

## Беспроводные системы ПД

### Лекция 05

### Протокол ZigBee



**ZigBee®** — это открытый стандарт беспроводной связи для систем сбора данных и управления. Технология ZigBee позволяет создавать самоорганизующиеся и самовосстанавливающиеся беспроводные сети с автоматической ретрансляцией сообщений, с поддержкой батарейных и мобильных узлов. Базируется на беспроводном стандарте IEEE 802.15.4. Технология относится к беспроводным персональным вычислительным сетям (WPAN).

Спецификация ZigBee ориентирована на приложения, требующие гарантированной безопасной передачи данных при относительно небольших скоростях и возможности длительной работы сетевых устройств от автономных источников питания (батарей).

У истоков протокола стоит организация **ZigBee Alliance**, основанная в 2002 и включающая в себя более 300 компаний. Альянс отвечает за развитие и продвижение стандарта, а также за сертификацию оборудования. Спецификация ZigBee 1.0 была ратифицирована 14 декабря 2004 и доступна для членов альянса ZigBee. Через год спецификации первой версии протокола были утверждены, и он стал внедряться в конечные устройства. Сейчас первый вариант спецификации известен под названием ZigBee 2004. Второй выпуск стека называется ZigBee 2006. 30 октября 2007 г., была размещена спецификация ZigBee 2007, обеспечивающая полную совместимость с устройствами ZigBee 2006. В ZigBee 2007 разработчики представили сразу две реализации стандарта: простую ZigBee и продвинутую ZigBee Pro (ZigBee Pro Feature Set). Большинство современных устройств для автоматизации дома базируется именно на Pro-версии от 2007 года.

Протокол ZigBee имеет ряд ответвлений: в 2009 году был представлен стандарт ZigBee RF4CE (Radio Frequency for Consumer Electronics), а позднее появилась спецификация ZigBee IP, предназначенная для использования IPv6 в сенсорных сетях. Она позволяет развернуть сеть 6LoWPAN поверх маломощных устройств с поддержкой IEEE 802.15.4.

Большое количество версий протокола вкупе с тем, что производством коммуникационных чипов с поддержкой ZigBee занимается множество компаний, каждая из которых интерпретирует спецификации по-своему, а также вносит определенные оптимизации в работу протокола, приводит к проблемам с совместимостью. В литературе указывается, что оборудование разных стандартов в рамках одной сети лучше не использовать, и вероятность того, что устройства от разных производителей откажутся работать друг с другом, весьма велика.

## Программный интерфейс ZigBee

Для интерфейса ZigBee нет единого для всех платформ прикладного протокола API. Сделано это намеренно, чтобы предоставить совершенствование протоколов API производителю платформы. Для разработчика это означает, что при переходе на другую платформу необходимо вносить поправки в программное обеспечение. Чтобы упростить эту задачу, рекомендуется выполнять часть кода, отвечающую за обмен со стеком, на отдельном МК.

В стандарте прописаны только функции ZigBee. Команды, вызывающие ту или иную функцию, имеют разную структуру в зависимости от используемой платформы. Например, команда передачи данных APSDE-DATA.request на оборудовании Freescale вызывается инструкцией AF\_DataRequest(), а на платформе Ember — инструкцией emberSendDatagram(). Хотя обе функции называются по-разному и имеют неодинаковый набор аргументов, они производят одно и то же действие — передачу октета.

Сеть ZigBee не может сама определить тип оборудования того или иного узла, разработчику приходится догадываться об этом по косвенным признакам и особенностям поведения устройства. Оборудование с меткой ZigBee-certified является полностью совместимым, вне зависимости от производителя.

## Применение

Протоколы ZigBee разработаны для использования во встроенных приложениях, требующих низкую скорость передачи данных и низкое энергопотребление. Цель ZigBee — это создание недорогой, самоорганизующейся сети с ячеистой топологией предназначенной для решения широкого круга задач. Сеть может использоваться в промышленном контроле, встроенных датчиках, сборе медицинских данных, оповещении о вторжении или задымлении, строительной и домашней автоматизации и т. д. Созданная в итоге сеть потребляет очень мало энергии — индивидуальные устройства согласно данным сертификации ZigBee позволяют энергобатареям работать два года.

