ZigBee tutorial

Emad Ebeid
Ph.D. student @ CS depart
University of Verona, Italy
EmadSamuelMalki.Ebeid@univr.it

Davide Quaglia
Assistant Professor @ CS depart
University of Verona, Italy
Davide.Quaglia@univr.it

Outline

- Introduction
- ZigBee frequencies
- ZigBee concepts
  - protocol Stack , Profiles, Clusters
- ZigBee application
  - Addressing
- ZigBee Architecture
  - ZC,ZR,ZED
- Practical part and ZigBee tools

2

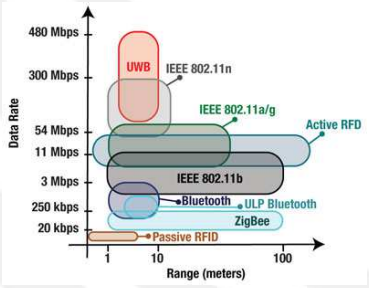
Introduction

- **ZigBee** stands for " **Z**onal **I**ntercommunication **G**lobal-standard, where **B**attery life was long, which was **E**conomical to deploy, and which exhibited **E**fficient use of resources."
- ZigBee stands over IEEE 802.15.4 PHY & MAC
- ZigBee aims:
  - Low data rate
  - Low power consumption
  - Small packet devices

3

802.15.4/ZigBee Frequencies

- Operates in ISM radio bands:
  - 868 MHz **European** Band at 20kbps
  - 915 MHz **North American** Band at 40kbps
  - 2.4 GHz **Global** Band at 250kbps



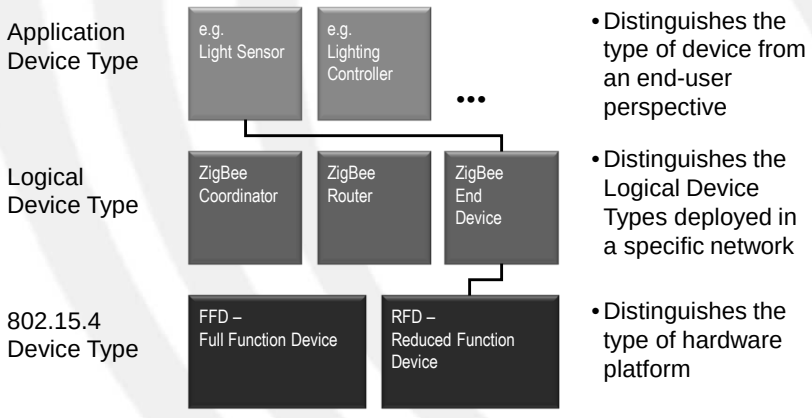
4

ZigBee and Other Wireless Technologies

Market Name	ZigBee™	---	Wi-Fi™	Bluetooth™
Standard	802.15.4	GSM/GPRS CDMA/1xRTT	802.11b	802.15.1
Application Focus	Monitoring & Control	Wide Area Voice & Data	Web, Email, Video	Cable Replacement
System Resources	4KB - 32KB	16MB+	1MB+	250KB+
Battery Life (days)	100 - 1,000+	1-7	.5 - 5	1 - 7
Network Size	Unlimited (2^{64})	1	32	7
Bandwidth (KB/s)	20 - 250	64 - 128+	11,000+	720
Transmission Range (meters)	1 - 100+	1,000+	1 - 100	1 - 10+
Success Metrics	Reliability, Power, Cost	Reach, Quality	Speed, Flexibility	Cost, Convenience

5

Application Device Type Model



- Distinguishes the type of device from an end-user perspective
- Distinguishes the Logical Device Types deployed in a specific network
- Distinguishes the type of hardware platform

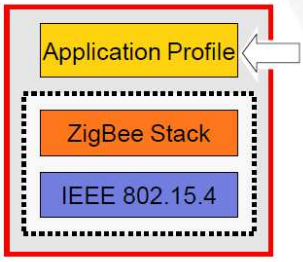
- ZigBee products are a combination of Application, Logical, and Physical device types
- Profiles may define specific requirements for this combination, but can also leave this up to manufacturers

