

ZigBee/IEEE 802.15.4 Fundamentals

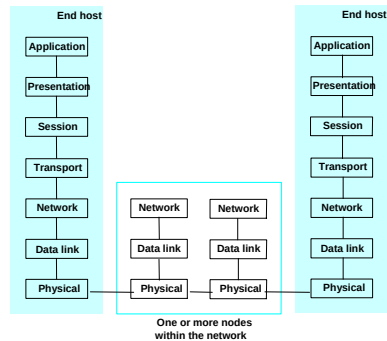
1

IEEE 802.15.4

- IEEE 802.15.4 is a standard which specifies the physical layer and medium access control for low-rate wireless personal area networks (LR-WPAN's).
- It is the basis for the ZigBee specification
- ZigBee application space
 - Home Networking
 - Automotive Networks
 - Industrial Networks
 - Interactive Toys
 - Remote Metering

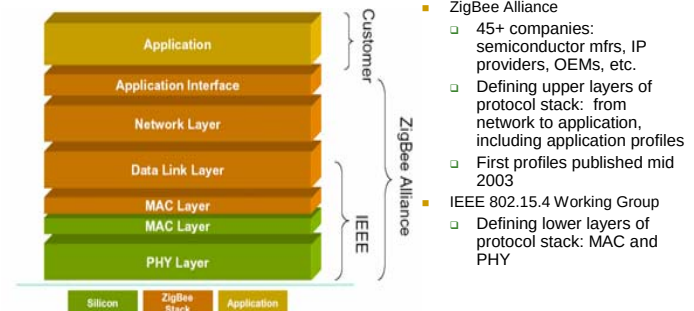
2

Open System Interconnect (OSI) Layered Architecture



3

ZigBee/802.15.4 Architecture



- ZigBee Alliance
 - 45+ companies: semiconductor mfrs, IP providers, OEMs, etc.
 - Defining upper layers of protocol stack: from network to application, including application profiles
 - First profiles published mid 2003
- IEEE 802.15.4 Working Group
 - Defining lower layers of protocol stack: MAC and PHY

4

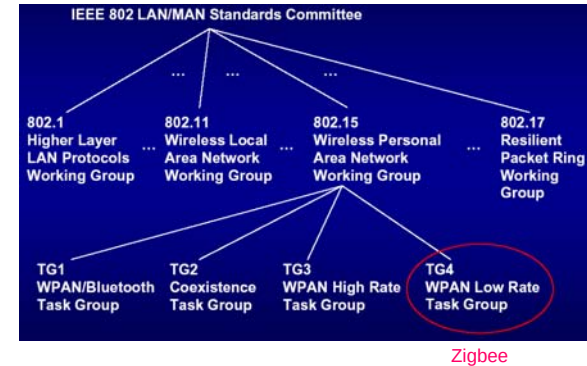
What is ZigBee Alliance?

- An organization with a mission to define reliable, cost effective, low-power, wirelessly networked, monitoring and control products based on an open global standard
- The alliance provides interoperability, certification testing, and branding.



5

IEEE 802.15 Working Group



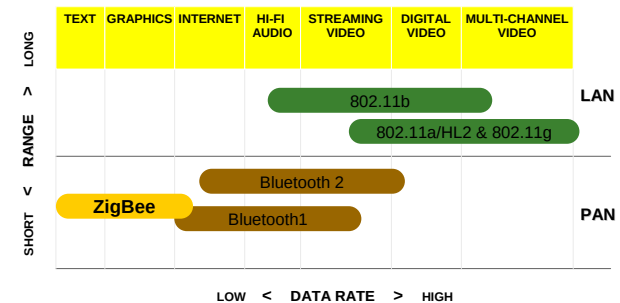
6

Comparison Between WPAN

Project	Data Rate	Range	Configuration	Other Features
802.15.1 (Bluetooth)	1 Mbps	10M (class 3) 100M (class 1)	8 active device Piconet/ Scatternet	Authentication, Encryption, Voice
802.15.3 High Rate	22, 33, 44, 55 Mbps	10M	256 active device Piconet/ Scatternet	FCC part 15.249 QoS, Fast Join Multi-Media
802.15.4 Low Rate	up to 250Kbps	10M nominal 1M-100M based on settings	Master/Slave (256 Devices or more) Peer to Peer	Battery Life: multi-month to infinite
802.15.2 Coexistence	Develop a Coexistence Model and Mechanisms Document as a Recommended Practice			