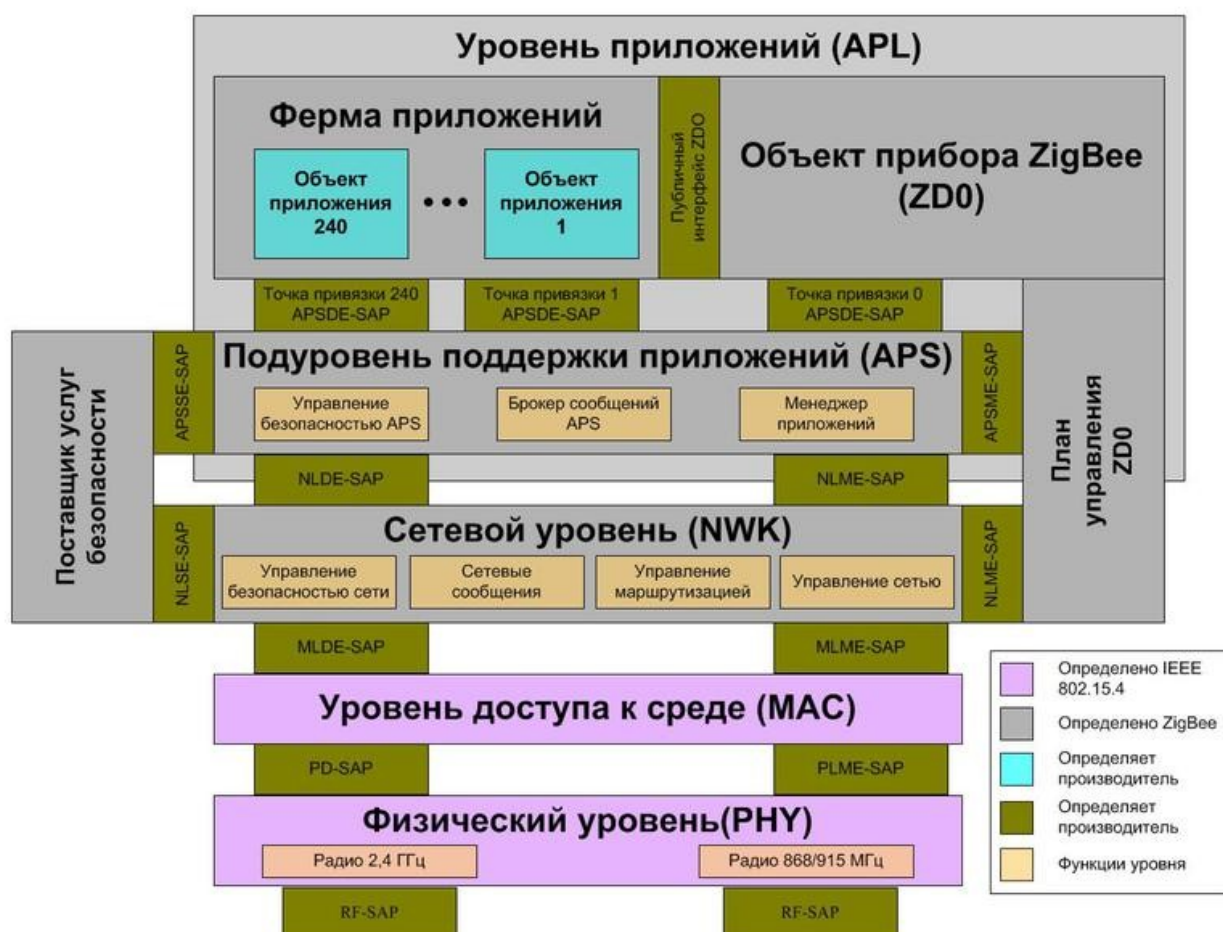
Типовые области применения:

- Домашние развлечения и контроль — рациональное освещение, продвинутый температурный контроль, охрана и безопасность, фильмы и музыка.
- Домашнее оповещение — датчики воды и энергии, мониторинг энергии, датчики задымления и пожара, рациональные датчики доступа и переговоров.
- Мобильные службы — мобильные оплата, мониторинг и контроль, охрана и контроль доступа, охрана здоровья и телепомощь.
- Коммерческое строительство — мониторинг энергии, HVAC (Heating, Ventilation, & Air Conditioning – Отопление, вентиляция и кондиционирование – ОВК), света, контроль доступа.
- Промышленное оборудование — контроль процессов, промышленных устройств, управление энергией и имуществом.

## Сетевые протоколы

Протоколы, регламентированные стандартами IEEE 802.15.4 и ZigBee 2007 Specification, обеспечивают формирование и функционирование беспроводной сенсорной сети.

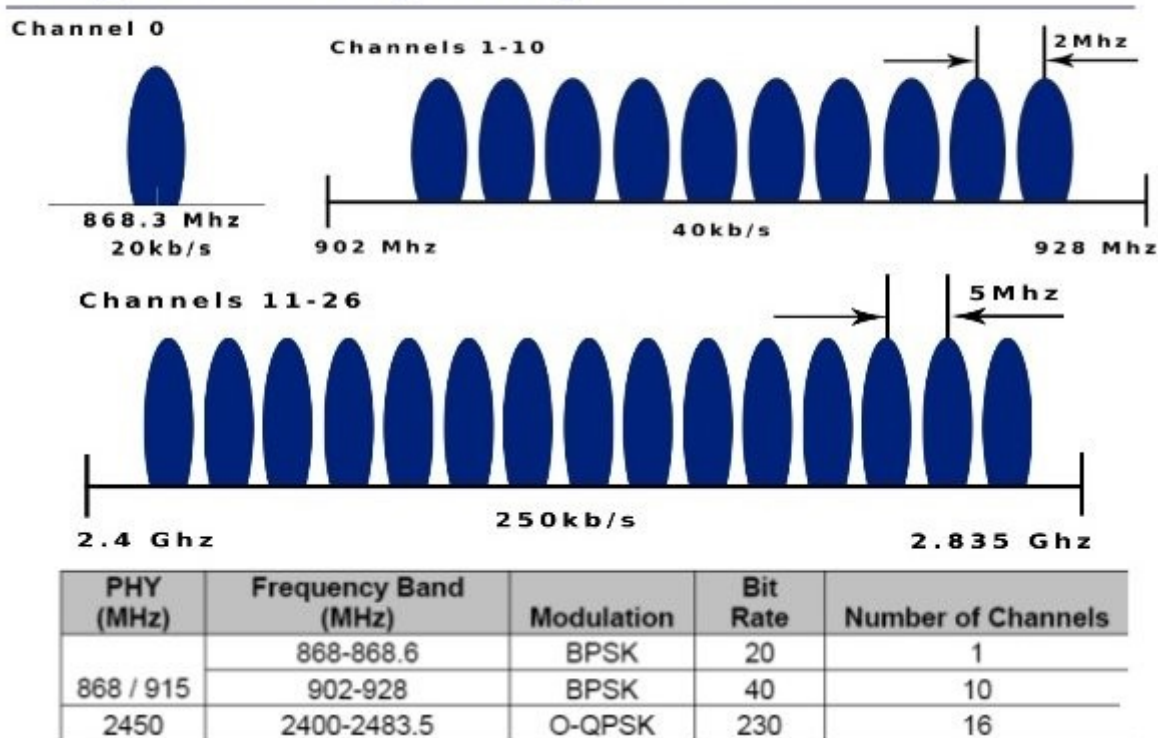
Стандарт IEEE 802.15.4 определяет физический и MAC уровни, а спецификация ZigBee определяет сетевой уровень и уровень приложений. На рисунке показан стек протоколов ZigBee.



