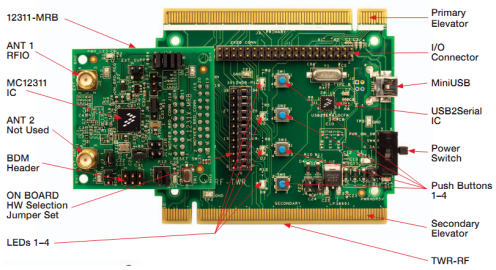
Section 7. Wireless Communication

Wireless Communication with 802.15.4/Zigbee Protocol

Outline

- Introduction to Freescale MC12311
- 802.15.4/Zigbee Protocol

TWR-12311 Module



TWR-MC12311 Smart Radio Features

- MC12311 sub-1 GHz system-in-package operating from 315 MHz to 960 MHz
- Programmable 32 KB flash memory and 2 KB RAM
- Programmable output power from -18 dBm to +17 dBm in 1 dB steps
- Two SMA antenna connectors
  - Unbalance input/output port
  - Power amplifier output
- High sensitivity: Down to -120 dBm at 1.2 Kbps
- On-board BDM port for MCU flash reprogramming and in-circuit hardware debugging
- USB port to interface with PC
- LEDs and switches for demonstration, monitoring and control

TWR-MC12311 Software Solutions

- **SMAC (Simple Media Access Controller)**
  This codebase provides simple communication and test apps based on drivers/PHY utilities available as source code. This environment is useful for hardware and RF debug, hardware standards certification, and developing proprietary applications.
- **IEEE 802.15.4 MAC with custom PHY layer**
  The Freescale MAC is a robust, mature codebase useful for developing networking solutions. Freescale is implementing an IEEE 802.15.4 MAC-compatible custom sub-1 GHz PHY template that can be used across different frequency bands.
  This capability allows users to build powerful networking solutions on a known, stable codebase.
- **Wireless MBUS stack**
  Freescale is porting an existing wireless MBUS codebase to the MC12311 platform which will be available through an external partner.

Different Wireless Protocols

1. Why ZigBee?

- We have WiFi, Cellular, Bluetooth, Why another Standard?

Standard	Bandwidth	Power Consump	Protocol Stack Size	Advantages	Applications
Wi-Fi (802.11)	Up to 54Mbps	400+mA TX, standby 20mA	100+KB	High data rate	Internet browsing, PC networking, file transfers
Bluetooth (802.15.1)	1Mbps	40mA TX, standby 0.2mA	~100+KB	Interoperability, cable replacement	Wireless USB, handset, headset
ZigBee (802.15.4)	250kbps	30mA TX, standby 3uA	4-32KB	Long battery life, low cost	Remote control, battery-operated products, sensors

Battery Life Examples

Example 1 **High-Duty Cycle**
- 5 Byte Data Transmission in intervals of 1.28 seconds
- assuming 200 mAh available battery capacity

- Battery lifetime based on **Bluetooth: 15 days**
- Battery lifetime based on **Freescale ZigBee: 33 days**

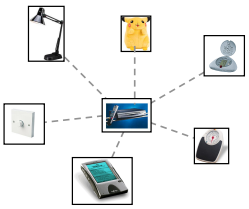
Example 2 **Event Driven Applications (security system scenario)**
- Network coordinator is on all the time (not battery powered)
- Sensor transmitting every 60 seconds + 10 events per days
- Based on 2 AA batteries

- Battery lifetime based on **Bluetooth: 100 days**
- Battery lifetime based on **Freescale ZigBee: 3559 days or 9.8 years**

UNIVERSITY of Rhode Island

Home Area Network/Personal Area Network

- Home Networking
- Automotive Networks
- Industrial Networks
- Interactive Toys
- Remote Metering



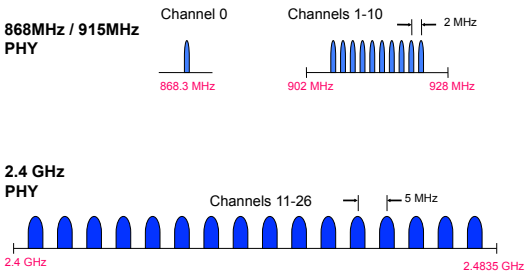
UNIVERSITY of Rhode Island

ZigBee Physical Layer Overview

- The IEEE 802.15.4 is a standard developed for Wireless Personal Area Networks (WPANs).
- An over the air data rate of 250 kbit/s in the 2.4 GHz band.
- 16 independent communication channels in the 2.4 GHz band.
- Large networks (up to 65534 devices).
- Devices use carrier sense multiple access with collision avoidance (CSMA-CA) to access the medium.
- Two topologies: star and p2p, both topologies use one and only one central device, the PAN coordinator, that is the principal controller of the network:
- Low power consumption.
- Devices use Energy Detection (ED) for channel selection.
- Devices inform the application about the quality of the wireless link - Link Quality Indication (LQI).

