**Facoltà di Scienze Matematiche, Fisiche e Naturali**

**Dipartimento di Scienze dell'Informazione**

**Corso di Laurea Specialistica in Scienze di Internet**

**Corso di Laurea Specialistica in Informatica (mutuato)**

# IEEE 802.15.4, ZigBee & Open Source

**Luciano Bononi**

**(bononi@cs.unibo.it)**
**http://www.cs.unibo.it/~bononi**

**This presentation includes some figures and slides available from the following Web sources: ZigBee Alliance (www.zigbee.org), IEEE 802.15.4 (www.ieee802.org/15), Motorola (www.motorola.com)**
**Slide and figure credits and copyrights are indicated.**

---

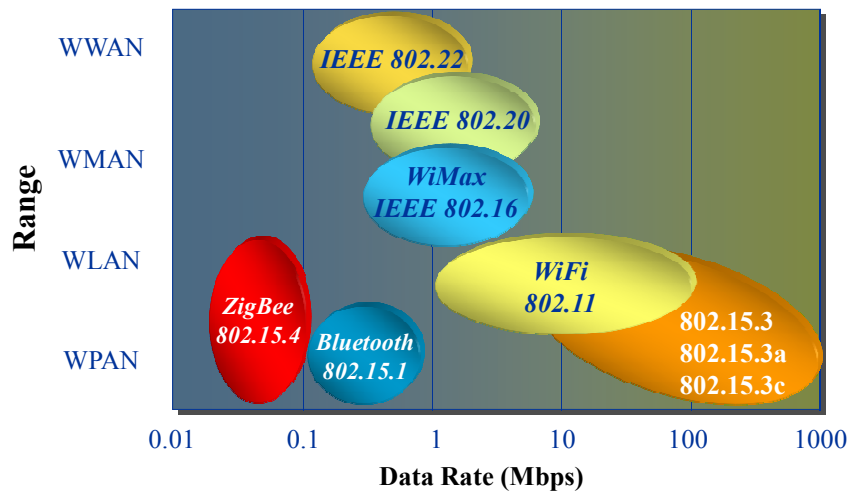## Outline

- **Introduction**
  - IEEE 802.15.4 technology and characteristics
  - ZigBee Alliance e ZigBee certification
  - Motivations and target scenarios/applications
- **ZigBee MAC**
- **ZigBee Network**
  - Devices, Nodes, Roles and Topologies
- **ZigBee Application**
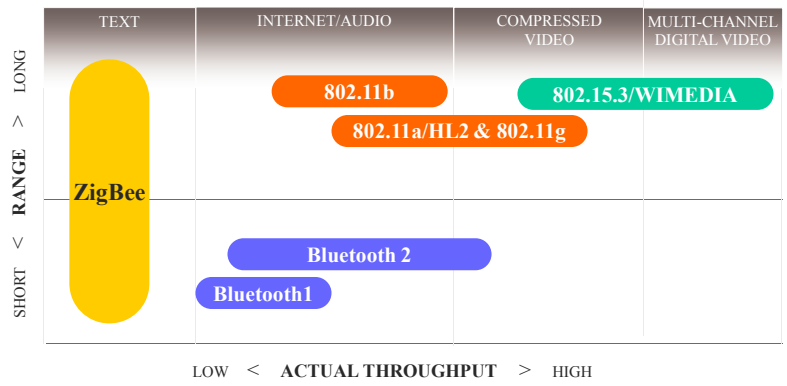- **Open Source Protocol Stack Initiatives**
- **Conclusions**

1

# IEEE 802.15.4
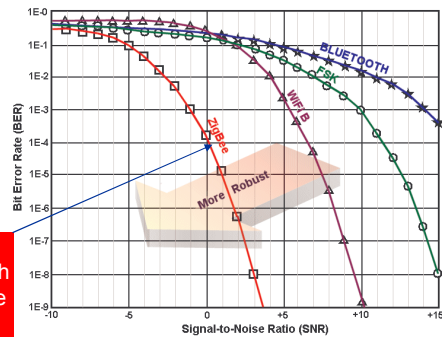# Technology and characteristics

# The 802 Wireless Space



Slide credits: ZigBee Alliance

# The Wireless Market

| | TEXT | INTERNET/AUDIO | COMPRESSED VIDEO | MULTI-CHANNEL DIGITAL VIDEO |
|---|---|---|---|---|
| **LONG** | | **802.11b** | **802.15.3/WIMEDIA** | |
| | | **802.11a/HL2 & 802.11g** | | |
| **RANGE** | **ZigBee** | | | |
| | | **Bluetooth 2** | | |
| **SHORT** | | **Bluetooth1** | | |

LOW < **ACTUAL THROUGHPUT** > HIGH

# Basic Radio Characteristics



ZigBee technology relies upon IEEE 802.15.4, which has excellent performance in low SNR environments

| Frequency Band | License Required? | Geographic Region | Data Rate | Channel Number(s) |
|---|---|---|---|---|
| 868.3 MHz | No | Europe | 20kbps | 0 |
| 902-928 MHz | No | Americas | 40kbps | 1-10 |
| 2405-2480 MHz | No | Worldwide | 250kbps | 11-26 |

Slide credits: ZigBee Alliance

# IEEE 802.15.4 Frequencies and Data Rates
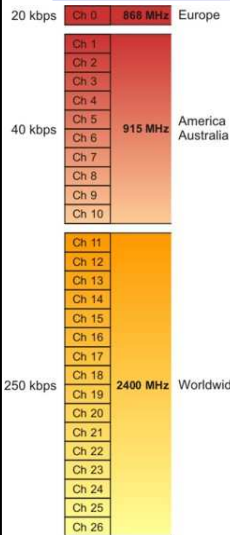
Max power: 1mW (0 dBm)

Max range: 10-75 m (up to 1500 with ZigBee Pro)*

| BAND | COVERAGE | DATA RATE | # OF CHANNEL(S) | |
|------|----------|-----------|-----------------|---|
| 2.4 GHz | ISM | Worldwide | 250 kbps (5 Mhz each) $F_C = (2405 + 5 * (ch - 11))$ MHz, where ch = 11, 12, ..., 26. | (DSSS) Orthog. QPSK |
| 868 MHz | | Europe | 20 kbps | BPSK |
| 915 MHz | ISM* | Americas | 40 kbps | BPSK |

Left diagram labels:
- 20 kbps — Ch 0 — 868 MHz — Europe
- 40 kbps — Ch 1–Ch 10 — 915 MHz — America Australia
- 250 kbps — Ch 11–Ch 26 — 2400 MHz — Worldwide

Slide credits: ZigBee Alliance

---

# Comparison of complementary protocols

| Feature(s) | IEEE 802.11b/g/a | Bluetooth | ZigBee |
|------------|------------------|-----------|--------|
| Application focus | Web, e-mail, Mmedia | Cable replacement | Monitoring & control |
| Stack size | >1000kB | >250kB | < 64kB |
| Power Profile | Hours | Days | Years |
| Complexity | Very Complex | Complex | Simple |
| Nodes/Master | many (IP) | 7 | 65536 (local).. Up to 2^64 |
| Latency | Enumeration upto 3 seconds | Enumeration upto 10 seconds | Enumeration 30ms |
| Range | 100 m | 10m | 70m-300m |
| Extendability | Roaming possible | No | YES |
| Data Rate | 11-54 Mbps (up to 108) | 1Mbps | up to 250Kbps |
| Target cost | 50 EUR | 10 EUR | 2 EUR |
| Security | Authentication Service Set ID (SSID) | 64 bit, 128 bit | 128 bit AES and Application Layer user defined |

# How is ZigBee related to IEEE 802.15.4?

- ZigBee takes full advantage of a powerful physical radio specified by IEEE 802.15.4

- ZigBee adds logical network, security and application software

- ZigBee continues to work closely with the IEEE to ensure an integrated and complete solution for the market

---

## IEEE 802.15.4 Protocol Mission

- 15.4 Protocol was developed for very different reasons than Bluetooth
  - 802.15.4
    - *Very low duty cycle, very long primary battery life applications as well as mains-powered*
    - *Static and dynamic mesh, cluster tree and star network structures with potentially a very large number (>65534) of client units, low latency available as required*
    - *Ability to remain quiescent for long periods of time without communicating to the network*
  - Bluetooth
    - *Moderate duty cycle, secondary battery operation where battery lasts about the same as master unit*
    - *Wire replacement for consumer devices that need moderate data rates with very high QoS and very low, guaranteed latency*
    - *Quasi-static star network structure with up to 7 clients (and ability to participate in more than one network simultaneously)*
    - *Generally used in applications where either power is cycled (headsets, cellphones) or mains-powered (printers, car kits)*
- Protocol differences can lead to tremendous optimizations in power consumption

