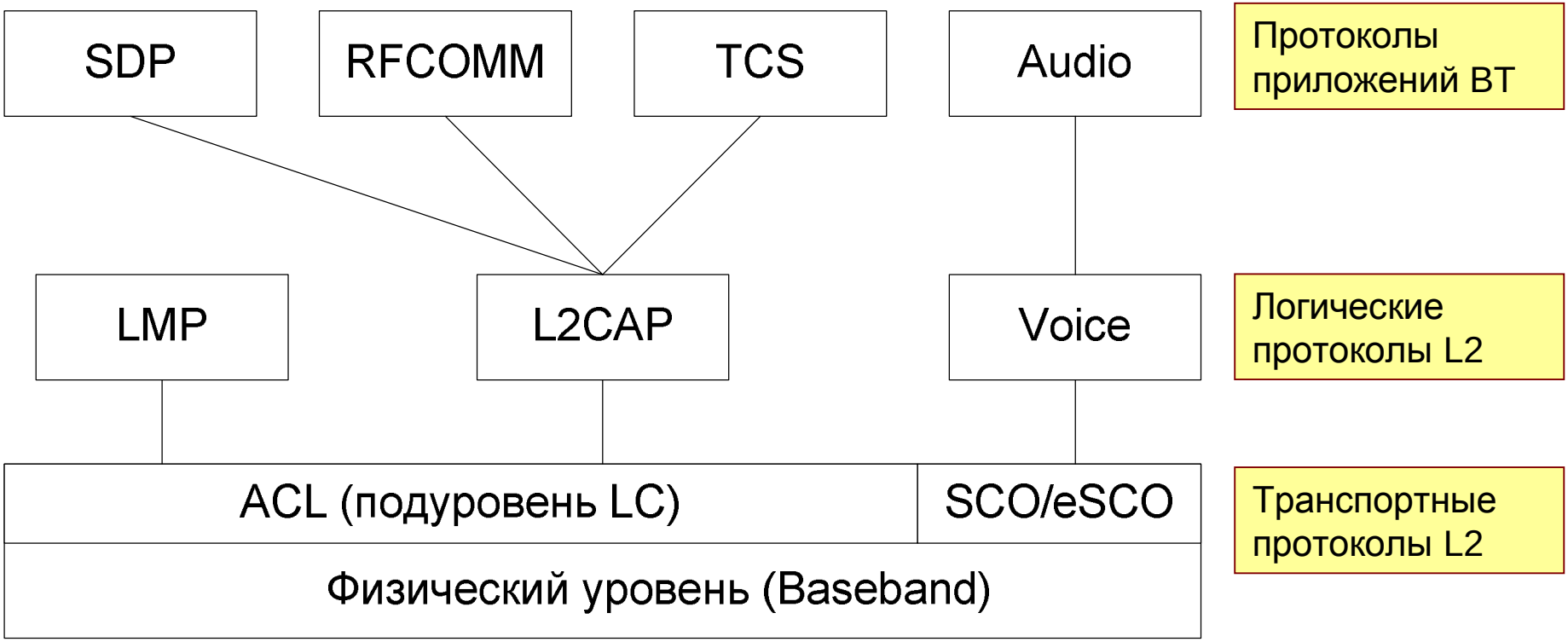
Логические протоколы L2

Транспортные протоколы L2

**Подуровень управления соединениями** (*Link Manager - LM*) предназначен для осуществления управления как **синхронными** (постоянно выделенными) SCO, так и **асинхронными** ACL (виртуальными, непостоянно выделенными) соединениями. На слое LC реализуются транспортные соединения ACL, SCO и eSCO (синхронное транспортное соединение с расширенными свойствами - поддержка технологии ARQ)



# Иерархия протоколов Bluetooth



# Структура протоколов стандарта Bluetooth

| | |
|---|---|
| *Высшие уровни модели OSI* | Кодирование аудиосигналов |
| *Канальный уровень* | Уровень LC |
| *Физический уровень (PHY)* | Радиоинтерфейс 802.15.1 |

**а**

| | |
|---|---|
| *Высшие уровни модели OSI* | Управление и контроль сети |
| *Канальный уровень* | Уровень LMP |
| | Уровень LC |
| *Физический уровень (PHY)* | Радиоинтерфейс 802.15.1 |

**б**

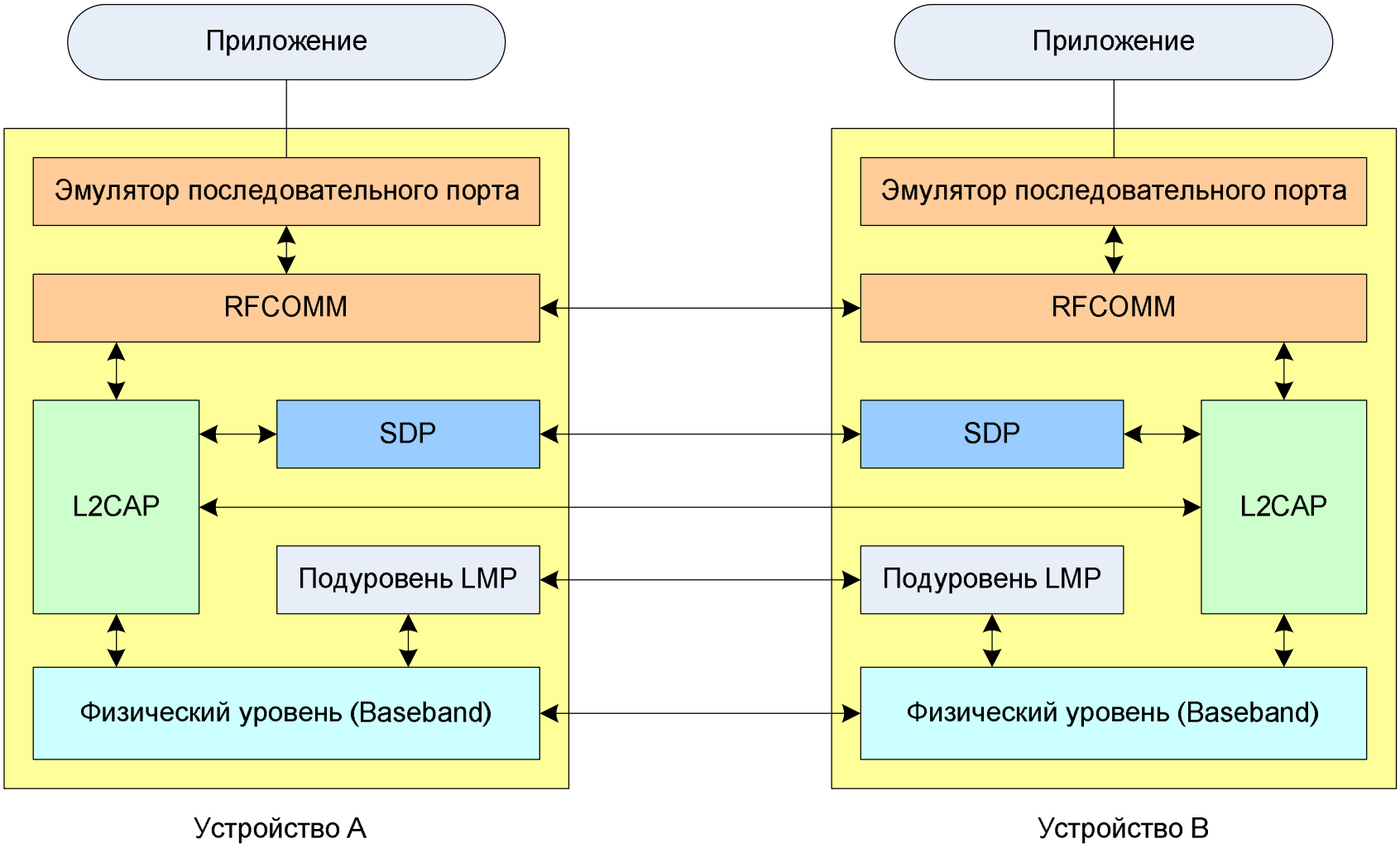
| | | | |
|---|---|---|---|
| *Сеансовый уровень* | TCP | AT команды | OBEX |
| *Транспортный уровень* | IP | | |
| *Сетевой уровень* | RF COMM | | |
| *Канальный уровень* | L2 CAP | | |
| | Уровень LC | | |
| *Физический уровень (PHY)* | Радиоинтерфейс 802.15.1 | | |

**в**

| | | |
|---|---|---|
| *Высшие уровни модели OSI* | TCS BIN | SDP |
| *Канальный уровень* | L2 CAP | |
| | Уровень LC | |
| *Физический уровень (PHY)* | Радиоинтерфейс 802.15.1 | |

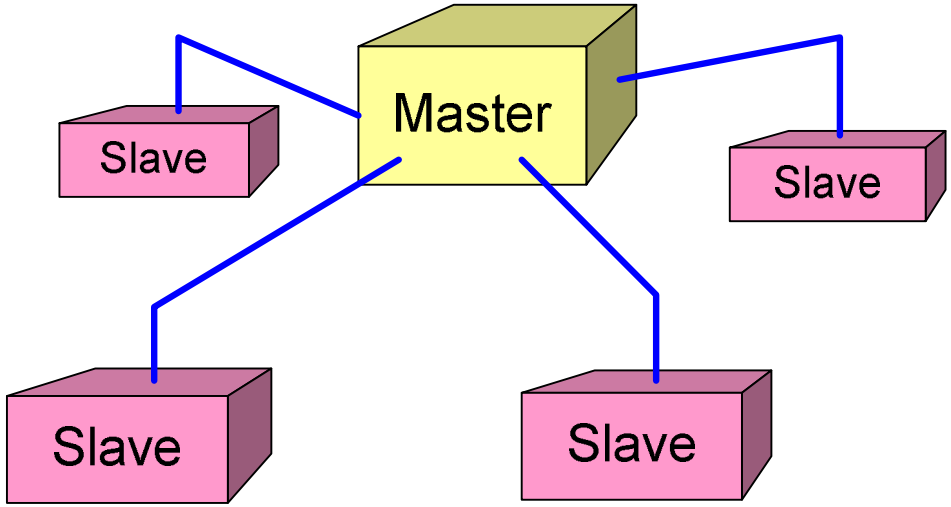
**г**

# Модель организации протокола RFCOMM



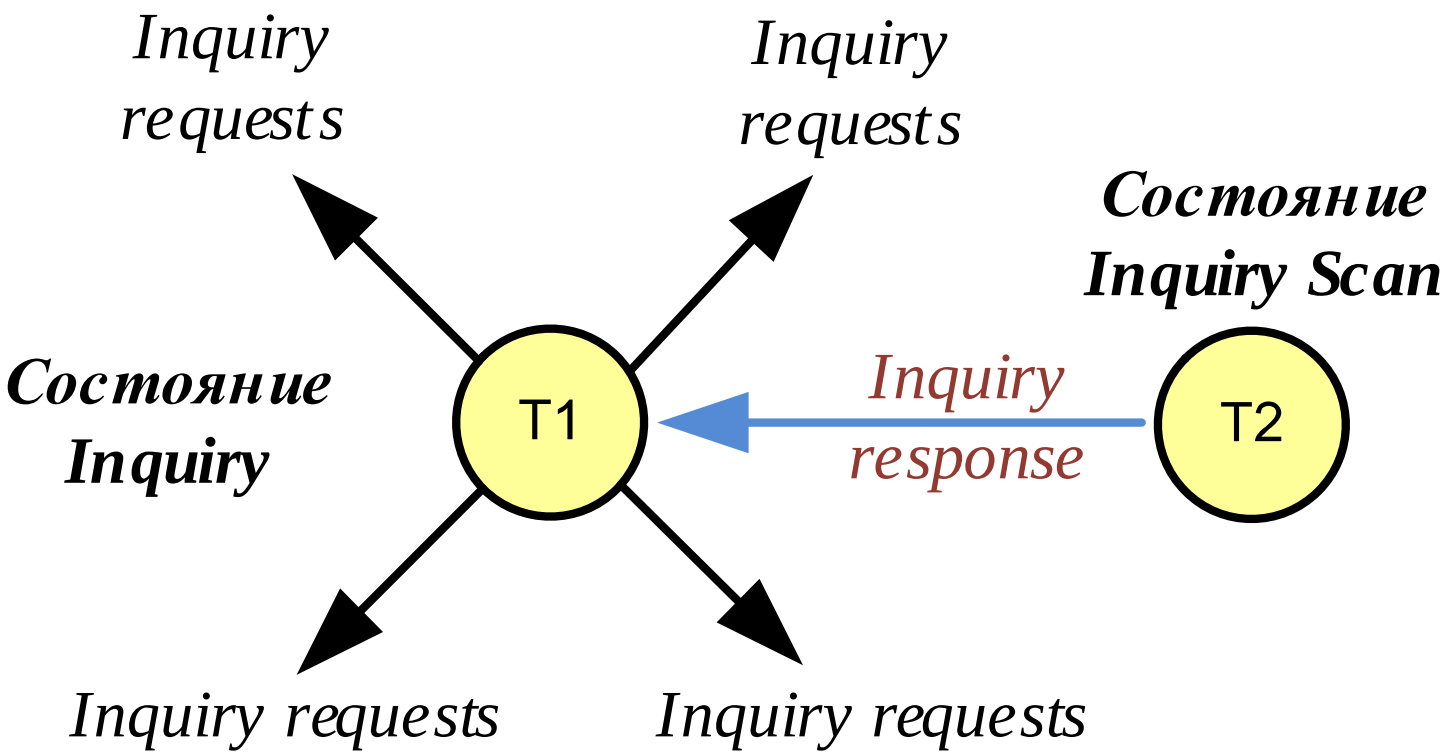
# Физический уровень Bluetooth

# Топология физических соединений




Топология связей L1 уровня является иерархической. Два и более устройства Bluetooth образуют пикосеть (*piconet*). Пикосеть устанавливается станцией, которая заявляет о себе передачей специального сообщения *inquiry requests*. Эта станция становится *ведущей*. Другие Bluetooth терминалы этой пикосети становятся *ведомыми*. Однако любая ведомая станция может передавать свое сообщение *inquiry requests*, становясь таким образом ведущей станцией в соседней пикосети. В одной пикосети может быть до семи активных *ведомых* устройств, при этом остальные *ведомые* устройства находятся в состоянии "парковки", оставаясь синхронизированными с *ведущим* устройством.

# Идея образования пикосети Bluetooth




Передавая сообщение *Inquiry requests* терминал T1 объявляет о появлении новой сети, к которой он приглашает присоединиться на правах ведомого устройства

# Основные параметры физического уровня Bluetooth

| **Параметр** | **Значение** |
|---|---|
| Диапазон частот | 2400…2483,5 МГц |
| Максимальная мощность излучения для наружных устройств | < 2,5 мВт |
| Максимальная мощность излучения для устройств внутри здания | < 100 мВт |
| Тип модуляции | GFSK (h=0,3), $\pi/4-DQPSK$, $8DPSK$ |
| Максимальная скорость передачи данных | 1 Мбит/с (2 Мбит/с при использовании $\pi/4-DQPSK$ и $8DPSK$ ) |
| Частотное разнесение несущих | 1МГц |
| Ширина спектра радиосигнала | 0,22МГц (по уровню -3дБ) и 1МГц (-20дБ) |
| Количество частотных каналов | 79 |
| Количество активных участников пикосети | 8 (1+7) |

# Технология множественного доступа к физической среде FHSS (*Frequency Hopping* Spread Spectrum)

Выделенный системе диапазон разделен на 79 частотных каналов шириной 1 МГц. За время передачи любого пакета L1 уровня Bluetooth используется только один из этих каналов в соответствии с определенной схемой перестройки частоты.

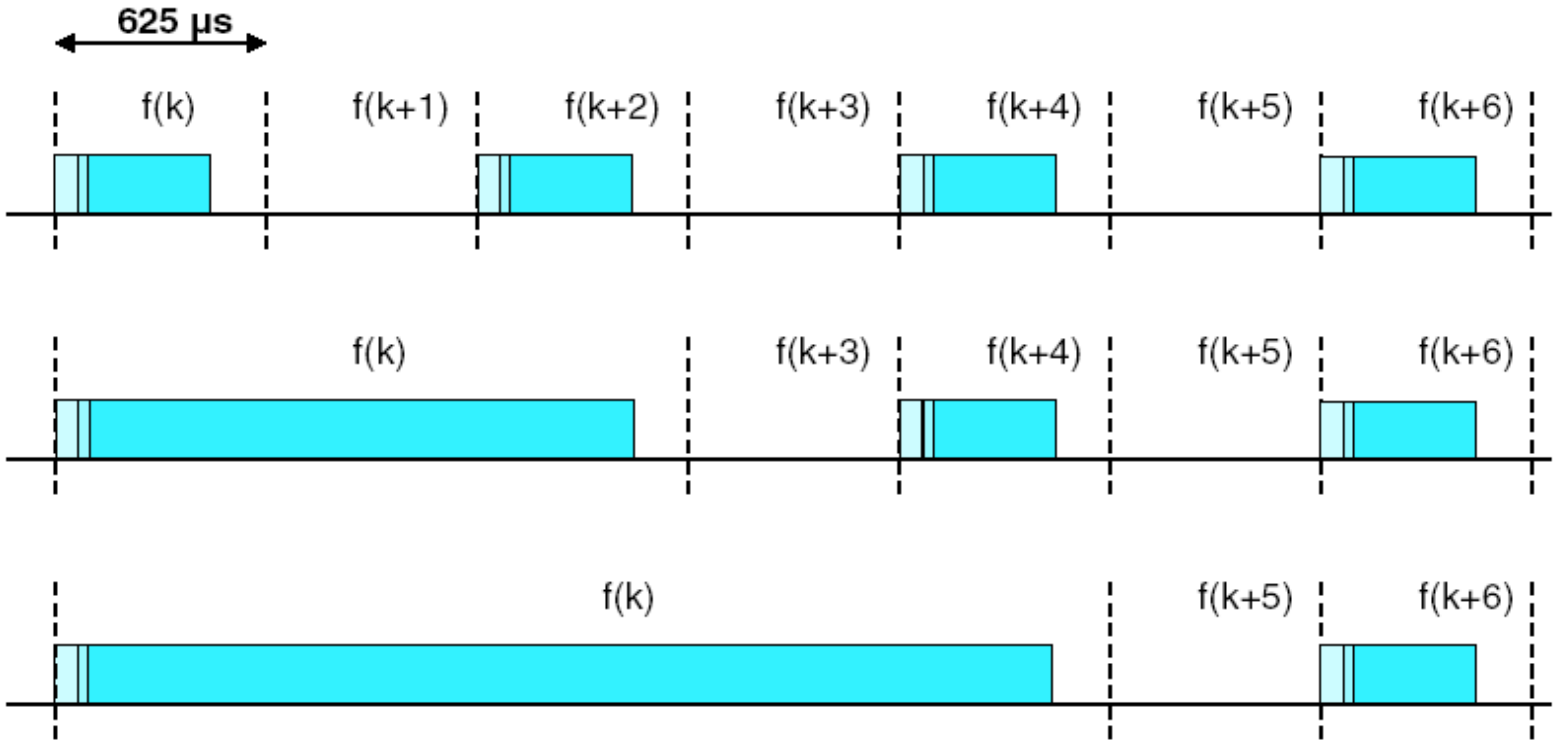
Как правило, для передачи одного пакета используется один временной слот длительностью 625 мкс, при этом скорость смены несущей частоты составляет 1600 скачков в секунду.

Физические каналы Bluetooth образуются последовательностями смены частотных каналов. Перестройка частоты происходит синхронно на ведущем и ведомом устройствах в соответствии с определенной последовательностью смены частоты.

На L1 уровне реализовано 6 типов последовательностей смены частот: 4 коротких типа с 32 элементами и два вида длинных последовательностей с длиной $2^{27}$ элементов. Нетрудно убедиться в исчерпывающем количестве потенциальных ФК в Bluetooth.

| | Последовательности смены частот $f_i$ |
|---|---|
| Channel 0 | 17 → 3 → 59 → 21 → 37 → … |
| Channel 1 | 32 → 12 → 4 → 11 → 73 → … |
| Channel 3 | 45 → 19 → 68 → 10 → 9 → … |
| … | … |
| Channel N | 71 → 2 → 34 → 55 → 15 → … |

# Однослотовый и многослотовый режимы L1 уровня




В Bluetooth на L1 уровне используется скачкообразная перестройка частоты (*frequency hopping, FH*) и дуплексная передача с разделением времени (*time division duplexing,TDD*). Данные на физическом уровне передаются в виде пакетов, занимающих один или несколько временных слотов длительностью 625 мкс. Пакеты в зависимости от длины могут занимать до пяти временных слотов. Обменом L1 пакетов управляет **ведущее** устройство по типу «запрос-ответ», т.е. если четные слоты использует ведущее устройство, то нечетные должны применять **ведомые** для ответа или для передачи данных. Т.е. *ведущее (master)* устройство чередует передачу пакетов с *ведомыми (slave)* устройствами. При этом несущая частота не меняется до окончания передачи пакета.

# Последовательности смены частот для формирования физических каналов

В стандарте BT имеются шесть типов последовательностей смены частот:

- последовательность смены частоты в режиме вызова *page hopping sequence* – 32 частоты, распределенные в выделенном частотном диапазоне (определяется **идентификатором вызываемой станции**);

- последовательность смены частоты в состоянии ответа на вызов *page response hopping sequence* – совпадает с текущей *page hopping sequence* (определяется **идентификатором вызываемой станции**);

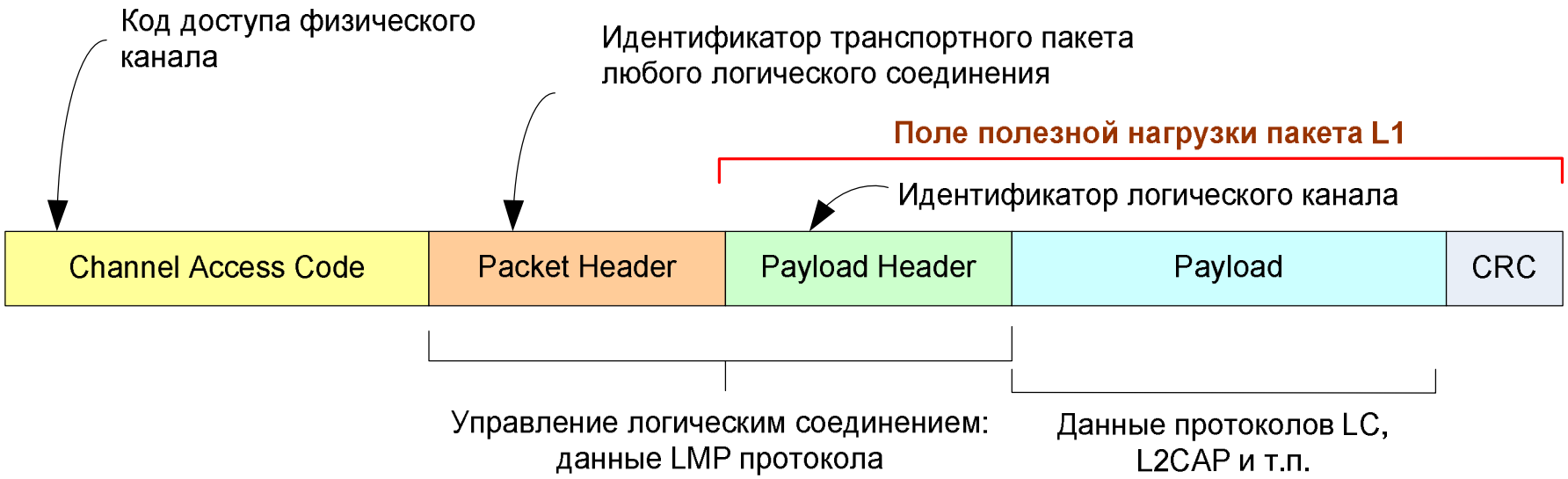
- последовательность смены частоты в состоянии опроса *inquiry hopping sequence* – 32 частоты, распределенные в выделенном частотном диапазоне (определяется **зарезервированными в Bluetooth адресами**);

- последовательность смены частоты в режиме ответа на *inquiry response hopping sequence* - совпадает с текущей *inquiry hopping sequence* (определяется **зарезервированными адресами**);

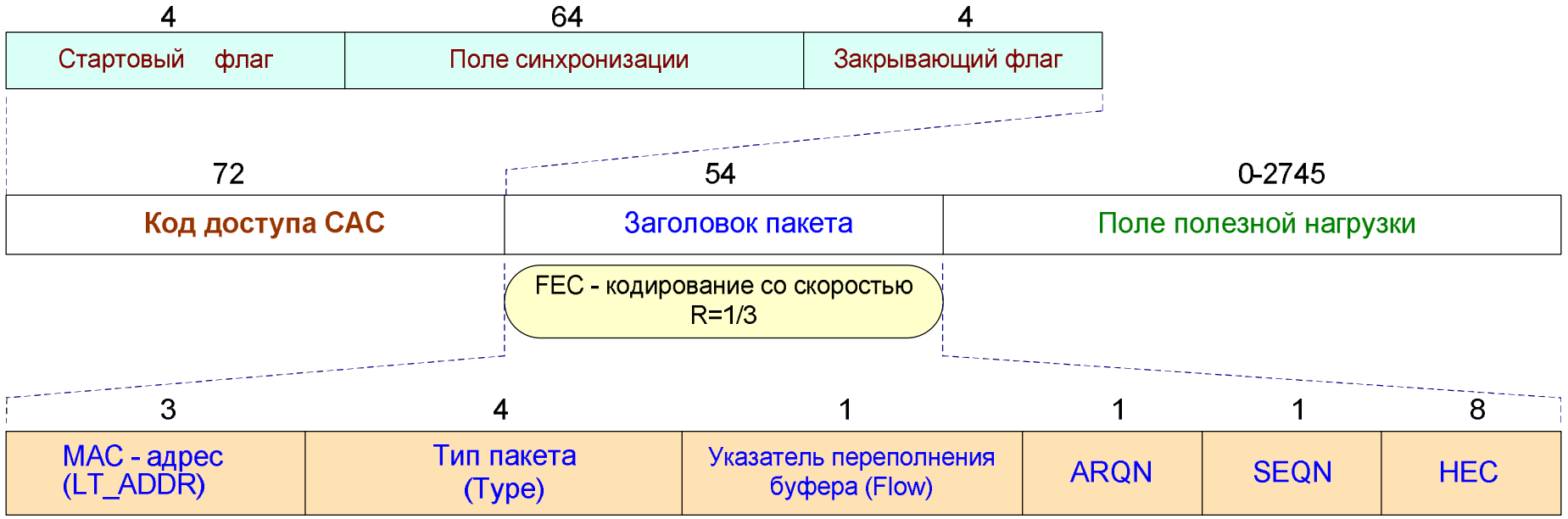
- основная последовательность смены частоты *basic channel hopping sequence*, имеющая очень большой период повторения и обладающая практически отсутствующей корреляцией на малых интервалах. Длина последовательности составляет $2^{27}$ элементов, период повтора - примерно 23 ч. Используется исключительно в режиме *Connection* и определяется **идентификатором ведущей станции**;

- дополнительная последовательность смены частоты *adapted channel hopping sequence*, определяется *basic channel hopping sequence* и используется в специальных режимах связи.