6

Application Profiles

Clusters
0: off
1: on
2: scene 1
3: scene 2

Clusters
0: off
1: on
2: temp set
3: time set



- Application profiles define what messages are sent over the air for a given application
- Devices with the same application profiles interoperate end to end

7

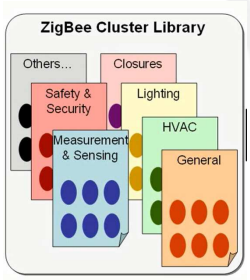
ZigBee Application profiles

- Determines application-level features, protocol
- Defines device types with different capabilities (clusters)
  - 2 bytes "device ID" enumerates device type within the profile
- Inherits network-level features from stack feature set
- Identified by **2 bytes** application profile IDs
  - assigned by ZigBee Alliance
  - can request private profile IDs for custom applications or use one of ZigBee's published application profiles
- *Examples:*
  - Home Automation (HA) — based on ZigBee or Zigbee Pro
  - Commercial Building Automation (CBA) — based on ZigBee Pro
  - Smart Energy (SE) — based on ZigBee or ZigBee Pro
  - Manufacturer-Specific Profile (MSP) — anything proprietary

8

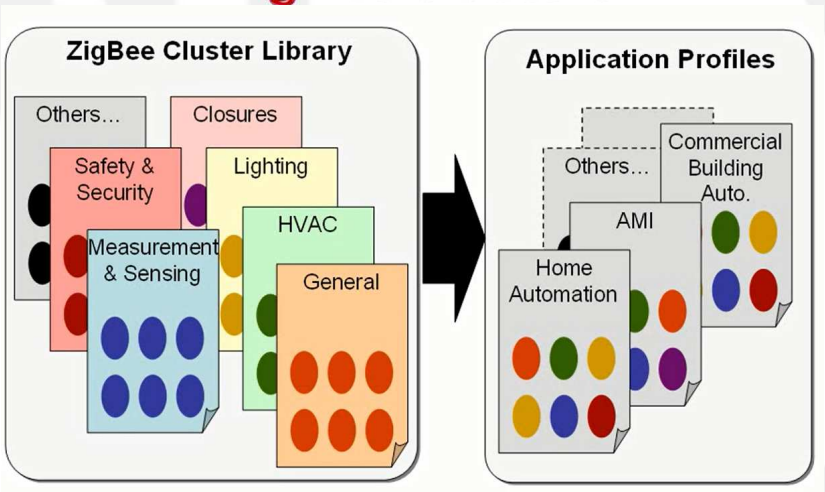
ZigBee clusters

- A "cluster" is a set of message types related to a certain device function
- Enumerated by **2 bytes** Cluster ID
- Defines clusters for use in public profiles
  - Same cluster (and ID) can be used in multiple profiles
- Defines "attributes" and "commands" for a given cluster
- Groups clusters into "functional domains", e.g. Lighting, HVAC
- Uses "client" and "server" model of communication
  - Client sends messages to server: server maintains attributes



9

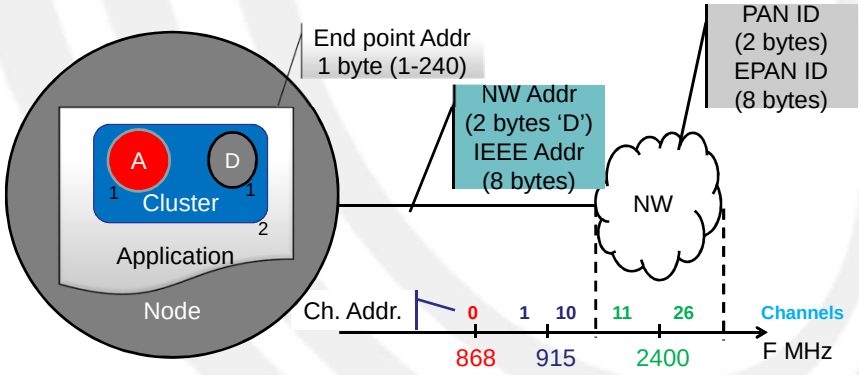
ZigBee clusters



10

ZigBee addressing

- Addressing is the way in which a message gets from one place to another in a network.