## Why ZigBee?

- Reliable and self healing
- Supports large number of nodes
- Easy to deploy
- Very long battery life
- Secure
- Low cost
- Can be used globally
- Designer concentrates on end application
  - Silicon vendors and ZigBee Alliance take care of transceiver, RF channel and protocol stack (*)

- More Information
  - ZigBee: www.zigbee.org

e.g. ZigBee module

---

# ZigBee Alliance e ZigBee certification

# What is the ZigBee Alliance?

- An Organization with a mission to define reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard
- Alliance provides
  - upper layer stack and application profiles
  - compliance and certification testing
  - branding
- Result is a set of interoperable solutions recognizable in the market

# Who is supporting the ZigBee Alliance?

- Eight promoter companies
  - Ember, Freescale, Honeywell, Invensys, Mitsubishi, Motorola, Philips and Samsung
- A rapidly growing list (Over 120 participants) of industry leaders worldwide committed to providing ZigBee-compliant products and solutions

# The ZigBee Platform and certification



Public Application Profile

ZigBee Stack

IEEE 802.15.4

Certified Product

Compliant Platform
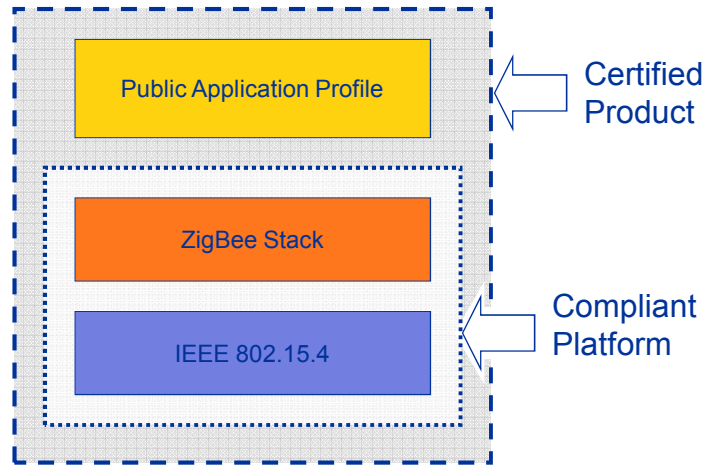
Slide credits: ZigBee Alliance

# ZigBee Motivations

# need for ZigBee technology?

- No standard approach today that addresses the unique needs of most remote monitoring and control applications
  - Enables the broad-based deployment of reliable wireless networks with low complexity, low cost solutions
  - Provides the ability to run for years on inexpensive primary batteries for a typical monitoring application
  - Capable of inexpensively supporting robust mesh networking technologies

# Advantages of ZigBee vs. proprietary solutions?

- Product interoperability
- Vendor independence
- Increased product innovation as a result of industry standardization
- A common platform is more cost effective than creating a new proprietary solution from scratch every time
- Companies can focus their energies on finding and serving customers

- How is Open Source intended in this vision?

Slide credits: ZigBee Alliance
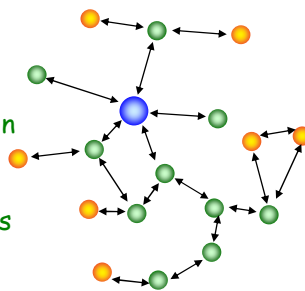
# ZigBee:
# Examples of target scenarios/applications

---

# 802.15.4 Application Space
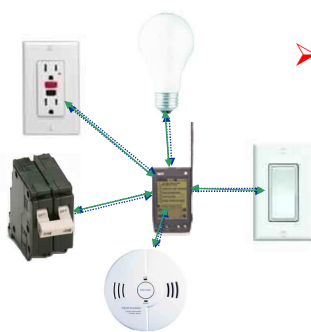
➢ **Sensors & Controls:**

- Home Automation
- Industrial Automation
- Remote Metering
- Automotive Networks
- Interactive Toys
- Active RFID/ asset tracking
- Medical
- ...and more

Slide credits: ZigBee Alliance

## Sensor/Control Network Requirements

- Large networks (large number of devices and large coverage area)
  - can form autonomously
  - operate very reliably for years without any operator intervention
- Very long battery life (years off of a AA cell)
- very low infrastructure cost (low device & setup costs) and very low complexity and small size
- Device data rate and QoS needs are low (*)
- Standardized protocols are necessary to allow multiple vendors to interoperate

## Applications field



Slide credits: ZigBee Alliance
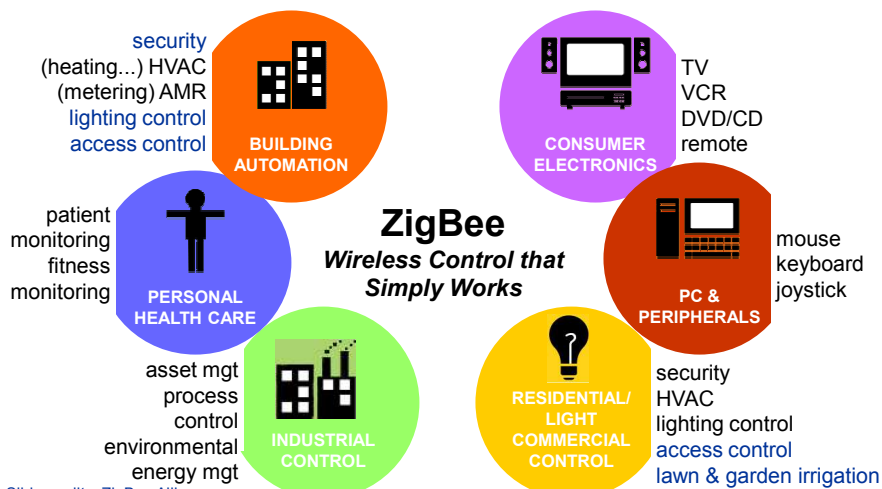
# ZigBee Application classes and traffic types

- ZigBee networks can support different traffic:

  - Periodic data
    - *E.g. wireless sensors and metering applications*
    - *beaconing principle: scheduled wakeup time + send + sleep*
  - Intermittent data
    - *E.g. wireless light switch*
    - *Beaconless system: device attach to network only upon need, and sleep o.w.*
  - Repetitive (low latency) data
    - *E.g. security systems*
    - *Guaranteed Time Slot (GTS) capability: a MAC superframe structure managed by network coordinator for QoS-based scheduling of reserved slots within fixed latency limits (no contention)*

---

# Application examples: Lighting Control

- Advance Transformer
  - Wireless lighting control
    - *Light switches anywhere*
    - *Customizable lighting schemes*
    - *Energy savings on bright days*
  - Extendable networks
    - *Additional sensors*
    - *Other networks*

Slide credits: ZigBee Alliance

# HVAC Energy Management

- Hotel energy management
  - Major operating expense for hotel
    - *Centralized HVAC management allow hotel operator to make sure empty rooms are not cooled*
  - Retrofit capabilities
  - Battery operated t-stats can be placed for convenience
  - Personalized room settings at check-in

Slide credits: ZigBee Alliance

---

# Asset Management

- Within each container, sensors form a mesh network.
- Multiple containers in a ship form a mesh to report sensor data
- Increased security through on-truck and on-ship tamper detection
- Faster container processing. Manifest data and sensor data are known before ship docks at port.
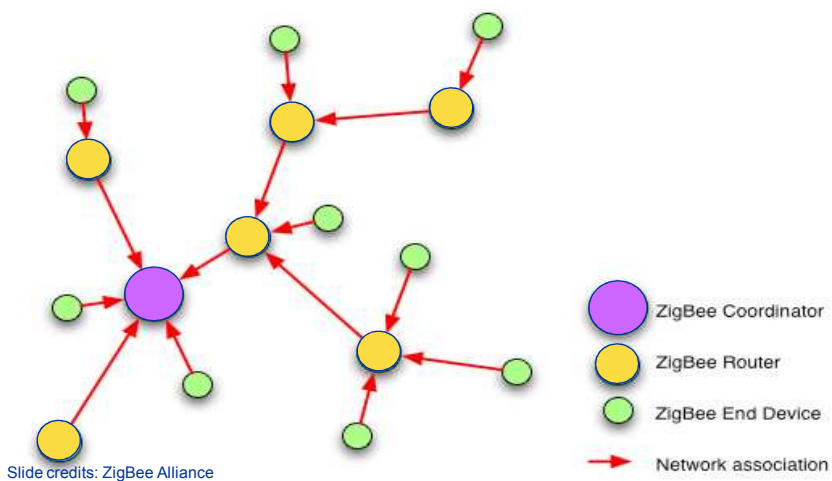
Slide credits: ZigBee Alliance