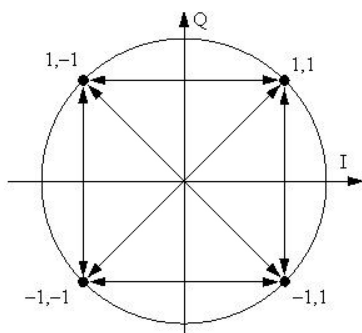
## Используемые частоты

Передача данных в рамках сети осуществляется по радиоканалу. Используемые частоты зависят от региона: для Европы выбрано значение 868 МГц, для США и ряда других стран — 915 МГц. Кроме того, стандарт предусматривает работу на частоте 2,4 ГГц — она не имеет привязки к географическому положению. При этом, подобное обилие вариантов мало сказывается на вопросах совместимости: по факту, практически все ZigBee-оборудование использует частоту 2,4 ГГц. Этот вариант обеспечивает наибольшую пропускную способность — в теории, она может достигать значения в 250 Кбит/с. Дальность передачи сигнала внутри помещения составляет 10–20 метров.

# ZigBee Frequency Bands

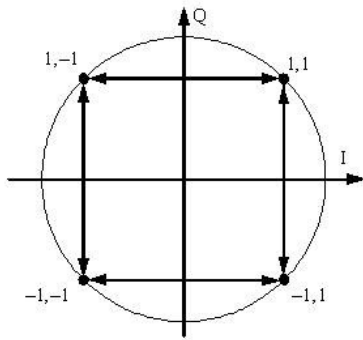


ZigBee на полосе 2,4 ГГц использует каналы 11–26, разделенные интервалом 5 МГц. В устройствах Freescale каналы имеют номера 0–15, поэтому их надо транслировать в каналы 11–26. В сетях ZigBee используется уплотнение спектра (DSSS — Direct Sequence Spread Spectrum). Передача производится в полудуплексном режиме. В каждый момент времени доступен только один канал. Обычно в протоколах ZigBee не используется переключение канала. Высокое качество работы даже в условиях сильной зашумленности обеспечивается модуляцией O-QPSK и уплотнением DSSS.



При квадратурной фазовой манипуляции QPSK (Quadrature Phase Shift Keying или 4-PSK) используется созвездие из четырёх точек, размещённых на равных расстояниях на окружности. На символ приходится два бита. Скорость может быть увеличена в два раза относительно BPSK при той же полосе сигнала, либо оставить скорость прежней, но уменьшить полосу вдвое.

Хотя QPSK можно считать квадратурной манипуляцией (QAM-4), иногда её проще рассматривать в виде двух независимых модулированных несущих, сдвинутых на 90°. При таком подходе чётные (нечётные) биты используются для модуляции синфазной составляющей I, а нечётные (чётные) — квадратурной составляющей несущей Q. Так как BPSK используется для обеих составляющих несущей, то они могут быть демодулированы независимо.



В четырехпозиционной фазовой модуляции со сдвигом квадратур (OQPSK – Offset QPSK) битовые потоки, подаваемые на модуляторы квадратур I и Q, сдвинуты друг относительно друга на длительность одного бита (половина символического интервала). Поэтому в конкретно взятый момент времени только один из квадратурных битовых потоков может изменять свое значение. Это создает диаграмму переходов состояний, существенно отличающуюся от диаграммы переходов состояний модуляции QPSK. В OQPSK сигнальные траектории не проходят рядом с началом координат квадратурной плоскости. В результате максимальное изменение амплитуды передаваемого сигнала достигает 3 дБ. Это существенно меньше изменения амплитуды в сигналах двоичной и квадратурной модуляции. В результате удается получить существенный выигрыш по коэффициенту полезного действия усилителя мощности радиопередатчика.

