

# Introduction to ZigBee

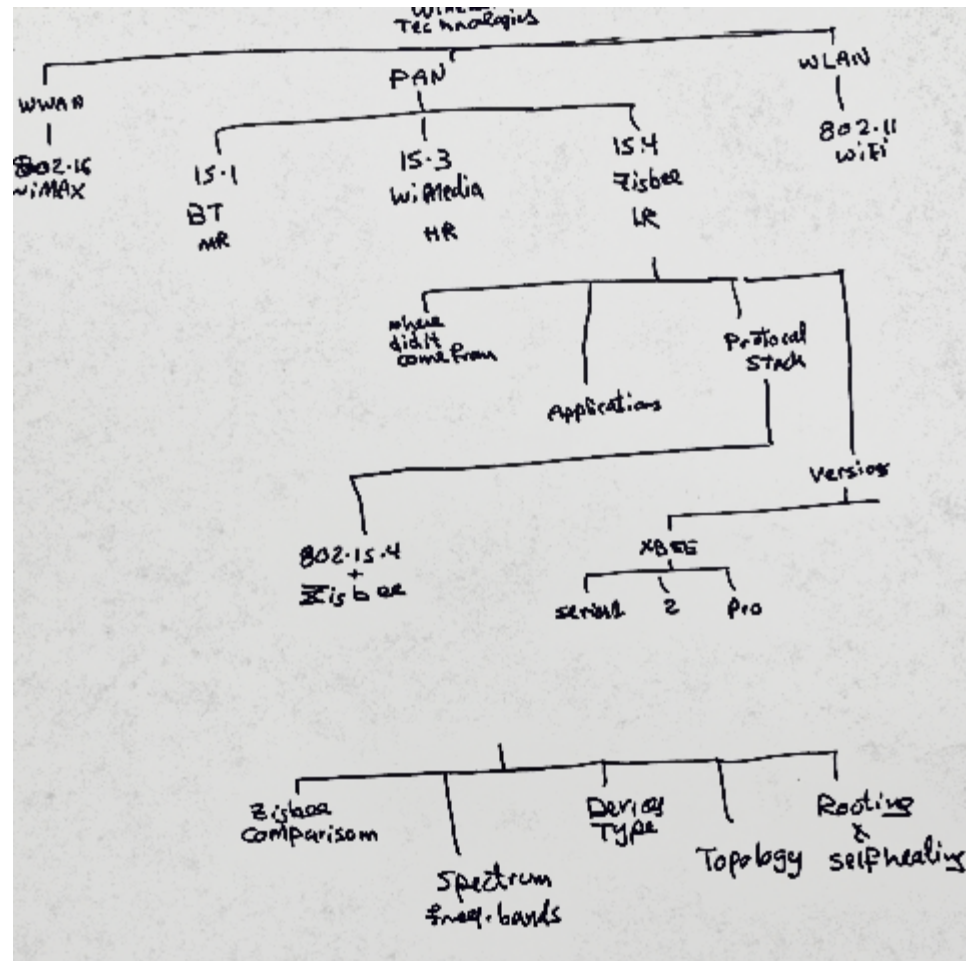
Dr. Farid Farahmand

11/13/13

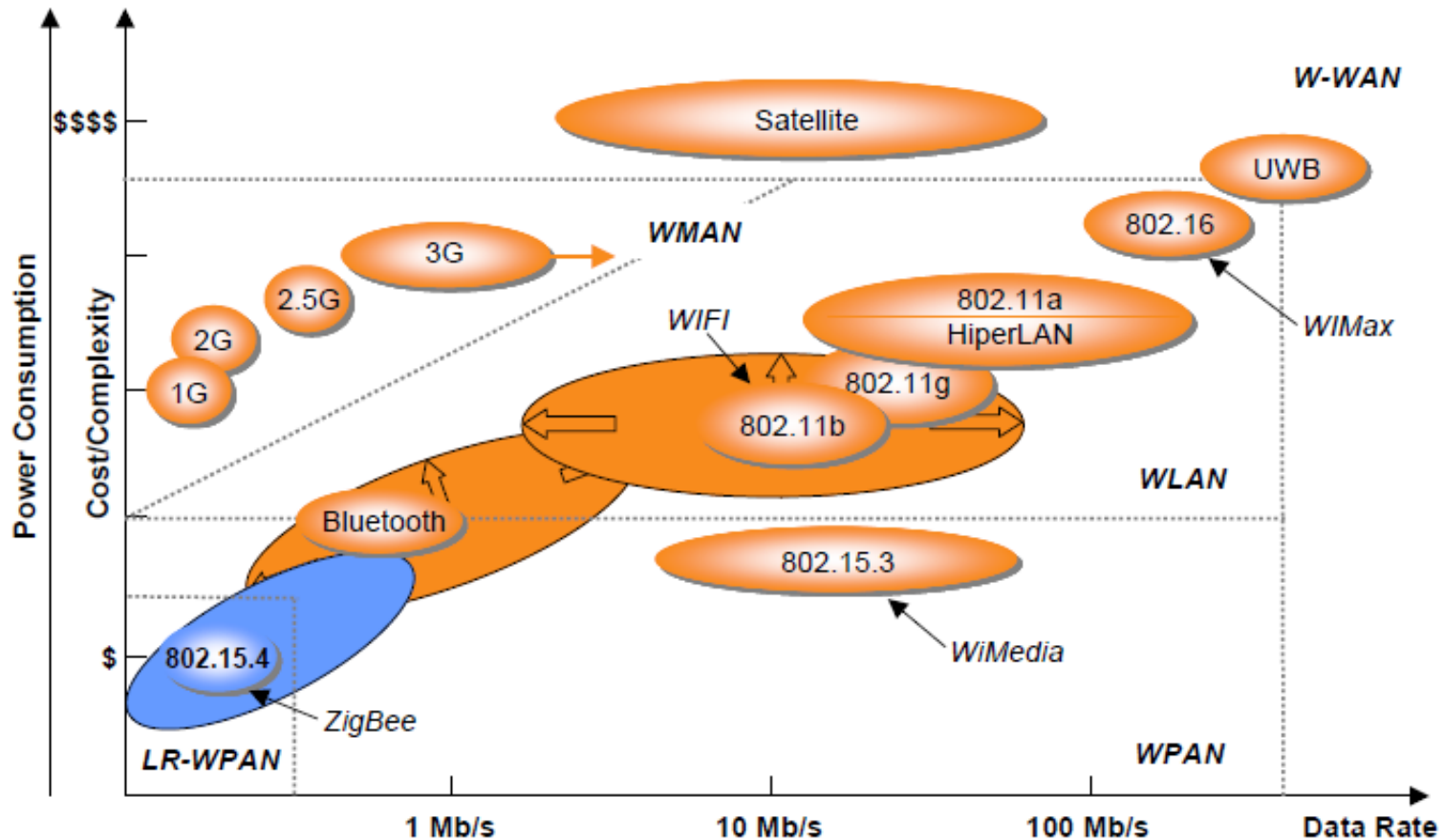
# Credits....