UNIVERSITY of Rhode Island

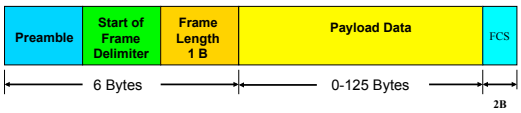
Operating Frequency Bands



UNIVERSITY of Rhode Island

Packet Structure

- Preamble (4 bytes) – synchronization
- Start of Frame Delimiter (1 byte)
- Frame Length (1 byte)
- Data field up to 125 Bytes



UNIVERSITY of Rhode Island

Physical Layer Primitives

PHY Data Service
- PD-DATA – exchange data packets between MAC and PHY

e.g.

```
/***************************************
*Function: Transmit data packet
*Parameters: packet pointer
*Return:status
***************************************/
int pd_data_request(tx_packet_t *packet)
```

PHY Management Service
- PLME-CCA – clear channel assessment
- PLME-ED - energy detection
- PLME-GET / -SET– retrieve/set PHY PIB *(PAN Info Base)* parameters
- PLME-TRX-ENABLE – enable/disable transceiver

UNIVERSITY of Rhode Island

3. MAC Layer System Overview

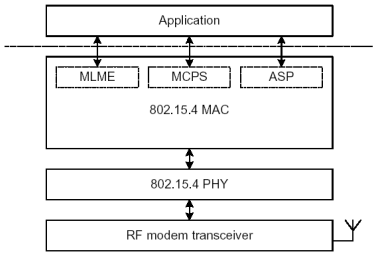


Figure 1-4. System Block Diagram

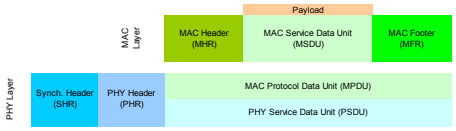
Two Types of Devices

- Full function device (FFD)
  - Any topology: Star, P2P (both use one and only one central device: the PAN coordinator)
  - Network coordinator capable
  - Talks to any other device
- Reduced function device (RFD)
  - Limited to star topology
  - Cannot become a network coordinator
  - Talks only to a network coordinator
  - Very simple implementation

Long Addresses and Short Addresses

- All devices have 64 bit IEEE addresses
- Short addresses (2 bytes long) can be allocated
- Addressing modes:
  - Network + device identifier (star)
  - Source/destination identifier (peer-peer)

MAC Frame Structure

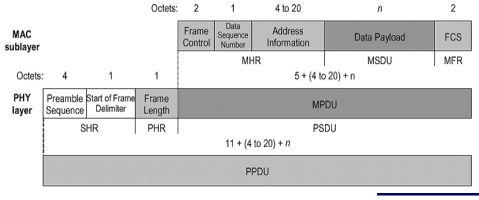


4 Types of MAC Frames:

- Data Frame
- Beacon Frame
- Acknowledgment Frame
- MAC Command Frame

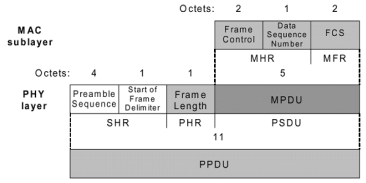
Data Frame Format

- Is one of two most basic and important structures in 15.4.
- Provides up to 104 byte data payload capacity
- Data sequence numbering ensures that packets are tracked
- Robust structure improves reception in difficult conditions
- Frame Check Sequence (FCS) validates error-free data



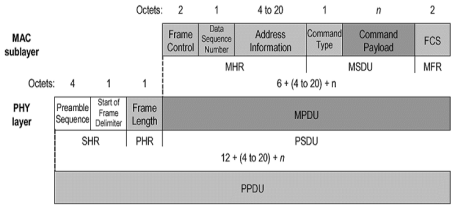
Acknowledgment Frame Format

- The other most important structure for 15.4: It provides active feedback from receiver to sender that packet was received without error.
- Short packet that takes advantage of standards-specified quiet time immediately after data packet transmission.



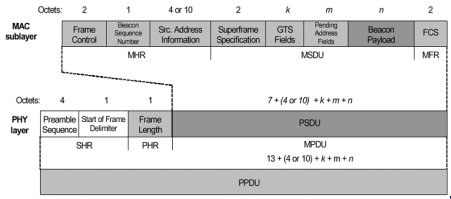
MAC Command Frame Format

- Is a mechanism for remote control and configuration of client nodes
- Allows a centralized network manager to configure individual clients no matter how large the network



Beacon Frame Format

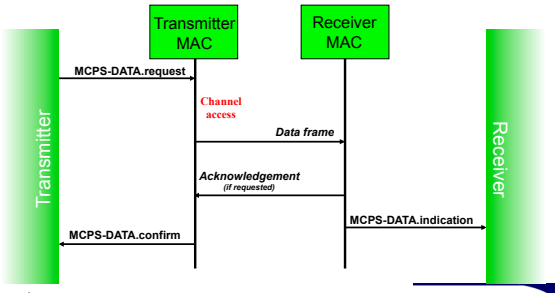
- Beacons add a new level of functionality to a network.
- Client devices can wake up only when a beacon is to be broadcast, listen for their address, and if not heard, return to sleep.
- Beacons are important for mesh and cluster tree networks to keep all of the nodes synchronized without requiring nodes to consume precious battery energy listening for long periods of time.