**Метод прямой последовательности для расширения спектра DSSS (Direct Sequence Spread Spectrum) — широкополосная модуляция с прямым расширением спектра.** Исходный двоичный сигнал преобразуется в псевдослучайную последовательность, используемую для модуляции несущей. Вся используемая «широкая» полоса частот делится на некоторое число подканалов (в 802.11 этих подканалов 11). Каждый передаваемый бит информации превращается, по заранее зафиксированному алгоритму, в последовательность из 11 бит, и эти 11 бит передаются как бы одновременно и параллельно (физически сигналы передаются последовательно), используя все 11 подканалов. При приеме, полученная последовательность бит декодируется с использованием того же алгоритма, что и при её кодировке. Другая пара приемник-передатчик может использовать другой алгоритм кодировки — декодировки, и таких различных алгоритмов может быть очень много. Первый очевидный результат применения этого метода — защита передаваемой информации от подслушивания («чужой» DSSS-приемник использует другой алгоритм и не сможет декодировать информацию не от своего передатчика). При этом сильно уменьшается отношение уровня передаваемого сигнала к уровню шума, (то есть случайных или преднамеренных помех), так что передаваемый сигнал уже как бы неразличим в общем шуме. Но благодаря его 11-кратной избыточности принимающее устройство все же сумеет его распознать.

Выбор канала производится пользователем. Устройство при подключении к сети сканирует все каналы. При формировании сети сканирование проводится дважды: в пассивном и активном режимах. Разработчику предоставляется возможность использовать два режима работы сети: с маячком (beacon-enabled) и без него (beacon-disabled). Режим beacon-enabled обеспечивает строго структурированную по времени передачу данных в рамках суперциклов, что позволяет определить время задержки на отсылку пакета. Маячком в сети является координатор, который рассылает сообщения синхронизации.

Пассивное сканирование позволяет выбрать наиболее свободный канал, а при активном сканировании координатор рассылает найденные в сети запросы маяка (beacon request), чтобы определить занятые идентификаторы PAN. По умолчанию сеть ZigBee выбирает канал с наименьшим количеством сетей и с самым низким уровнем шума. При подключении устройства к сети проводится только активное сканирование. Если сеть уже сформирована и подключаемое устройство получило ответный кадр маяка (beacon response), то канал считается достаточно тихим.

## Лицензирование

Спецификация ZigBee доступна для широкой публики при условиях некоммерческого использования. Входной уровень членства в альянсе ZigBee, называемый Adopter, обеспечивает доступ к ещё не опубликованным спецификациям и разрешает создавать продукты для коммерческого использования спецификации. Регистрация в ходе использования спецификации ZigBee требует от коммерческого разработчика присоединения к альянсу ZigBee.

## Государственное регулирование

Согласно Решению ГКРЧ при Мининформсвязи России от 07.05.2007 № 07-20-03-001 на территории РФ применение сетей ZigBee в частотном диапазоне 2400–2483,5 МГц не требует получения частотных разрешений и дополнительных согласований.

## Топология сети ZigBee

ZigBee поддерживает простые топологии сети, такие как «точка-точка», «дерево» и «звезда». Однако, основным вариантом топологии является самоорганизующуюся и самовосстанавливающуюся ячеистую (mesh) топологию с ретрансляцией и маршрутизацией сообщений. В такой сети, каждое устройство может связываться с любым другим устройством как напрямую, так и через промежуточные узлы сети. Ячеистая топология предлагает альтернативные варианты выбора маршрута между узлами. Сообщения поступают от узла к узлу, пока не достигнут конечного получателя. Возможны различные пути прохождения сообщений, что повышает доступность сети в случае выхода из строя того или иного звена.



В сети ZigBee существует 3 типа узлов: координатор (ZC), роутер/маршрутизатор (ZR), конечные устройства (ZED), которые делятся на спящие устройства и мобильные устройства.

Главное устройство в ZigBee-сети – это координатор. В каждой сети есть один координатор ZigBee. Координатор выполняет функции по формированию сети, а также является одновременно доверительным центром (trust-центром). Доверительный центр устанавливает политику безопасности, хранит ключи безопасности и задает настройки во время подключения устройства к сети.

Конечное устройство обменивается информацией с материнским узлом (координатором или маршрутизатором). Оно не может передавать данные с других устройств. Из-за этого узел большую часть времени может пребывать в спящем состоянии (режим пониженного энергопотребления), что позволяет экономить энергоресурс батарей (как правило такие устройства имеют автономное питание). Обычно конечные устройства выполняют роль датчиков или контроллеров каких-либо

исполнительных устройств. Их количество диктуется потребностью конкретного приложения.

Роутеры осуществляют маршрутизацию пакетов по сети и должны быть готовы к передаче данных в любой момент времени. Поэтому эти узлы не используют режимов пониженного энергопотребления и имеют стационарное питание. Их количество в сети должно быть достаточным для обслуживания требуемого количества спящих и мобильных узлов. Максимальное количество спящих или мобильных узлов, обслуживаемых одним роутером - 32.

### **Обмен данными и задержки**

При индивидуальной рассылке сначала между узлами автоматически выбирается маршрут. После подтверждения пакет посылается повторно до трех раз. Иногда маршрут передачи изменяется, если промежуточный узел выходит из строя. Широковещательные данные передаются всем узлам сети, находящимся в пределах досягаемости. Групповая передача осуществляется в пределах определенной группы узлов.