# Пакеты L1 Уровня. Инкапсуляция данных логических каналов Bluetooth




# Формат пакета физического уровня и полей заголовка



# Защита от ошибок на физическом уровне

## Пакеты подуровня LC

| Тип пакета | Payload (bytes) | FEC | CRC | Максимальная скорость передачи данных | |
|---|---|---|---|---|---|
| | | | | Симметричный канал | Асимметричный канал |
| ID | - | - | - | - | - |
| NULL | - | - | - | - | - |
| POLL | - | - | - | - | - |
| FHS | 18 | 2/3 | + | - | - |

## Пакеты асинхронного соединения ACL

| Тип пакета | Payload header (bytes) | Payload (bytes) | FEC | CRC | Максимальная скорость передачи данных в симметричном режиме, кбит/с | Максимальная скорость передачи данных в асимметричном режиме, кбит/с | |
|---|---|---|---|---|---|---|---|
| | | | | | | Прямой канал | Обратный канал |
| DM1 | 1 | 0-17 | 2/3 | + | 108,8 | 108,8 | 108,8 |
| DH1 | 1 | 0-27 | - | + | 172,8 | 172,8 | 172,8 |
| DM3 | 2 | 0-121 | 2/3 | + | 258,1 | 387,2 | 54,4 |
| DH3 | 2 | 0-183 | - | + | 390,4 | 585,6 | 86,4 |
| DM5 | 2 | 0-224 | 2/3 | + | 286,7 | 477,8 | 36,3 |
| DH5 | 2 | 0-339 | - | + | 433,9 | 723,2 | 57,6 |
| AUX1 | 1 | 0-29 | - | - | 185,6 | 185,6 | 185,6 |

## Пакеты синхронного соединения SCO

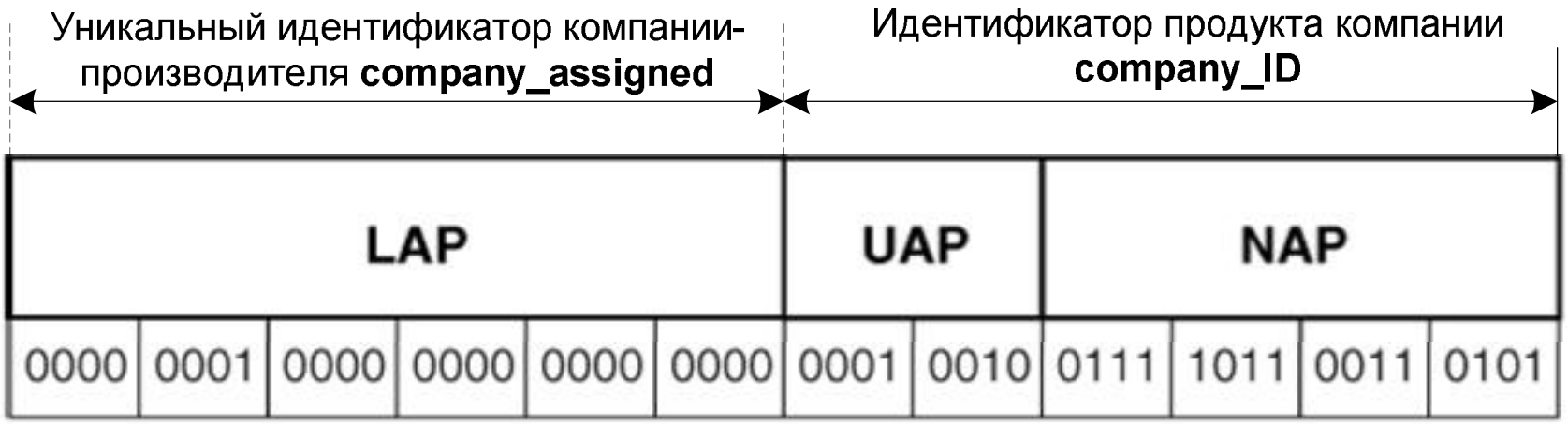
| Тип пакета | Payload header (bytes) | Payload (bytes) | FEC | CRC | Максимальная скорость передачи данных в симметричном режиме, кбит/с |
|---|---|---|---|---|---|
| HV1 | - | 10 | 1/3 | + | 64 |
| HV2 | - | 20 | - | + | 64 |
| HV3 | - | 30 | 2/3 | + | 64 |
| DV | D | 10+(0-9)D | 2/3 | + | 64+57,6D |

# Идентификаторы Bluetooth

## Идентификатор BD_ADDR

В соответствии со стандартом IEEE 802.15.1 каждое устройство сети наделяется уникальным 48-битным идентификатором BD_ADDR Bluetooth (Bluetooth Device Address - BD_ADDR), состоящим из трех полей: существенно значимых младшей **LAP** и старшей **UAP** частей адреса устройства, а также незначащей **NAP** части идентификатора. Этот адрес назначается управлением регистрации IEEE для производителей телекоммуникационного оборудования. Адресная емкость Bluetooth составляет $2^{32}$ адресов.

Идентификатор BD_ADDR определяет в пикосети основную последовательность частотных скачков, используемую для передачи пакетов данных, а системное время указывает текущую фазу псевдослучайной последовательности.



# Коды доступа Bluetooth

На основе LAP формируются коды доступа Bluetooth:

1. код доступа устройства **Device access code (DAC)**;
2. код доступа канала **Channel access code (CAC**);
3. код запроса идентификации **Inquiry access code (IAC).**

Код доступа DAC используется в режимах вызова (*page*) и ожидания вызова (*page scan*) и основан на LAP-адресе вызываемой станции.

Идентификатор CAC используется в режиме соединения (*connection*) и основан на LAP-адресе ведущего устройства.

В качестве идентификаторов IAC используются 64 зарезервированных LAP-адреса.

# Идентификаторы канального уровня (логические адреса)

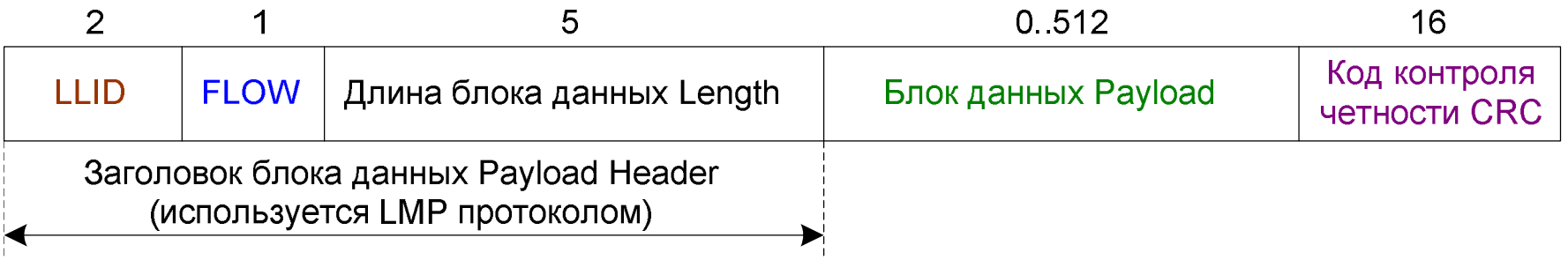
Для адресации сетевых объектов на канальном уровне используются следующие идентификаторы

- адрес активного объекта AM_ADDR (Active Member Address - AM_ADDR), назначается мастером пикосети активным ведомым терминалам, доступные варианты 1..7, значение AM_ADDR=0 используется мастером;

- адрес устройства, находящегося в состоянии парковки (Parked Member Address - PM_ADDR), уникальный для всех терминалов в состоянии парковки, 8 битов;

- адрес требования доступа из состояния парковки (Access Request Address - ARADDR), назначается мастером и отражает номер временного окна, когда запаркованный терминал сможет передать запрос о его выводе из состояния парковки, 8 битов.

# Структура поля полезной нагрузки в однослотовом режиме




Идентификатор типа блока данных **LLID** указывает на тип логического канала:

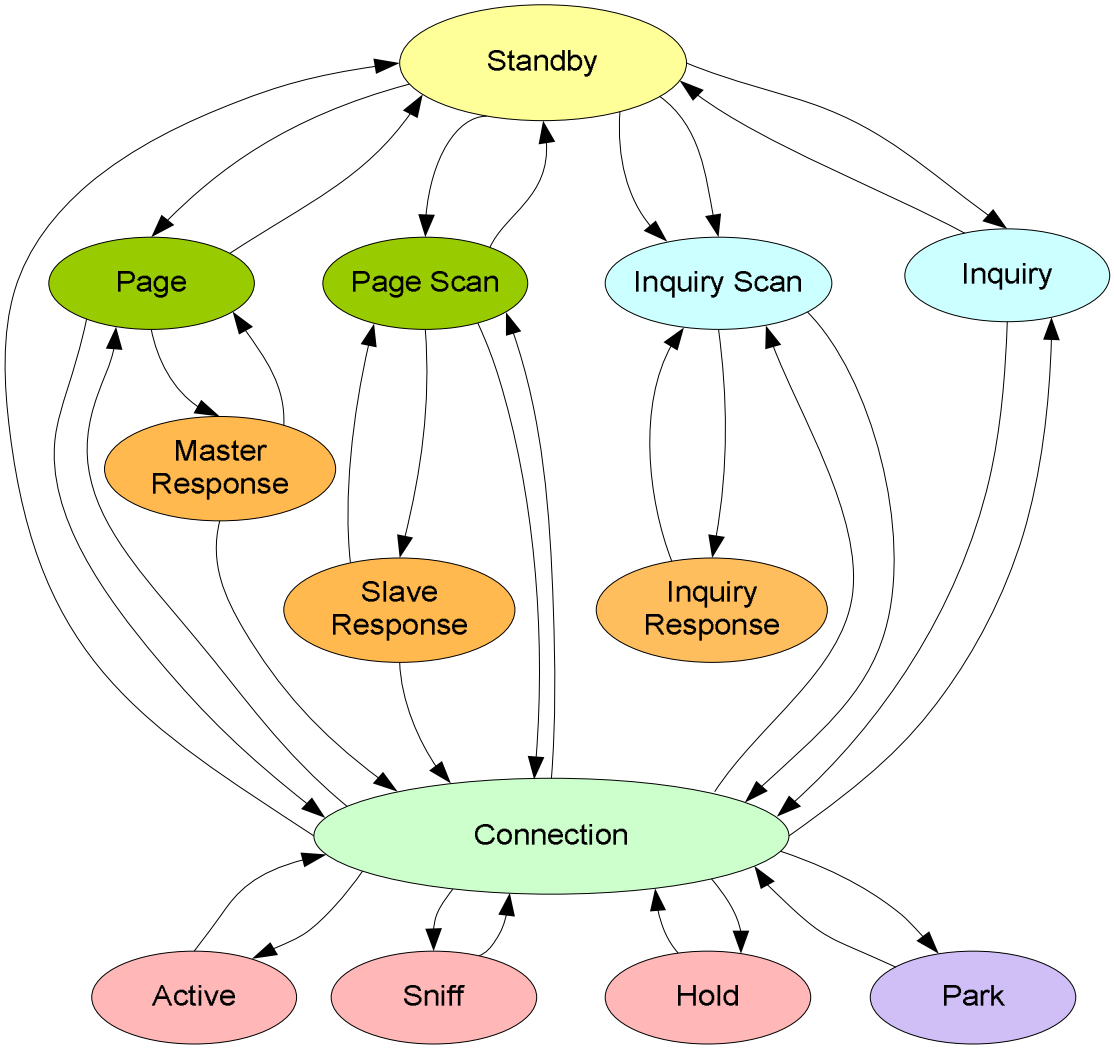
00 – резерв;

01 – продолжение сообщения канала **L2 CAP**;

10 – первый блок **L2 CAP**;

11 – сообщение канала **LMP**

# Принцип установления логических соединений Bluetooth



# Состояния устройств BT

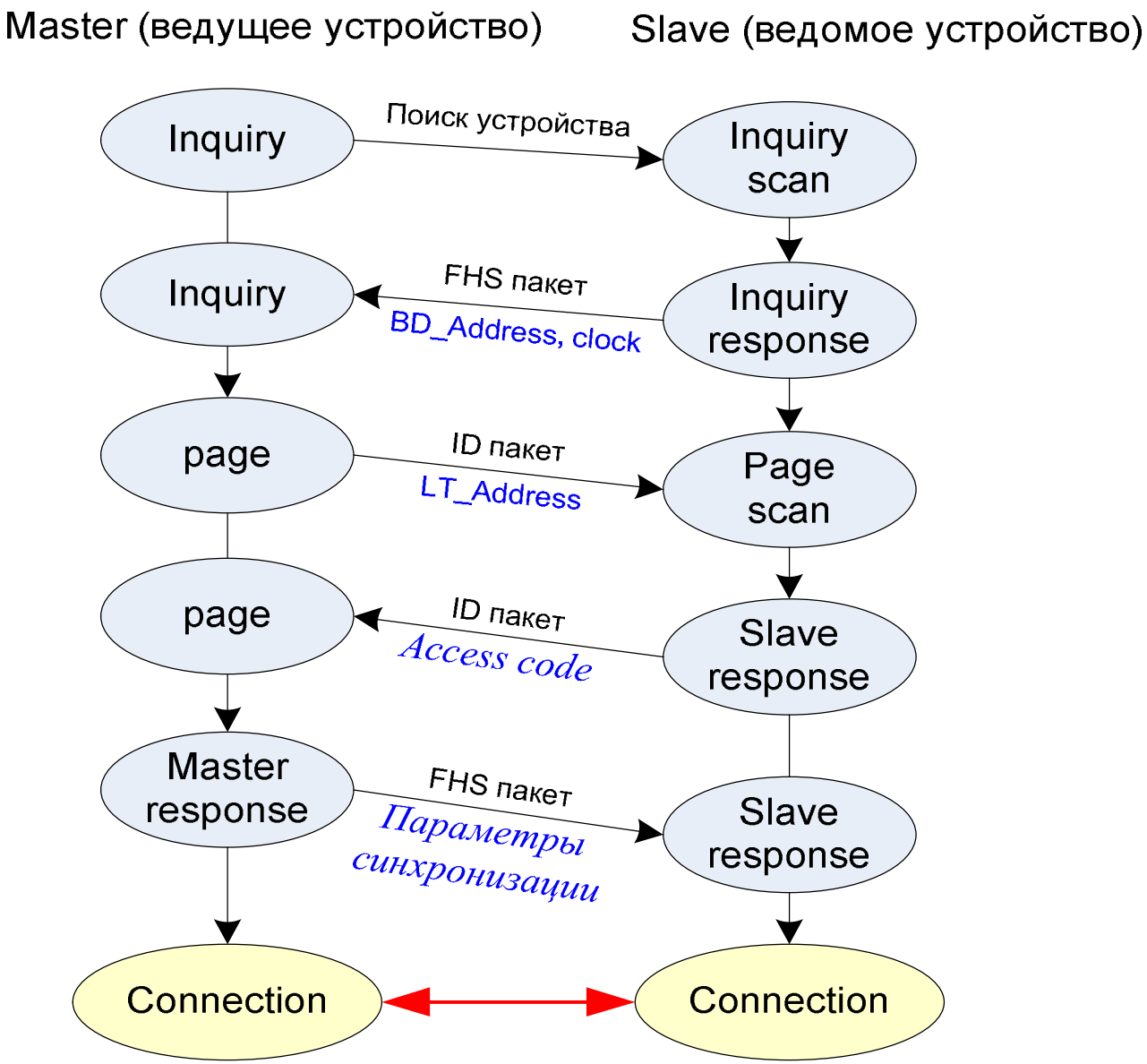
Любое устройство Bluetooth на подуровне LC (*link control*) может находиться в одном из трех главных состояний:

- спящий режим (Standby) – режим ожидания вызова;
- состояние соединения (Connection);
- состояние парковки (Park).

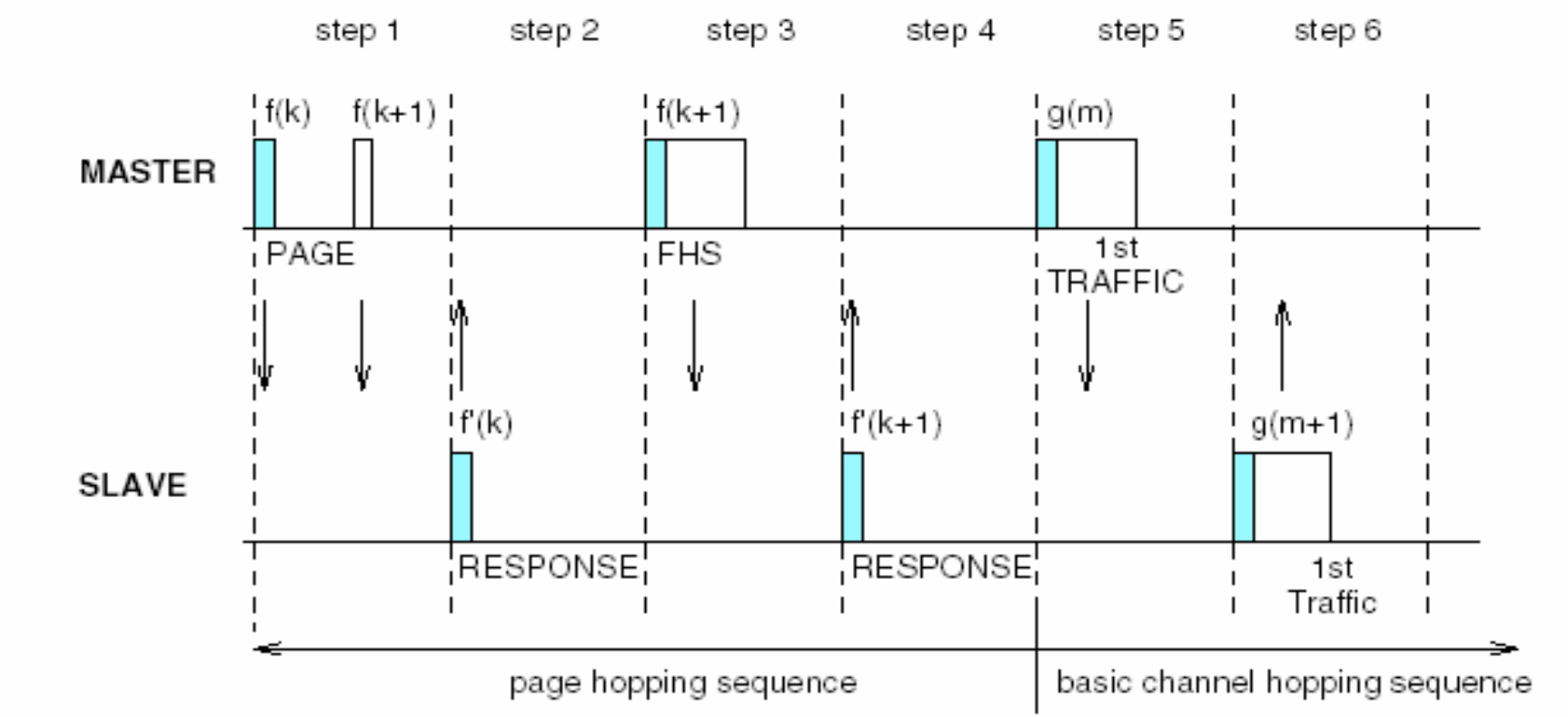
В дополнение основным состояниям имеется 7 промежуточных подрежимов (*substate*), относящихся к режиму соединения и уточняющих текущее состояние устройства Bluetooth:

- вызов (**page**);
- ответ ведущего устройства (**Master Response**);
- поиск сигналов вызова (**page scan**);
- ответ ведомого (**slave response**);
- поиск запроса на регистрацию (**inquiry scan**);
- ответ на запрос регистрации (**inquiry response**);
- поиск станций (**inquiry**).