7

Wireless Markets



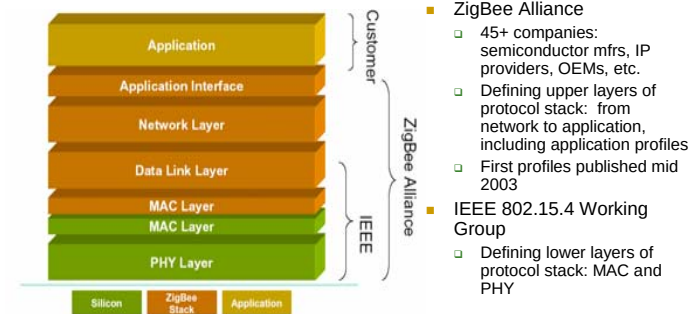
8

ZigBee/IEEE 802.15.4 Features

- Low power consumption
- Low cost
- Low offered message throughput
- Supports large network orders ($\leq 65k$ nodes)
- Low to no QoS guarantees
- Flexible protocol design suitable for many applications

9

ZigBee/802.15.4 Architecture



10

ZigBee/802.15.4 Technology: General Characteristics

- Data rates of 250 kbps, 20 kbps and 40kbps.
- Star or Peer-to-Peer operation.
- Support for low latency devices.
- CSMA-CA channel access.
- Dynamic device addressing.
- Fully handshaked protocol for transfer reliability.
- Low power consumption.
- 16 channels in the 2.4GHz ISM band, 10 channels in the 915MHz ISM band and one channel in the European 868MHz band.
- Extremely low duty-cycle ($<0.1\%$)

11

IEEE 802.15.4 Basics

- 802.15.4 is a simple packet data protocol for lightweight wireless networks
 - Channel Access is via **Carrier Sense Multiple Access with collision avoidance** and **optional time slotting**
 - **Message acknowledgement** and an **optional beacon structure**
 - Multi-level security
 - Works well for
 - **Long battery life**, selectable latency for controllers, sensors, remote monitoring and portable electronics
 - Configured for maximum battery life, has the potential to last as long as the shelf life of most batteries

12

Carrier sense multiple access with collision avoidance

In computer network, CSMA/CA belongs to a class of protocols called multiple access methods.

In CSMA, a station wishing to transmit

- (1) listen to the channel for a predetermined amount of time
- (2) If the channel is sensed "idle" then transmit.

If the channel is sensed as "busy". the station has to defer its transmission.

- (3) once the channel is clear, a station sends a signal telling all other stations not to transmit, and then sends its packet.

13

Carrier sense multiple access with collision detection

- CSMA/CD used in Ethernet
- The transmit algorithm works as follows:
 - If line is idle...
 - send immediately
 - upper bound message size of 1500 bytes
 - must wait 9.6us between back-to-back frames
 - If line is busy...
 - wait until idle and transmit immediately
 - called *1-persistent*, with probability of 1 in transmitting (special case of *p-persistent*, with a probability of p)

14

Carrier sense multiple access with collision detection

- If collision...
 - jam for 32 bits, then stop transmitting frame
 - minimum frame is 64 bytes (header + 46 bytes of data)
 - delay and try again
 - 1st time: 0 or 51.2us
 - 2nd time: 0, 51.2, or 102.4us
 - 3rd time: 51.2, 102.4, or 153.6us
 - n th time: $k \times 51.2\mu s$, for randomly selected $k=0..2^n - 1$
 - give up after several tries (usually 16)
 - exponential backoff

15

Carrier sense multiple access with collision avoidance

- CSMA/CA is used where CSMA/CD cannot be implemented due to the nature of the channel.
- CSMA/CA is used wireless LANs.
- Problems of wireless LANs
 - impossible to listen while sending, therefore collision detection is not possible. "listening" means detecting the energy in the air at certain frequency band.
 - the hidden terminal problem, whereby a node A, in range of the receiver R, is not in range of the sender S, and therefore cannot know that S is transmitting to R.