11

ZigBee addressing

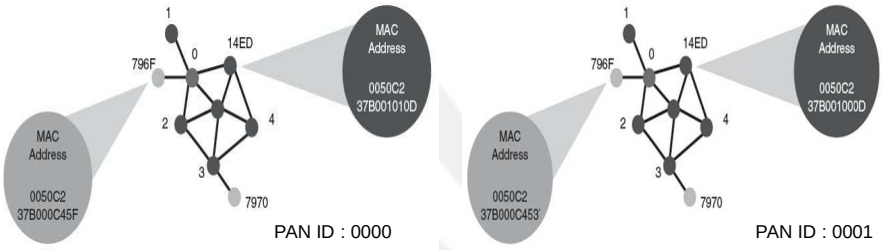
- For 2.4 GHz

Name	Range	Description
Channel	11–26	A physical portion of the RF spectrum
PAN ID	0x0000–0x3fff	The address of a network within a channel
NwkAddr	0x0000–0xfff7	The address of a node within a network
Endpoint	1–240	The address of an application within a node
Cluster	0x0000–0xffff	The object within the application
Command	0x00–0xff	An action to take within the cluster
Attribute	0x0000–0xffff	A data item within the cluster

12

ZigBee addressing

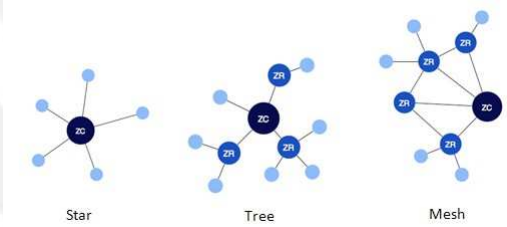
- The MAC address, also called IEEE address, long address, or extended address, is a 64bit number that uniquely identifies this board from all other ZigBee boards in the world



13

ZigBee architecture

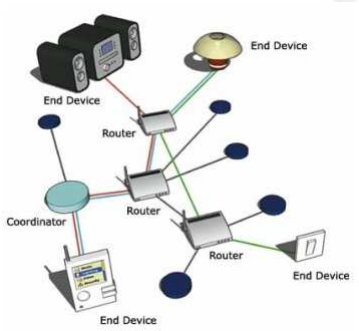
- There are three different types of ZigBee devices:
  - ZigBee coordinator (ZC)
  - ZigBee Router (ZR)
  - ZigBee End Device (ZED)



14

ZigBee Coordinator (ZC)

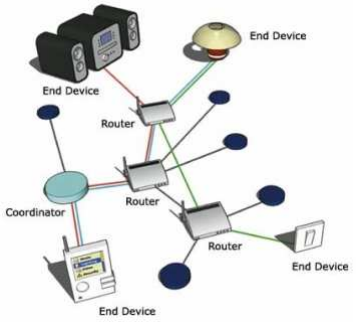
- only one in a network
- initiates network
- stores information about the network
- all devices communicate with the ZBC
- routing functionality
- bridge to other networks



15

ZigBee Router (ZR)

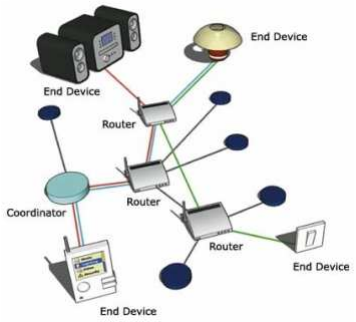
- optional component
- routes between nodes
- extends network coverage
- manages local address allocation/de-allocation



16

ZigBee End Device (ZED)

- optimized for low power consumption
- cheapest device type
- communicates only with the coordinator via routers
- sensor would be deployed here