# Пример диаграмм состояний при организации соединения



# Организации соединения на L1 уровне




Установление транспортного соединения

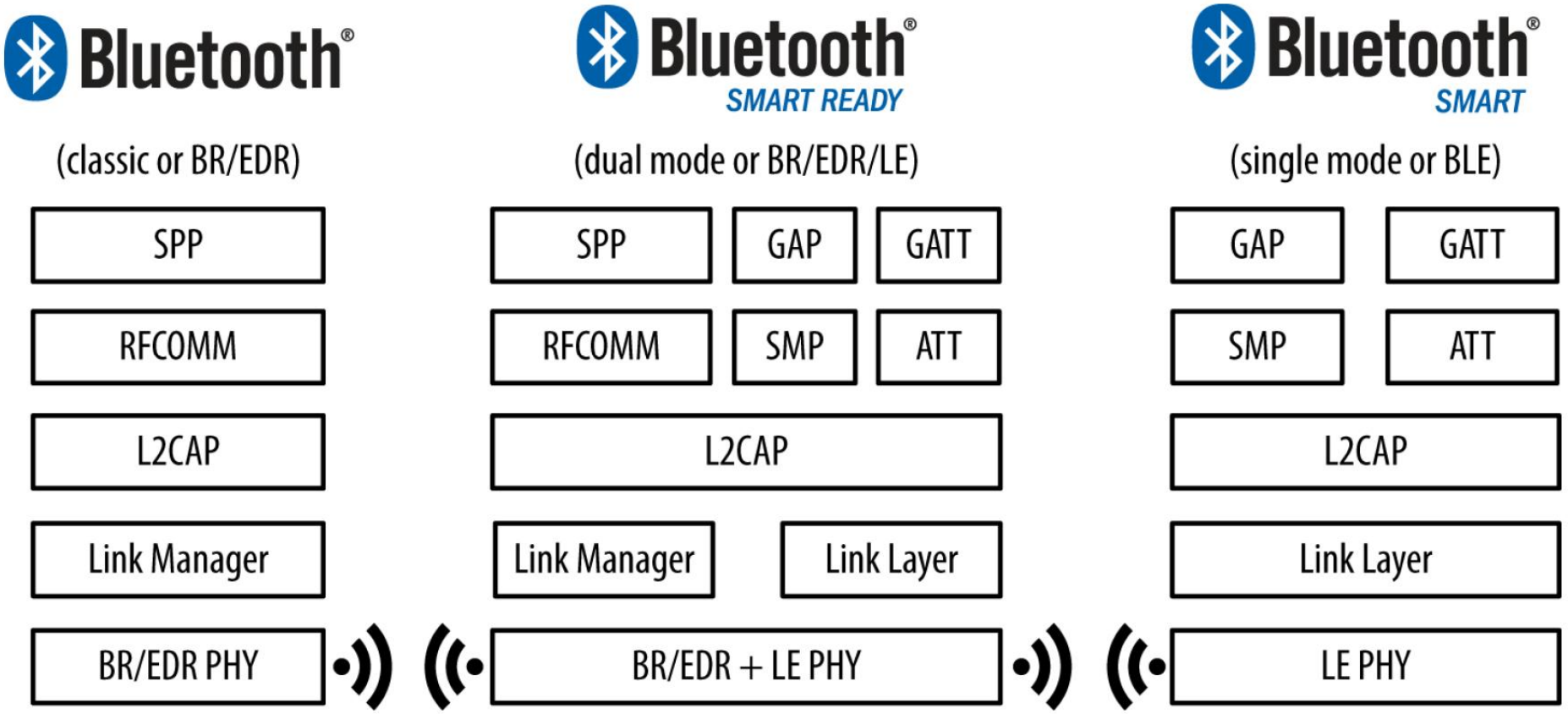
Передача данных по транспортному соединению

# Технология Bluetooth с низким энергопотреблением

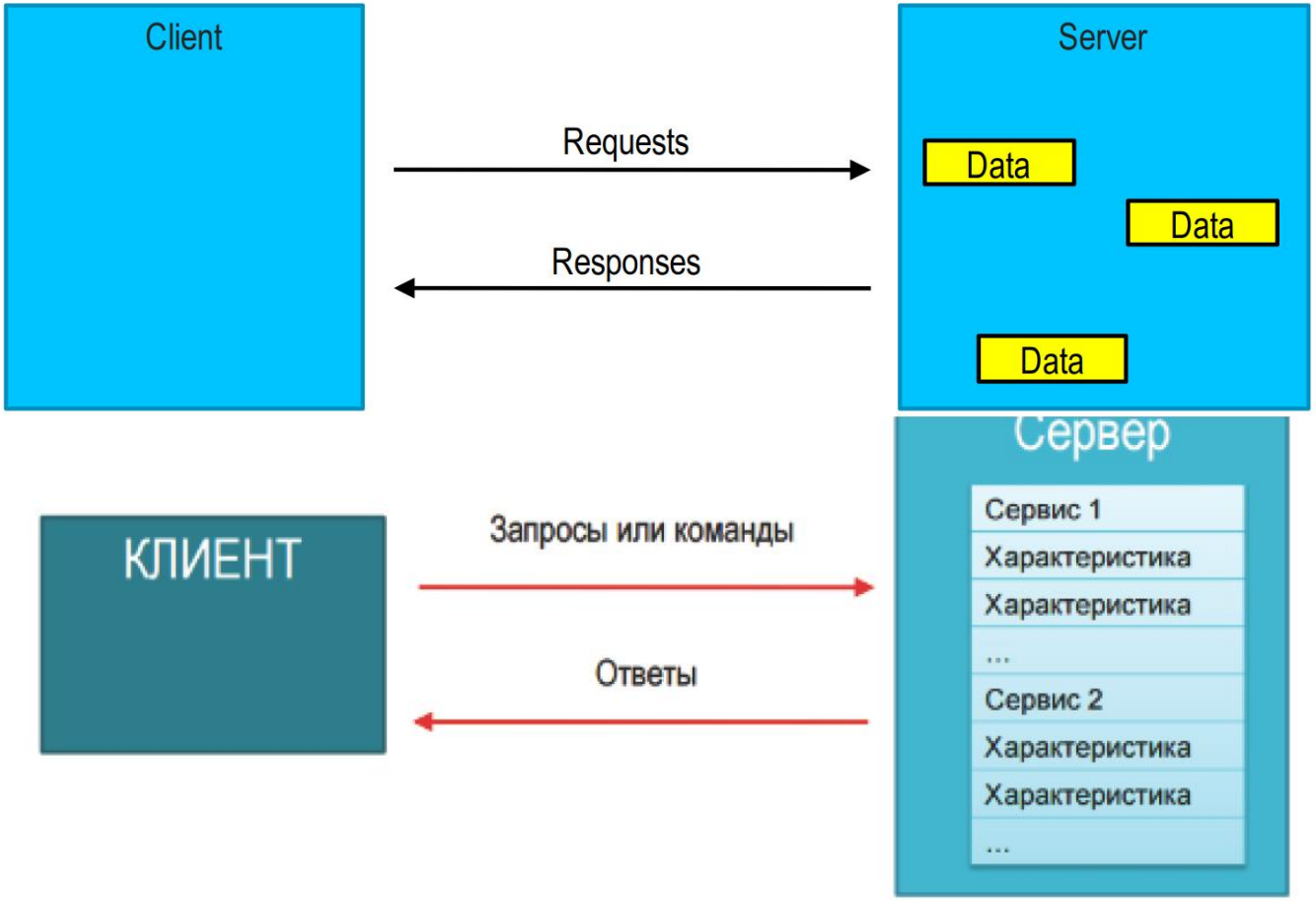
Bluetooth Low Energy (BLE)

Bluetooth v.4

# Иерархические модели трех типов Bluetooth устройств



# Архитектура GATT/ATT

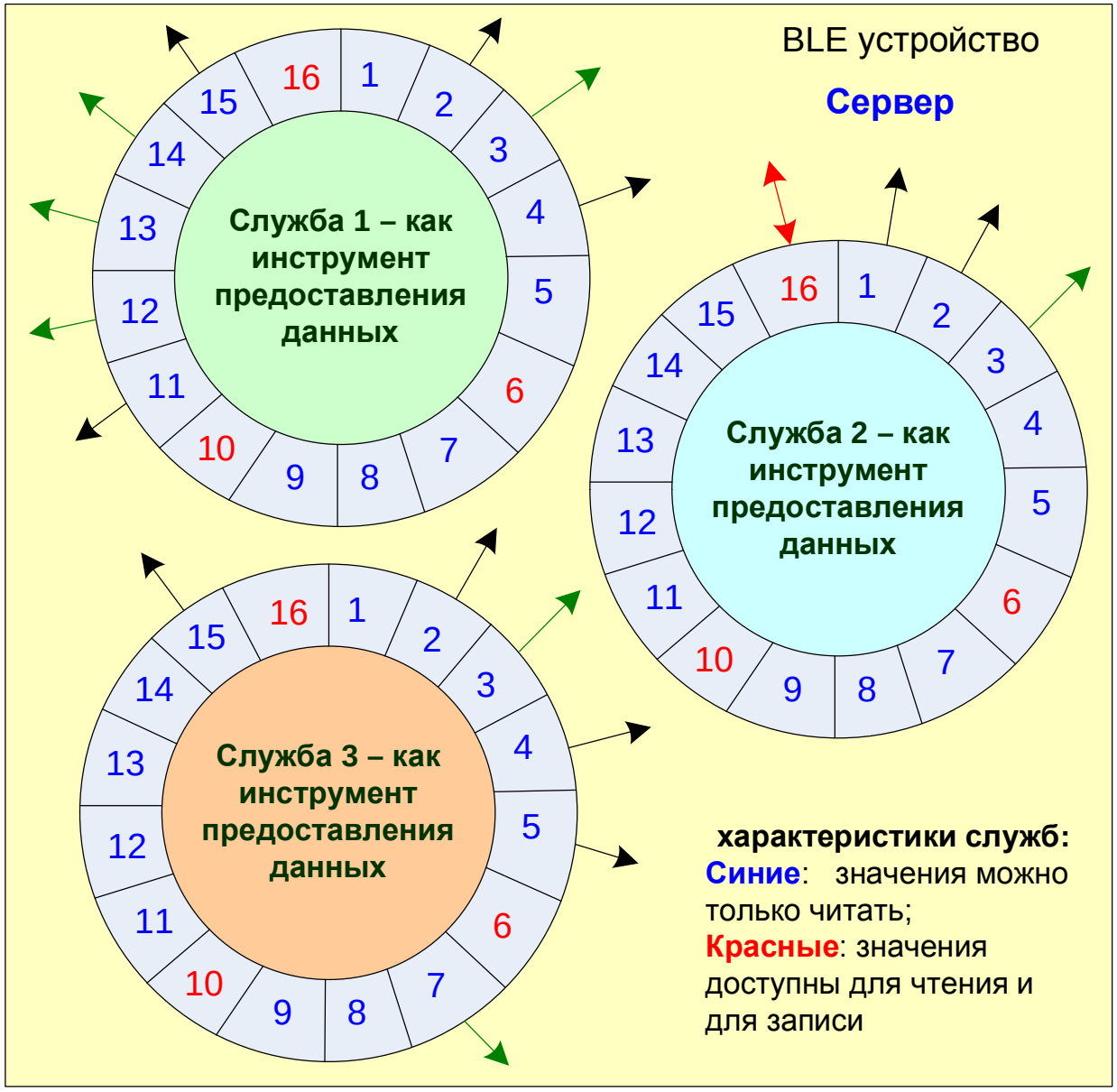



*Архитектура GATT (General Attribute Profile)*

Методы протокола ATT:

request - запрос;
response - ответ;
command - команда;
notification - уведомление;
indication - индикация;
confirmation - подтверждение.

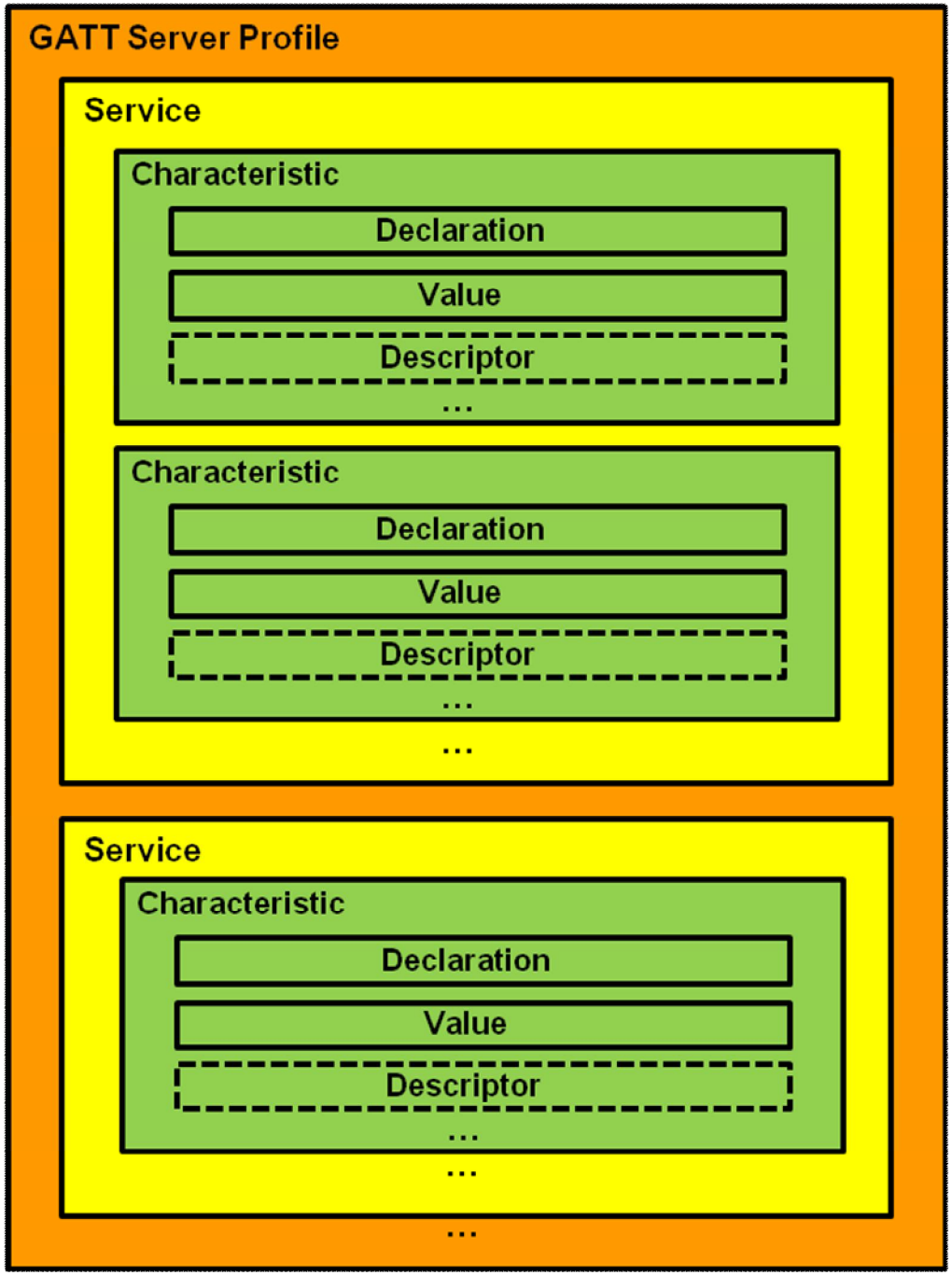
# Сервер, службы и характеристики



# Профиль общих атрибутов GATT

* В клиент-серверной терминологии **Сервер** – источник данных.
* Видов данных на сервере может быть много.
* Каждый вид данных в BLE называется **характеристикой**.
* Характеристики могут объединяться в группы – это **службы** BLE
* В составе BLE устройства может быть реализовано несколько служб.
* Формат представления доступных в BLE устройстве служб и их характеристик носит название профиля общих атрибутов GATT

Профиль общих атрибутов GATT устанавливает иерархию сервисов и характеристик BLE




# Generic Attribute Profile (GATT)

Каждая характеристика должна включать 2 обязательных параметра:

- **Декларация** – наименование характерситики;
- **Значение** – собственно значение характеристики

и необязательные параметры для «тонкой» настройки характеристики:

- Дескритпор 1
- Дескритпор 2
- Дескритпор 3

....

Каждая характеристика может обладать правом (Permission) на чтение, на запись или на то и другое.

....

# Атрибуты GATT/ATT

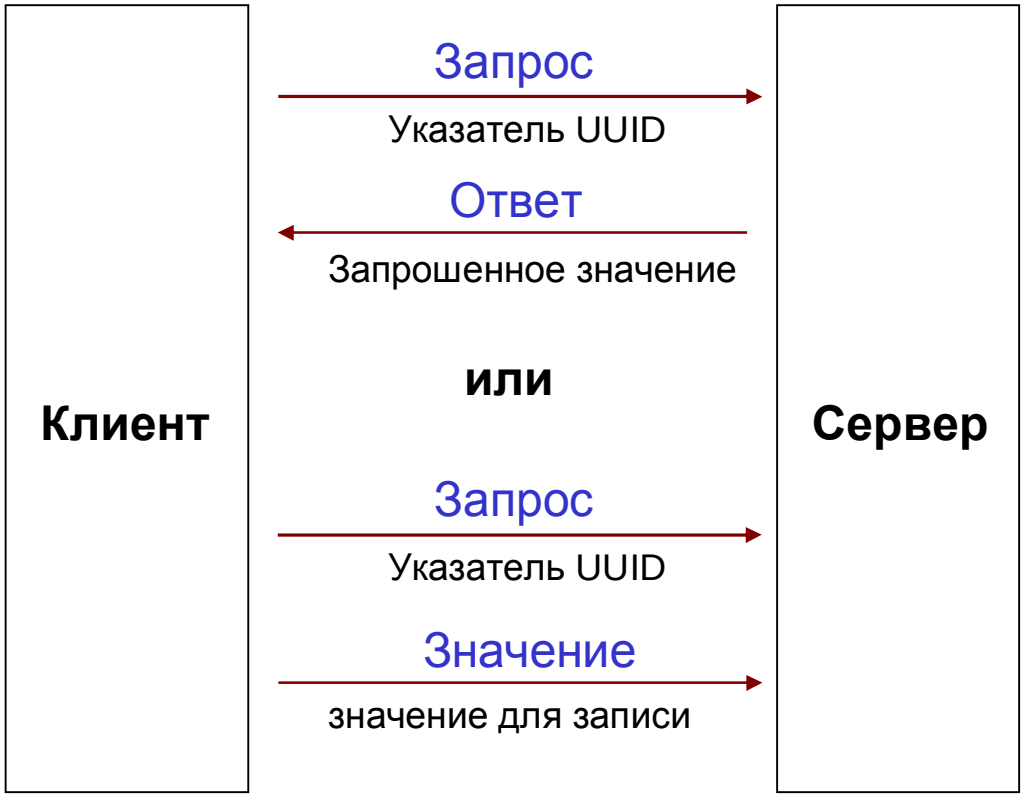
**Атрибут GATT/ATT**

Указатель (UUID)

Тип значения (UUID)