- ▶ Motivated by many other slides, authors, papers, discussions with colleagues, talks, conference manuals, etc.

# Outline



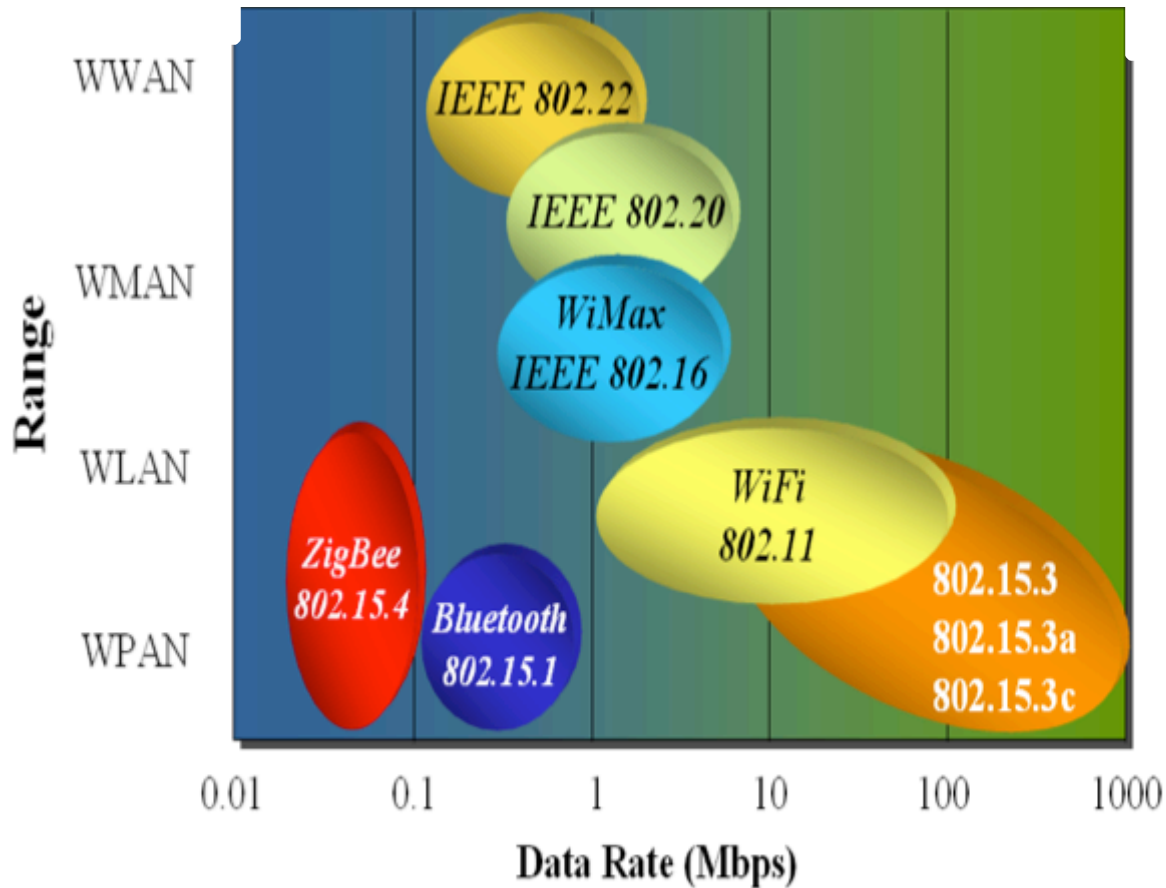
# Standard Technology Map



# The 802 Wireless Space

HR-WPANs (802.15.3)

Source: <http://www.zigbee.org/en/resources/>



# Short Range Wireless Networks – WLAN & WPAN

## ▶ WLAN

- IEEE 802.11

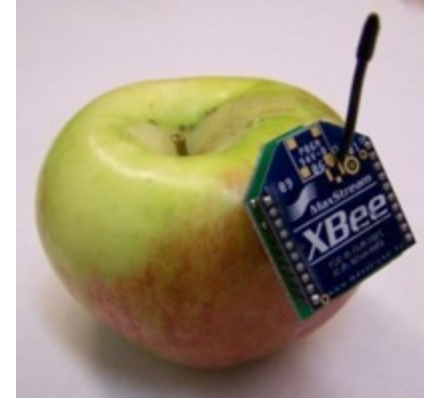
## ▶ WPAN Classification

- High-rate WPANs (HR-WPANs) – **WiMedia** (IEEE 802.15.3)
  - 11–55 Mbps
  - Used for real-time video transmission
- Medium-rate WPANs (MR-WPANs) – **Bluetooth** (IEEE 802.15.1 )
  - 1–3 Mbps
  - Used for high-quality voice transmission
- Low-rate WPANs (LR-WPANs) –(IEEE 802.15.4)
  - About 250 kbps
  - Low data rate support
  - Including **ZigBee** (Zigbee protocol uses 802.15.4)

## ▶ Aims of WPAN

- Power efficiency
- No need for infrastructure
- Personal spacing coverage
- Note replacing LAN

# ZigBee Basics



- ▶ Technological Standard defining set of communication protocols
- ▶ Created for Control and Sensor Networks
- ▶ Uses IEEE 802.15.4 Standard
  - Operates on unlicensed bands
- ▶ Created by the ZigBee Alliance
- ▶ Aims at
  - Reduced complexity
  - Lower implementation cost
  - Short range communication
  - Low data rate (250kbps)
  - Low power (extended battery life using sleeping mode)
  - Large mesh networks