# Residential Control



Slide credits: ZigBee Alliance

# System Simplicity and Flexibility (example)



**ZigBee Example Block Diagram for a Sensor Application**

RF Data Modem

| RX Analog/RF | RX Baseband |
| Freq Gen | SPI/ Control |
| TX Analog/RF | TX Baseband |

Power Management

8-bit Microcontroller

Sensor App — Sensor Driver — Sensor
ZigBee NWK
15.4 MAC

RF Packet Radio     8-Bit MCU

Slide credits: Motorola

# ZigBee (and IEEE 802.15.4) Protocol Stack:

## General concepts

Useful link: http://www.jennic.com/elearning/zigbee/index.htm

# ZigBee 1.0: (static) tree network structure



Slide credits: ZigBee Alliance

Legend:
- ZigBee Coordinator
- ZigBee Router
- ZigBee End Device
- → Network association

ZigBee Pro: (dynamic) Mesh Networking
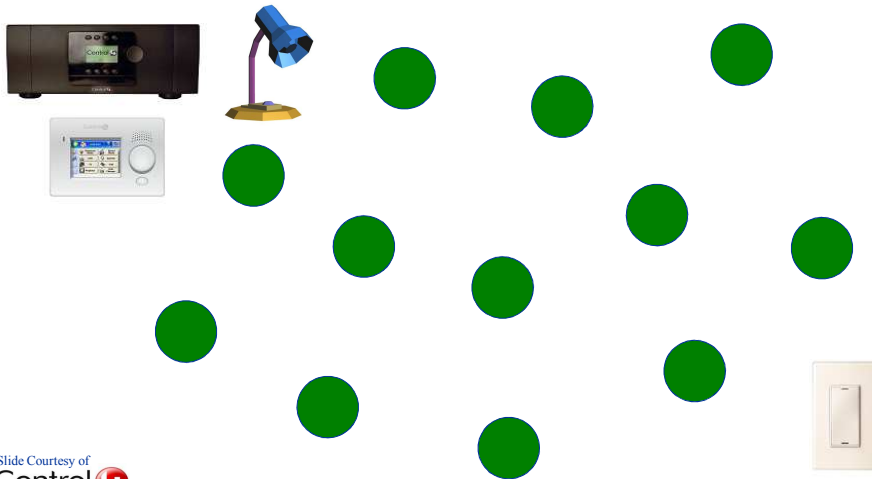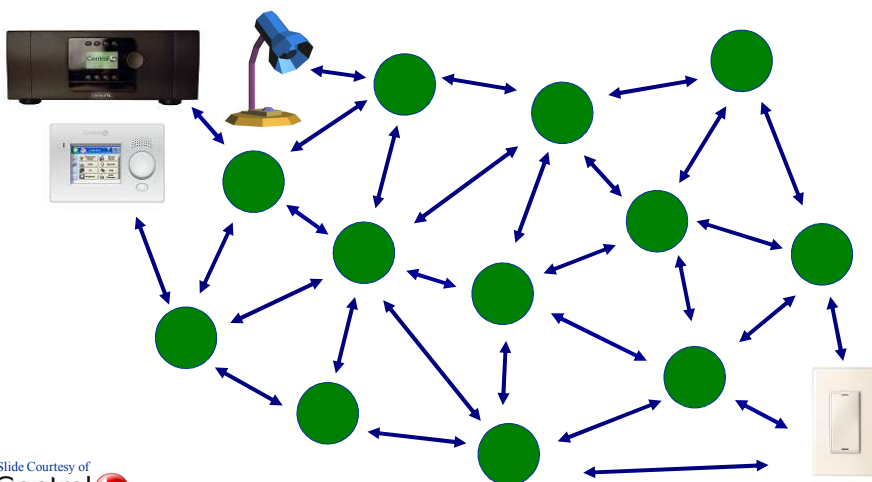
ZigBee Mesh Networking example
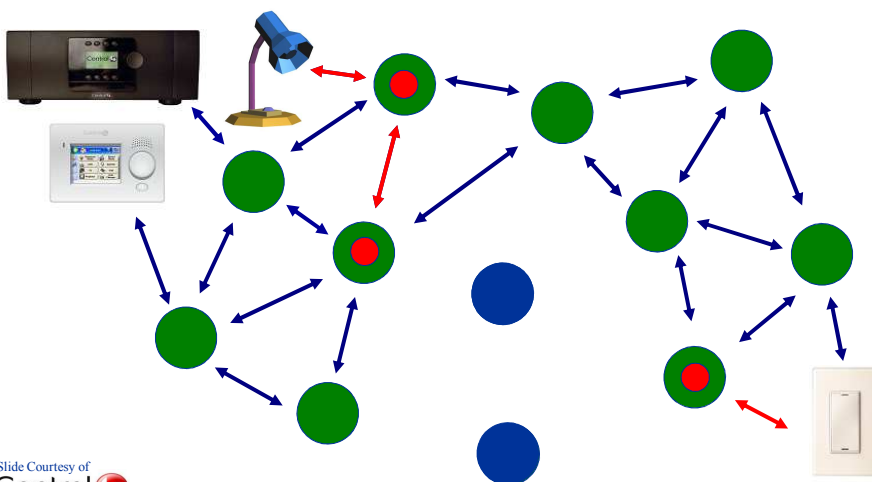
ZigBee Mesh Networking example
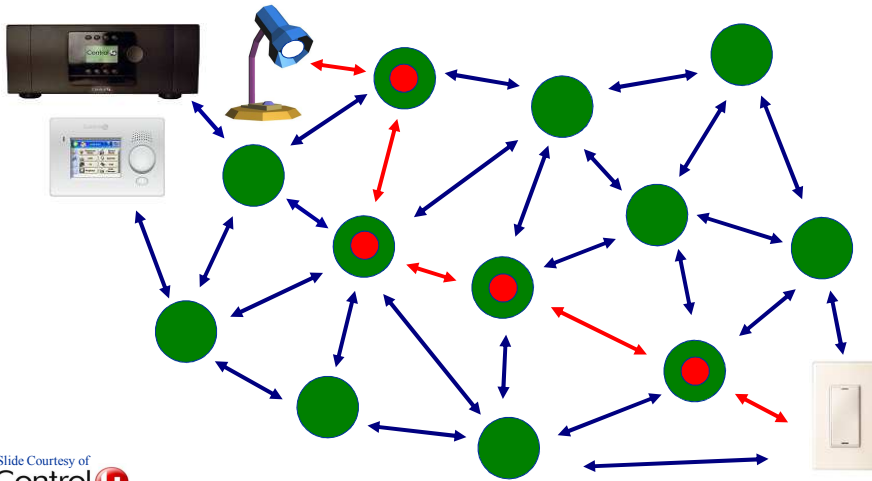
Slide Courtesy of
Control

Luciano Bononi 2006          seminar on IEEE 802.15.4 and ZigBee          33
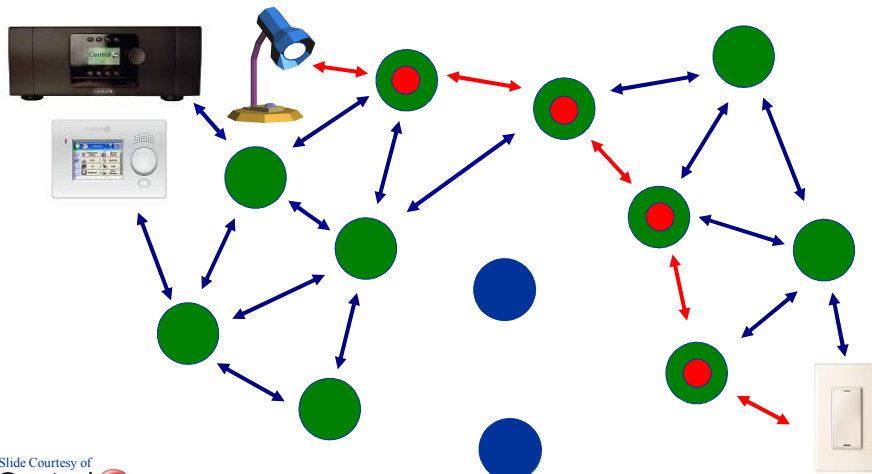


ZigBee Mesh Networking example

Slide Courtesy of
Control

Luciano Bononi 2006          seminar on IEEE 802.15.4 and ZigBee          34

17

## ZigBee Mesh Networking example



Slide Courtesy of
**Control**

---

## ZigBee Device Types

- **ZigBee Network Coordinator (ZNC)**
  - One and only one required for each ZB network.
  - Initiates network formation.
  - Acts as 802.15.4 2003 PAN coordinator (FFD).
  - May act as router once network is formed.

- **ZigBee Network Router (ZNR)**
  - Optional network component.
  - May associate with ZNC or with previously associated ZNR.
  - Acts as 802.15.4 2003 coordinator (FFD).
  - Participates in multihop routing of messages.