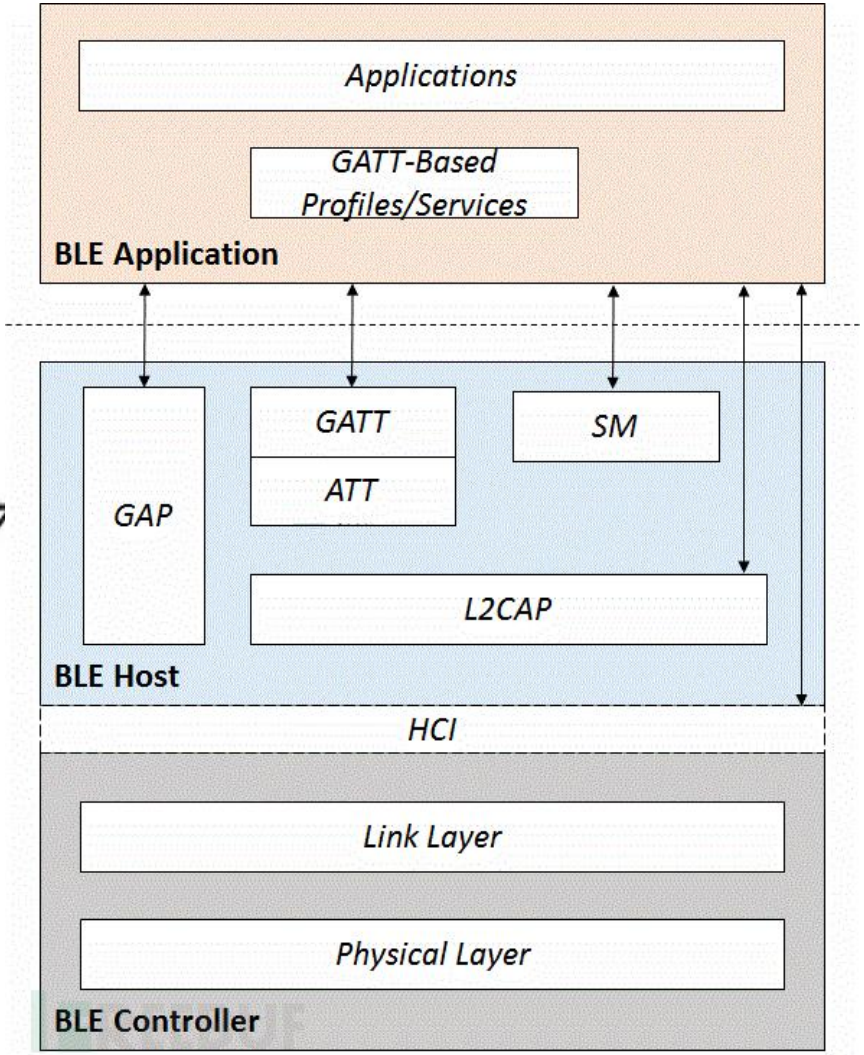
Значение

Тип доступа: R,W, R/W

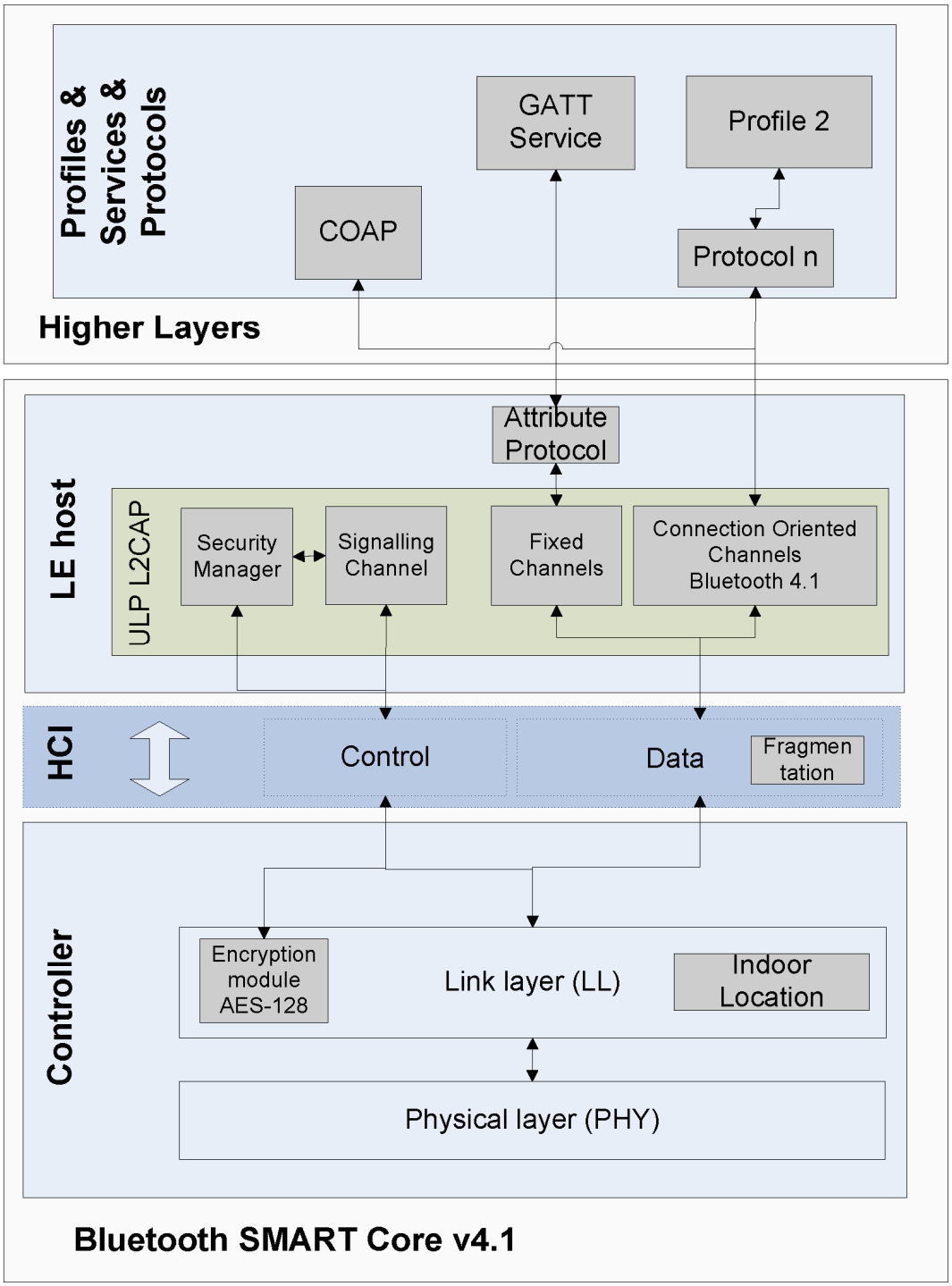



**Обмен атрибутами**

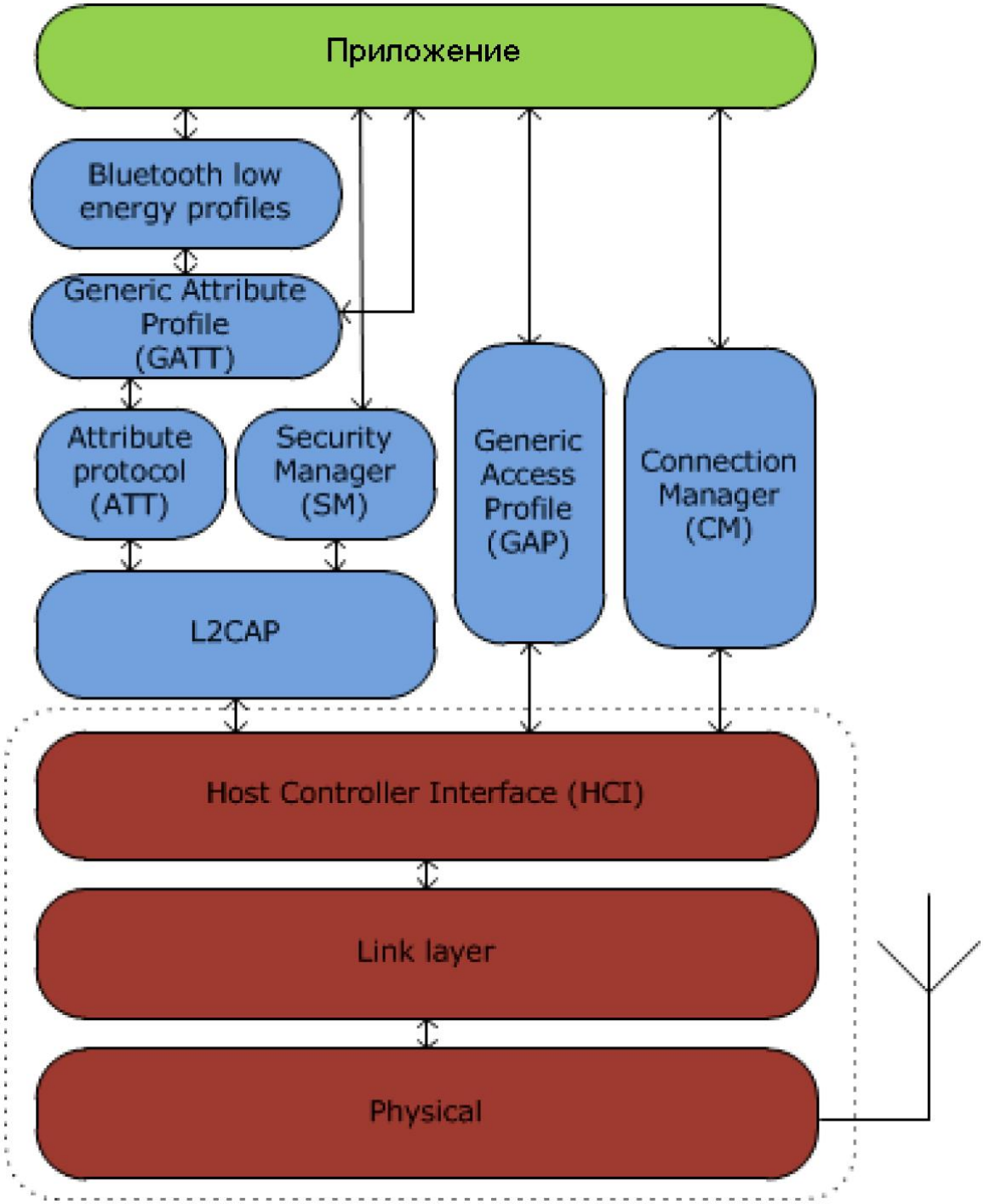
# Структура стека протоколов BLE

# Иерархическая модель BLE (идея)



# Иерархическая модель BLE (факт)




Узел сети: HOST

Контроллер

# Значения атрибутов

Attributes have values

- array of octets
- 0 to 512 octets in length
- can be fixed or variable length

| Value |
| --- |
| 0x54656d7065726174757265205365e736f72 |
| 0x04 |
| 0x0802 |

# Дескриптор атрибута

Each attribute has a “handle”

used to address an individual attribute by a client

Clients use handles to address attributes

Read (0x0022) => 0x04 ; Read (0x0098) => 0x0802

| Handle | Value |
|---|---|
| 0x0009 | 0x54656d7065726174757265205365e736f72 |
| 0x0022 | 0x04 |
| 0x0098 | 0x0802 |

# Тип атрибута UUID

Attributes have a type

type is a «UUID», determines what the value means

Types are defined by “Characteristic Specifications”

or Generic Access Profile or Generic Attribute Profile

| Handle | Type | Value |
|---|---|---|
| 0x0009 | «Device Name» | 0x54656d7065726174757265205365e736f72 |
| 0x0022 | «Battery State» | 0x04 |
| 0x0098 | «Temperature» | 0x0802 |

# Типы атрибутов

«Device Name»

defined by GAP

formatted as UTF-8

0x54656d70657261747572652053656e736f72 = “Temperature Sensor”

| Handle | Type | Value |
|---|---|---|
| 0x0009 | «Device Name» | “Temperature Sensor” |
| 0x0022 | «Battery State» | 0x04 |
| 0x0098 | «Temperature» | 0x0802 |

# Типы атрибутов

«Battery State»

defined by “Battery State Characteristic” specification

enumerated value

0x04 = Discharging

| Handle | Type | Value |
|---|---|---|
| 0x0009 | «Device Name» | “Temperature Sensor” |
| 0x0022 | «Battery State» | Discharging |
| 0x0098 | «Temperature» | 0x0802 |

# Типы атрибутов

«Temperature»

defined by “Temperature Characteristic” specification

Signed 16 bit Integer in 0.01 ºC

0x0802 = 2050 * 0.01 ºC = 20.5 ºC

| Handle | Type | Value |
|---|---|---|
| 0x0009 | «Device Name» | “Temperature Sensor” |
| 0x0022 | «Battery State» | Discharging |
| 0x0098 | «Temperature» | 20.5 ºC |

# Типы атрибутов

Type is a «UUID»

UUIDs are 128 bits in length

Bluetooth defines a Bluetooth Base UUID

allowing a 16 bit «UUID» to be defined

0000**xxxx**-0000-1000-8000-00805F9B34FB

0000**1234**-0000-1000-8000-00805F9B34FB

= 16 bit UUID 0x**1234**

# Идентификаторы UUID

**UUID** (*universally unique identifier* - универсальный уникальный идентификатор. Использование и формирование **UUID** регламентируется стандартом идентификации Open Software Foundation (OSF), используемый при разработке программного обеспечения для распределенных приложений (среды распределённых вычислений).

Основное назначение UUID - это позволить ПО или другим распределенным объектам уникально идентифицировать информацию без центра координации.

# Атрибуты служб GATT

Атрибуты стандартных служб GATT имеют шаблон
**0000XXXX-0000-1000-8000-00805f9b34fb**,
где XXXX — это ID профиля, например:

1. 0x1800 — Generic Access
   UUID=**00001800-0000-1000-8000-00805f9b34fb**;
2. 0x1801 — Generic Attribute
   UUID=**00001801-0000-1000-8000-00805f9b34fb**;
3. 0x180A — Device Information
   UUID=**0000180A-0000-1000-8000-00805f9b34fb.**

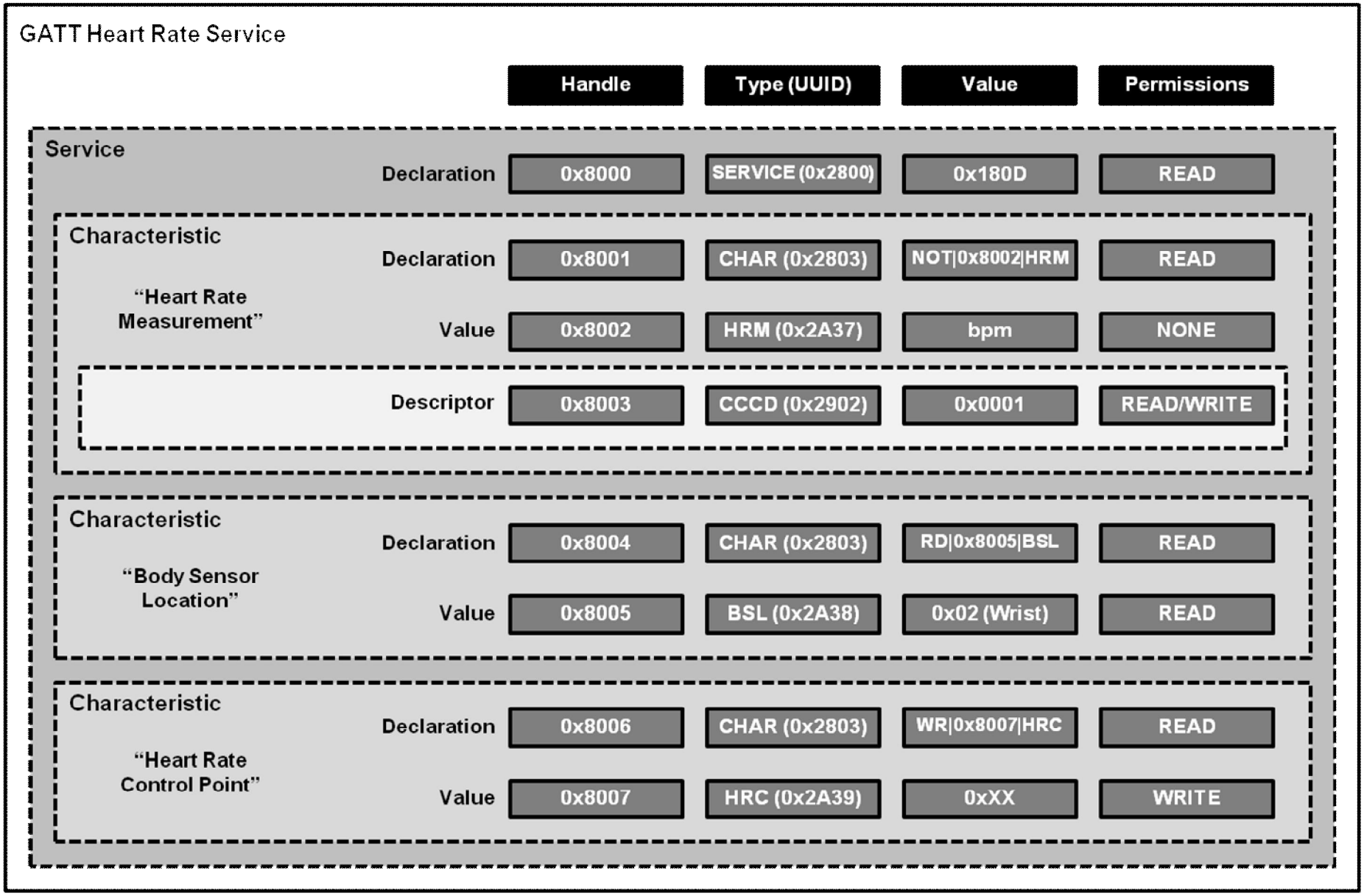
В устройствах BLE кроме стандартных профилей (служб) GATT реализуются пользовательские GATT-службы:

- Датчик температуры: **f000aa00-0451-4000-b000-000000000000**
- Датчик влажности: **f000aa20-0451-4000-b000-000000000000**
- Акселерометр: **f000aa10-0451-4000-b000-000000000000**
- Магнетометр: **f000aa30-0451-4000-b000-000000000000**
- Барометр: **f000aa40-0451-4000-b000-000000000000**
- Гироскоп: **f000aa50-0451-4000-b000-000000000000**

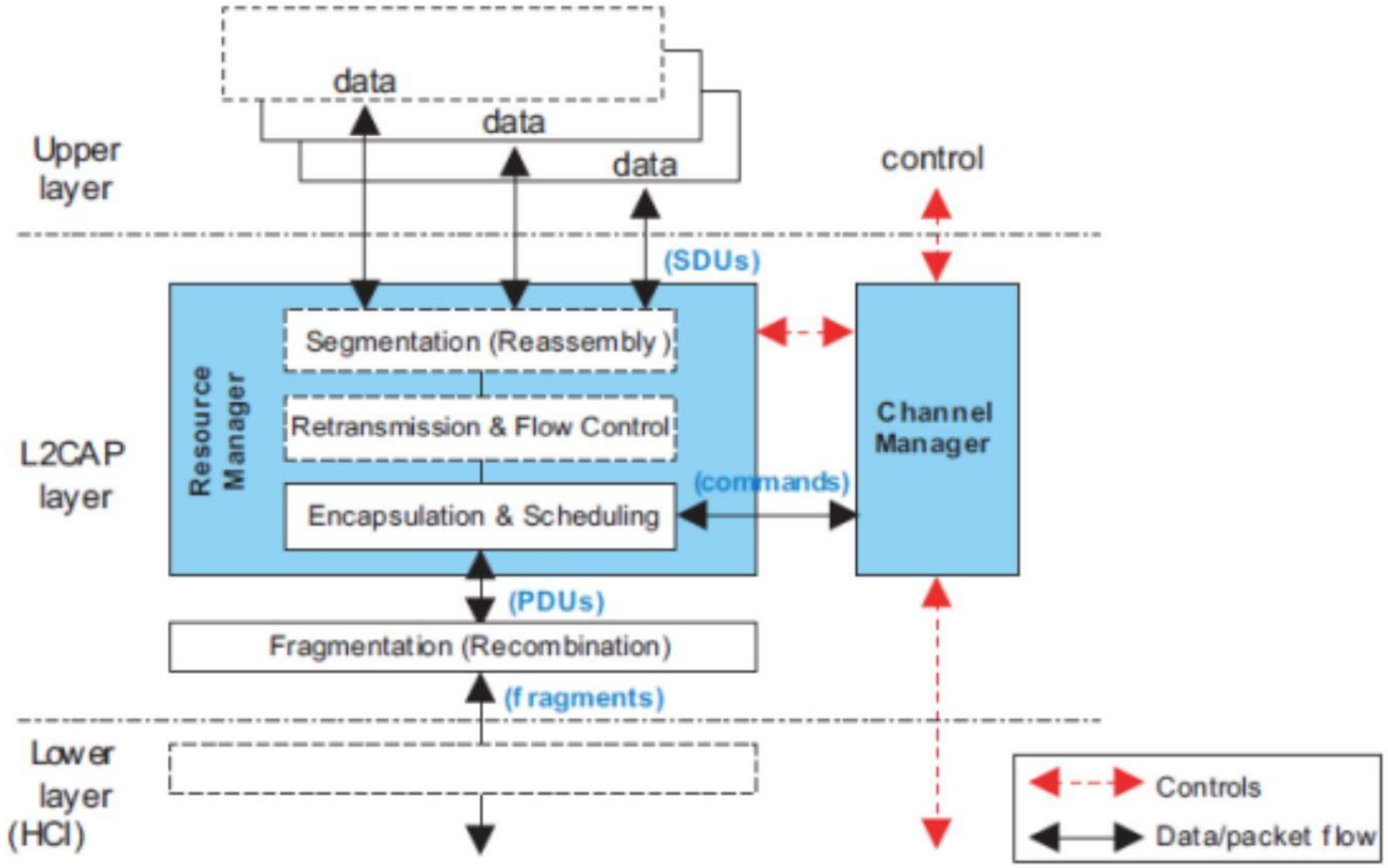
# Пример профиля GATT для BLE термометра

| Handle | Type | Value | Permissions |
|---|---|---|---|
| 0x0001 | «Primary Service» | «GAP» | R |
| 0x0002 | «Characteristic» | {r, 0x0003, «Device Name»} | R |
| 0x0003 | «Device Name» | “Temperature Sensor” | R |
| 0x0004 | «Characteristic» | {r, 0x0006, «Appearance»} | R |
| 0x0006 | «Appearance» | «Thermometer» | R |
| 0x000F | «Primary Service» | «GATT» | R |
| 0x0010 | «Characteristic» | {r, 0x0012, «Attribute Opcodes Supported»} | R |
| 0x0012 | «Attribute Opcodes Supported» | 0x00003FDF | R |
| 0x0020 | «Primary Service» | «Temperature» | R |
| 0x0021 | «Characteristic» | {r, 0x0022, «Temperature Celsius»} | R |
| 0x0022 | «Temperature Celsius» | 0x0802 | R* |

# Пример профиля GATT для службы мониторинга сердечной деятельности



# Logical Link Control and Adaptation Layer Protocol (L2CAP)



# Виды каналов L2CAP

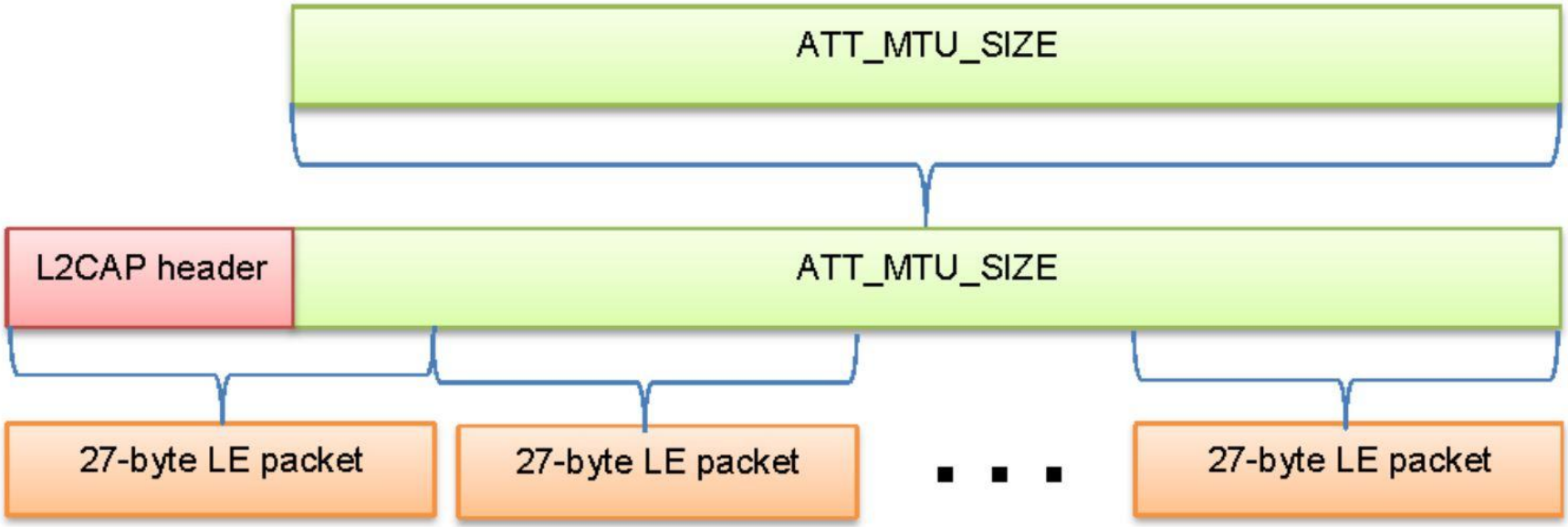
В соответствии с моделью BLE v.4.1 уровень L2CAP может поддерживать работу с фиксированными (дискретными, **fixed**) и непрерывными (ориентированными на постоянное соединение, **connection-oriented**) логическими каналами.

Дискретный логический канал существует только при установленном физическом соединении на время передачи или приема сообщения. Существует три типа дискретных каналов: для доставки сигнализации (1), для службы Security Manager (2) и канал для доставки сообщений протокола GATT/ATT (3). **В BLE v.4 реализованы только дискретные логические каналы**.

Поле **Channel ID** определяет принадлежность сообщения определенному логическому каналу. Значения **Channel ID** в диапазоне от 0x0001 до 0x003F относятся к дискретным каналам, идентификаторы с 0x0040 по 0xFFFF зарезервированы для непрерывных **connection-oriented** соединений (dynamically allocated)

| Channel Identifier | Use |
|---|---|
| 0x0000 | Reserved: cannot be used |
| 0x0001 | Bluetooth Classic signaling channel |
| 0x0002 | “Connectionless” channel |
| 0x0003 | AMP manager protocol |
| 0x0004 | Attribute Protocol |
| 0x0005 | LE signaling channel |
| 0x0006 | Security Manager Protocol |
| 0x0007 to 0x003E | Reserved: may be used in the future |
| 0x003F | AMP test protocol |
| 0x0040 to 0xFFFF | Connection-oriented channels |

# Структура пакета L2CAP

# Пакеты BLE

BLE Packet

| Preamble | Access Address | Protocol Data Unit (PDU) | CRC |
|---|---|---|---|
| 1 Byte | 4 Bytes | 2-257 Bytes | 3 Bytes |

Data Channel PDU

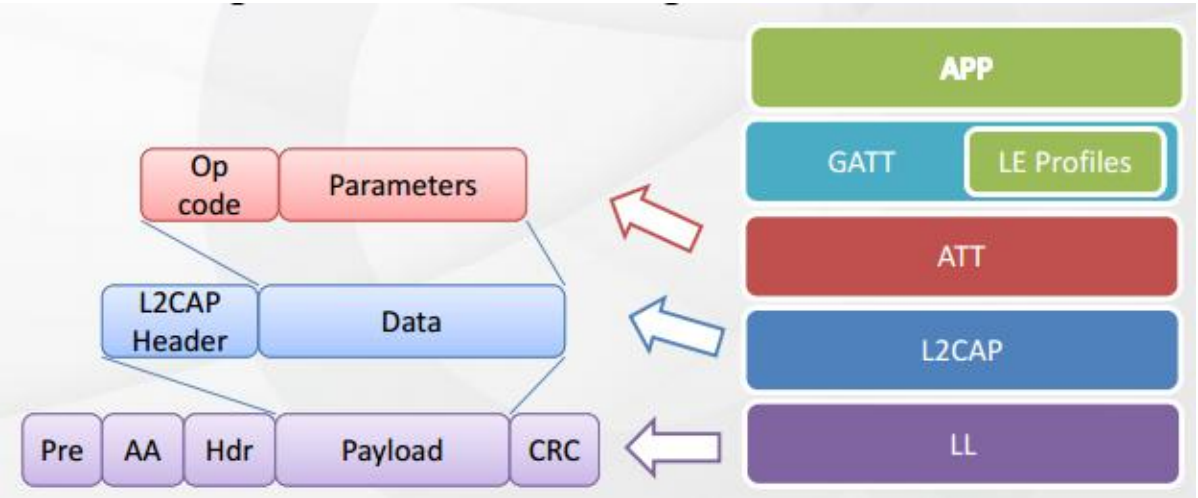
| 2 | ≤ 251 | 4 | |
|---|---|---|---|
| PDU He | | MIC | LL |

Для режима «connection»