16

IEEE 802.15.4 Device Types

- There are two different device types :
 - A full function device (FFD)
 - A reduced function device (RFD)
- The FFD can operate in three modes serving
 - Device
 - Coordinator
 - PAN coordinator
- The RFD can only operate in a mode serving:
 - Device

17

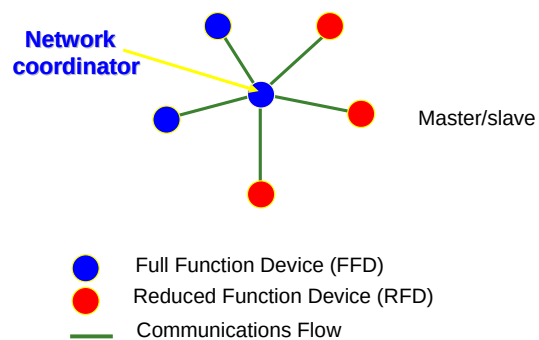
FFD vs RFD

- Full function device (FFD)
 - Any topology
 - 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



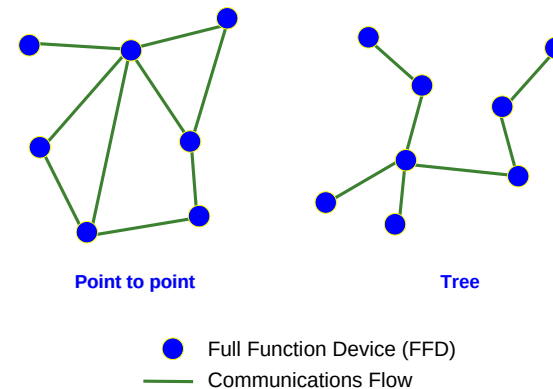
18

Star Topology



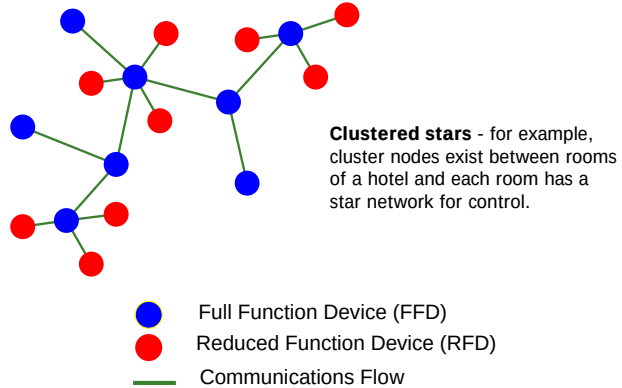
19

Peer-Peer Topology



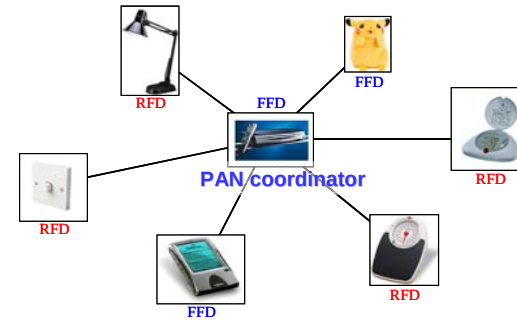
20

Combined Topology



21

Example Network



22

Device Addressing

- Each independent PAN will select a unique **PAN identifier**
- All devices operating on a network shall have unique **64-bit extended address**. This address can be used for direct communication in the PAN
- A member can use a 16-bit short address, which is allocated by the PAN coordinator when the device is associated.
- Addressing modes:
 - star: Network (64 bits) + device identifier (16 bits)
 - peer-to-peer: Source/destination identifier (64 bits)
 - cluster tree: Source/destination cluster tree + device identifier (unclear yet)

23

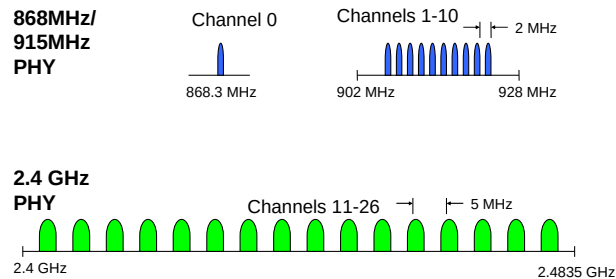
IEEE 802.15.4 PHY Overview

- PHY functionalities:
 - Activation and deactivation of the radio transceiver
 - Energy detection within the current channel
 - Link quality indication for received packets
 - Clear channel assessment for CSMA-CA
 - Channel frequency selection
 - Data transmission and reception