ZigBee — асинхронный протокол, поэтому каждый узел может инициировать передачу в любой момент времени. Например, когда пользователь включает свет, данные посылаются мгновенно, независимо от быстродействия выключателя. Недостаток ZigBee заключается в том, что нельзя предсказать задержку пакета. Обычно принимается, что для передачи пакета требуется по 10 мс на каждый промежуток между абонентами. Сложности возникают, когда требуется повторная посылка или вычисление маршрута. Для выбора маршрута производится широковещательная рассылка, а устройство, начавшее передачу, должно ждать. Повторные посылки делятся на пошаговые — MAC и между конечными устройствами — APS. Если один узел инициирует передачу другому, находящемуся на расстоянии четырех скачков, то в среднем пакет будет принят через 40 мс, а подтверждение придет через 80 мс.

При индивидуальной передаче с подтверждением может быть произведено до трех повторных передач с интервалом 1.5 с, т.е. в худшем случае задержка может составить около 5 с. Размер пакета не влияет на задержку, если канал относительно свободен, поскольку время ожидания выбирается случайным образом, уменьшая время передачи. Но если канал загружен, то вероятность повторной посылки экспоненциально возрастает с увеличением длины пакета. В связи с этим рекомендуется пересылать короткие пакеты, чтобы сократить задержку и уменьшить занимаемую полосу, освобождая ресурс для других приложений. Передача в больших пакетах целесообразна только в случае, если данные имеют очень большой объем.

### **Адресация сети**

Типы адресов ZigBee и диапазон их значений приведены в таблице 1. Сетевой адрес, обозначаемый NwkAddr, представляет собой 16-разрядное число, уникально определяющее узел в сети, то есть один координатор, теоретически, может взять под свою опеку порядка 65 000 устройств. Вместе с тем, предусмотрена возможность

одновременного использования нескольких сетей. Например, в отеле Aria (Лас-Вегас) одновременно используется около 75 тыс. устройств с поддержкой ZigBee. Координатор всегда имеет адрес 0x0000. На одном канале могут существовать два координатора с одинаковыми адресами, поскольку они имеют разные PAN ID (Personal Area Network ID – идентификатор сети).

Таблица 1

Адреса ZigBee

Название	Диапазон	Описание
Канал	11–26	Физическая часть РЧ–спектра
Идентификатор PAN	0x0000–0x3fff	Адрес сети в канале
Сетевой адрес (NwkAddr)	0x0000–0xffff7	Адрес узла в сети
Конечная точка	1–240	Адрес приложения в узле
Кластер	0x0000–0xffff	Объект внутри приложения
Команда	0x00–0xff	Действие внутри кластера
Атрибут	0x0000–0xffff	Единица данных внутри кластера
Расширенный PAN ID Extended PAN ID (EPID)	0x0000000000000000– 0xffffffffffffffff	Уникальный 64-разрядный идентификатор сети
Группа	0x0000–0xffff	Выбранная часть узлов сети
Идентификатор профиля	0x0000–0xffff	Профиль ZigBee

В стеке ZigBee (0x01) поле NwkAddr характеризует расположение узла в сети. Например, устройство с NwkAddr = 0x0001 является первым подключившемся к сети ZR, а узел с адресом NwkAddr = 0x796F — это первое конечное устройство. В стеке ZigBee Pro (0x02) адрес присваивается произвольным образом.

### MAC-адрес

MAC-адрес — это расширенный адрес, представляющий собой уникальный 64-разрядный номер, присвоенный устройству. Между адресом MAC и NwkAddr нет связи. При отключении устройства от сети и подсоединении его к другой MAC-адрес обязательно останется прежним, а NwkAddr может измениться.

Приемники ZigBee не содержат MAC-адрес. Он назначается производителем и записывается во флэш-память микроконтроллера, расположенного на плате. MAC-адрес записывается от младшего бита к старшему, поэтому во флэш-память устройства он заносится в обратном порядке.

MAC-адрес может иногда использоваться вместо короткого адреса узла, например, если узел перемещается и меняет свой короткий адрес. Так, когда пульт дистанционного управления выходит из зоны охвата своего родителя, он ищет новое родительское устройство, чтобы быть доступным для узлов сети.



## **Идентификаторы PAN**

Идентификаторы PAN ID используются для логического отделения узлов одной сети ZigBee от узлов другой, если сети расположены на одной и той же территории либо работают в одном канале. Благодаря разным ID несколько сетей могут существовать в непосредственной близости друг от друга без интерференции.

Идентификатор ZigBee представляет собой 16-разрядное число от 0x0000 до 0x3fff. В стандарте 802.15.4 идентификаторы имеют значения в диапазоне 0x0000–0xffff. В версии ZigBee 2006 идентификаторы имеют уникальное значение на данном канале, т. е. в разных каналах могут работать устройства с одинаковым ID. В ZigBee 2007 это запрещено из-за применения функции быстрой подстройки частоты (frequency agility), которая разрешает сети переключать каналы для поиска лучшего.