17

Summery for ZigBee device types

ZigBee Type	Notes
ZigBee Coordinator (ZC)	Special router that forms the network; only 1 per PAN
ZigBee Router (ZR)	No duty cycling available
ZigBee End Device (ZED)	Does not participate in routing; may be sleepy; requires ZC/ZR "parent" for network participation

ZC ZR ZED

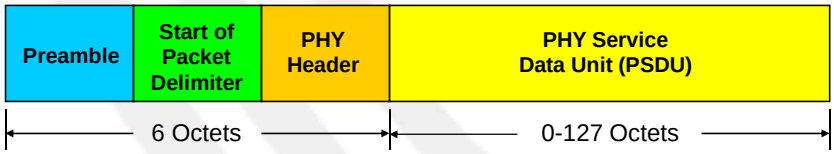
18

IEEE 802.15.4 PHY Overview

Packet Structure

PHY Packet Fields

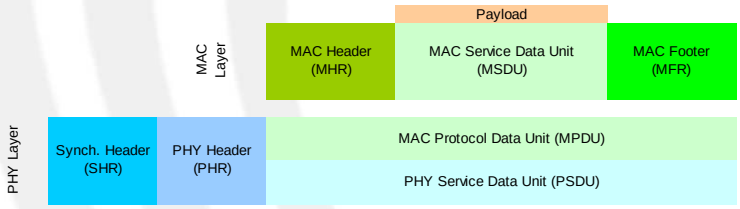
- Preamble (32 bits) – synchronization
- Start of Packet Delimiter (8 bits)
- PHY Header (8 bits) – PSDU length
- PSDU (0 to 1016 bits) – Data field



19

IEEE 802.15.4 MAC Overview

General Frame Structure



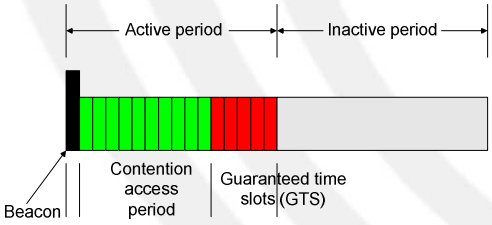
4 Types of MAC Frames:

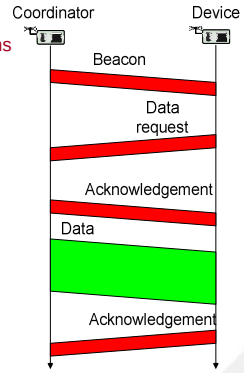
- Data Frame
- Beacon Frame
- Acknowledgment Frame
- MAC Command Frame

20

IEEE 802.15.4 MAC overview

- Star networks: ***devices*** are associated with ***coordinators***
  - Forming a PAN, identified by a PAN identifier
- Coordinator
  - Bookkeeping of devices, address assignment, generate beacons
  - Talks to devices and peer coordinators
- Beacon-mode superframe structure





21

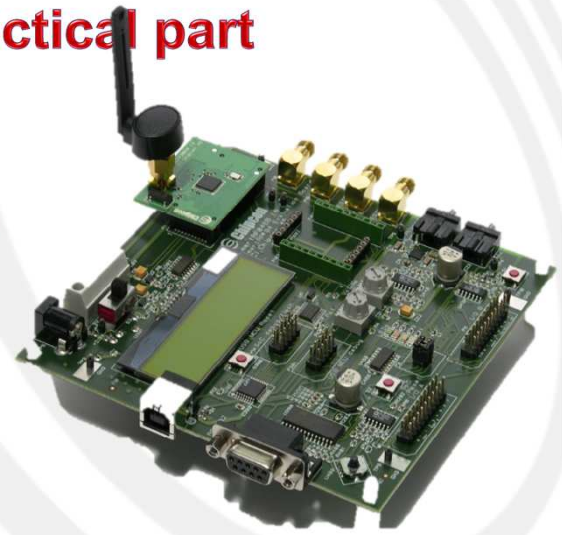
ZigBee tools

- Z-Stack™: is TI's ZigBee compliant protocol stack for a growing portfolio of IEEE 802.15.4 products and platforms
- IAR: is a development tools for testing and compiling Z-Stack based applications.
  - It incorporates IAR C/C++ Compiler for ARM Cortex-M3, assembler, linker, librarian, text editor, project manager, and debugger
- SmartRF™ Studio: is a Windows application that can be used to evaluate and configure Low Power RF-ICs from Texas Instruments.