- **ZigBee End Device (ZED)**
  - Optional network component.
  - Shall not allow association.
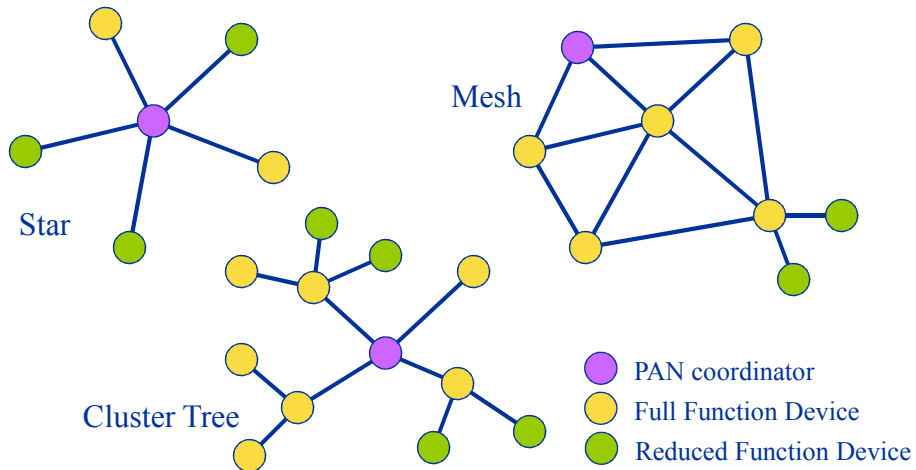  - Shall not participate in routing.

Slide credits: ZigBee Alliance

# ZigBee Network Topologies

Mesh

Star

Cluster Tree

PAN coordinator

Full Function Device

Reduced Function Device

seminar on IEEE 802.15.4 and ZigBee

37

# Network Structure (association)

ZigBee Coordinator

ZigBee Router

ZigBee End Device

Network association

seminar on IEEE 802.15.4 and ZigBee

38

# Network Structure



ZigBee Coordinator
ZigBee Router
ZigBee End Device
Network association

# Network Structure



ZigBee Coordinator
ZigBee Router
ZigBee End Device
Network association

# Cluster Tree Networks

- Cluster tree networks enable a peer-peer network to be formed with a minimum of routing overhead.



"Parent"

"Child"

Links indicate familial relationship, not communications capability
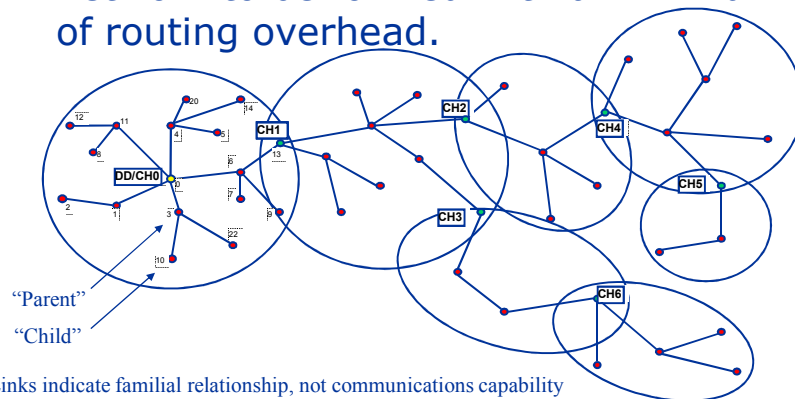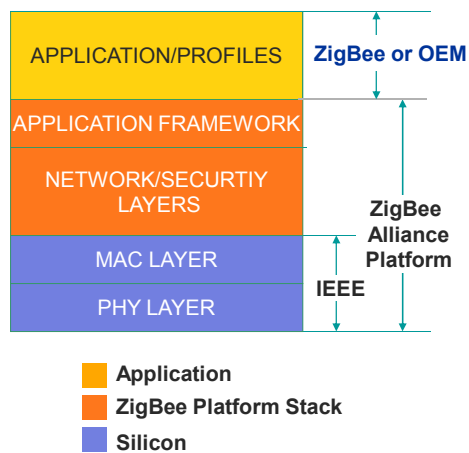
Slide credits: ZigBee Alliance

---

# Cluster Tree Networks

- Employ multi-hop routing (table driven)
  - AODV considered for dynamic routing in Meshes
- Can be very large:  255 clusters of 254 nodes each = 64,770 nodes
- May span physically large areas
- Suitable for latency-tolerant applications

Slide credits: ZigBee Alliance

## Protocol Stack Features

- 8-bit microcontroller (e.g. 80c51)
- Compact protocol stack
- Supports even simpler slave-only stack

| | |
|---|---|
| APPLICATION/PROFILES | ZigBee or OEM |
| APPLICATION FRAMEWORK | |
| NETWORK/SECURTIY LAYERS | ZigBee Alliance Platform |
| MAC LAYER | IEEE |
| PHY LAYER | |

**Application**
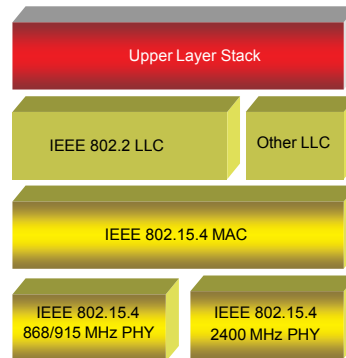**ZigBee Platform Stack**
**Silicon**

Slide credits: ZigBee Alliance

---

# IEEE 802.15.4
# Protocol Stack:

# Phy and MAC layers

# What IEEE 802.15.4 Addresses

- **IEEE 802.15.4**
  - MAC and PHY only

| | |
|---|---|
| **Upper Layer Stack** | |
| **IEEE 802.2 LLC** | **Other LLC** |
| **IEEE 802.15.4 MAC** | |
| **IEEE 802.15.4 868/915 MHz PHY** | **IEEE 802.15.4 2400 MHz PHY** |

Slide credits: ZigBee Alliance

---
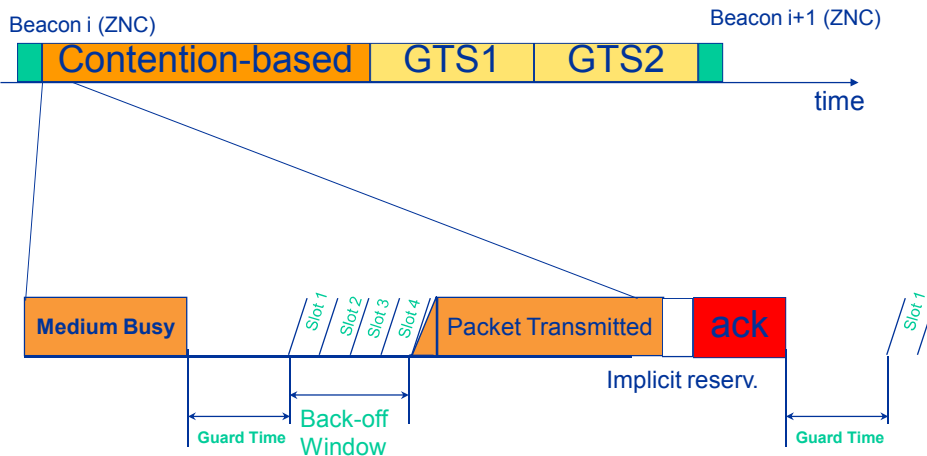
# ZigBee Channel Access Options

Two channel access mechanisms:

- Non-beacon network
  - A simple, traditional multiple access system used in simple peer and near-peer networks
  - Standard ALOHA CSMA-CA communications
  - Positive acknowledgement for successfully received packets

- Beacon-enabled network
  - Superframe structure- network coordinator transmits beacons at predetermined intervals
  - Dedicated bandwidth and low latency
  - Low Power Consumption mode for Coordinator

Slide credits: ZigBee Alliance

## IEEE 802.15.4 MAC channel access in one slide

- Example of superframe structure (optional) and basic contention-based MAC access scheme

Beacon i (ZNC)  Beacon i+1 (ZNC)

Contention-based | GTS1 | GTS2

time

Medium Busy | Slot 1 | Slot 2 | Slot 3 | Slot 4 | Packet Transmitted | ack | Slot 1

Implicit reserv.