При формировании сети PAN ID принимает значение 0xffff, которое говорит о том, что приложение запрашивает у стека случайный идентификатор, не конфликтующий с ID других, работающих поблизости, сетей. При подключении к сети ID = 0xffff означает, что узел хочет подключиться к любой сети. Идентификатор выбирается пользователем.

## **Расширенный идентификатор PAN**

Расширенные идентификаторы (EPID — Extended PAN ID) представляют собой 64-разрядные числа, которые уникальным образом идентифицируют персональную сеть. Обмен данными производится с использованием 16-разрядного идентификатора, кроме одного случая. Ответный кадр, посланный на запрос маяка, содержит расширенный идентификатор сети, чтобы узел, который хочет подключиться к сети, выбрал нужный ID.

Когда узел ZigBee хочет подключиться к сети, он всегда высылает запрос маяка. Затем он анализирует все полученные ответные маяки и выбирает подходящий. Расширенные идентификаторы не устанавливаются ни одним комитетом стандартов. Для старших 24 разрядов EPID рекомендуется использовать OUI — уникальный номер, присвоенный сетевому устройству производителем. Расширенные ID абсолютно не связаны с 16-разрядными идентификаторами и MAC-адресами и используются исключительно для нахождения узлом нужной сети.

## **Адресация внутри узла**

Выше были приведены параметры узла, необходимые для его определения в сети. Однако ZigBee обеспечивает также совместимость на уровне приложения за счет использования кластеров, конечных точек, команд, атрибутов и профилей. Каждый пакет должен содержать PAN ID (поле MAC), NwkAddr (поле NWK), адрес конечной точки приемника и передатчика, ID профиля и кластера (поле APS).

## Конечные точки

Конечные точки позволяют относить один узел к различным профилям или объединять несколько ZigBee-устройств в узел. Каждый узел сети может содержать 1–240 конечных точек в соответствии с количеством выполняемых приложений. Номера конечных точек могут идти не по порядку.

Например, выключатель может быть предназначен как для внутреннего, так и для внешнего освещения. Соответственно, он представляет собой две конечные точки. Такие устройства как термостат могут содержать несколько независимых устройств с точки зрения сети (датчик, интерфейс пользователя, нагревательный и охлаждающий элементы).

## Кластеры

Кластер похож на класс в объектно-ориентированном программировании и представляет собой совокупность:

- *описания стандартного устройства ZigBee* (осветительное устройство, диммер, выключатель, счетчик)
- *описания стандартных атрибутов* для этого устройства (вкл./выкл., яркость, показания счетчика)
- *описания стандартных команд* для этого устройства (установить уровень яркости, считать показания, включить/выключить)

Кластеры имеют клиент-серверную природу. ZigBee-сервер – это устройство, которое хранит значение атрибута, в то время, как ZigBee-клиент дистанционно считывает или записывает значение этого атрибута. Например, пара стандартных устройств лампочка и выключатель могут вместе реализовать функционирование стандартного кластера включить/выключить. При этом лампочка будет ответственна за серверную часть кластера. Она хранит значение атрибута включено/выключено. Выключатель дистанционно устанавливает значение этого атрибута и реализует, таким образом, клиентскую часть кластера. Одно и то же устройство может содержать клиентские части одних кластеров и серверные части других. Например, выключатель в нашем примере может дополнительно содержать серверную часть кластера конфигурация, при помощи которого он будет получать информацию о режимах своей работы от конфигурирующего устройства.

Кластеры определяются 16-разрядным идентификатором и являются объектами приложения. В то время как NwkAddr и конечные точки относятся к адресации, кластер определяет назначение приложения. Например, кластер включения и выключения On/Off выполняет действие перевода устройства из одного состояния в другое. При этом тип исполнительного устройства неважен.

Текущее состояние устройства определяется приложением по атрибуту внутри кластера. Некоторые кластеры, определенные в ZigBee, приведены в таблице 2. Кластеры определены только внутри конкретного профиля. Например, в одном профиле кластер 0x0000 может выполнять отключение сети (Off), а в другом — содержать основные установки (Basic). Кроме идентификатора кластеры имеют

направление. В свойстве SimpleDescriptor конечной точки кластер обозначается как вход или выход.

Таблица 2

### Кластеры ZigBee

Наименование	ID
Basic (основной)	0x0000
Power Configuration (регулировка мощности)	0x0001
Temperature Configuration (настройка температуры)	0x0002
Identify (кластер распознавания)	0x0003
Groups (кластер группы)	0x0004
Scenes (кластер сцен)	0x0005
On/Off (включение/выключение)	0x0006
On/Off Configuration (настройка включения и выключения)	0x0007
Level Control (управление уровнем)	0x0008
Time (время)	0x000a
Location (местоположение)	0x000b