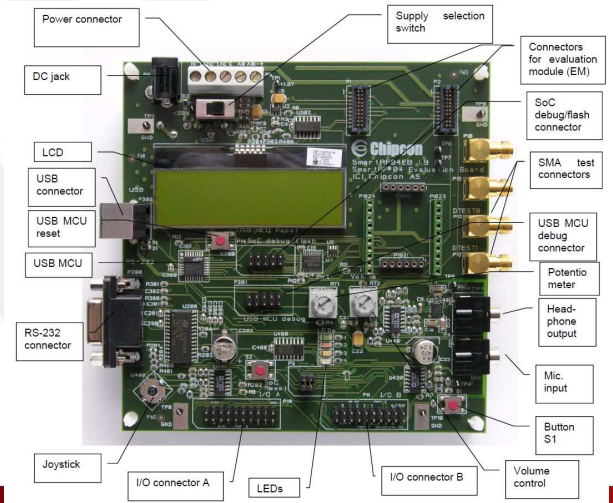
22

Practical part

- Zigbee boards:
  - **Chipcon SmartRF04EB Evaluation Board with CC2430EM**

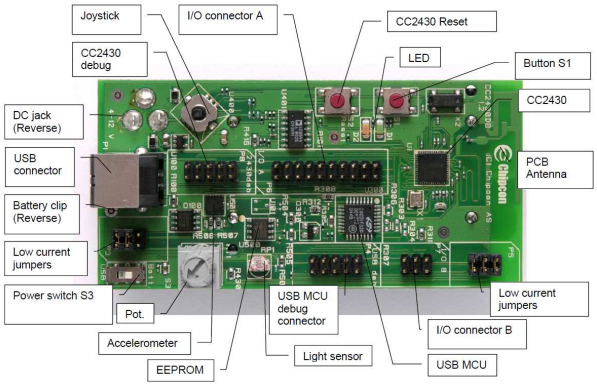


Practical part



Practical part

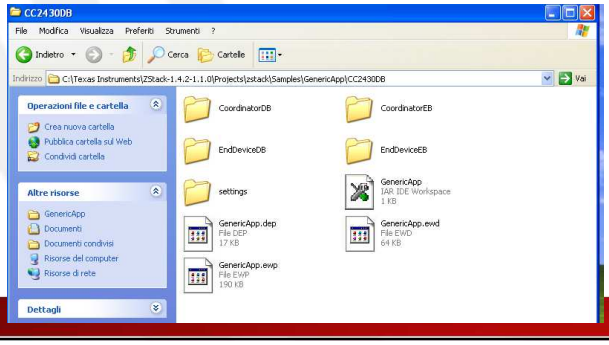
- Zigbee boards:
  - **Chipcon CC2430DB Development Board**



25

Open example

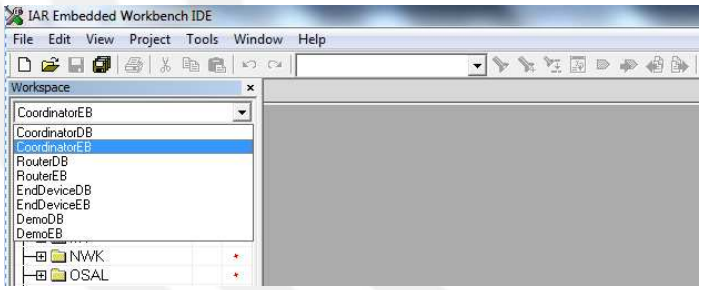
- Open GenericApp example(Zstack & IRA tools) from example folder as shown bellow:
  - C:\texasInstrument\Zstack-1.4.2.1.1.0\project\Zstack\samples\GenericApp\CC2430DB\GenericApp