Guard Time | Back-off Window | Guard Time

Luciano Bononi 2006 — seminar on IEEE 802.15.4 and ZigBee — 47

---

## Other Benefits of Beacon Mode

- Beacon Mode

  - A very powerful mechanism for controlling power consumption in extended networks like cluster tree or mesh
  - Allows all clients in a local piece of the network the ability to know when to communicate with each other
  - PAN has a coordinator that manages the channel and arranges the calls
  - Significant value will be in system power consumption for networks which are primarily battery powered

Slide credits: ZigBee Alliance

Luciano Bononi 2006 — seminar on IEEE 802.15.4 and ZigBee — 48

## ZigBee – Highly Reliable

- Mesh and tree networking protocol provides redundant paths
- Automatic retries and acknowledgements
- Broadcast delivery scheme ensures reliable broadcasts across the network
- Parents keep track of messages for sleeping children
- High intrinsic interference tolerance
  - Multiple channels
  - Frequency agility
  - Robust modulation

Slide credits: ZigBee Alliance

## ZigBee – Highly Secure

- Utilizes AES 128-bit encryption
- Concept of a "trust center"
- Link and network keys
- Authentication and encryption
- Security can be customized for the application
- Keys can be "hard-wired" into application

Slide credits: ZigBee Alliance

## IEEE 802.15.4 MAC summarized

- Employs 64-bit IEEE & 16-bit short addresses
  - Up to $2^{64}$ nodes (more than we'll probably need…)
  - local addressing, simple networks (65,000 nodes = 2^16)
- Two (physical) devices specified
  - Full Function Device (FFD)
  - Reduced Function Device (RFD)
- Three (logical) device roles specified:
  - ZigBee Network Coordinator (ZNC)
  - ZigBee Network Router (ZNR)
  - ZigBee End Node (ZED)
- Simple frame structure
- Reliable delivery of data (ACK)
- Association/disassociation
- AES-128 security
- Distribued CSMA-CA channel access (basic access mode)
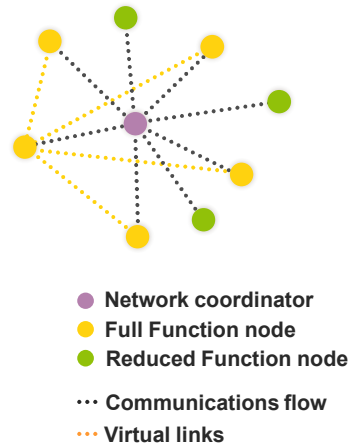- Optional superframe structure with beacons: GTS mechanism

## ZigBee Pro is Mesh Networking



- ZigBee Coordinator (FFD)
- ZigBee Router (FFD)
- ZigBee End Device (RFD or FFD)
- Mesh Link
- Star Link
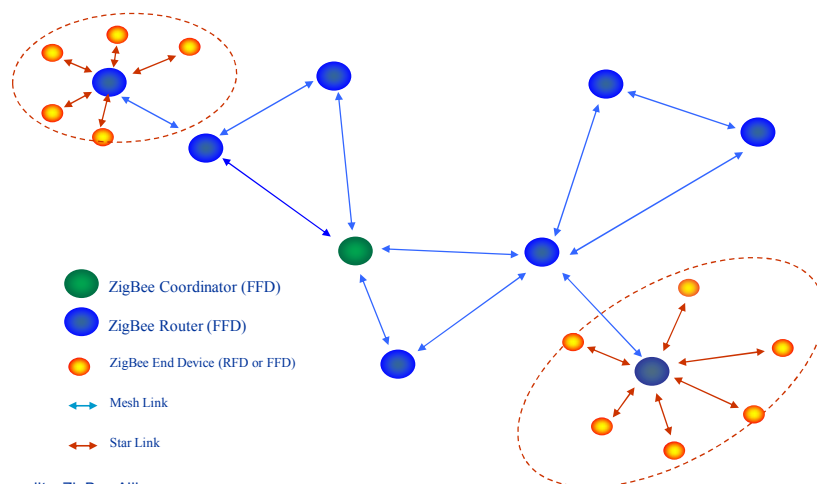
Slide credits: ZigBee Alliance

## Basic Network Characteristics

- 65,536 network (client) nodes

- Optimized for timing-critical applications
  - **Network join time**: 30 ms (typ)
  - Sleeping slave changing to active: 15 ms (typ)
  - Active slave channel access time: 15 ms (typ)

● Network coordinator
● Full Function node
● Reduced Function node

··· Communications flow
··· Virtual links

Slide credits: ZigBee Alliance

---

## ZigBee Stack components

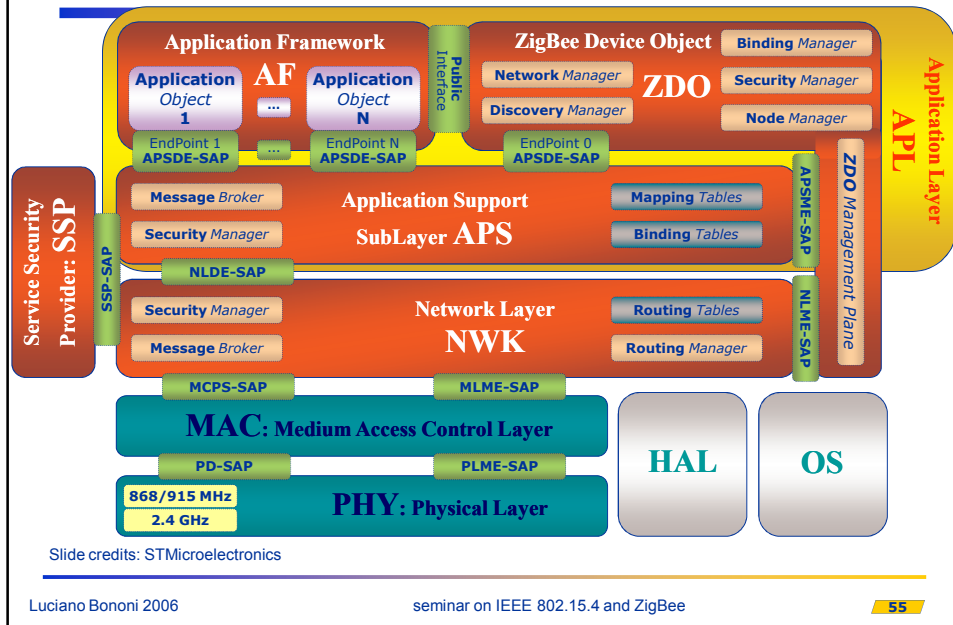Communication Protocol library
- IEEE 802.15.4
  - Phy & Mac
- ZigBee
  - Networking Layer
  - Application Framework
  - Security
- Cross-functions
  - HAL: hardware abstraction layer
  - OS-like functionalities

## IEEE 802.15.4/ZigBee Architecture

---

## ZigBee Stack "iper-space" (dimensions)

- **Depending on Topology/features**
  - ZigBee stack: Tree-based (static case),
  - ZigBee Pro stack: Mesh-based (dynamic case)
- **Depending on functionalities**
  - ZigBee Standard
  - Standard + proprietary extension
- **Depending on Nodes' type** (and Responsibilities)
    - *FFD (routing capabilities)*
    - *RFD (simple, end devices)*
  - Resources (Energy)
    - *Sleepy vs Non Sleepy*
    - *Mobile vs quasi-static*

# IEEE 802.15.4 PHY/MAC basics

**802.15.4 is a <u>simple</u> packet data protocol for <u>lightweight</u> wireless networks**

- **3 ISM bands**, 27 channels specified
- **Channel Access**
  - CSMA/CA slotted and unslotted
- Support for Message **Acknowledgement**, optional **Beacon** and **Guaranteed Time Slots**
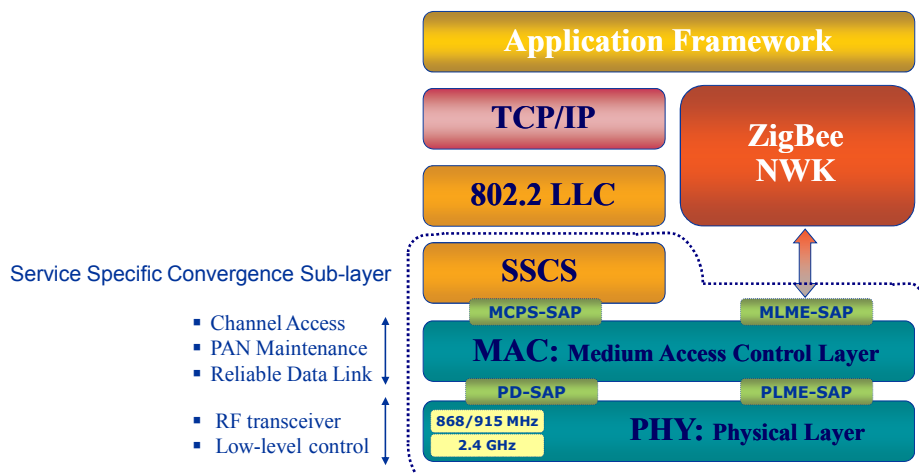- Multi-level **security**

Slide credits: STMicroelectronics

---

# IEEE 802.15.4 Architecture



Service Specific Convergence Sub-layer

- Channel Access
- PAN Maintenance
- Reliable Data Link

- RF transceiver
- Low-level control

Application Framework
TCP/IP
ZigBee NWK
802.2 LLC
SSCS
MCPS-SAP
MLME-SAP
**MAC:** Medium Access Control Layer
PD-SAP
PLME-SAP
868/915 MHz
2.4 GHz
**PHY:** Physical Layer

Slide credits: STMicroelectronics

# Services and Primitives

- For <u>confirmed service</u>, 4 primitive's types:
    1) request – higher entity asks for some service
    2) indication - entity is informed about event or remote service request
    3) response - entity to responds to event/requets
    4) confirm - entity is informed about its request status
- For <u>unconfirmed service</u>, only the first 2 types.
- Apply to all Layers.