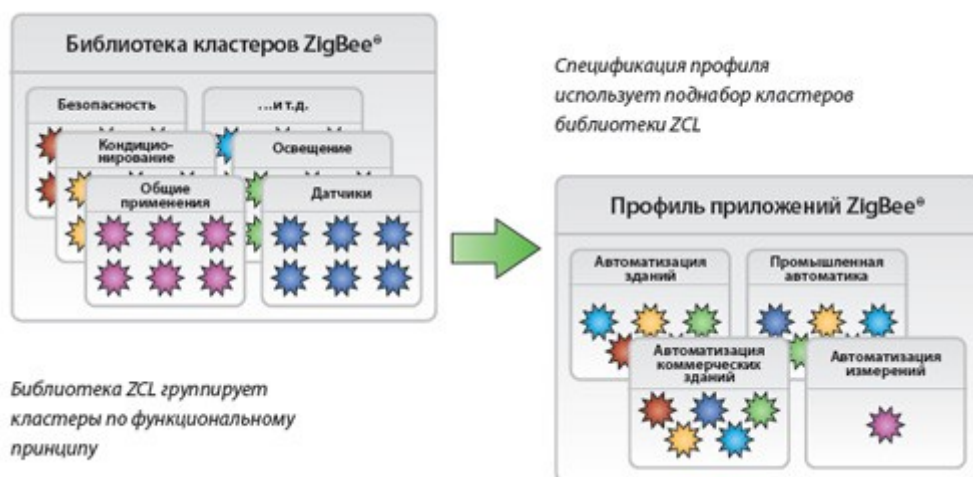
В стандартных профилях (Public profile) используется библиотека кластеров ZigBee (ZigBee Cluster Library, ZCL), содержащая команды и атрибуты. С помощью библиотеки легко получить или присвоить атрибут, используя общий набор команд. Библиотека ZCL группирует кластеры по функциональному признаку: общего назначения, для работы с датчиками, для управления осветительными устройствами, вентиляцией и т. д. Использование стандартных кластеров для пересылки сообщений является обязательным требованием спецификации ZigBee PRO Feature Set.

**Команды** представляют собой 8-разрядное число и могут быть внутрикластерными или межкластерными. Кластерные команды зависят от номера кластера и обычно начинаются с 0x00. Например, 0x00 — команда выключения в кластере On/Off и команда движения к заданному уровню в кластере LevelControl.

В индивидуальных профилях использовать библиотеку кластеров необязательно. Это позволяет сократить программный код. Атрибуты являются 16-разрядными числами и описывают текущее состояние кластера. Совокупность атрибутов всех кластеров, поддерживаемых устройством, определяет состояние устройства.

### Профили

*Профилем называется совокупность настроек программного обеспечения узлов сети, обеспечивающая их совместную работу.* Спецификация профиля определяет такие параметры, как способы задания идентификационных параметров сети, режимы образования сети, способы защиты данных, используемый поднабор кластеров, который включает кластеры из разных функциональных групп библиотеки ZCL.



Все запросы данных посылаются в профиль приложения. Для этого используются идентификаторы профиля — 16-разрядные числа в диапазоне 0x0000–0x7fff для стандартных профилей и 0xbf00–0xffff — для профилей, определенных производителем.

Профиль относится к приложению или устройству. Стандартные профили определяются альянсом ZigBee, индивидуальные — производителем.

Home Automation (автоматизация дома) — стандартный профиль для объединения в сеть бытовых устройств, в т.ч. осветительных приборов, выключателей, розеток, пультов управления, кондиционеров, термостатов, нагревателей. Другой пример — стандартный профиль Commercial Building Automation, который определяет такие устройства ZigBee как сложные осветительные приборы и многопозиционные выключатели, системы отпирания дверей без использования ключа и системы безопасности.

В одной сети может существовать несколько стандартных и индивидуальных профилей. В ZigBee Alliance постоянно идет работа над расширением набора стандартных профилей, чтобы удовлетворить все потребности клиентов. Именно производители определяют, каких профилей не хватает в первую очередь. Краткий список стандартных профилей приведен в таблице 3.

Таблица 3

Стандартные профили ZigBee

ID проф.	Название профиля
0101	Industrial Plant Monitoring (IPM, мониторинг предприятия)
0104	Home Automation (HA, автоматизация жилых помещений)
0105	Commercial Building Automation (CBA, автоматизация коммерческих помещений)
0107	Telecom Applications (TA, телекоммуникация)
0108	Personal Home & Hospital Care (PHHC, амбулаторное или стационарное лечение)
0109	Advanced Metering Initiative (AMI, дополнительные измерения)

Профили позволяют соединять устройства различных производителей без дополнительной настройки. Индивидуальные профили, также называемые профилями производителей (Manufacturer Specific Profiles, MSP), не закреплены альянсом ZigBee. Они создаются для таких приложений, которые рассчитаны на взаимодействие с устройствами только одного производителя.

Профили, определенные производителем, позволяют задавать любой набор кластеров, конечных точек и устройств. Стандарт не накладывает каких бы то ни было ограничений на тип передаваемых данных при условии, что скорость передачи находится в допустимом диапазоне и приложение не перегружает канал.

ZigBee Alliance по запросу производителя — члена организации — присваивает идентификатор предложенному им профилю. Чтобы задать кластеры в индивидуальном профиле, необходимо сначала составить карту всех устройств сети и определить, какого типа информацию они должны обрабатывать. В этом случае структура будет наиболее прозрачна и легка в управлении.