# ZigBee Alliance



- ▶ Formed in 2002 as a non-profit organization
- ▶ Has hundreds of member companies
- ▶ Adapted IEEE 802.15.4 as the physical layer and MAC protocols
- ▶ Zigbee-compliant is also compliant with IEEE 802.15.4 standards



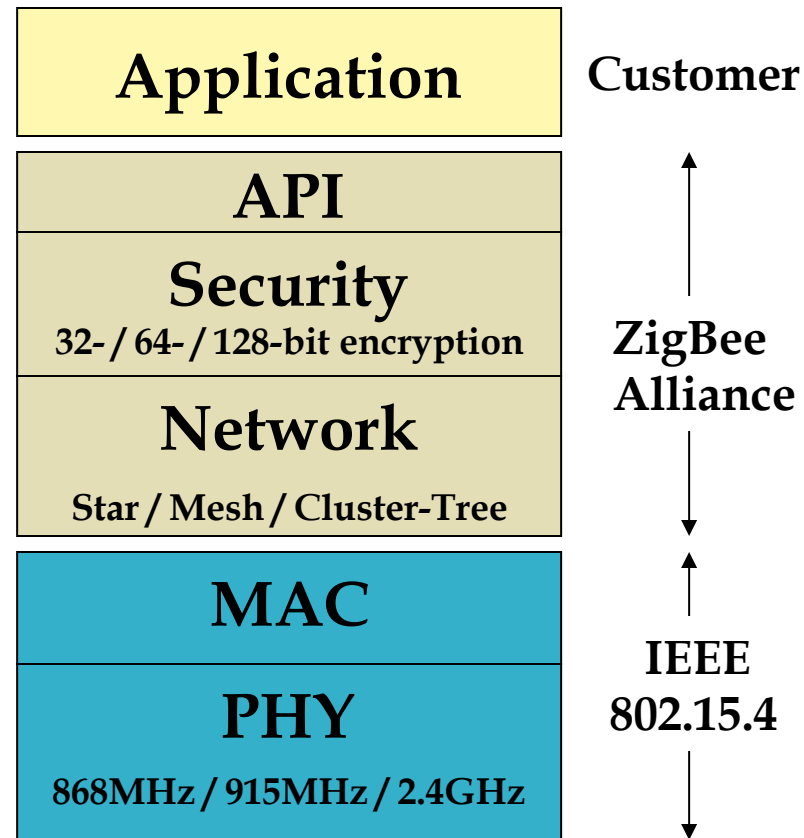
# Applications



- ▶ In-home patient monitoring
  - Continuous monitoring of vital information remotely and securely
- ▶ Monitoring structural health of buildings
  - Sensor network
- ▶ Security systems
  - Using ZigBee for wireless camera system (low quality, not CD-quality)
- ▶ Utility meter-reading systems
  - Passing the information to one or more node and connecting to the Internet using ZigBee gateway
  - Self-forming mesh network to connect to the corporate office
- ▶ Irrigation and water management
  - Sensors across landscaping fields
- ▶ Wireless light control Industrial automation and control
- ▶ Livestock tracking
  - Replacing passive RFID tags with limited storage – ZigBee will be considered as active tags with extended life
- ▶ Hotel guest room access
  - A portable zigBee device acting as the key – replacing card readers for each door and eliminating the wiring

# What is XBee

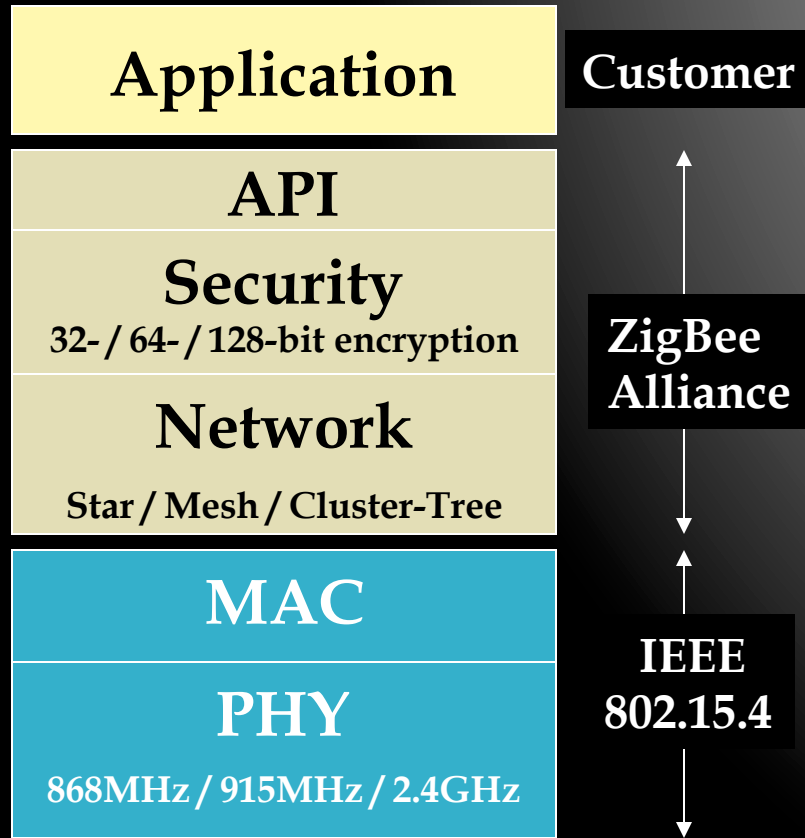
- ▶ ZigBee / ZigBee Pro are mesh communication protocols that sit on top of IEEE 802.15.4 PHY
- ▶ DigiMesh is an alternative to ZigBee that changes a few things, and adds some features to make it generally better to work with
- ▶ XBee / XBee Pro are product names for a radio communication modules made by Digi



# More on XBee...

- ▶ There are three radio types
  - Series 1
    - freescale board, supports P2P, limited MESH
  - Series 2
    - Implement ZigBee mesh standard and full ZigBee protocol
  - Series 2B
    - From Digi, low power consumption
- ▶ XBee types
  - Regular and Pro
  - Each one comes with many different antenna types