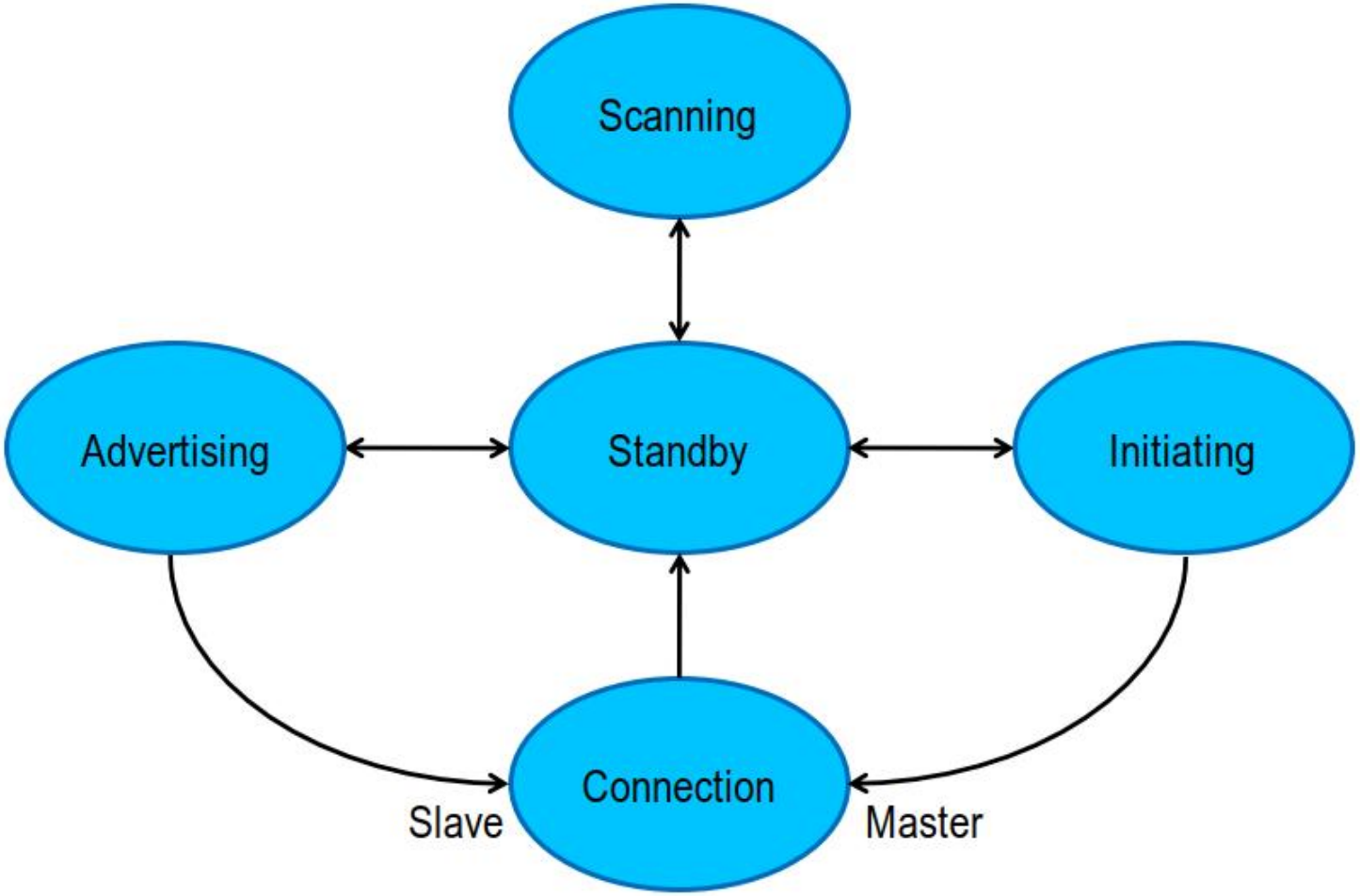
| 4 | ≤ 247 | |
|---|---|---|
| L2 He | | L2CAP |

| 1 | ≤ 246 | |
|---|---|---|
| Op | Par/Pay | ATT |

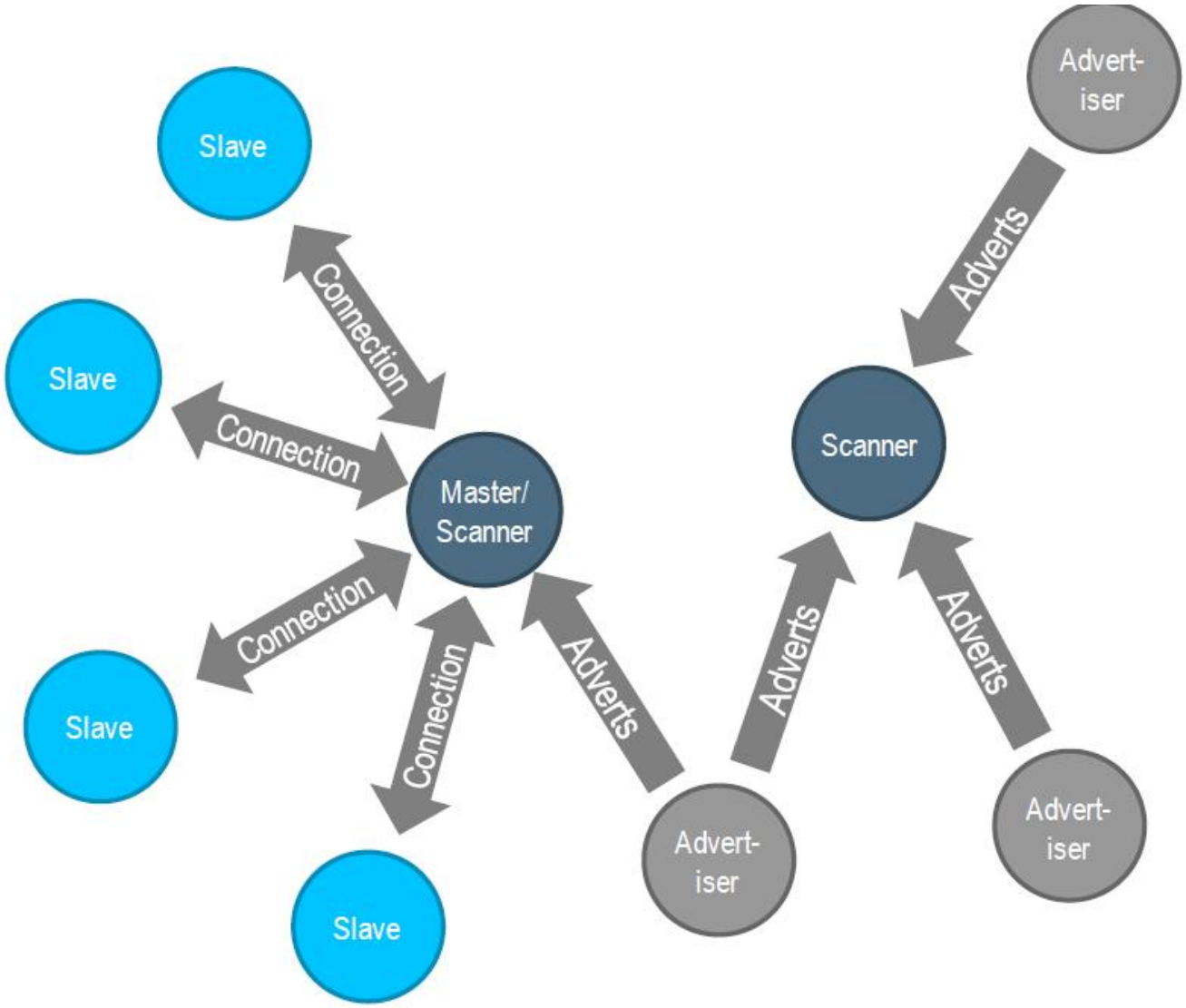
In BLE v4.0 and v4.1 the maximum ATT Parameter+Payload size is 22 bytes.



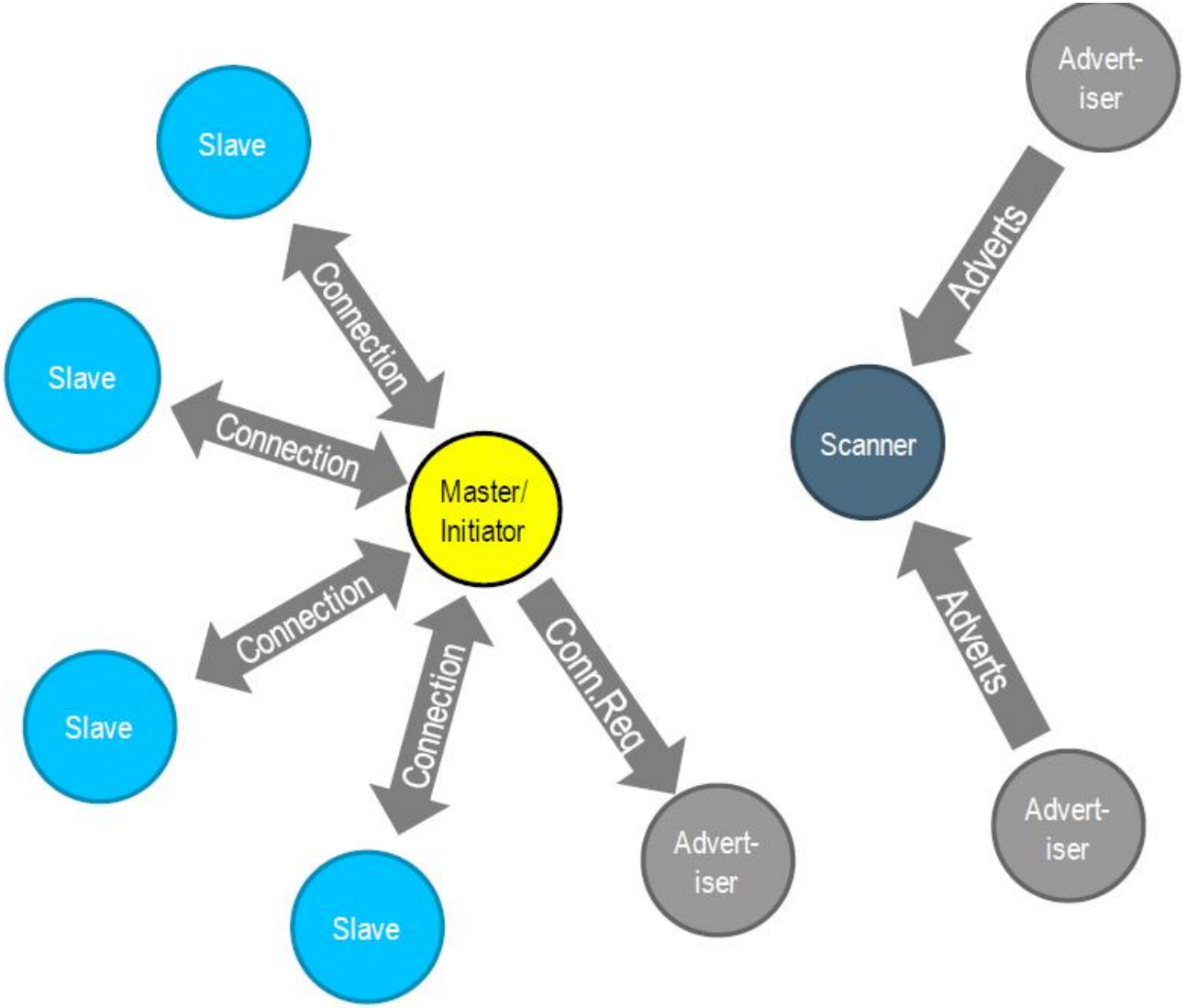
# Диаграмма состояний BLE устройства на канальном уровне



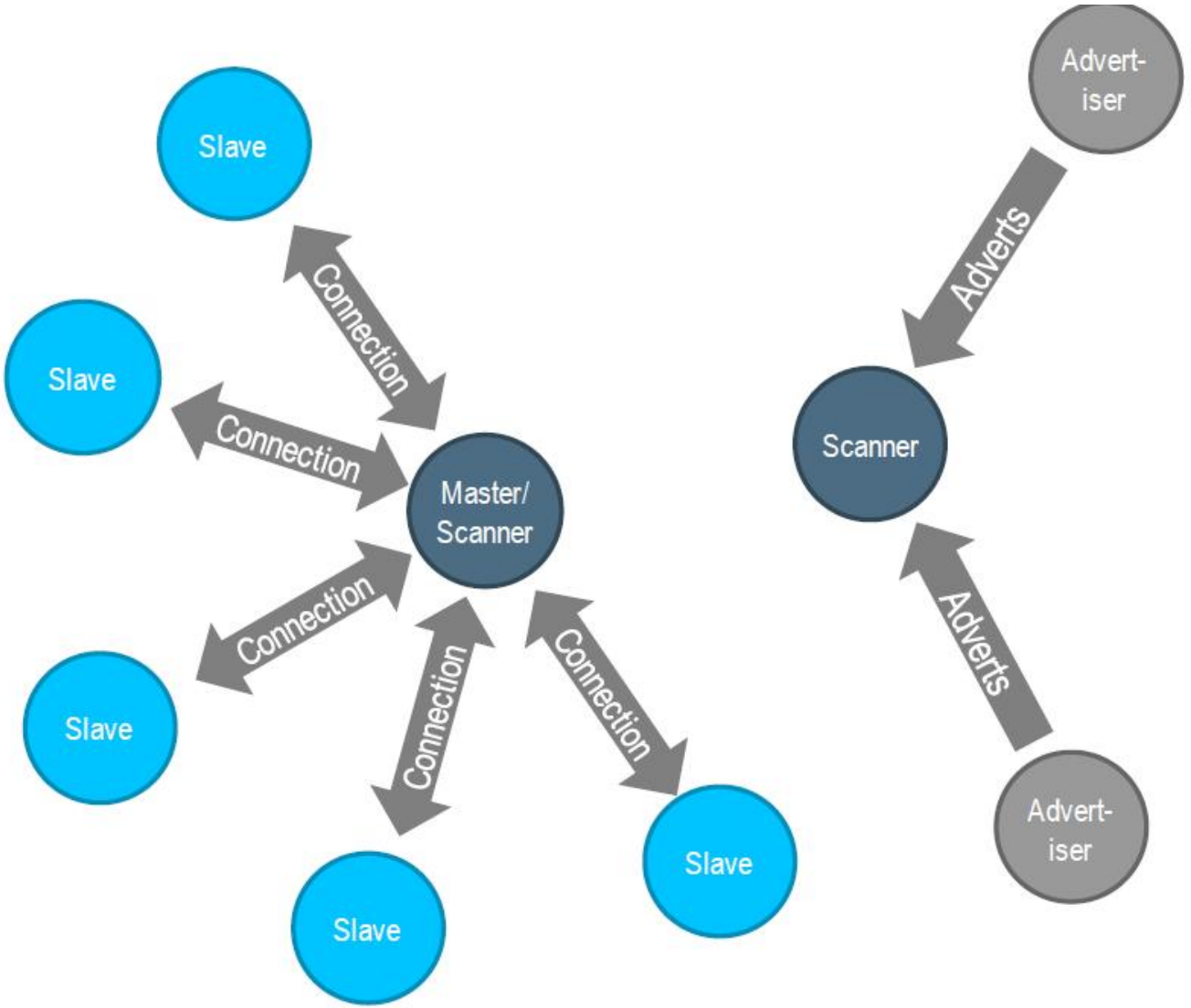
# Топология пикосети



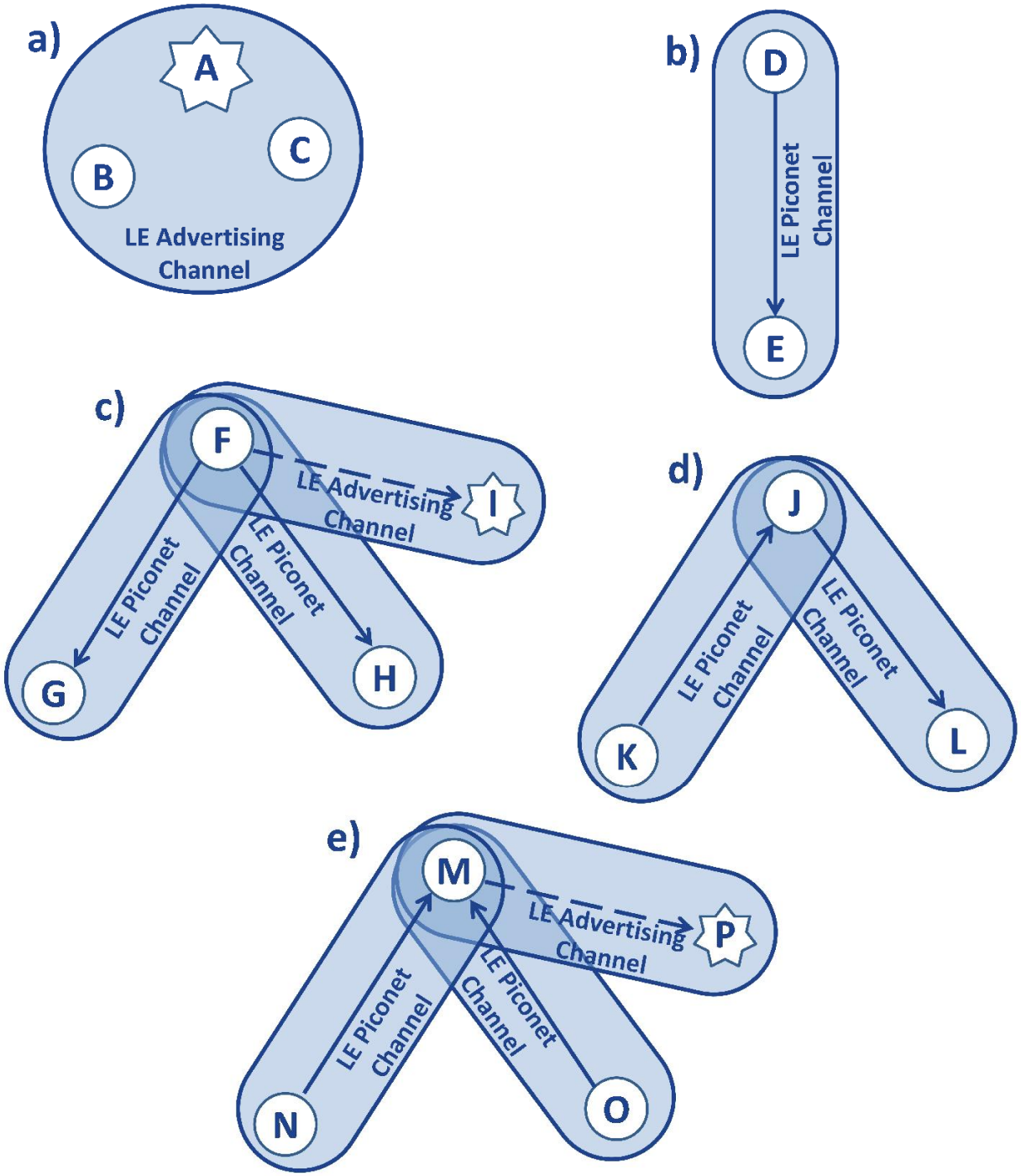
# Топологии BLE: запрос на присоединение вещателя к пикосети



# Топологии BLE: расширение пикосети



# Топологии BLE



# Физический уровень BLE

| Feature | Value |
|---|---|
| Frequency band | 2.4GHz (2402Mhz - 2480MHz |
| Modulation | GFSK, 1 Mbps |
| Modulation index | 0.5 |
| Channel spacing | 2 MHz |
| Advertising channels | 3 |
| Data channels | 37 |
| Frequency hopping | Adaptive FHSS |

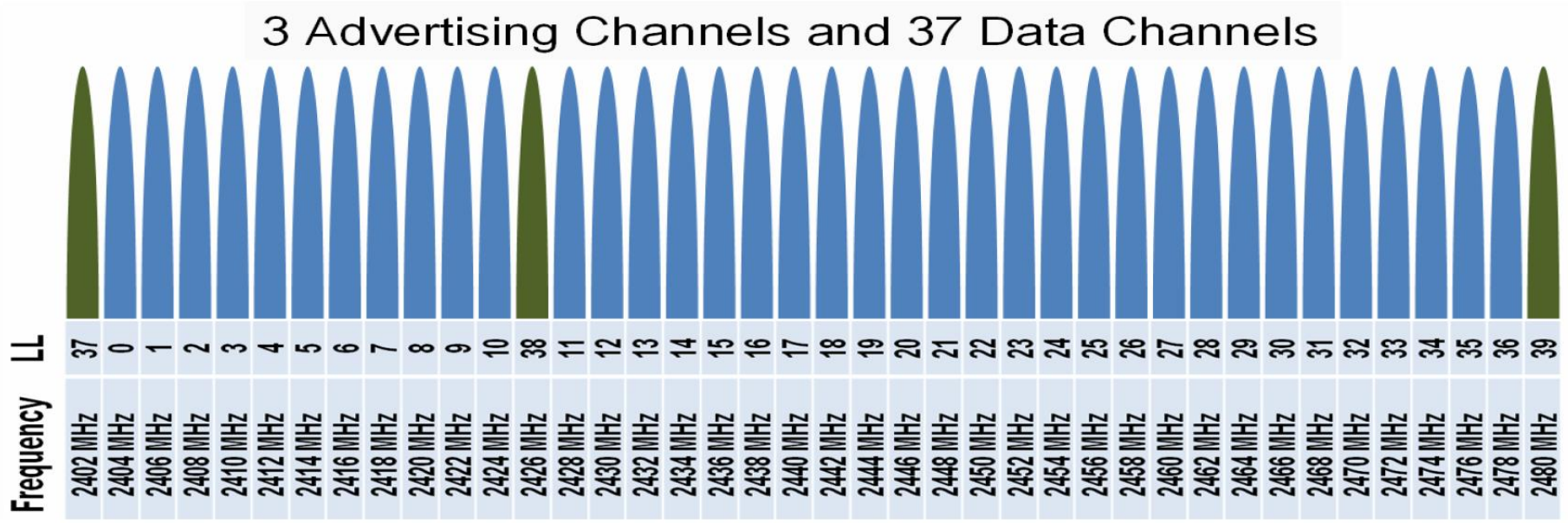
| Feature | Value |
|---|---|
| Minimum TX power | 0.01mW (-20 dBm) |
| Maximum TX power | 10 mW (10 dBm) |
| Minimum RX sensitivity | -70 dBm (BER 0.1%) |

| TX power | RX sensitivity | Range |
|---|---|---|
| 0 dBm | -70 dBm | ~30 meters |
| 10 dBm | -90 dBm | 100+ meters |

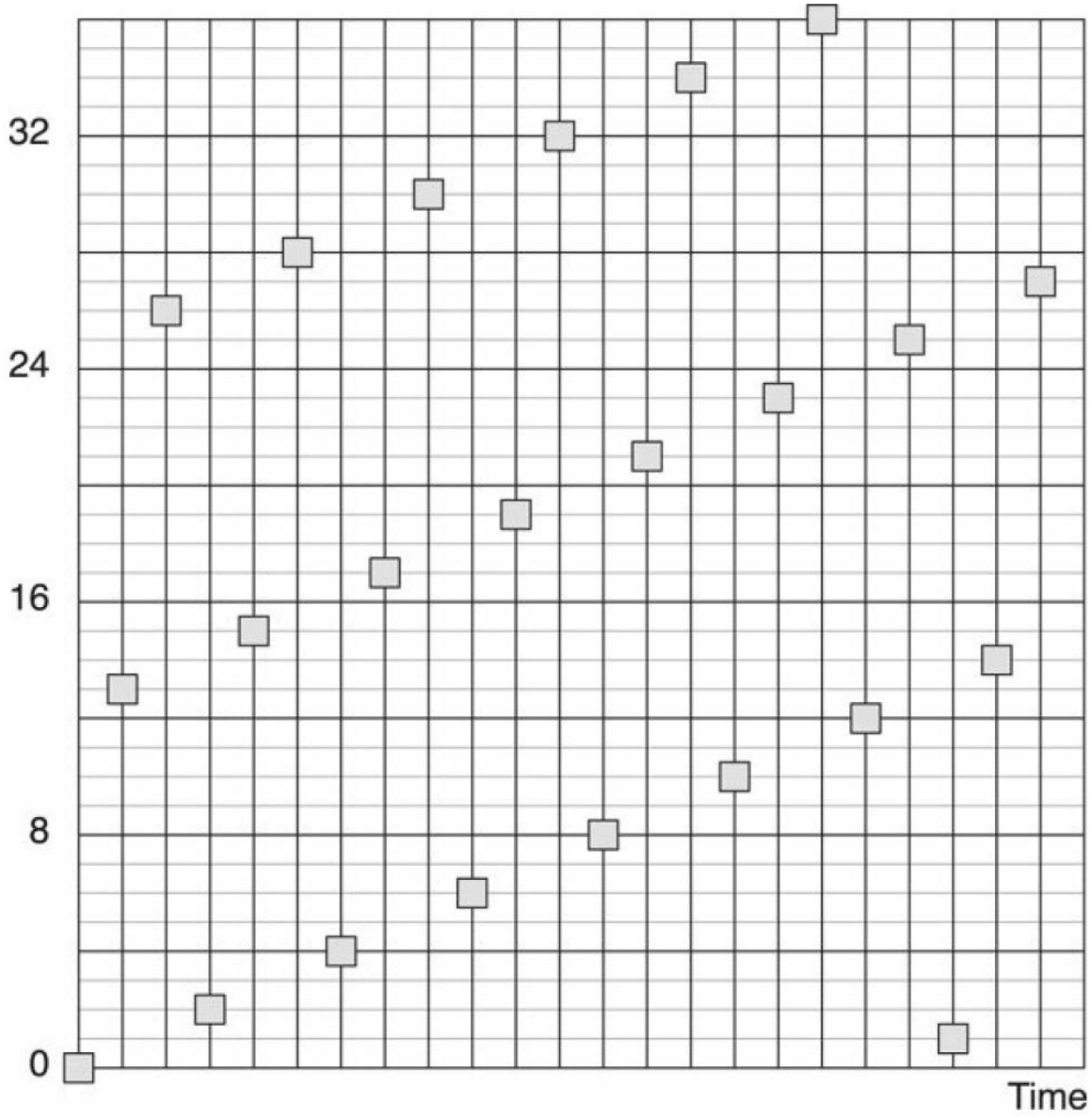
| Path Loss ($path\ loss$) | Distance ($d$) |
|---|---|
| 50dB | 2.5 m |
| 60dB | 6.3 m |
| 70dB | 16 m |
| 80dB | 40 m |
| 90dB | 100 m |
| 100dB | 250 m |
| 110dB | 630 m |