Slide credits: STMicroelectronics

**Service Primitives**

- Indication = Interrupt

| Higher Layer | | Higher Layer |
|---|---|---|
| ① ↓ ↑ ④ | | ③ ↓ ↑ ② |
| Lower Layer | | Lower Layer |

1. Request      3. Response
2. Indication   4. Confirm

Unconfirmed service: No confirmation or response

The Ohio State University                                   Raj Jain

2-15

---

# IEEE 802.15.4 PHY: Functionalities

- TX/RX packets (PPDU) across physical medium
- Activation/deactivation of the radio transceiver
- Clear channel assessment (CCA)
- Energy detection (ED)
- Link quality indication (LQI)
- Channel selection

| Primitives | Description | Req | Conf | Resp | Indic |
|---|---|---|---|---|---|
| PD-DATA | Transmitting/ receiving packets | X | X | | X |
| PLME-GET | Getting PHY PAN information base | | | | |
| PLME-SET | Setting PHY PAN information base | | | | |
| PLME-SET-TRX-STATE | Activation/deactivation of the radio transceiver | X | X | | |
| PLME-CCA | Clear channel assessment | X | X | | |
| PLME-ED | Energy detection (ED) | X | X | | |

Slide credits: STMicroelectronics

## MAC responsibilities

- **MAC Data services**
  - enables MPDU exchange with PHY data service
- **MAC Management services**
  - Association/Disassociation
  - Orphaning and Sync with parent node
  - Beacon Management
  - Frame validation
  - Frame delivery ACK
  - Hooks up with security mechanisms

## IEEE 802.15.4 Security

- **Security modes**
  - Unsecured mode
  - ACL mode
  - Secured mode
- **Security Services**
  - Access Control
  - Data Encryption
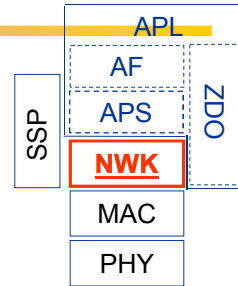  - Frame Integrity
  - Sequential Freshness

# NWK Layer

- **NWK Layer**
  - Structure/Functionalities
  - Responsibilities
- **Reference model**
  - NLDE: Data service
  - NLME: Management services

| | APL |
| SSP | AF |
| | APS |
| | NWK |
| | MAC |
| | PHY |

ZDO

---

# NWK Layer responsibilities

- Starting a network
  - the ability to successfully establish a new network.

- Joining and leaving a network
  - the ability to gain (join) or relinquish (leave) membership to a node of the network.

- Configuring a new device
  - the ability to sufficiently configure the stack for operation as required.

# NWK Layer responsibilities (cont)

- Addressing
  - the ability of a ZBC to assign short addresses (16 bits) to devices joining the network.
- Routing
  - rightful node/route discovery & maintenance operations
  - routing frames to their intended destinations
  - store of pertinent neighbor information
- Security
  - applying security to outgoing frames and removing security to terminating frames

---

# Routing: device's responsibilities

- **Mandatory** functionalities for both **ZBC** and **ZBR**:
  - Relay DATA frames on behalf of higher layers and/or other ZBRs.
  - Participate in route discovery in order to establish routes for subsequent DATA frames and/or on behalf of end devices.
  - Participate in end-to-end and local route repair.
  - Employ the ZigBee path cost metric as specified in route discovery and route repair.
- **Optional** functionalities for both **ZBC** and **ZBR**:
  - Maintain routing tables in order to remember best available routes.
  - Initiate route discovery on behalf of higher layers and/or of other ZBR.
  - Initiate end-to-end route repair.
  - Initiate local route repair on behalf of other ZigBee routers.

## Tree (1.0) vs Mesh (Pro) Stack

| Feature | Tree Stack "ZigBee" | Mesh Stack "ZigBee Pro" |
|---|---|---|
| ZigBee Stack Profile | HCL: HW comp. list | ZigBee<br>ZigBee Pro |
| ZigBee application profiles | HA: home automation | HA, CBA (commercial Buidling), IPM (industrial plant monitoring. WSA... |
| Messaging model | ZigBee APS messages with fragmentation | APS messages with (Uni-Multi-Broad)-cast |
| Routing method | Tree or Mesh | Mesh only (table driven) |
| Addressing method | Distributed Hierarchical (tree based) | Distributed alternative method (stochastic) |
| Bindings | Centralized: stored on Coordinator or source storage | Source only |
| Asymmetric Links | No detection | Detected and avoided |
| ZigBee End Devices | Sleepy ZED supported | Sleepy, Mobile ZEDs supported |
| Large sensor networks (100+ devices) | Not supported | Single-step route establishment back to data gateway |

Slide credits: STMicroelectronics

---

## The Application Layer

### Components:

- **APS**: Application Support <u>sub-layer</u>

- **ZDO**: ZigBee Device <u>Object</u>

- **AF**: Application <u>Framework</u>
  *the manufacturer-defined application objects*

- ZigBee **Application Profiles**

  - ZDP: ZigBee Device Profile

  - Per Application segment (HA, CBA, IPM, WSA, …)
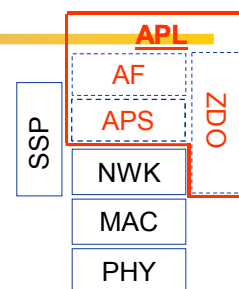
APL
AF
APS
ZDO
SSP
NWK
MAC
PHY

Slide credits: STMicroelectronics

## ZigBee Profiles

- Generalities:
    - 3 classes: private, public or published
    - Identifier has to be unique (assigned by the Alliance).
- Defined ZigBee profiles
    - ZDP: ZigBee Device Profile (*private*)
    - ZAP: ZigBee Application Profile (*public*)
        - HCL (obsolete), HA, CBA, IPM, WSA, …
- ZCL: ZigBee Cluster Library
    - Device and Cluster descriptions are independent from Profile Identifiers
    - Service types (KVP or MSG) → Replaced by ZCL

---

## APS Sub-layer

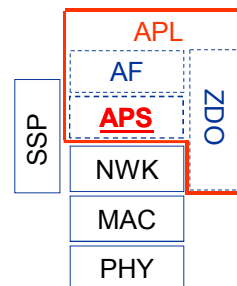- **APS Sub-Layer**
    - Responsibilities
    - Services
- **Reference model**
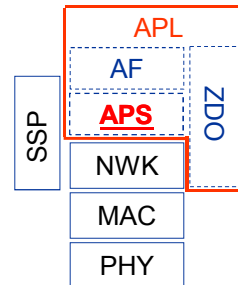    - APSDE: Data service
    - APSME: Management services

35

# APS Sub-layer

- **APS** <u>responsibilities</u>
  - maintaining tables for **binding**
    - (the ability to match 2 devices together based on their services and their needs)
  - forwarding messages between bound devices
- Its <u>services</u> are used by
  - the ZDO
  - Manufacturer-defined Application Objects

```
        APL
      ┌──────┐
 S    │  AF  │  Z
 S    ├──────┤  D
 P    │ APS  │  O
      ├──────┤
      │ NWK  │
      ├──────┤
      │ MAC  │
      ├──────┤
      │ PHY  │
      └──────┘
```

---

# APSME: APS Management Entity

## Management services

- Functionalities
  - <u>Binding</u>
    - *The ability to match 2 devices together based on their services and their needs.*
  - <u>Multicast Endpoint groups</u> management
    - *Single address shared by multiple sub-units (application objects).*
  - <u>Information management</u>
    - *To provide to read/write the value of an attribute from the AIB, Mapping/Binding tables, and Multicast Group tables*
  - <u>Security</u>
    - *The ability to set up authentic relationships with other devices through the use of secure keys.*
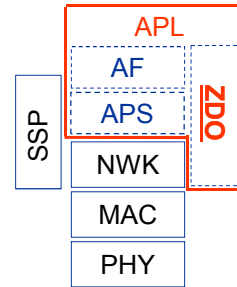
# ZigBee Device Object: ZDO