# IEEE 802.15.4 & ZigBee In Context



■ Silicon ■ Stack ■ App



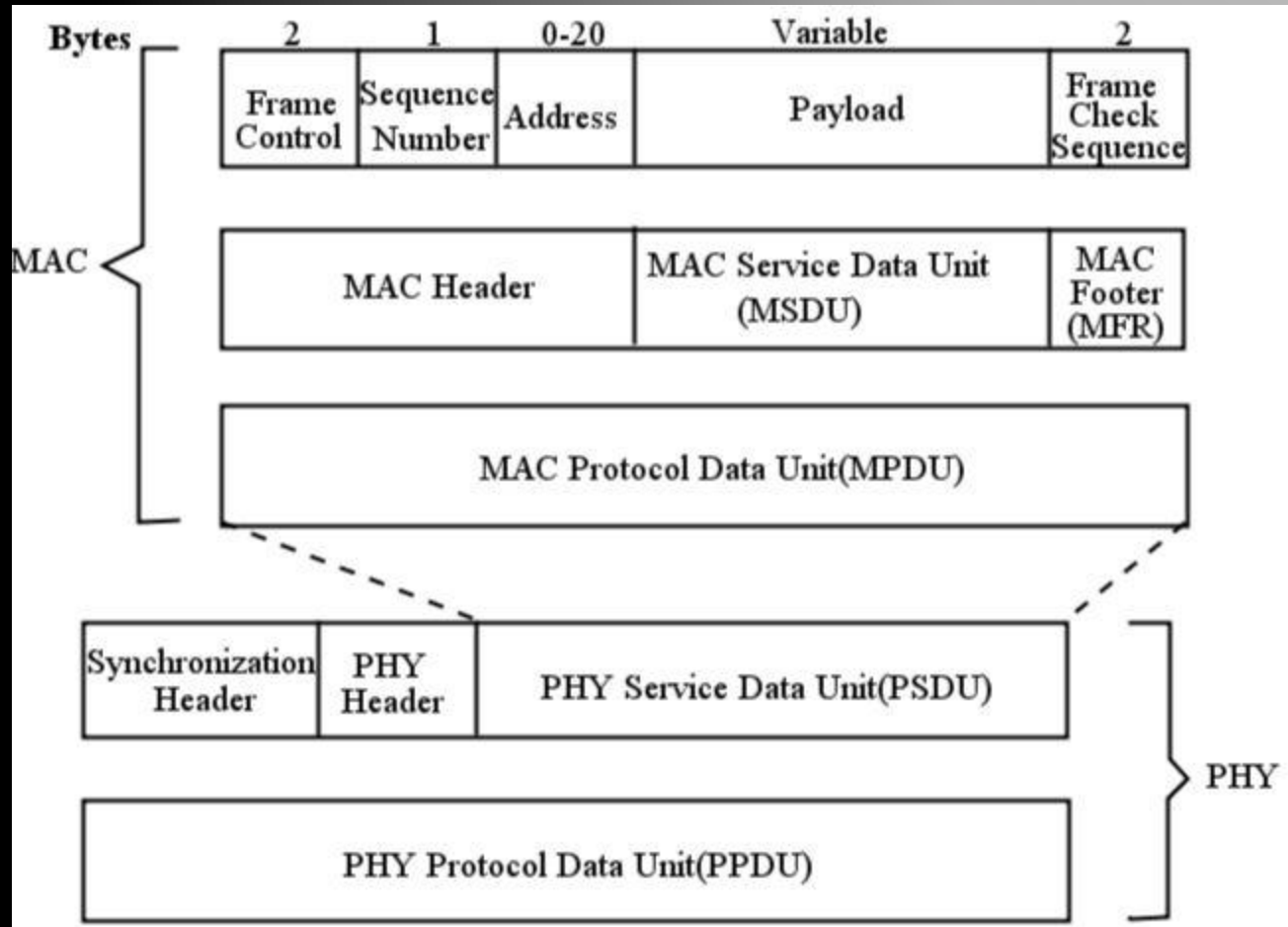
- “the software”
- Network, Security & Application layers
- Brand management

## IEEE 802.15.4

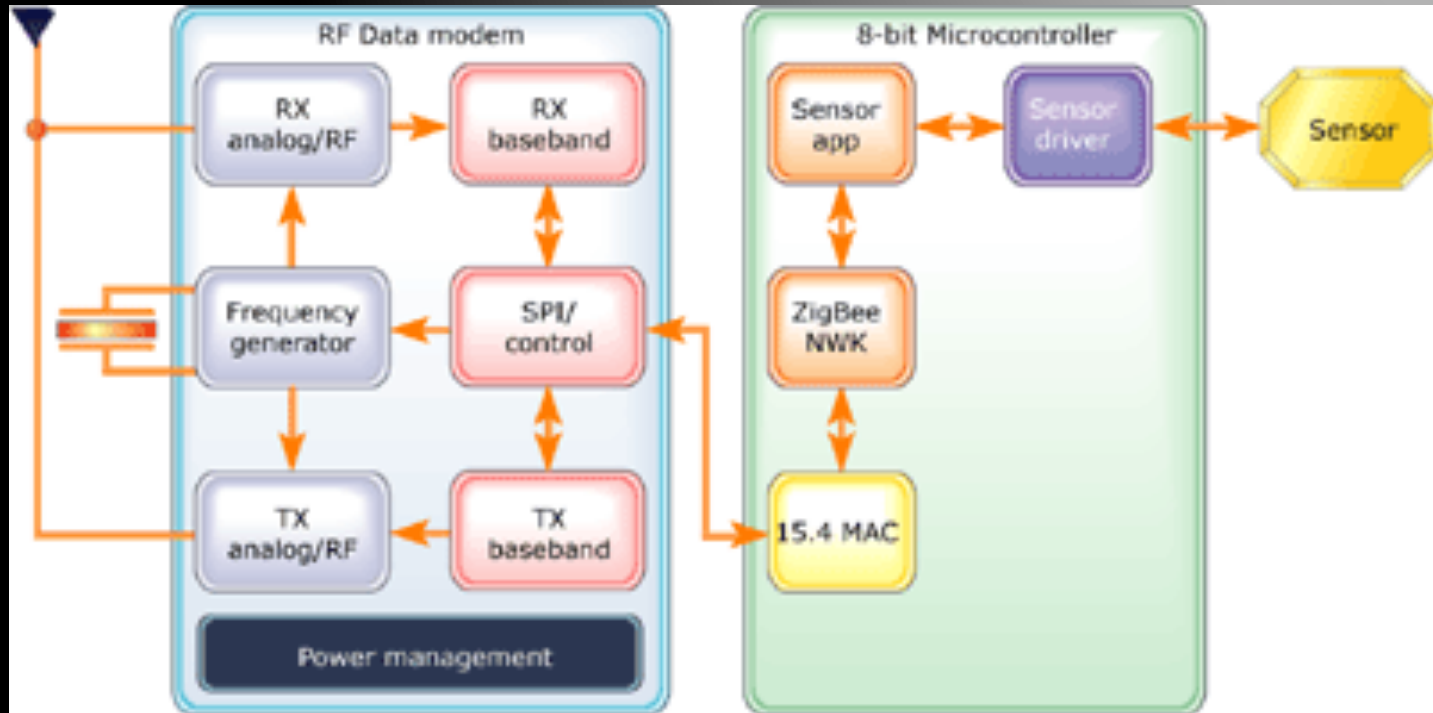
- “the hardware”
- Physical & Media Access Control layers