# Физический уровень BLE

- 2.4 GHz ISM band
- 1 Mbps GFSK
- 40 Channels - 2MHz spacing
- Frequency Hopping in connections
  - Pseudo-random
  - Set in connection request
- Transmit power
  - -20 to +10dBm
- Receive sensitivity
  - -70 dBm



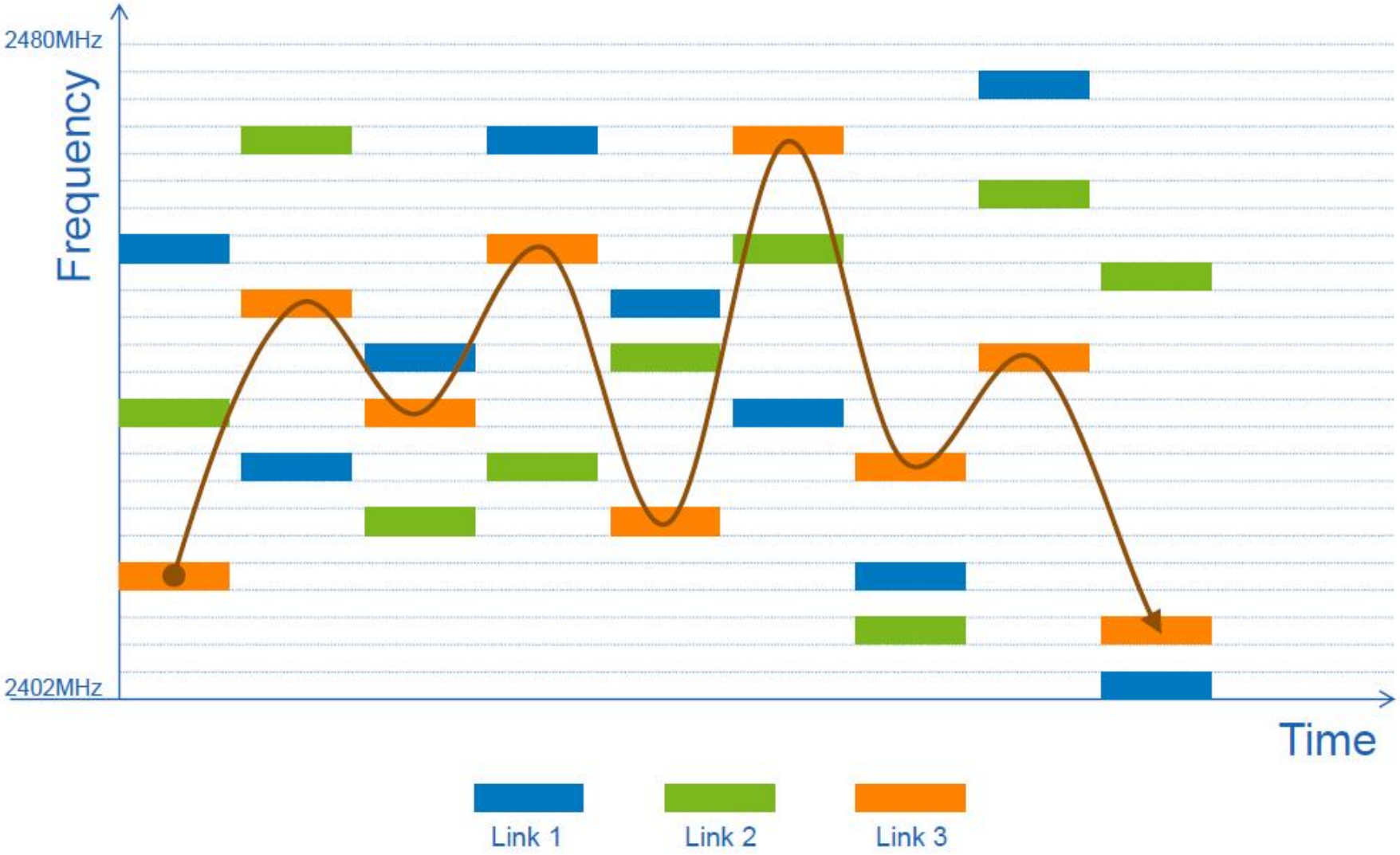
# Псевдослучайный выбор частоты несущего колебания в режиме Connection

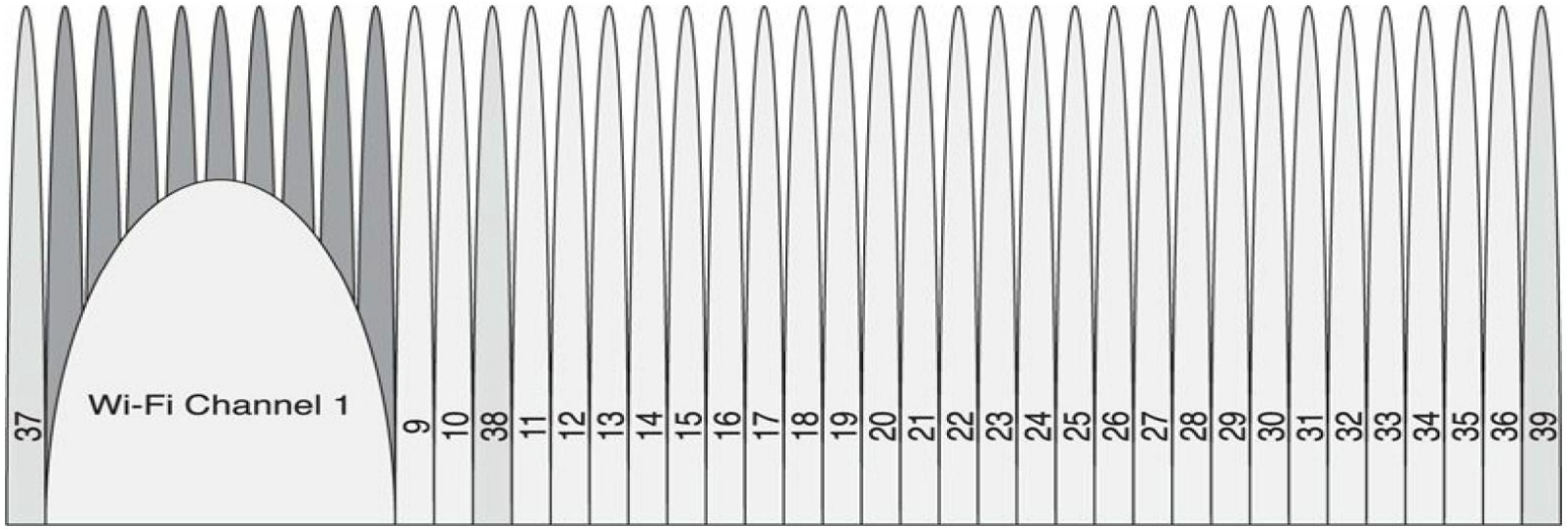



В режиме *Connection:*

$$f_{n+1} = (f_n + hop) \ mod \ 37$$

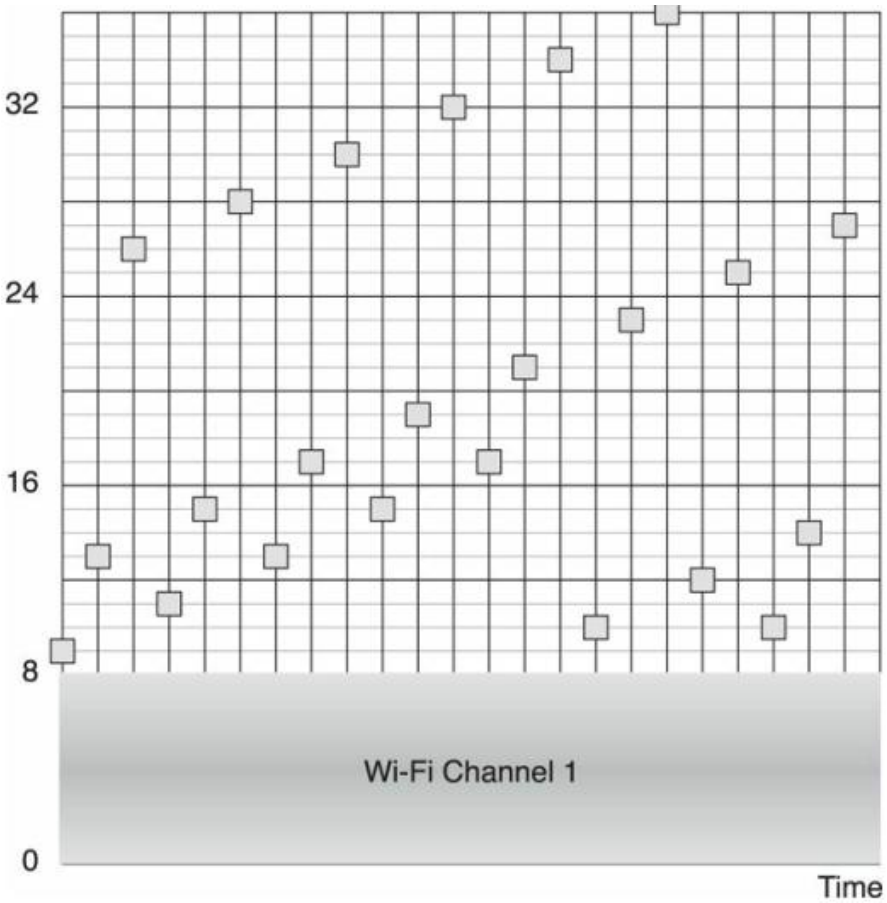
# Пример трех активных соединений BLE



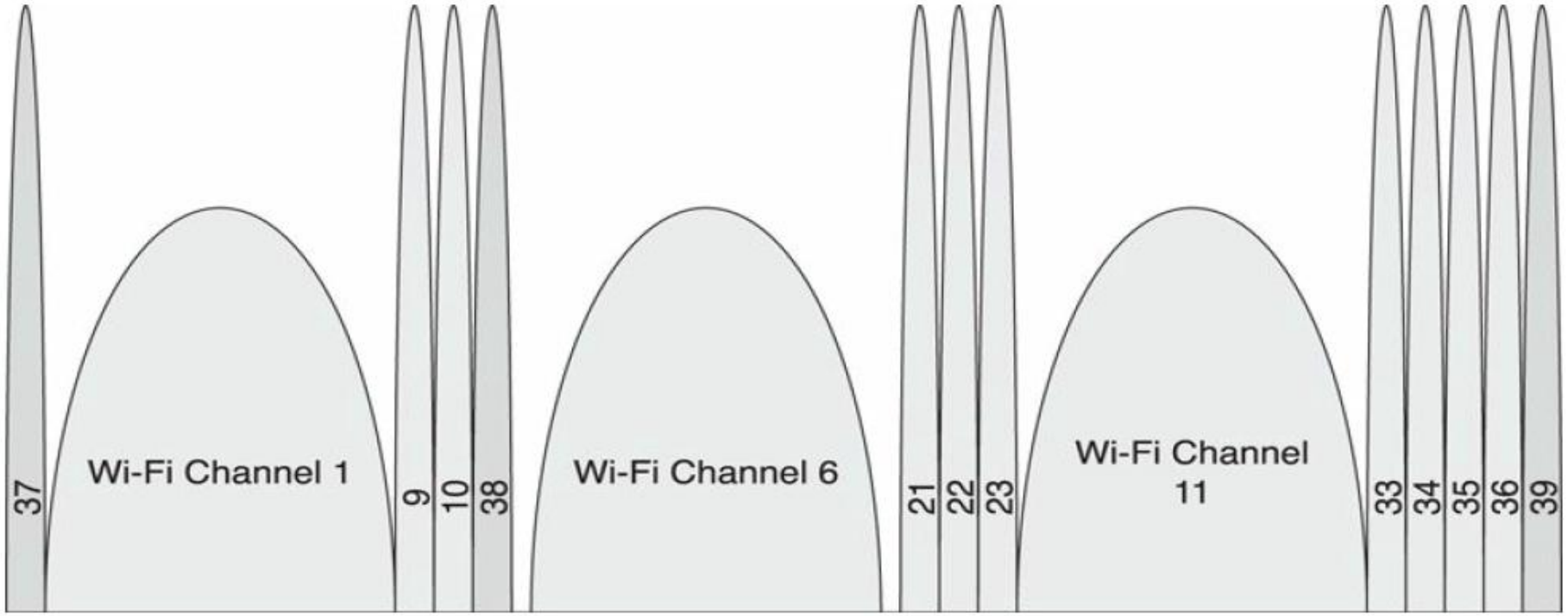



# Адаптивное изменение плана частотных скачков

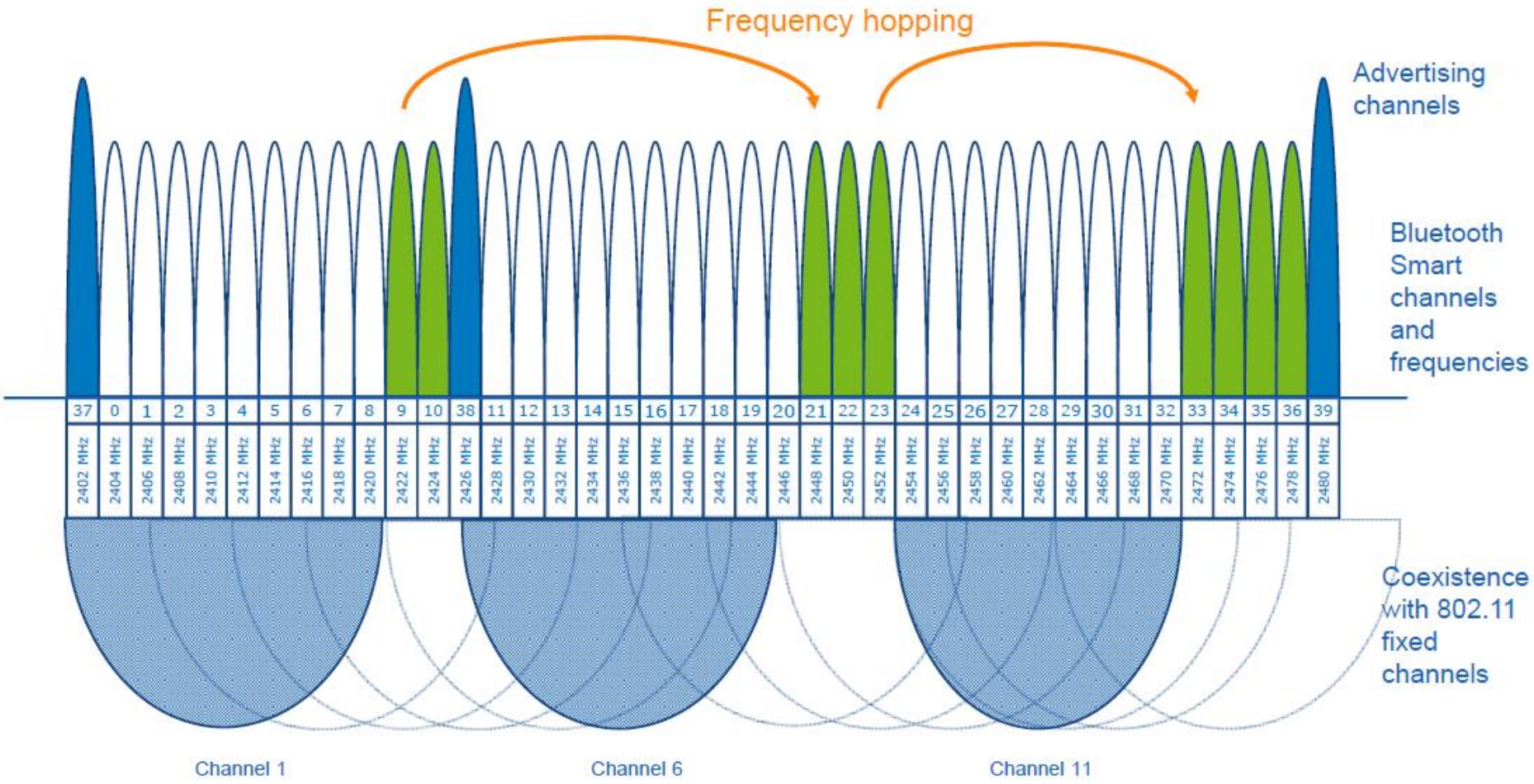
| Original Channel | Good/Bad | Remapped Channel |
|---|---|---|
| 0 | Bad | 9 |
| 13 | Good | 13 |
| 26 | Good | 26 |
| 2 | Bad | 11 |
| 15 | Good | 15 |
| 28 | Good | 28 |
| 4 | Bad | 13 |
| 17 | Good | 17 |
| 30 | Good | 30 |