Two Operation Modes

- **Beacon Mode:**
  Beacon Frames Transmitted by network coordinator to synchronize data transfers.
- **Non Beacon Mode**:
  Data transmission can take place at any time
- **Traffic Types:**
  - Periodic data
    - Application defined rate (e.g. sensors)
  - Intermittent data
    - Application/external stimulus defined rate (e.g. light switch)
  - Repetitive low latency data
    - Allocation of time slots (e.g. mouse)

MAC Data Service



MAC Primitives

MAC Data Service
- MCPS-DATA – exchange data packets between MAC and PHY
- MCPS-PURGE – purge an MSDU from the transaction queue

- **MAC Management Service**
- MLME-ASSOCIATE/DISASSOCIATE – network association
- MLME-SYNC / SYNC-LOSS - device synchronization
- MLME-SCAN - scan radio channels
- MLME- COMM-STATUS – communication status
- MLME-GET / -SET– retrieve/set MAC PIB parameters
- MLME-START / BEACON-NOTIFY – beacon management
- MLME-POLL - beaconless synchronization
- MLME-GTS - GTS management
- MLME-RESET – request for MLME to perform reset
- MLME-ORPHAN - orphan device management
- MLME-RX-ENABLE - enabling/disabling of radio system

Creating Applications Using ZigBee 1

1. **Basic Setup**
   - **Initialization:** by calling `Init_802_15_4()`
   - **Resetting:** using MLME-RESET.request
   - **Implementing SAP's**
2. **Starting a New PAN:** After setup, MLME,MCPS, and ASP can be accessed by apps
   - First thing is to set up a coordinator because all IEEE 802.15.4 Standard PANs must have a PAN coordinator.

Creating Applications Using ZigBee 2

3. Energy Detection Scan

- The first task that a PAN coordinator must perform is to choose which radio frequency to use for its PAN.
- Selective or all channel scan using mask bits in `scanChannels`
- A channel that showed no sign of activity at the time of the scan, shows an energy level of approximately 0x00.
- how long to scan on each channel is specified in `scanDuration` parameter
- A byte value is returned for each channel: `pEdList[0]` contains the result for channel 11, `pEdList[1]` contains the result for channel 12 and so on. pEdList[15] for channel 26

UNIVERSITY of Rhode Island

Creating Applications Using ZigBee 3

4. Choosing Short Address

- All units come with a pre-assigned long address, but a short address must be assigned before starting the PAN. Otherwise, the start request will fail.
- Because the PAN coordinator is the first unit to participate in its own PAN, it can chose any short address for itself.
- The short address must be different from 0xFFFF.
- A long address is 8 bytes long; a short address is 2 bytes long.

5. Choosing PAN ID

- the last thing required before a PAN coordinator can start a PAN, is for the coordinator to select an identification number for the PAN which is called the PANid, that must be unique in the logical channel.

UNIVERSITY of Rhode Island

Creating Applications Using ZigBee 4

6. Starting a PAN

- After choosing a logical channel, PANid, and short address, it is time to start up the PAN using the MLME_START.request primitive.
- The `panCoordinator` parameter indicates whether the start request is to start up a PAN for a PAN coordinator or for a coordinator without PAN coordinator capability.
- `beaconOrder` and `superFrameOrder` parameters are set to 0x0F because users want to start a non-beacon network.
- Finally, the `securityEnable` parameter tells the MLME if it should apply any security to the transactions taking place over the air.

UNIVERSITY of Rhode Island

Application Support Features

- **Profile:** an agreement on a series of messages defining an application space (for example, "Home Controls – Lighting")
- **Endpoint:** a physical dimension added to a single ZigBee radio that permits support for multiple applications, addressed by the Endpoint number (0-31)
- **Interface:** a logical extension, defined per Endpoint, which permits advertisement of multiple Profiles per Endpoint (to support proprietary extensions, backward compatibility and other application needs)
- **Key Relationships:**
  - Maximum of 30 Endpoints per ZigBee device (0 is reserved to describe the device itself and 31 is reserved for broadcast messaging to all endpoints)
  - Maximum of 8 Interfaces per Endpoint
  - One Profile described per Interface

UNIVERSITY of Rhode Island