24

IEEE 802.15.4 PHY Overview

Operating Frequency Bands



25

Frequency Bands and Data Rates

The standard specifies two PHYs :

- 868 MHz/915 MHz direct sequence spread spectrum (DSSS) PHY (11 channels)
 - 1 channel (20Kb/s) in European 868MHz band
 - 10 channels (40Kb/s) in 915 (902-928)MHz ISM band
- 2450 MHz direct sequence spread spectrum (DSSS) PHY (16 channels)
 - 16 channels (250Kb/s) in 2.4GHz band

26

direct-sequence spread spectrum (DSSS)

- direct-sequence spread spectrum (DSSS) is a **modulation** technique.
- As with other **spread spectrum** technologies, the transmitted signal takes up more **bandwidth** than the information signal that is being modulated.
- The name 'spread spectrum' comes from the fact that the carrier signals occur over the full bandwidth (spectrum) of a device's transmitting frequency.

27

direct-sequence spread spectrum (DSSS)

- It phase-modulates a sine wave pseudorandomly with a continuous string of pseudonoise (PN) code symbols called "chips",
- Each chip has a much shorter duration than an information bit. That is, each information bit is modulated by a sequence of much faster chips.
- Therefore, the chip rate is much higher than the information signal bit rate
- The resulting signal resembles white noise, like an audio recording of "static".
- The resulting effect of enhancing signal to noise ratio on the channel is called *processing gain*.
- By employing a longer PN sequence and more chips per bit, , larger processing gain, but physical devices used to generate the PN sequence impose practical limits on attainable processing gain.

28

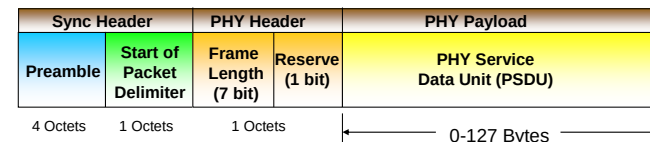
DSSS -CDMA

- At the receiving end, by multiplying it by the same pseudorandom sequence (because $1 \times 1 = 1$, and $-1 \times -1 = 1$) to reconstruct the original signal.
- This process, known as "de-spreading", mathematically constitutes a correlation of the transmitted PN sequence with the receiver's assumed sequence.
- The transmit and receive sequences must be **synchronized**. This requires the receiver to synchronize its sequence with the transmitter's sequence via some sort of timing search process.
- With a different PN sequence (or no sequence at all), the de-spreading process results in no processing gain for that signal.
- This effect is the basis for the **code division multiple access (CDMA)** property of DSSS, which allows multiple transmitters to share the same channel within the limits of the cross-correlation properties of their PN sequences.

29

PHY Frame Structure

- PHY packet fields**
 - Preamble (32 bits) – synchronization
 - Start of packet delimiter (8 bits) – shall be formatted as "11100101"
 - PHY header (8 bits) –PSDU length
 - PSDU (0 to 127 bytes) – data field



30

General Radio Specifications

- Transmit Power**
 - Capable of at least 3dBm (all power levels are referenced by 1 mW, a 1-mW signal is 0 dBm, 1uW signal corresponds to -30dBm)
- Receiver Sensitivity**
 - 85 dBm (2.4GHz) / -91dBm (868/915MHz)
- Link quality indication**
 - A characterization of the strength and/or quality of a received packet used by above layers
 - The measurement may be implemented using
 - Receiver energy detection
 - Signal to noise ratio estimation

31

General Radio Specifications

- Clear Channel Assessment (CCA)**
 - CCA mode 1: energy above threshold (lowest)
 - CCA mode 2: carrier sense (medium)
 - CCA mode 3: carrier sense with energy above threshold (strongest)
- The energy detection threshold shall be at most 10 dB above the specified receiver sensitivity.
- The CCA detection time shall equal to 8 symbol periods.