# Использование частотного ресурса совместно с WIFI

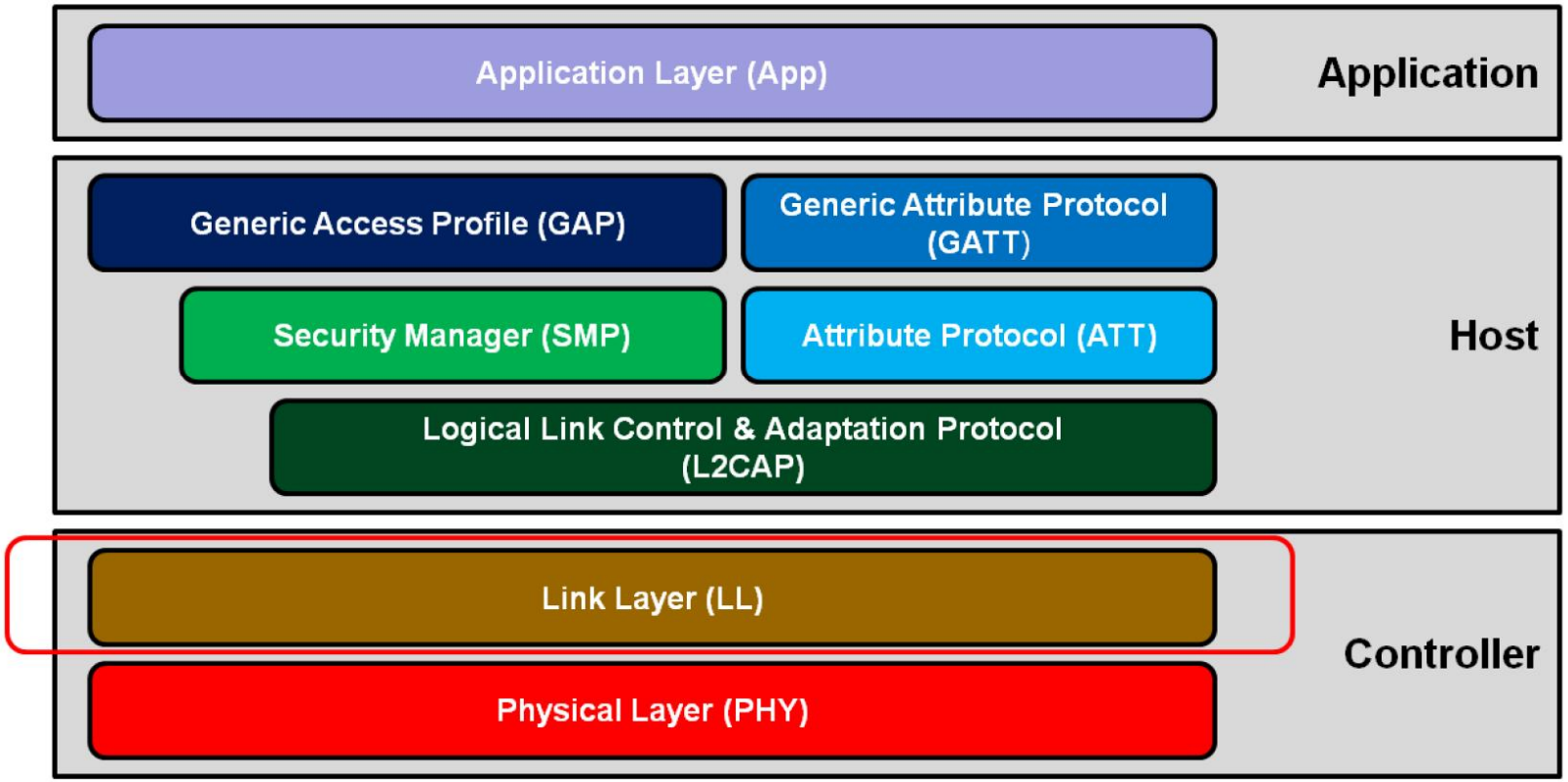


# Адаптивное изменение плана частотных скачков



# Канальный уровень BLE

## (Link Layer)



# Канальный уровень (Link layer)

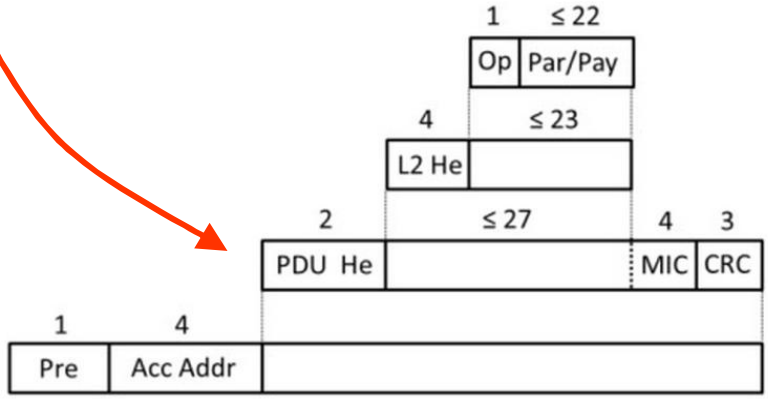
1 packet format

2 Protocol Data Unit types – Advertising or Data Channel

7 Advertising Protocol Data Unit Types

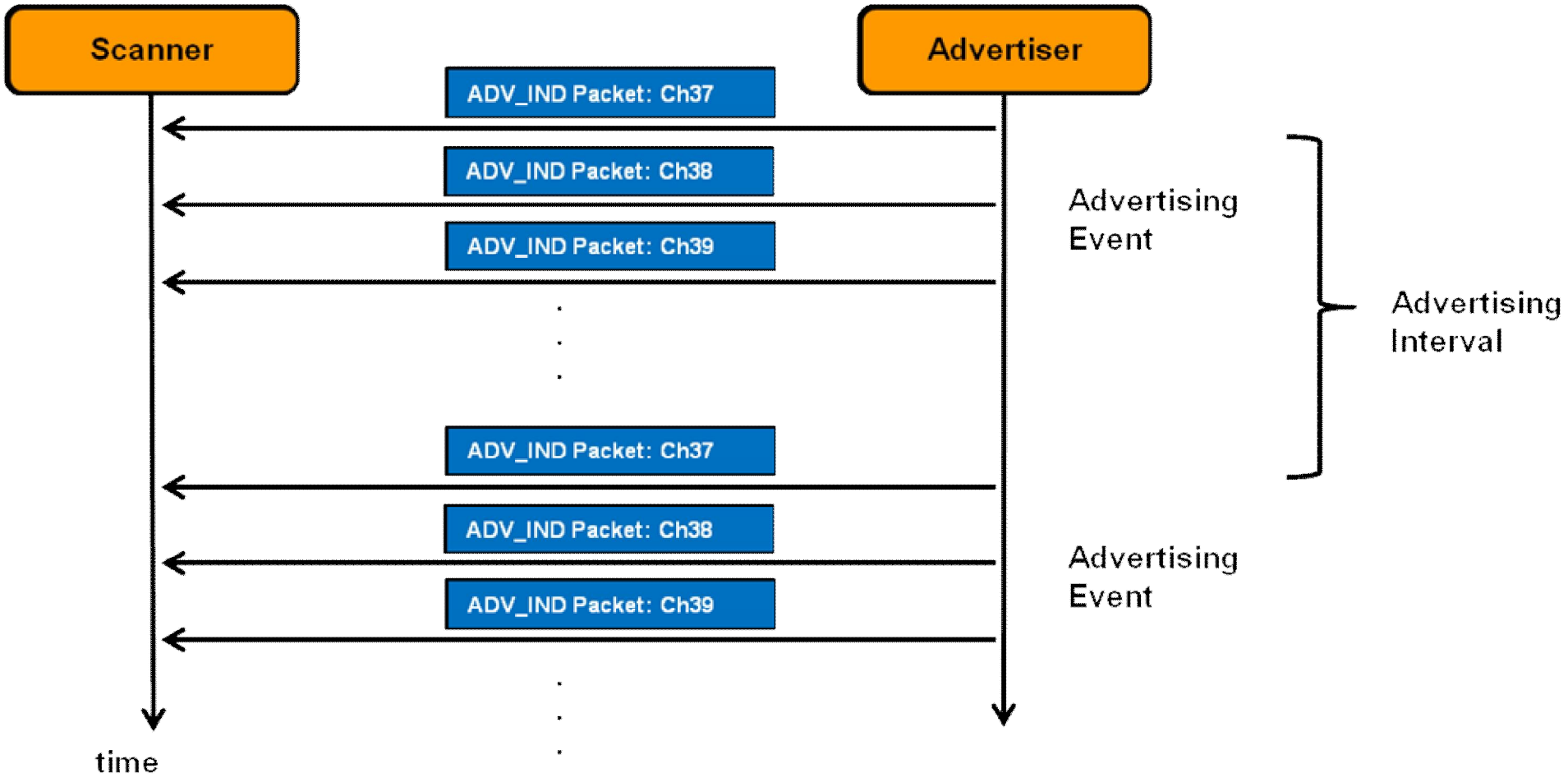
7 Link Layer Control Procedures

4 Advertising, 2 Scanning, 1 Connect-request

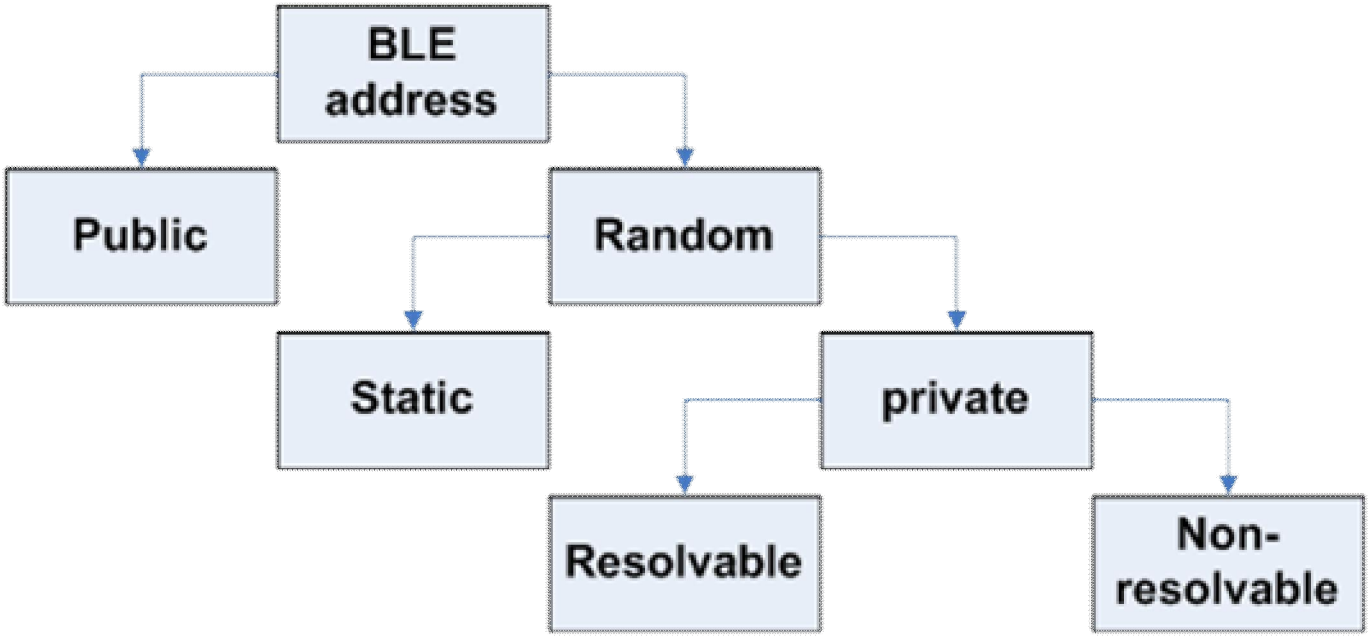



| | |
|---|---|
| Par/Pay: | Parameters and Payload |
| Op: | ATT Opcode |
| PDU He: | PDU Header |
| L2 He: | L2CAP Header |
| Acc Addr: | Access Address |
| Pre: | Preamble |
| MIC: | Message Integrity Check |
| CRC: | Cyclic Redundancy Check |

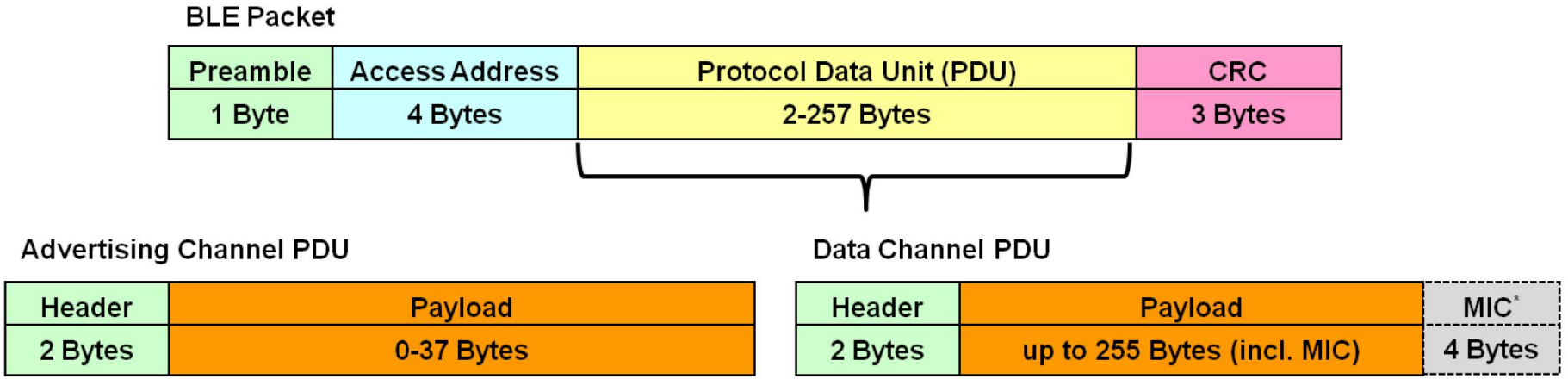
# Пассивное сканирование



# L2 адреса BLE устройств



# Пакеты физического и канального уровней BLE

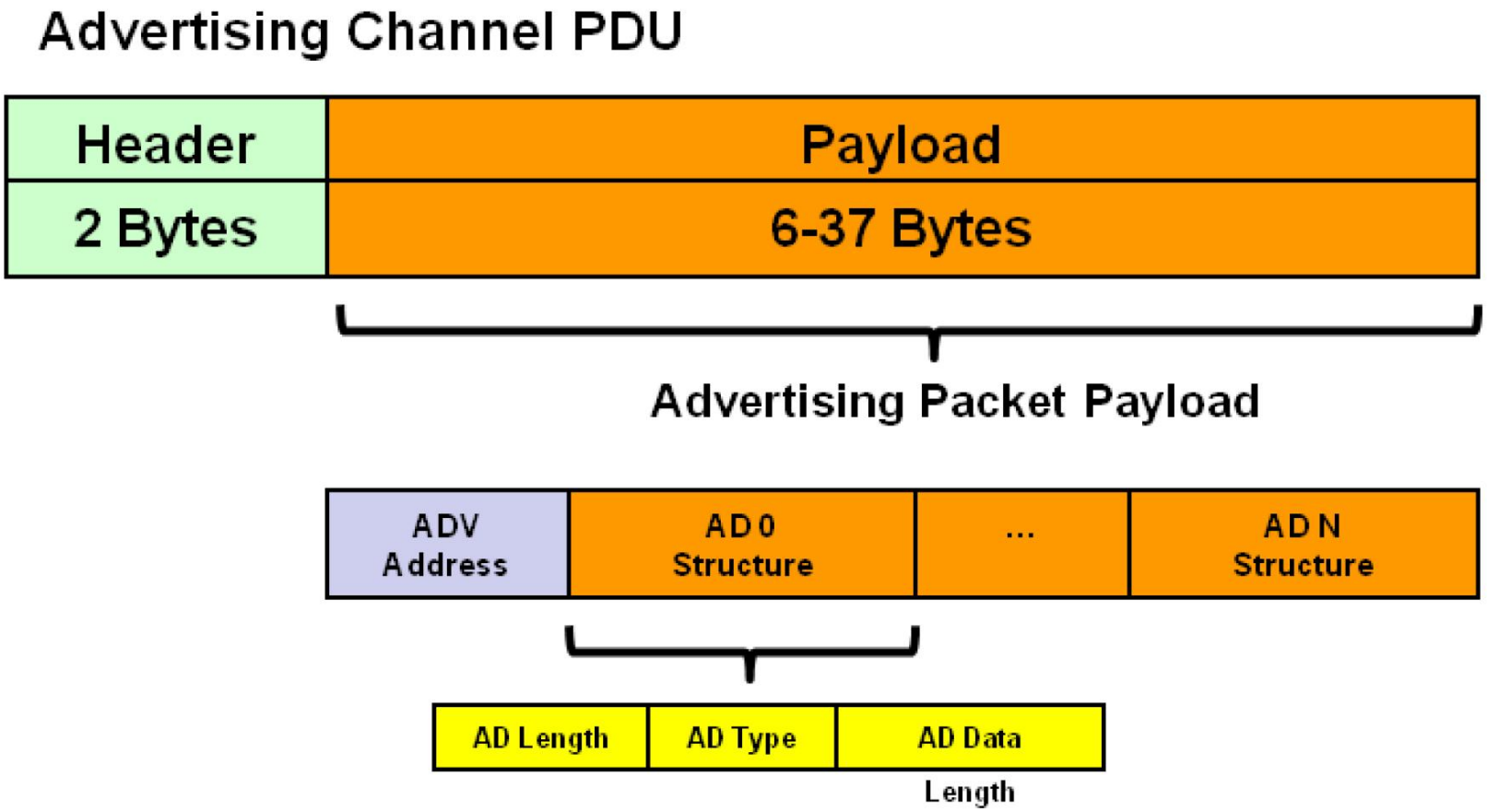



## Типы сообщений режима вещания

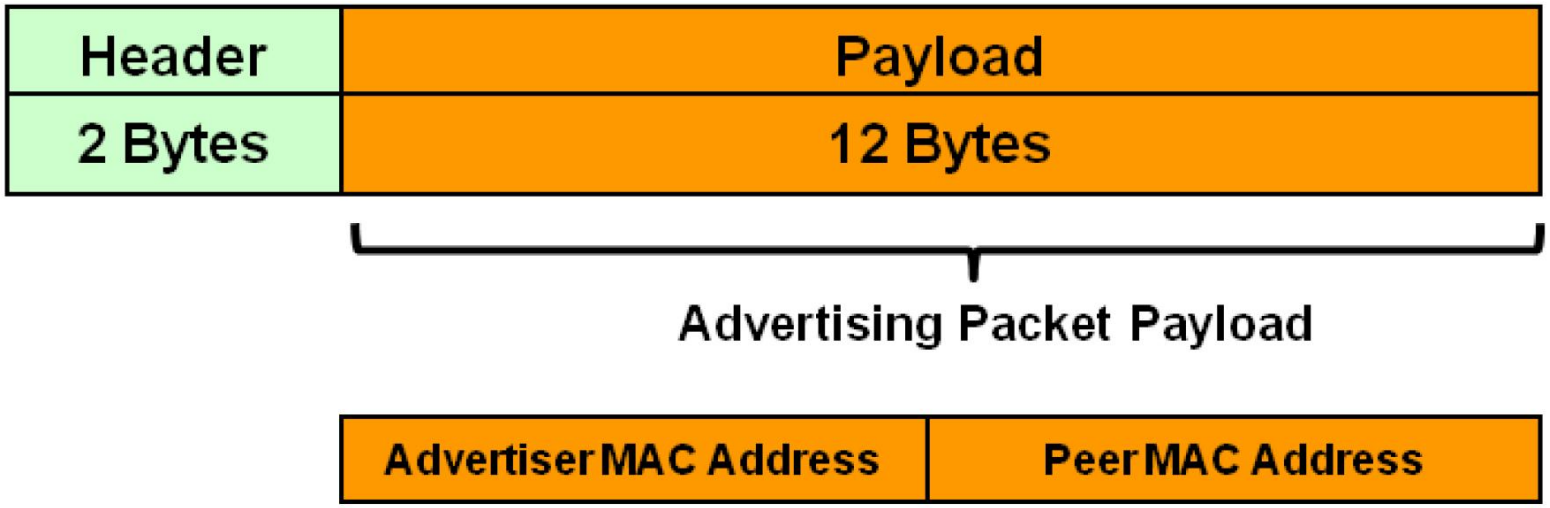
- **Advertising PDUs**
  - ADV_IND, ADV_DIRECT_IND, ADV_NONCONN_IND, ADV_SCAN_IND
- **Scanning PDUs**
  - SCAN_REQ, SCAN_RSP
- **Initiating PDUs**
  - CONNECT_REQ

| | |
|---|---|
| ADV_IND | Connectable Undirected Advertising |
| ADV_DIRECT_IND | Connectable Directed Advertising |
| ADV_NONCONN_IND | Non-Connectable Undirected Advertising |
| ADV_SCAN_IND | Scannable Undirected Advertising |