# PHY and MAC Details



# Typical ZigBee Enabled Device



# Comparing ZigBee with Other Wireless Technologies



Market Name	ZigBee™	Wi-Fi™	Bluetooth™
Standard	802.15.4	802.11b	802.15.1
Application Focus	Monitoring & Control	Web, Email, Video	Cable Replacement
System Resources	4KB - 32KB	1MB+	250KB+
Battery Life (days)	100 - 1,000+	.5 - 5	1 - 7
Network Size	Unlimited (2 <sup>64</sup> )	32	7
Bandwidth (KB/s)	20 - 250	11,000+	720
Transmission Range (meters)	1 - 100+	1 - 100	1 - 10+
Success Metrics	Reliability, Power, Cost	Speed, Flexibility	Cost, Convenience



# ZigBee Frequencies

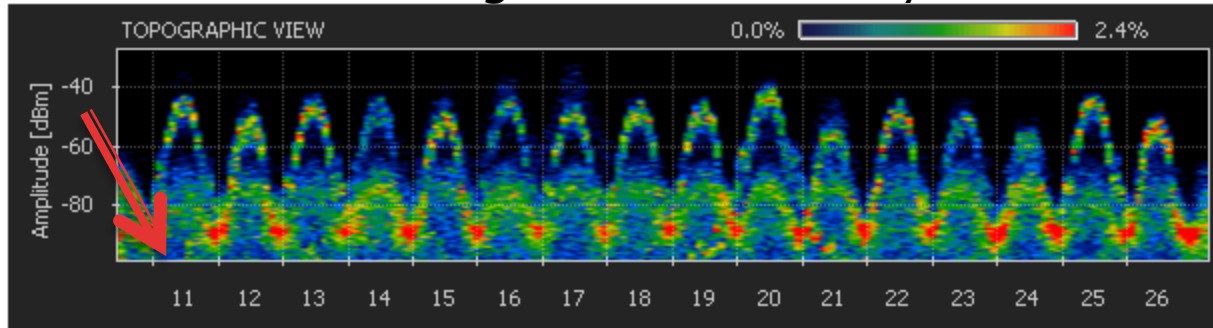
Operates in **Unlicensed** Bands

- ▶ 868–868.6 (868 MHz) European Band at 20kbps
  - Bit rates: 20/100/250 Kb/s
- ▶ 902–928 MHz (915 MHz) North American Band at 40kbps
  - Bit rates 40/250 Kb/s
- ▶ 2400–2483.5 GHz (ISM 2.4 GHz) Global Band at 250kbps
  - Bit rate: 250 Kb/s

	Channel	Center Frequency (MHz)	Availability
868 MHz Band	0	868.3	 <i>Europe</i>
	1	906	
915 MHz Band	2	908	 <i>Americas</i>
	3	910	
	4	912	
	5	914	
	6	916	
	7	918	
	8	920	
	9	922	
	10	924	
	2.4 GHz Band	11	
12		2410	
13		2415	
14		2420	
15		2425	
16		2430	
17		2435	
18		2440	
19		2445	
20		2450	
21		2455	
22		2460	
23		2465	
24		2470	
25		2475	
26		2480	

# ZigBee Frequency Bands

Signal Power Density



Calculate the channel spacing!

## Frequency Spectrum and Center Frequencies

### ZigBee Channels in the 2.4GHz ISM Band

ZigBee Channels 11-26	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Center Freq.(MHz)	2405	2410	2415	2420	2425	2430	2435	2440	2445	2450	2455	2460	2465	2470	2475	2480
Control4	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	

## ZigBee Channels 11-26

### ZigBee Channels in the 915MHz ISM Band

ZigBee channels 1-10	1	2	3	4	5	6	7	8	9	10
Center Frequency (MHz)	906	908	910	912	914	916	918	920	922	924

Lower Frequencies European Bands Not Shown!

## ZigBee Channels 1-10

# ZigBee Frequency Bands

The receivers must have no more than **1% PER (packet error rate)**  
Thus, special attention must be paid to interferences

Alternate channels  
(+/- 10 MHz)

Adjacent channels  
(+/- 5 MHz)

## Frequency Spectrum and Center Frequencies

### ZigBee Channels in the 2.4GHz ISM Band

ZigBee Channels 11-26	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Center Freq.(MHz)	2405	2410	2415	2420	2425	2430	2435	2440	2445	2450	2455	2460	2465	2470	2475	2480
Control4	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	