Each data bit → Symbol → 32-Chip PN sequence → O-QPSK modulator

32

PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

33

Symbol	Chip sequence ($C_0, C_1, C_2, \dots, C_{31}$)
0	11011001110000110101001000101110
1	11101101100111000011010100100010
2	00101110110110011100001101010010
3	00100010111011011001110000110101
4	01010010001011101101100111000011
5	00110101001000101110110110011100
6	11000011010100100010111011011001
7	10011100001101010010001011101101
8	10001100100101100000011101111011
9	10111000110010010110000001110111
10	01111011100011001001011000000111
11	01110111101110001100100101100000
12	00000111011110111000110010010110
13	01100000011101111011100011001001
14	10010110000001110111101110001100
15	11001001011000000111011110111000

34

IEEE 802.15.4 MAC Overview

- Simple frame structure
- Association/disassociation
- AES-128 security
- CSMA/CA channel access
- GTS mechanism

35

IEEE 802.15.4 MAC

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**)

36

Frame Structure: Data transport concepts

- Frames are the basic unit of data transport
- Four fundamental types: **data**, **acknowledgment**, **beacon** and **MAC command frames**
- A **superframe** structure, defined by the coordinator, may be used, in which case **two beacons** act as its limits and provide synchronization to other devices.
- A superframe consists of sixteen equal-length slots, which can be further divided into an active part and an inactive part, during which the coordinator may enter power saving mode, not needing to control its network.
- Within superframes **contention** occurs between their limits, and **is resolved by CSMA/CA**

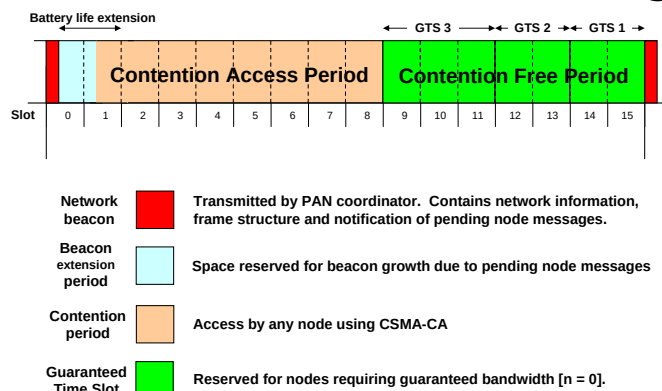
37

Data transport concepts

- Every transmission must end before the arrival of the second beacon.
- Applications can use up to **seven** domains of one or more contentionless **guaranteed time slots**, trailing at the end of the superframe.
- The first part of the superframe must be sufficient to give service to the network structure and its devices.
- Superframes are typically utilized within the context of low-latency devices, whose associations must be kept even if inactive for long periods of time.

38

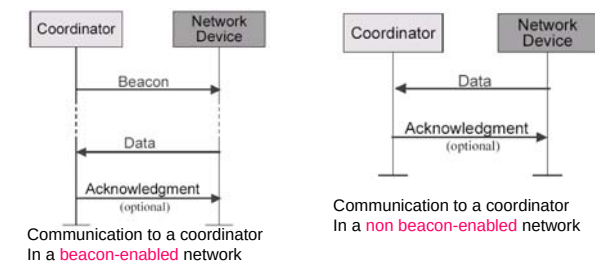
Frame Structure



39

Data Transfer Model

- Data transferred from device to coordinator
 - In a beacon-enabled network, device finds the beacon to synchronize to the superframe structure. Then using slotted CSMA/CA to transmit its data.
 - In a non beacon-enabled network, device simply transmits its data using unslotted CSMA/CA

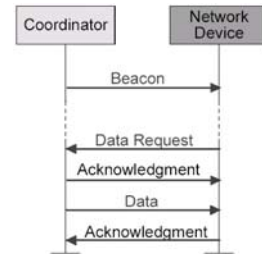


40

Data Transfer Model

- Data transferred from coordinator to device

- In a beacon-enabled network, the coordinator indicates in the beacon that "data is pending."
- Device periodically listens to the beacon and transmits a **MAC command request** using slotted CSMA/CA if necessary.



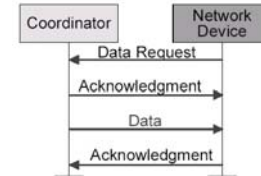
Communication from a coordinator
in a **beacon-enabled** network

41

Data Transfer Model

- Data transferred from coordinator to device

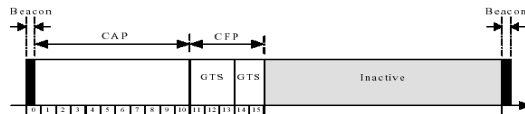
- In a non beacon-enabled network, a device transmits a **MAC command request** using **unslotted CSMA/CA**.
 - similar to unslotted ALOHA
- If the coordinator has its pending data, the coordinator transmits data frame using unslotted CSMA/CA.
- Otherwise, the coordinator transmits a data frame with zero length payload.