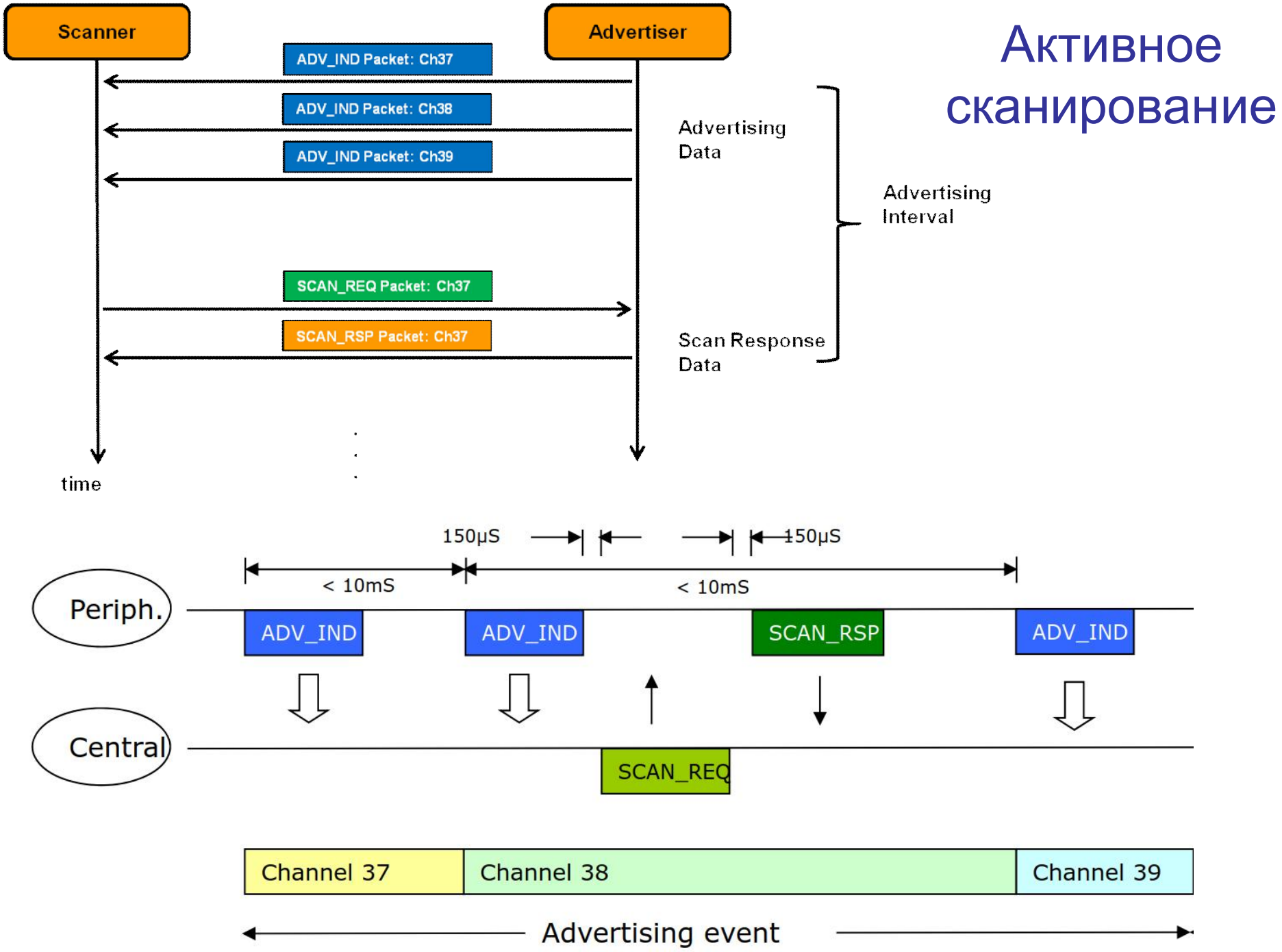
# Структура сообщения ADV_IND



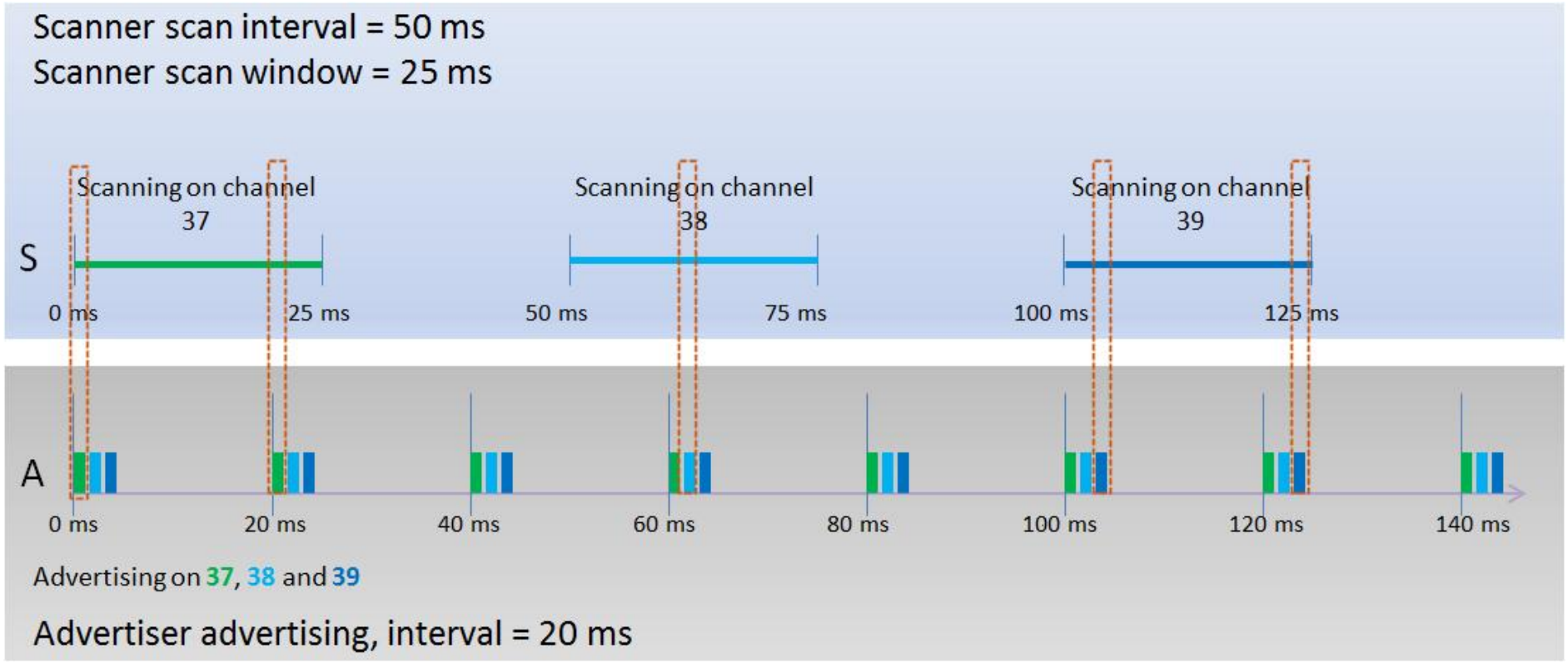
# Структура сообщения ADV_DIRECT_IND



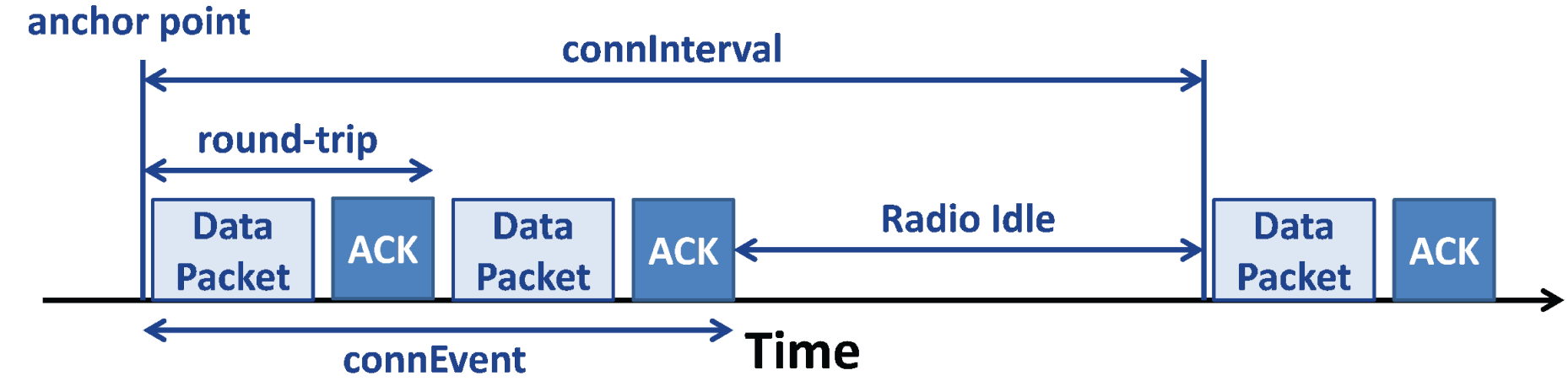
# Активное сканирование

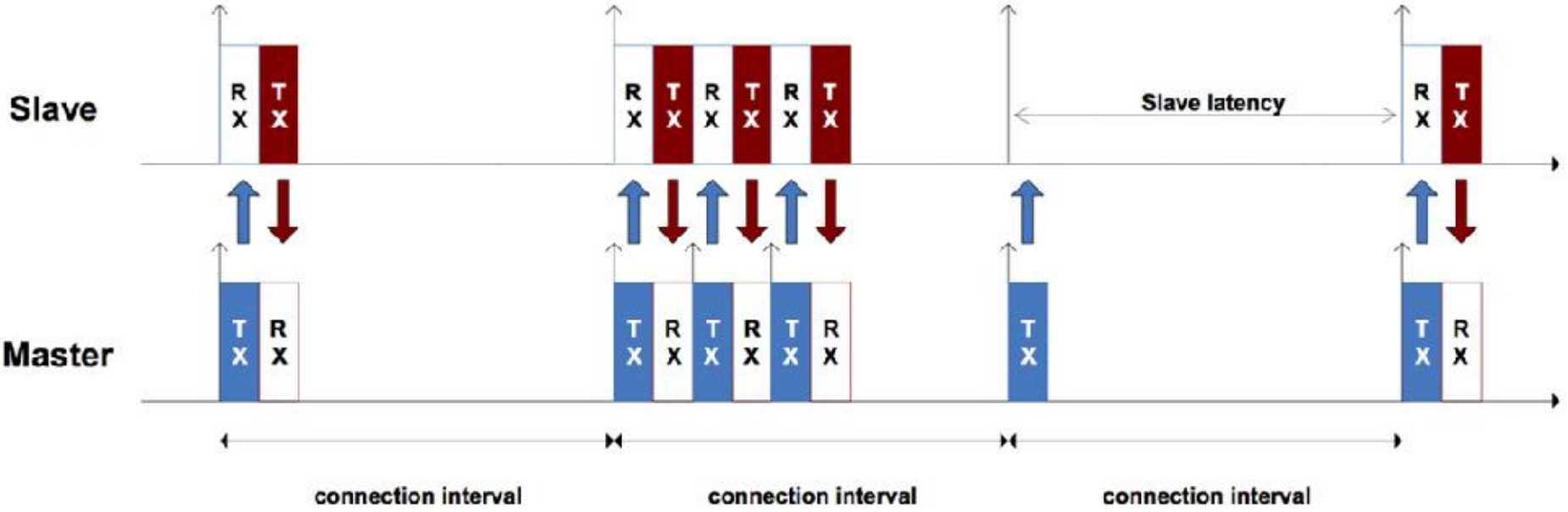


# Режим обнаружения узла BLE: процедуры вещания и сканирования

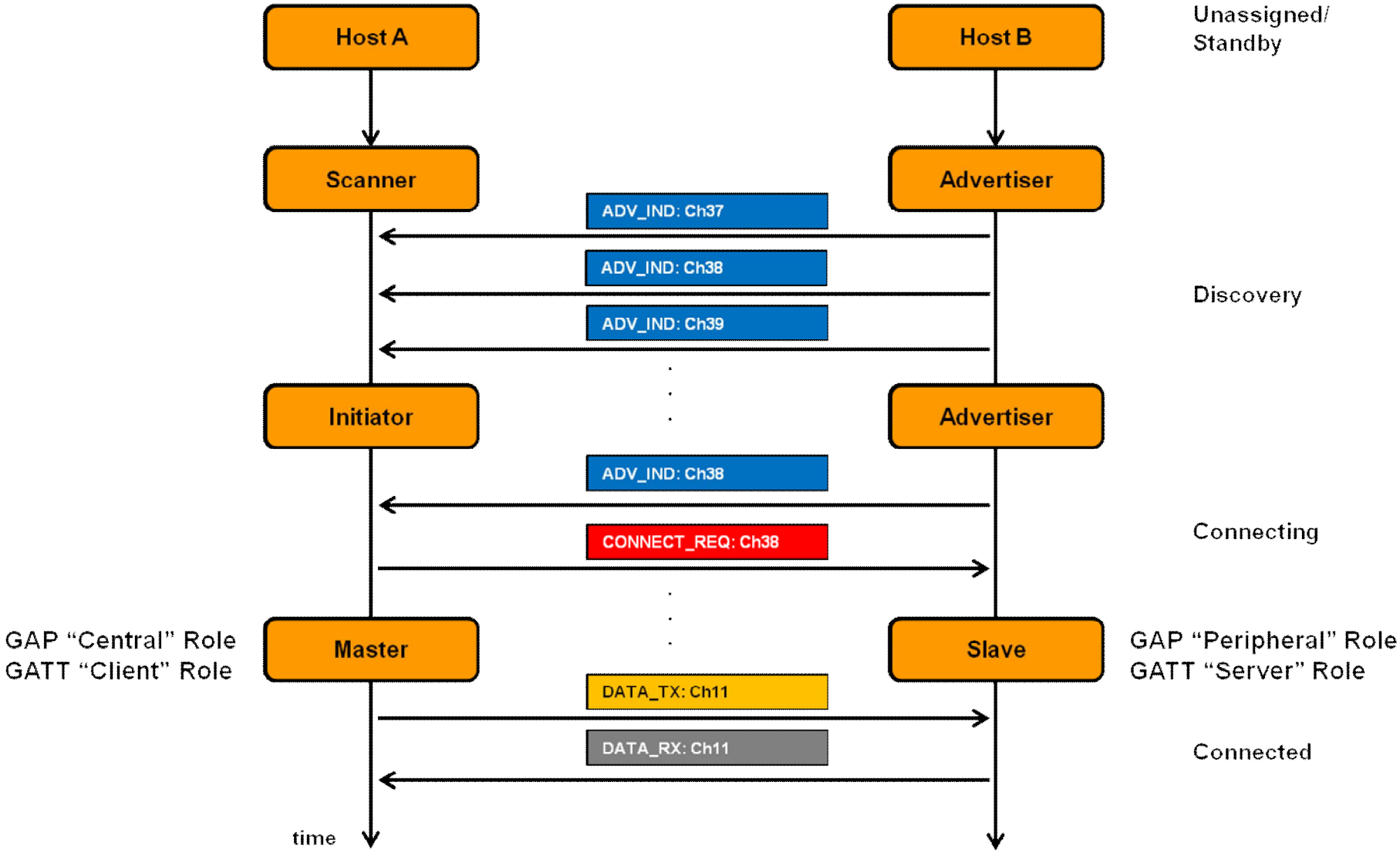


# Взаимодействие в режиме соединения

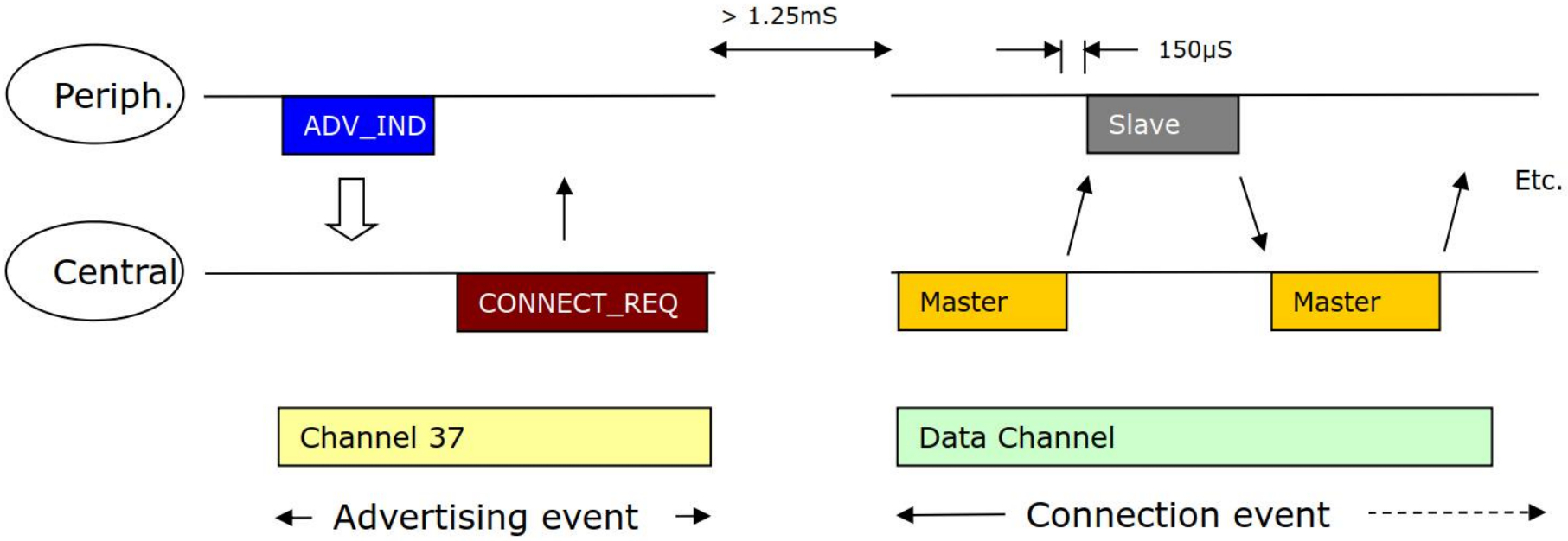


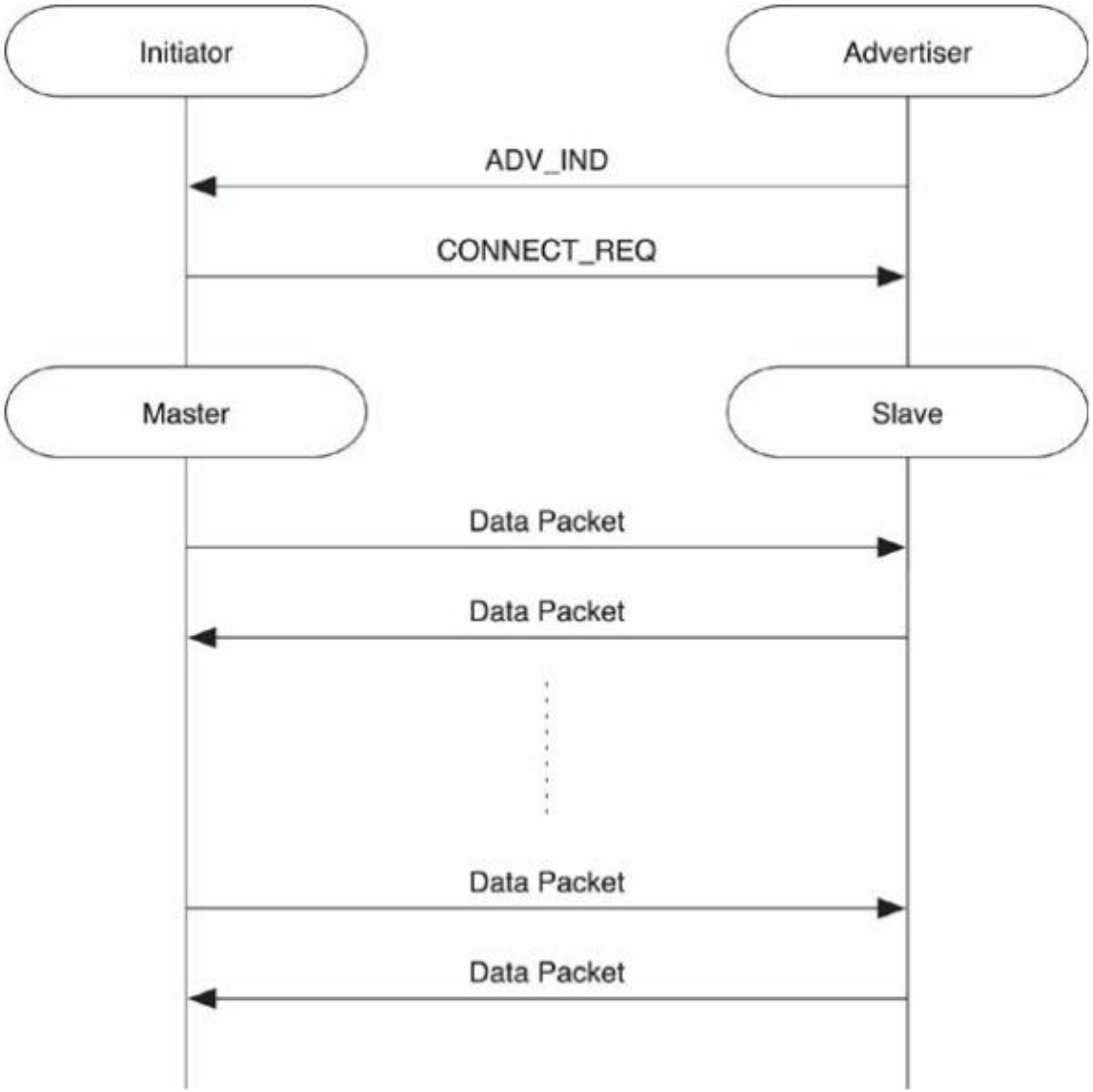
# Переход в режим соединения

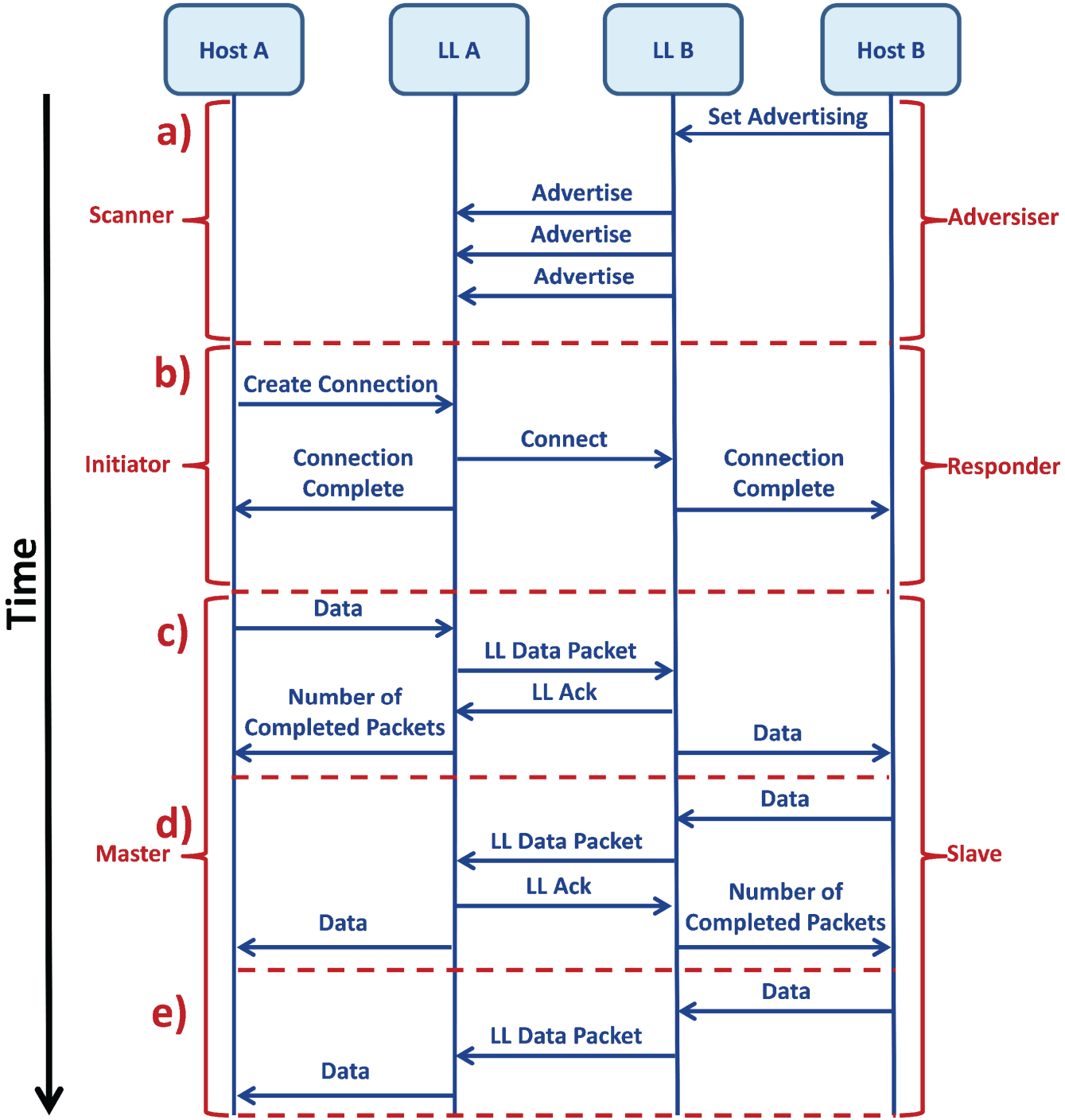


# Переход в режим «Соединение»

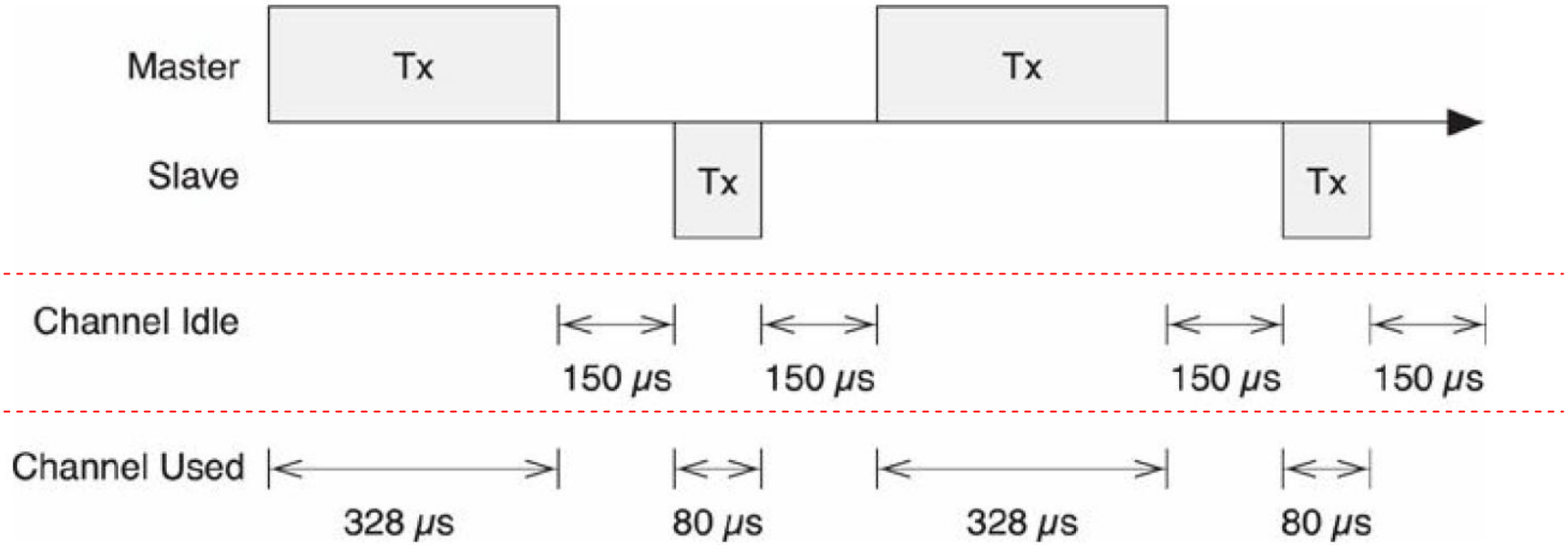


# Переход в режим «Соединение»




Host A
LL A
LL B
Host B
Time
a)
Scanner
Set Advertising
Advertise
Advertise
Advertise
Adversiser
b)
Initiator
Create Connection
Connect
Connection Complete
Connection Complete
Responder
c)
Data
LL Data Packet
LL Ack
Number of Completed Packets
Data
d)
Master
Data
LL Data Packet
LL Ack
Data
Number of Completed Packets
Slave
e)
Data
LL Data Packet
Data

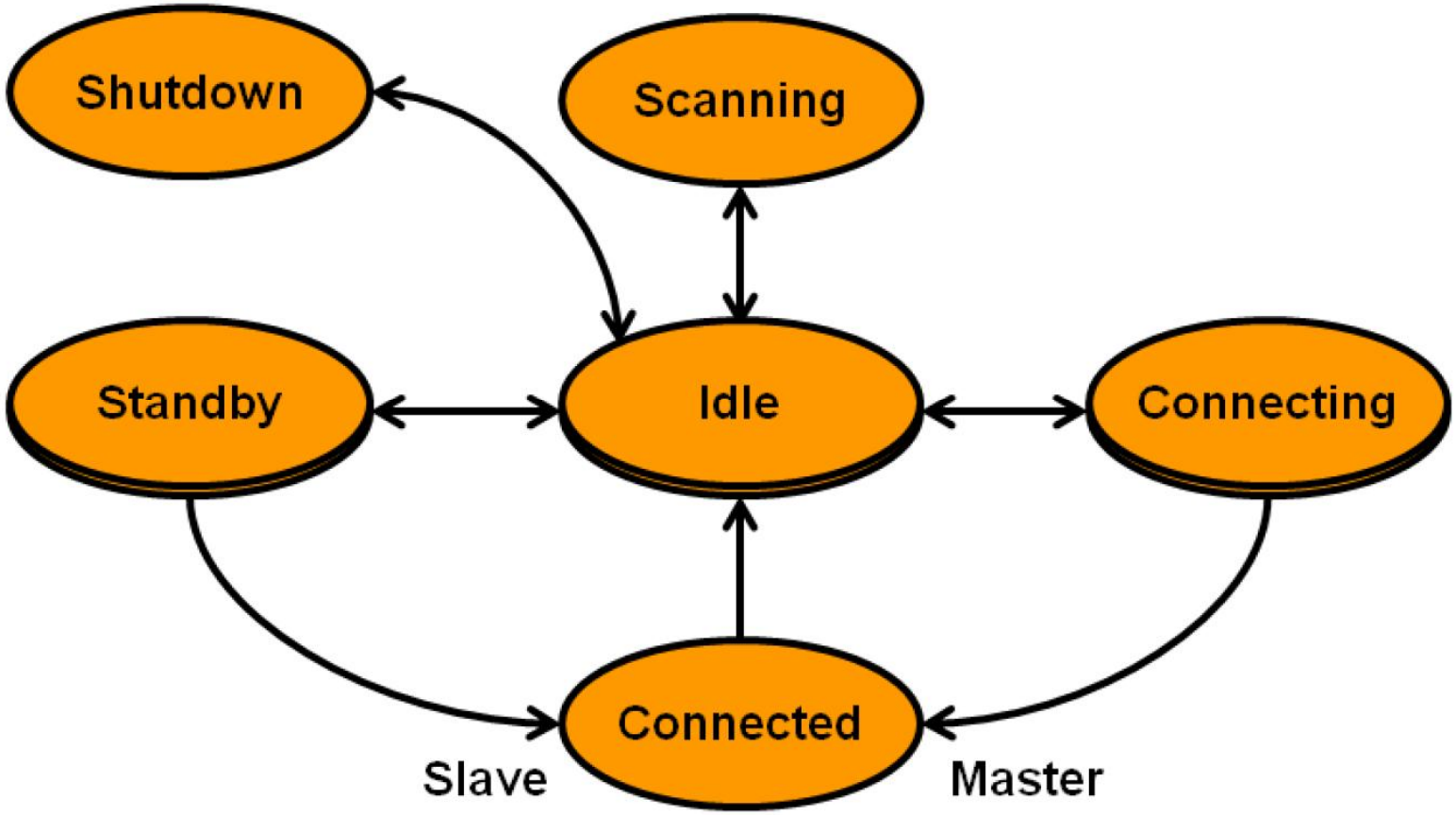
# Рабочий цикл режима пикосети (connection)




$$\frac{maximum\ size\ packet + acknowledge\ packet}{total\ time\ to\ send\ and\ acknowledge\ data}$$

$$\frac{328 + 80}{(328 + 150 + 80 + 150)} = \frac{408}{708} = \sim 58\%$$

# Диаграмма состояний LL может определяться спецификой реализации




Пример диаграммы состояний канального уровня для BLE устройства BM70