26

Practical part

– Choose Coordinator or End device based on your board type (ED, DB) and ZigBee role (ZC,ZR,ZED)



27

Practical part

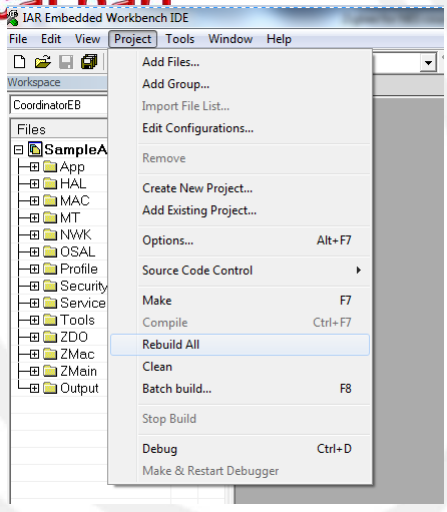
– then
  - Project-> buildall
  - Project->Debug

  (for configuration)

Reset zigBee kit from its switch.

– S300 for EB
– S2 for DB

- Repeat these steps to configure other devices

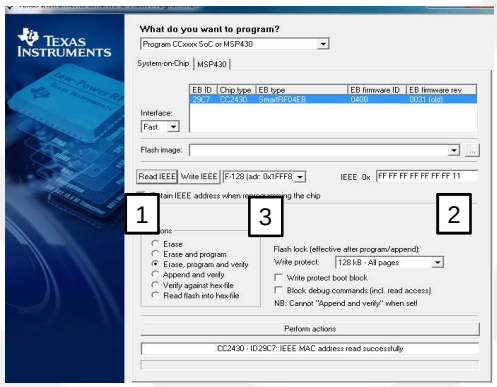


28

Practical part

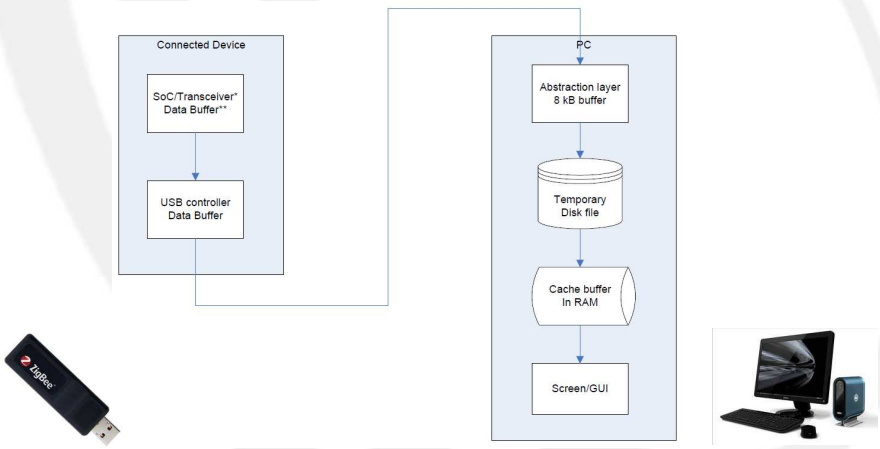
- SmartRF tool
  - IEEE address 8 bytes (static)