### Идентификаторы устройств

Каждая конечная точка содержит идентификатор профиля и идентификатор устройства. Как уже говорилось, одно физическое устройство может представлять собой несколько устройств ZigBee. Идентификаторы устройств ZigBee принимают значения от 0x0000 до 0xffff (см. табл. 4). Идентификаторы устройств имеют двойное назначение. Они позволяют отображать на дисплее пользователя иконки, соответствующие типу устройства, и в то же время помогают сделать инструменты ZigBee более совершенными.

Таблица 4

*Идентификаторы устройств для профиля Home Automation*

Устройство	Идентиф.	Устройство	Идентиф.
Расширитель диапазона	0x0008	Датчик света	0x0106
Розетка электросети	0x0009	Затенитель	0x0200
Выключатель света	0x0100	Контроллер затенителя	0x0201
Лампа с регулируемой яркостью	0x0101	Нагревательно-охлаждающий элемент	0x0300
Выключатель света	0x0103	Термостат	0x0301
Регулятор яркости	0x0104	Датчик температуры	0x0302

Рассмотрим двухпозиционный переключатель и штепсельную розетку. В плане удаленного мониторинга и управления эти устройства идентичны. Они принадлежат одному кластеру — 0x0006 (On/Off). Однако, с точки зрения пользователя, розетка относится к инструменту для ввода в эксплуатацию электронных устройств, а переключатель позволяет включить или выключить свет.

Сеть ZigBee не устанавливает интерфейса между человеком и устройствами. Выключателем может быть кнопка, тумблер, пластина датчика электрического поля,

датчик ускорения и т. д. Во всех стандартных профилях ZigBee содержится список устройств. Производители могут расширить его, используя поле Manufacturer Specific Extension, которое является частью интерфейса библиотеки кластеров ZigBee. Они также могут создать устройство в индивидуальном профиле (MSP), тогда оно будет взаимодействовать с устройствами из стандартного профиля через идентификаторы устройств и кластеры.

### **Формирование сети**

Сеть ZigBee – самоорганизующаяся, и ее работа начинается с формирования. Устройство, назначенное при проектировании координатором персональной сети (PAN координатор), определяет канал, свободный от помех, и ожидает запросов на подключение.

Устройства, пытающиеся присоединиться к сети, рассылают широковещательный запрос. Пока PAN координатор – единственное устройство в сети, отвечает на запрос и предоставляет присоединение к сети только он. В дальнейшем присоединение к сети могут предоставлять также присоединившиеся к сети маршрутизаторы.

Устройство, получившее ответ на широковещательный запрос, обменивается с присоединяющим устройством сообщениями, чтобы определить возможность присоединения. Возможность определяется способностью присоединяющего маршрутизатора обслужить новые устройства в дополнение к ранее подключенным.

### **Вступление в сеть (присоединение)**

Существует два способа присоединения: MAC ассоциация и повторное сетевое присоединение (NWK rejoin).

MAC ассоциация доступна любому устройству ZigBee и осуществляется на MAC уровне. Механизм MAC ассоциации следующий:

1. Устройство, позволяющее присоединиться к нему, выставляет на MAC уровне разрешение на присоединение.
2. Устройство, вступающее в сеть, выставляет на MAC уровне запрос на присоединение и передает широковещательный запрос маячка.
3. Получив маячок от устройств, готовых подключить присоединяемое устройство, последнее определяет, в какую сеть и к какому устройству оно желает присоединиться, и выставляет на MAC уровне требование о вступлении с флажком «повторное присоединение» в значении FALSE.
4. Затем вступающее устройство направляет на выбранное для присоединения устройство запрос присоединения и получает ответ с присвоенным ему сетевым адресом.

При MAC ассоциации данные передаются не зашифрованными, поэтому MAC ассоциация не является безопасной.

Повторное сетевое присоединение вопреки названию может применяться и при первичном присоединении. Оно выполняется на сетевом уровне. При этом, если вступающее устройство знает текущий сетевой ключ, обмен пакетами может быть безопасным. Ключ может быть получен, например, при настройке.

При повторном подключении присоединяющееся устройство выставляет на сетевом уровне запрос присоединения и обменивается с подключающим устройством пакетами «запрос присоединения» – «ответ на запрос присоединения».

### **Динамика сети**

Кроме случаев присоединения новых устройств структура сети меняется и в случаях, когда устройства покидают сеть и повторно присоединяются в других местах (это происходит, например, в случае перезагрузки устройства). Каждый раз такое устройство получает адрес из имеющегося в распоряжении присоединяющего маршрутизатора диапазона адресов.

### **Источники:**

1. Материалы с сайта <http://www.zigbee.org>
2. ZigBee. <https://ru.wikipedia.org>
3. В. Лекнин Сети ZigBee. Зачем и почему? <https://habrahabr.ru>
4. Протокол ZigBee: беспроводные технологии на службе «умного» дома. Н. Жогов. <http://www.ferra.ru>
5. Беспроводные сети ZigBee и Thread. <http://www.wless.ru>
6. А. Павлов Адресация и профили ZigBee. <http://www.russianelectronics.ru>
7. Дрю Гисласон (Drew Gislason). Приложения ZigBee: обмен данными, API и PAN [перевод]. <http://www.russianelectronics.ru>
8. Четырехпозиционная фазовая модуляция (QPSK). <http://digteh.ru>
9. Четырехпозиционная фазовая модуляция со сдвигом квадратур (OQPSK). <http://digteh.ru>