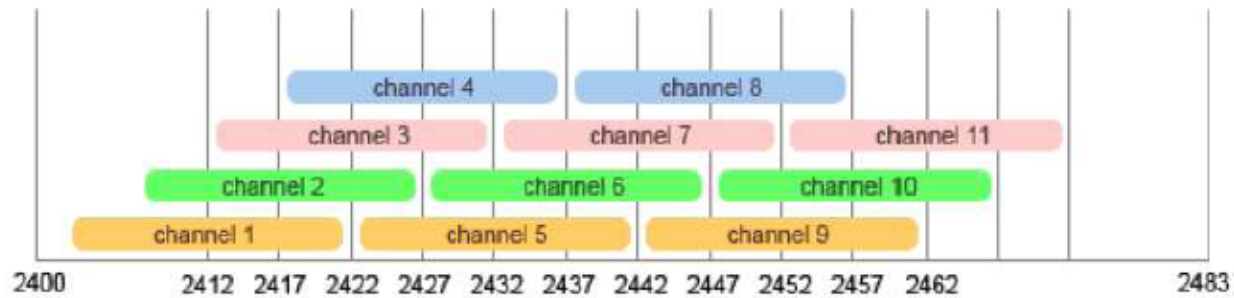
## ZigBee Channels 11-26

### ZigBee Channels in the 915MHz ISM Band

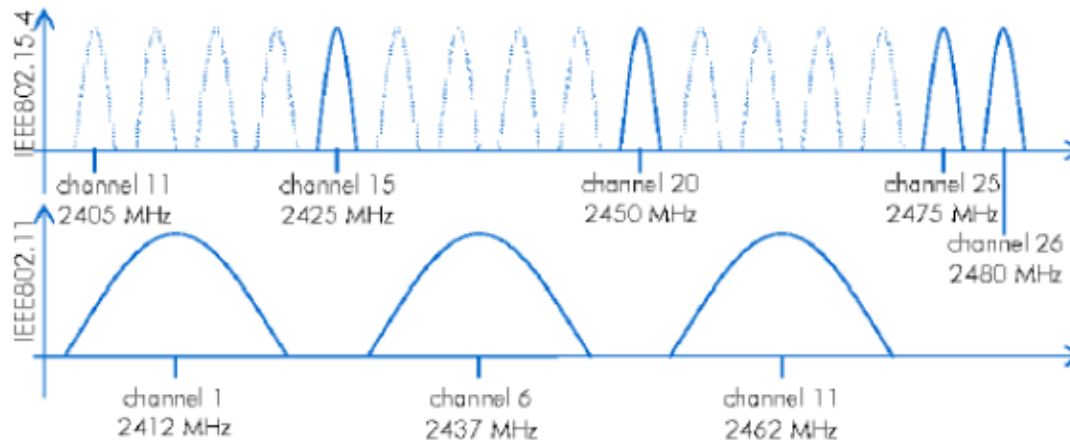
ZigBee channels 1-10	1	2	3	4	5	6	7	8	9	10
Center Frequency (MHz)	906	908	910	912	914	916	918	920	922	924

## ZigBee Channels 1-10

# 802.15.4 and 802.11 Overlap



## 802.11 channel assignments



Available  
802.15.4  
channels in a  
typical  
crowded  
network  
space

# 802.15.4 Device Types

- ▶ Only implementing the MAC and PHY
- ▶ IEEE 802.15.4 Devices
  - Full-function devices (FFD)
    - Accepts all roles (Node, Router, Base Station)
  - Reduced-function device (RFD)
    - Limited capacity and can only talk to FFD device
    - Used for simple applications (turning on and off a device)
    - Less memory and lower power consumption

# ZigBee Device Type

## **Coordinator**

- An FFD with network device functionality that provides coordination and other services to the network.

## **PAN Coordinator**

- A coordinator that is the principal controller of the PAN. A network has exactly one PAN coordinator.

## **Network Device**

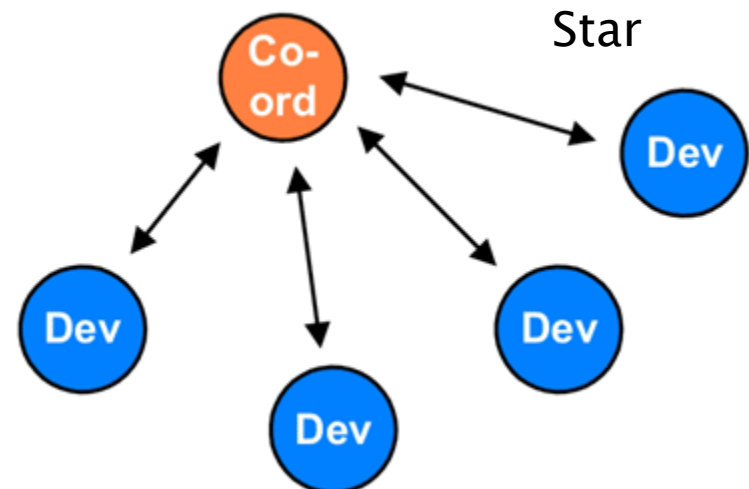
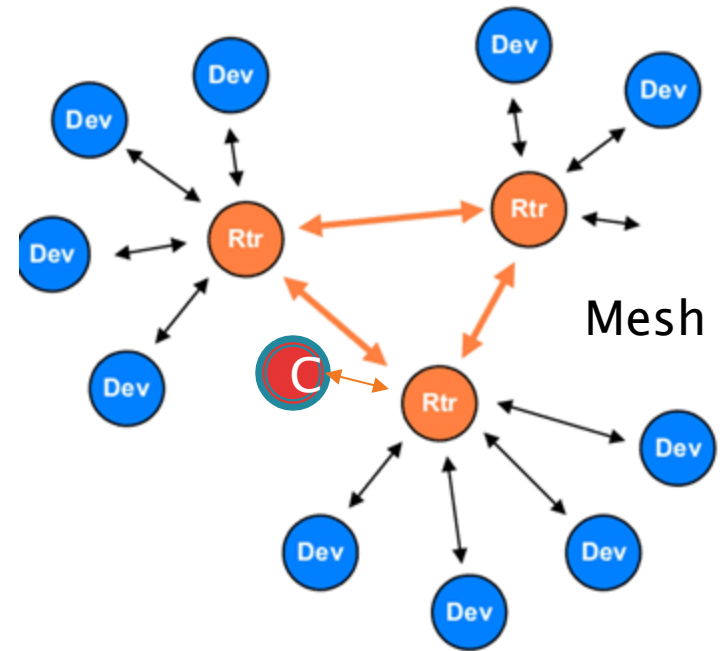
- An RFD or FFD implementation containing an IEEE 802.15.4 medium access control and physical interface to the wireless medium.