1. Read
2. Change IEEE
3. Write



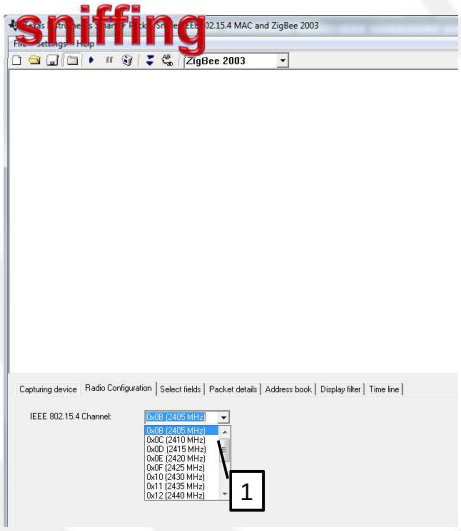
29

RF sniffing



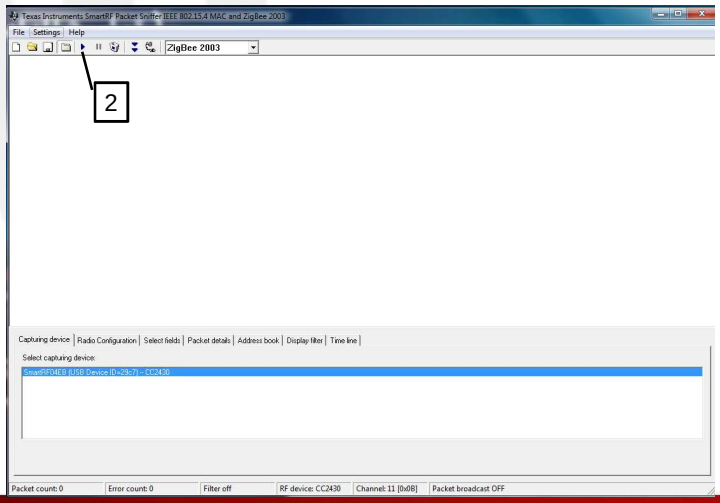
30

RF sniffing



31

RF sniffing



32

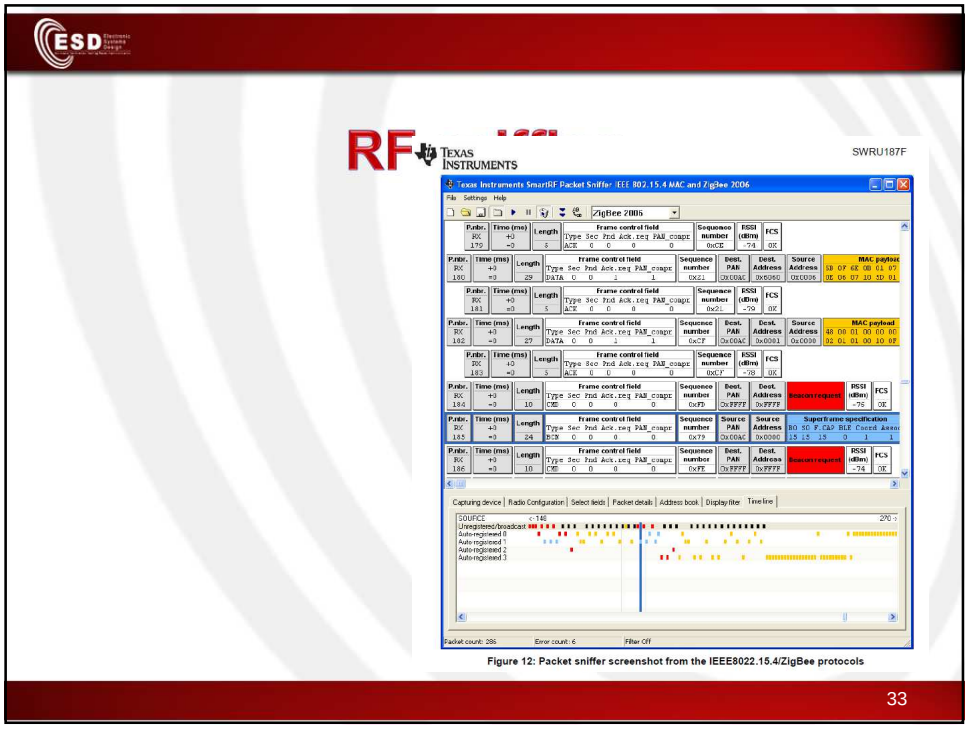


Figure 12: Packet sniffer screenshot from the IEEE8022.15.4/ZigBee protocols

33

34