Communication from a coordinator
in a **non beacon-enabled** network

42

Superframe Structure



- A superframe is divided into two parts

- Inactive: all stations sleep
- Active:
 - Active period will be divided into 16 slots
 - 16 slots can further divided into two parts
 - Contention Access Period (CAP)
 - Contention Free Period (CFP)

43

Superframe Structure (cont.)

- There are two parameters:

- **SO**: to determine the length of the active period
- **BO**: to determine the length of the beacon interval.
- In CFP, a GTS may consist of multiple slots, all of which are assigned to a single device, for either transmission (t-GTS) or reception (r-GTS).
 - GTS = guaranteed time slots
- In CAP, the concept of slots is not used.
 - Instead, the whole CAP is divided into smaller "contention slots".
 - Each "contention slot" is of 20 symbols long.
 - This is used as the smallest unit for contention backoff.
 - Then devices contend in a slotted CSMA/CA manner.

44

Channel Access Mechanism

- Two type channel access mechanism, based on the network configuration:
 - In non-beacon-enabled networks → unslotted CSMA/CA channel access mechanism
 - In beacon-enabled networks → slotted CSMA/CA channel access mechanism
 - The superframe structure will be used.
- Point-to-point networks may either use unslotted CSMA/CA or synchronization mechanisms; in this case, communication between any two devices is possible, whereas in “structured” modes one of the devices must be the network coordinator.

45

Channel Access Mechanism

- The backoff period boundaries of every device in the PAN shall be aligned with the superframe slot boundaries of the PAN coordinator
 - i.e. the start of first backoff period of each device is aligned with the start of the beacon transmission
- The MAC sublayer shall ensure that the PHY layer commences all of its transmissions on the boundary of a backoff period

46

GTS Concepts

- A guaranteed time slot (GTS) allows a device to operate on the channel within a portion of the superframe.
- A GTS shall only be allocated by the PAN coordinator.
 - ... and is announced in the beacon.
- The PAN coordinator can allocated up to seven GTSs at the same time
- The PAN coordinator decides whether to allocate GTS based on:
 - Requirements of the GTS request
 - The current available capacity in the superframe

47

GTS Concepts (cont.)

- A GTS can be de-allocated in two ways:
 - At any time at the discretion of the PAN coordinator.
 - By the device that originally requested the GTS.
- A device that has been allocated a GTS may also operate in the CAP.
- A data frame transmitted in an allocated GTS shall use only short addressing
- The PAN coordinator should store the info of devices with GTS:
 - including starting slot, length, direction, and associated device address.

48

GTS Concepts (cont.)

- Before GTS starts, the GTS direction shall be specified as either transmit or receive.
- Each device may request one transmit GTS and/or one receive GTS.
 - Each GTS may consist of multiple slots.
- A device shall only attempt to allocate and use a GTS if it is currently tracking the beacon.
 - If a device loses synchronization with the PAN coordinator, all its GTS allocations shall be lost.
- The use of GTSs of an RFD is optional.

49

The Network Coordinator

- Transmits network beacons
- Sets up a network
- Manages network nodes
- Stores network node information
- Routes messages between paired nodes
- Receives constantly

50

The Network Node

- Is generally battery powered
- Searches for available networks
- Transfers data from its application as necessary
- Determines whether data is pending
- Requests data from the network coordinator
- Can sleep for extended periods

51

Security

- Devices can have the ability to :
 - Maintain an access control list
 - Use symmetric cryptography
- Security modes
 - Unsecured mode
 - Access control list mode
 - Secured mode
- Security done in the higher layer.