# ZigBee Node Functionality

- ▶ Must be compatible with IEEE 802.15.4 – slightly different
- ▶ Device types
  - Coordinator
    - Same as a PAN coordinator
  - Router
    - Coordinator
  - End-device

# Network Topology

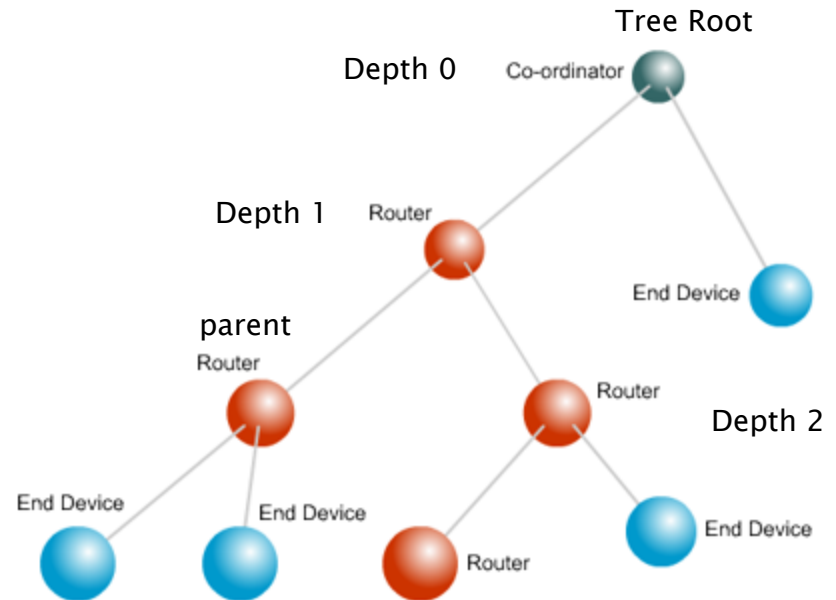
- ▶ Star
  - Includes a PAN coordinator and several FFD or RFD
  - Any FFD can play the role of PAN coordinator
- ▶ Mesh
  - Not hierarchical
  - A P2P topology that nodes have no restriction as to who to communicate with
  - Includes **Routers**





# Network Topology

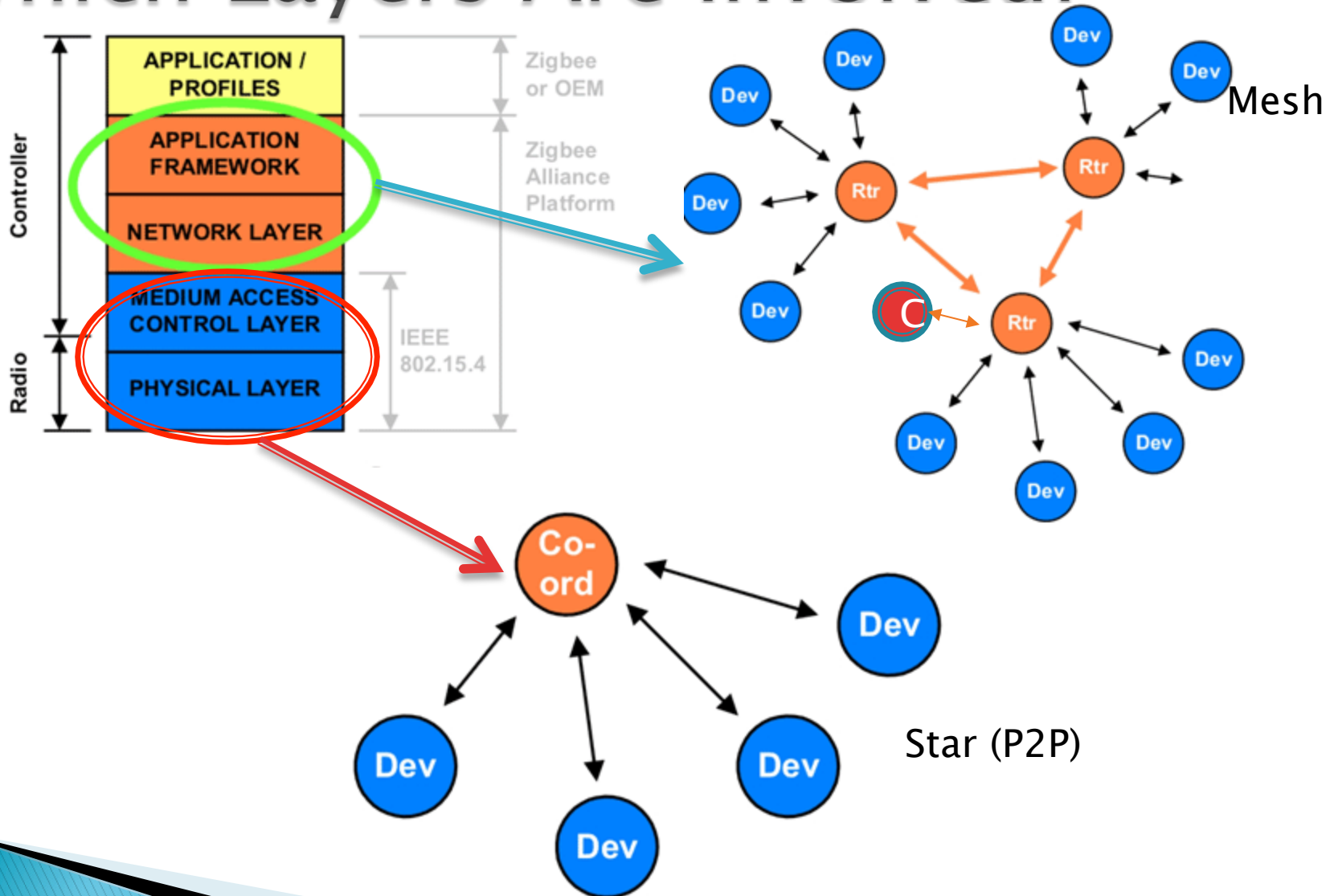
- ▶ Tree
  - Coordinator (PAN Coordinator) establishes the network
  - Based on hierarchical relationships
  - End devices act as leaves
  - Routers relay the messages
- ▶ Note that at least ONE PAN coordinator is required
  - Initiate message routing through the entire network
  - Select a unique PAN identifier for<sub>child</sub> the network
    - Thus communicating with devices inside and outside the network
  - Allocate addressing to each device