- **ZDO Layer**
  - Responsibilities
  - Structure
    - *Manager & Configuration Attributes*
- **ZDP: ZigBee Device Profile**
  - Client Services
  - Server Services

APL
AF
APS
SSP
ZDO
NWK
MAC
PHY

---

# ZigBee Device Object: ZDO

- It's a special application which employs NWK and APS primitives to implement ZBC, ZBR, ZED

- ZDO <u>responsibilities</u>:
  - Defining the role of the device
    - *Coordinator, Router, End Device*
  - Initialize APS, NWK, SSP
  - Devices & Service Discovery
  - Initiating and/or responding to binding requests
  - Establishing a secure relationship between network devices
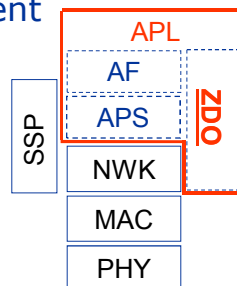
APL
AF
APS
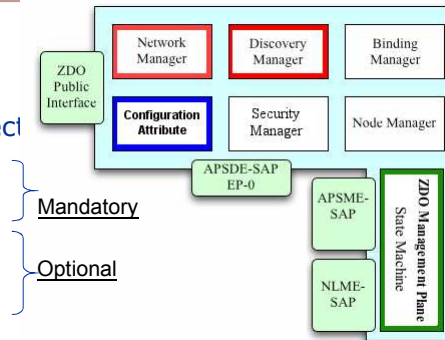SSP
ZDO
NWK
MAC
PHY

# ZDO: structure

- **ZDO structure:**

  - 1 Configuration Attributes Object
    (the .ini file for ZigBee devices)
  - 5 Manager Objects:
    - *Device and Service Discovery*
    - *Network Manager*
    - *Binding Manager*
    - *Security Manager*
    - *Node Manager*
  - It presents Public interfaces to the Application objects in the AF layer for control of device and network functions

  

  Mandatory

  Optional

Slide credits: STMicroelectronics

---

# ZDO: Device and Service Discovery

- Device discovery (other ZigBee device <u>by query</u>)
  - *IEEE address requests*
    - Unicast, the NWK address is known
  - *NWK address requests*
    - Broadcast, the IEEE address is known
- Service discovery
  - Discovery of the services available on endpoints
    - *By query for each endpoint on a given device*
    - *By using a match service feature (broadcast or unicast)*
    - *By having devices announce themselves*
  - Utilizes the complex, user, node, or power descriptors

Slide credits: STMicroelectronics

# Application Framework: AF
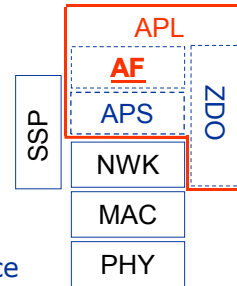
- ## AF <u>responsibilities</u>
  - **Hosting for the application objects**
    - *Addressed by an Endpoint number*
  - **APS functions used**
    - *Data services*
      - By using the new ZCL
      - Superseded KVP & MSG
  - **ZDO Functions used via the Public Interface**
    - *Control and management of the protocol layers in the ZigBee device*
    - *Initiation of standard network functions*

```
        APL
        AF      ZDO
SSP     APS
        NWK
        MAC
        PHY
```

Slide credits: STMicroelectronics

---

# Available ZigBee Stack (v.1.0) (old versions)

| Company | Stack name | MAC ver. | Platform used | |
|---|---|---|---|---|
| Ember | EmberZNet 2.x.0 | *integrated* | | |
| TI/Chipcon | F8W Z-Stack 1.0-1.3.0 | 0.71 -> 1.3 | TI 2420 TI 2430-2431 | |
| Freescale | Z-Stack 1.0-1.2.2 | v.1.063 | MC 13192-13193 | Old stack from F8W Probably not supported |
| Mindteck | BeeStack v.1.0 | | HCS08/MC13192 | for Freescale |
| Integration UK CompXs | ZigBee Stack v.1.25 | | Oki ML7065-032 | |
| AirBee | ZNS 0.92 | NA | | |
| Institute for Information Ind.-JP | III Zigbee Adv. Protocol | NA v3 / 1.0 | CC2420DB JN5121 / UZ2400DBK | for its own test for Jennic / Ubec |
| Helicomm | Helicomm Stack v.0.9.05 | Helicomm v.1.0 | iPLink EZDK | Also for Silabs |
| Silicon Lab | | | | |
| Korwin | WiniZB v.1.0 | | Atmel128+ CC2420 | |
| Renesas (RTA) | Renesas ZB v.0.97 | NA | M16C+ MC13192 M16C+ CC2420 | |

Slide credits: STMicroelectronics

## Available non-ZCP(zigbee certified platform) ZigBee Stack (v.?)

| Company | Stack name | MAC ver. | Platform used | |
|---|---|---|---|---|
| Microchip | ZigBee PicDem | | PicDemZ | NO ZCP |
| Atalum | GreenMesh | | | NO ZCP |
| Crossbow | | | | |
| BM | | | | |
| UbiWave | UbiNet | | | |
| Atmel | | | | |
| Meshnetics (ex LuxoftLabs) | ZigBeeNet | | | |
| Mitsubishi (MERL) | | | | Under development with Renesas |
| Dust Networks | | | | |
| ArchRock | | | | |
| One-RF Technology | ?? | ?? | | Available from Q4-06 |
| | | | | |
| OpenBee | OpenBee | | | Freeware |
| | | | | |

Slide credits: STMicroelectronics

---

## ZigBee
## Open Source protocol stack initiatives

…just old examples, more recent platforms are provided as experimental lab, based on Freescale MC1322x (ARM 7) and ATMEL (ATxmega256A3)

## Zigbee Projects on SourceForge

| Name | Description | Language | Code | Doc |
|---|---|---|---|---|
| **OpenBee** GPL, 12/2005 + Hw dev. kit | Design of an IEEE 802.15.4 compliant software, target independent | **C** | ✓ | ✗ |
| **OpenZig** LGPL, 06/2006 | Open source ZigBee and 802.15.4 stack Open Source (Atmel platform?) | – | ✗ | ✗ |
| **ZigBuzz** GPL, 01/2005 | "Implementation of Zigbee Phy, MAC, network, security and Application Stack on the Linux kernel 2.6.x" | – | ✗ | ✗ |
| **Linux Wireless Sensor LAN Project** GPL, 01/2005 | "Drivers and utility set for 802.15.4 standard low-rate wireless personal area networking" | – | ✓ | ✗ |
| **HomeRun 0.2.1** 10/2006 | Control and automation software for the home environment, multi-channel and multi-protocol (including Zigbee) | **Java** | ✓ | ✓ |
| **Open-zb** AFL (academic free), 10/2006 | Implementation of IEEE 802.15.4 in nesC for TinyOS and Crossbow Micaz motes | – | ✗ | ✗ |
| **FreakZ** (10/2008, sourceforge) | A GPL v2 open source Zigbee protocol stack. | **C** | ✓ | ✓ |

---

## ZigBee and (or vs.) TinyOS

- **TinyOS initiative proposed by Joe Polastre (Moteiv corp.)**

  - **"Zigbee should be the first network protocol released for TinyOS 2.0"**

- **Motivations:**

  - Zigbee is a standard.
  - TinyOS has received lukewarm, at best, recognition in the commercial sector. Embracing a standard protocol suite will bring attention to the project and interest from commercial users.
  - A standard protocol suite is valuable not just for commercial use, but also for academics.
  - A TinyOS-Zigbee implementation opens the door to improvements that the TinyOS community may propose to the Zigbee 2.0 technical working group.
  - Zigbee will help frame the design of TinyOS 2.0's networking architecture.
  - Think of the opportunities! "TinyOS inside" stickers for lightbulbs, thermostats, forklifts, trucks, toasters, microwaves, etc!