52

Example: Automatic Meter Reading

- Situation
 - Accurate and timely meter information
- Challenge
 - Enable Time of Use pricing
 - Widely varying meter density
 - Reliable, Secure Bidirectional communication
- Solution
 - ZigBee enabled Automatic Meter Reading system
- Benefits
 - Simplified installation via self configuring network
 - Enables Time of Use pricing
 - Simplifies and reduces cost of reading meters



53

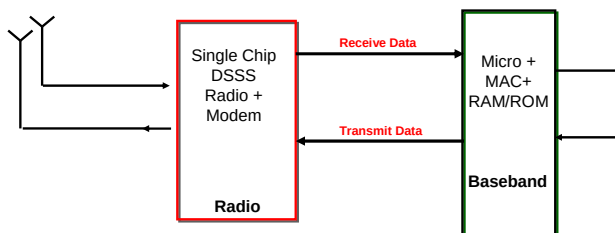
Stack System Requirements

- 8-bit μ C, e.g. 80c51
- Full protocol stack <32k
- Simple node only stack ~4k
- Coordinators require extra RAM
 - node device database
 - transaction table
 - pairing table

54

ZigBee Chip Set Solution

Low Data Rate, DSSS @ 2.4GHz



55

Feature Set RF Front-End IC

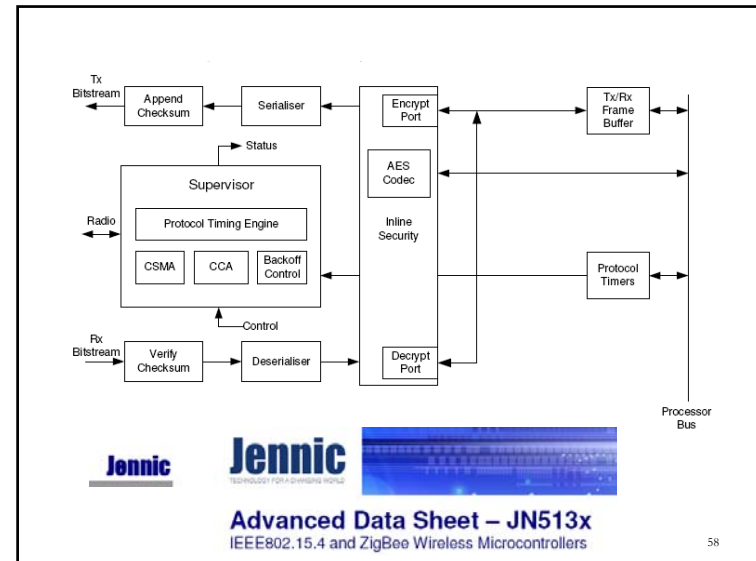
- Single chip direct conversion transceiver for ZigBee applications in the 2.4GHz ISM band
- DSSS 2.2Mchips/sec
- Integrated antenna filter, LNA, VCO, synthesizer, PLL, preamplifier
- 3-wire control bus interface
- Direct conversion architecture from 2.45 GHz RF directly base band
- Battery powered design (min. VCC=1.8V)
- Output power -4 to +20dBm (0dBm typical)
- Digitally controlled RX gain control for DSSS

56

ZigBee Base Band & MAC

- Single chip Modem and MAC
- 80C51 (or equivalent) 8-bit low power micro controller core
- Interfaces:
 - Full duplex UART for communication with host processor or other devices
 - 2 3 wire buses for host and RF Front-end communication
 - Master/slave I2C
 - 2 analog inputs
- CMOS 0.18 or other low cost similar capability process

57



58

More Information

- IEEE 2003 version of 802.15.4 MAC & Phy standard
 - <http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf>
- ZigBee Specification
 - http://www.zigbee.org/en/spec_download/download_request.asp
- 802.15.4 Tutorial
 - http://grouper.ieee.org/groups/802/15/pub/2003/Jan03/03036r0P802-15_WG-802-15-4-TG4-Tutorial.ppt
 - Slides 3 – 17 were adapted from this tutorial
- ZigBee Technology: Wireless Control that Simply Works
 - <http://www.hometoys.com/htinews/oct03/articles/kinney/zigbee.htm>
- ZigBee Technology: Wireless Control that Simply Works
 - <http://www.hometoys.com/htinews/oct03/articles/kinney/zigbee.htm>
- Home networking with Zigbee
 - <http://www.embedded.com/showArticle.jhtml?articleID=18902431>
 - Slides 19 – 21 were adapted from this article
- Can the competition lock ZigBee out of the home?
 - <http://www.techworld.com/mobility/features/index.cfm?FeatureID=1809>

59