  - **Problem:** by downloading ZigBee specifications you agree that any use of the spec for non-Zigbee members is for non-commercial purposes. A company would adopt Zigbee-TinyOS if they can't use it for their commercial purposes?
  - moreover: if open source version of Zigbee exist for TinyOS how can the Open Source community cover themselves against patent infringement cases?
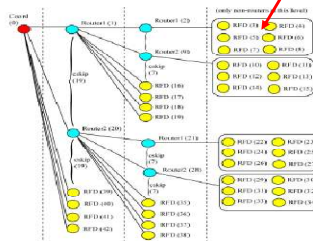
# e.g. ZigBee Stack Implementation (1)

- *Mississipi State University*, **Multi-platform Protocol Stack: Implementation of a subset of the Zigbee 1.0 Standard**.
- Source Code: www.ece.msstate.edu/!reese/msstatePAN/
- Zigbee functionalities:
  - Tree Routing topologies
  - Direct Messaging
  - Indirect Messaging

Tree routing with short address assignment
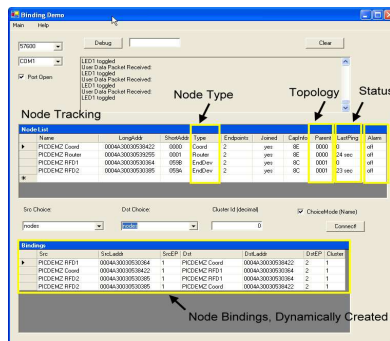
Multiplatorm devices supported

# ZigBee Stack Implementation (2)

- **Platform**: PICDEMOZ (PIC18 + CC2420 radio), Compiler: MCC18 or HI-TECH
- **Platform**: CC2430 Evaluation board/SOC_BB (CC2430/31 which has an 8051+802.15.4 Radio integrated in one die), Compiler: IAR51, HI-TECH C51
- **Platform**: WIN32 simulated RF nodes+ Virtual Board interface, Compiler: Microsoft Visual Studio .NET 2005

Emulation of virtual hardware sensor devices under Windows/.NET

Virtual device managent, network monitoring, application development

# e.g. TelosB Mote Platform (1)

- Crossbow's TelosB mote (TPR2400) is an open source platform designed to enable cutting-edge experimentation for the research community.
- http://www.xbow.com/Products/productsdetails.aspx?sid=126



TPR2400

Block diagram

Hardware with USB interface for device programming

---
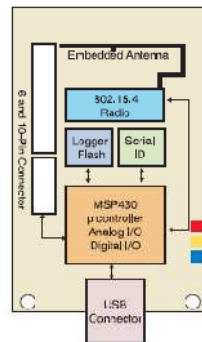
# e.g. TelosB Mote Platform (2)

- TelosB platform published by the Berkeley University

- Features:
  - IEEE 802.15.4 compliant
  - Integrated on-board antenna
  - Open-source Operating System (TinyOS)
  - Data Collection and programming via USB interface

- Applications:
  - Platform for low power research development
  - Wireless Sensor Network Experimentation

- Cost: $ 100 / $ 130 (Sw for Wireless sensor experimentation included)

## e.g. Chipcon CC2420 Mote Platform (1)

- The CC2420 Chipcon is a low-cost transceiver compliant with the IEEE 802.15.4 standard
- Evaluation of CC2420 performance by using the CC2420DK platform

**CC2420DK Evaluation Board:**

2 CC2420 chips

USB PORT

2 LEDS

2 TEST PORTS

1 SERIAL PORT

1 BUTTON

---
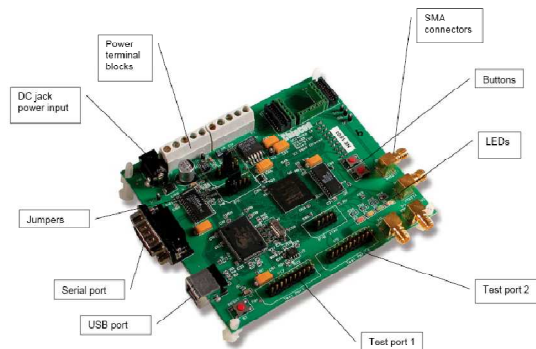
## CC2420 Mote Platform (2)
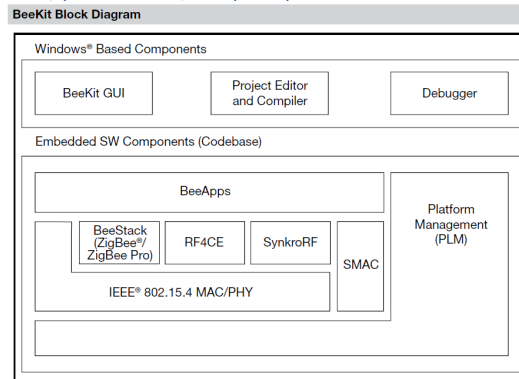
- CC2420 Web Page:
  - www.chipcon.com/index.cfm?kat_id=2&subkat_id=12&dok_id=115

- Resources available:
  - **SMARTRF Studio** sw for device programming
  - CC2420DBK Libraries and Examples
  - CC2420 IEEE 802.15.4 MAC Source Code

# Freescale BeeStack and MC 1322 (ARM7)

- Freescale 802.15.4 Platform
- Supports Freescale's simple media access controller (SMAC), IEEE 802.15.4 MAC, SynkroRF, RF4CE and BeeStack ZigBee/ZigBee Pro protocol stacks.
  - for different features, such as cost, performance, complexity and interoperability.



**BeeKit Block Diagram**

Windows® Based Components

| BeeKit GUI | Project Editor and Compiler | Debugger |

Embedded SW Components (Codebase)

BeeApps

| BeeStack (ZigBee®/ ZigBee Pro) | RF4CE | SynkroRF | SMAC | Platform Management (PLM) |

IEEE® 802.15.4 MAC/PHY

---

# Freescale BeeStack and MC 1322 (ARM7)

- Freescale 802.15.4 Platform
- Supports Freescale's simple media access controller (SMAC), IEEE 802.15.4 MAC, SynkroRF, RF4CE and BeeStack ZigBee/ZigBee Pro protocol stacks.
  - for different features, such as cost, performance, complexity and interoperability.
- **SMAC:** it is a simple and cost-effective start to wireless networking. Based on the 802.15.4 PHY, it provides commands to create simple point-to-point and star networks. The small 2.5–4K code size allows a low-cost platform for many applications requiring simple but effective wireless communication (over the air programming).
- **IEEE 802.15.4 MAC:** Freescale's fully compliant IEEE 802.15.4 MAC provides a robust building block for point-to-point, star and cluster tree networks. While the MAC is part of the SynkroRF, RF4CE and BeeStack protocol stacks, it is often used as the foundation for proprietary stacks as well. It supports optional features, including beaconed networks and guaranteed time (GTS).

# Freescale BeeStack

- **Freescale 802.15.4 Platform**
- **SynkroRF:** it is a 32 KB stack optimized for very quick design cycles and an easy to follow design process (when SMAC is too simple and ZigBee is too complex), N.B. it provides proprietary 802.15.4 wireless monitoring and control APIs. It is a network stack with both APIs or BlackBox access through a serial command set. Enhanced functionalities include interference avoidance (channel agility), larger data transfer with fragmentation, and low latency transmission. <u>SynkroRF as alternative when general interoperability is not required.</u>
- **RF4CE:** Freescale's RF4CE protocol is a 32 KB networking stack built on top of the IEEE 802.15.4 standard, optimized to support control, monitor and automate functions for **consumer electronics**, to replace old infrared (IR) technology with fast bidirectional link (!). Freescale's RF4CE builds on 802.15.4, and incorporates advances like in SynkroRF.
- **Beestack:** BeeStack is Freescale's ZigBee protocol stack that delivers a reliable and robust platform for ZigBee development, for larger, more complex networking (Zigbee/ZigbeePro) **+ mesh**, and reliable option for self-forming and self-healing mesh networks. Our Integrated Development Environment (IDE): IAR EWARM for ARM7 (32KB) (256KB IAR + 2000$)

---

# Freescale BeeStack

- **Freescale 802.15.4 Platform** (click to open MC 1322 data sheet)
- Freescale's BeeKit Wireless Connectivity Toolkit:
    - provides a simple GUI approach to configure network settings, allowing the embedded designer to concentrate on building the application.
    - BeeKit helps reduce development time for developers lacking extensive networking experience
    - BeeKit comes in all of Freescale's development kits and may also be downloaded at freescale.com. All protocol stacks are complimentary.
- **MC1322X Development Kit** (USB + J-TAG interf. debug/prog.)
    - 1322X-SRB (Sensor Reference Board): contains an MC13224 PiP, an MMA7260Q three-axis acceleration sensor, MPXV5010G pressure sensor and a temperature sensor.
    - 1322X-NCB (Network Coordinator Board): contains the MC13224 IC and a graphic LCD, creating the ideal demonstration platform for network coordinators. The LCD enables network monitoring by providing status messages.
    - 1322X-LPB (Low Power Board): contains the MC13224 and is ideal for power measurements. The small form factor supports both AAA batteries and coin cell use and has the optional buck converter enabled to provide a low-power option.
    - 1322X-USB: an 802.15.4/ZigBee packet sniffer, support cust. applications.

# Simulation and Commercial Products

- **802.15.4 implementation with ZigBee routing models (Ns2 simulator) free available at:**
  - http://ees2cy.engr.ccny.cuny.edu/zheng/pub/

- **ZigBee-related projects and products (at National Institute of Standards and Techonlogy (NIST):**
  - http://w3.antd.nist.gov/wctg/manet/adhoclinks.html #BLUETOOTH