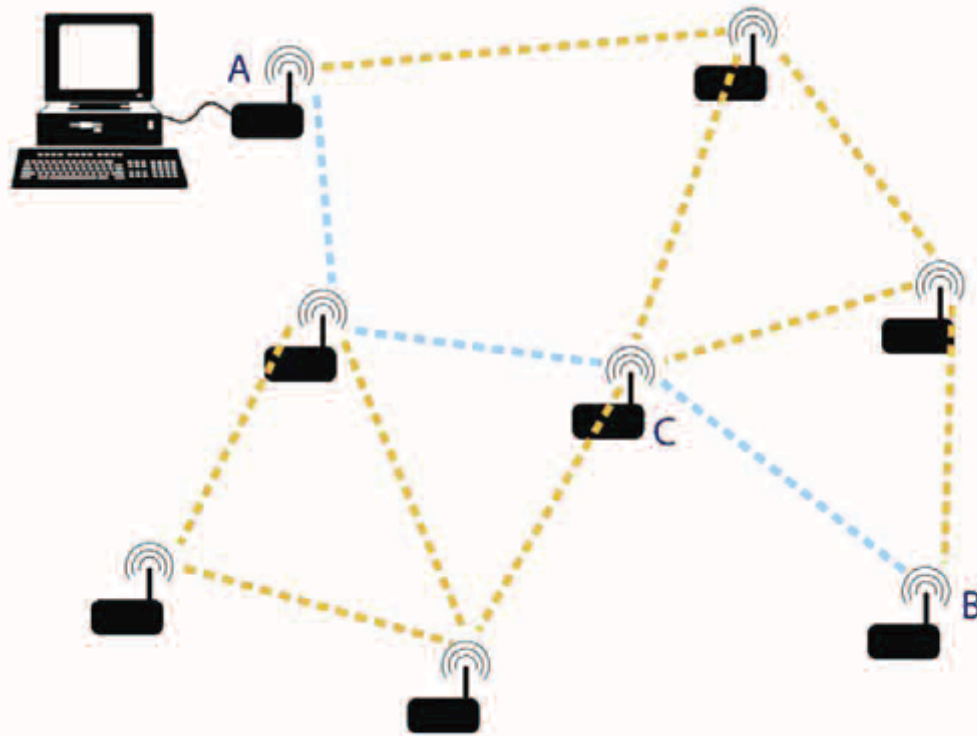
Animation!

More information (read it!)

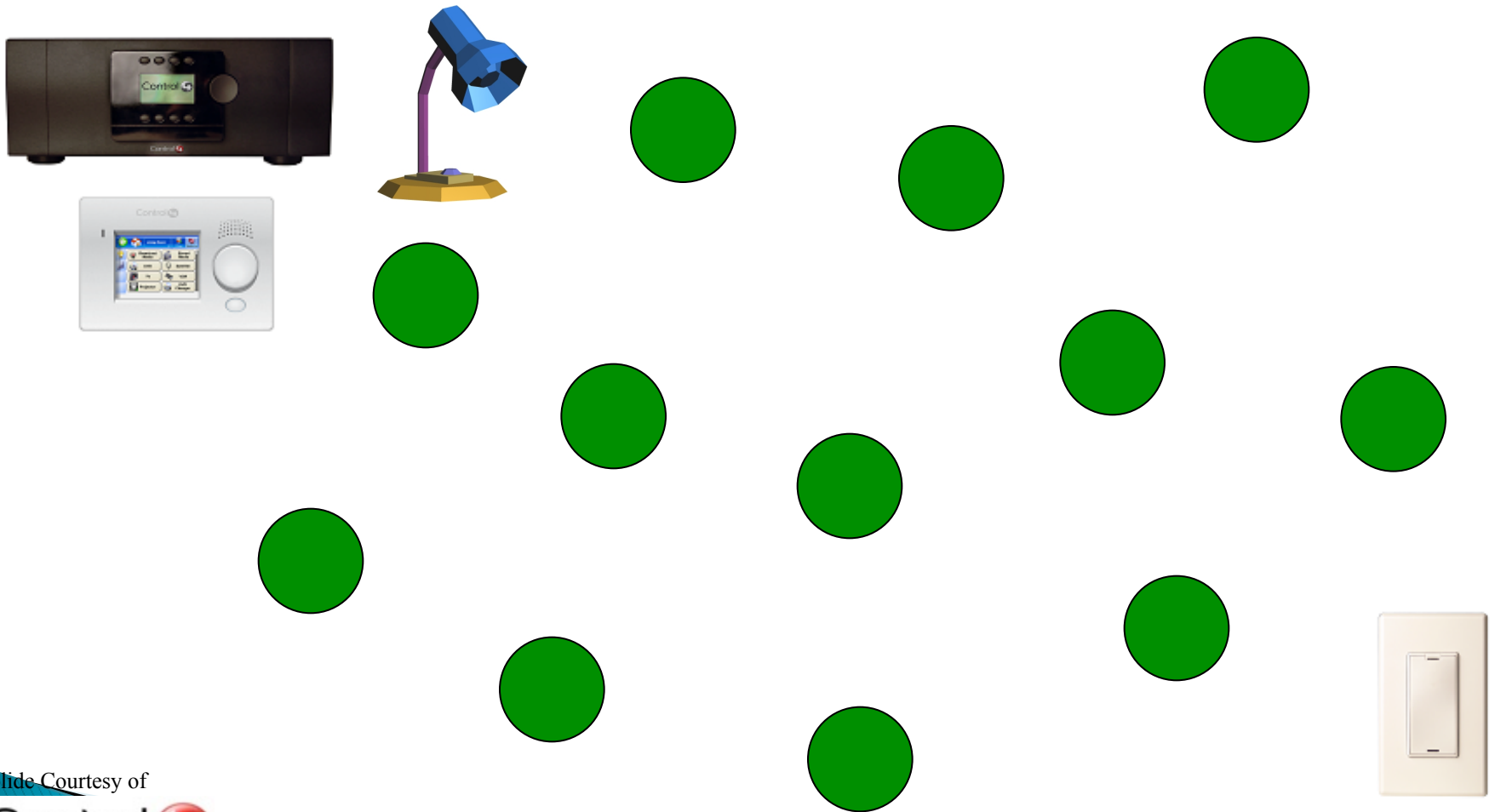
# Which Layers Are Involved?



# Actual Setup (Mesh Topology)



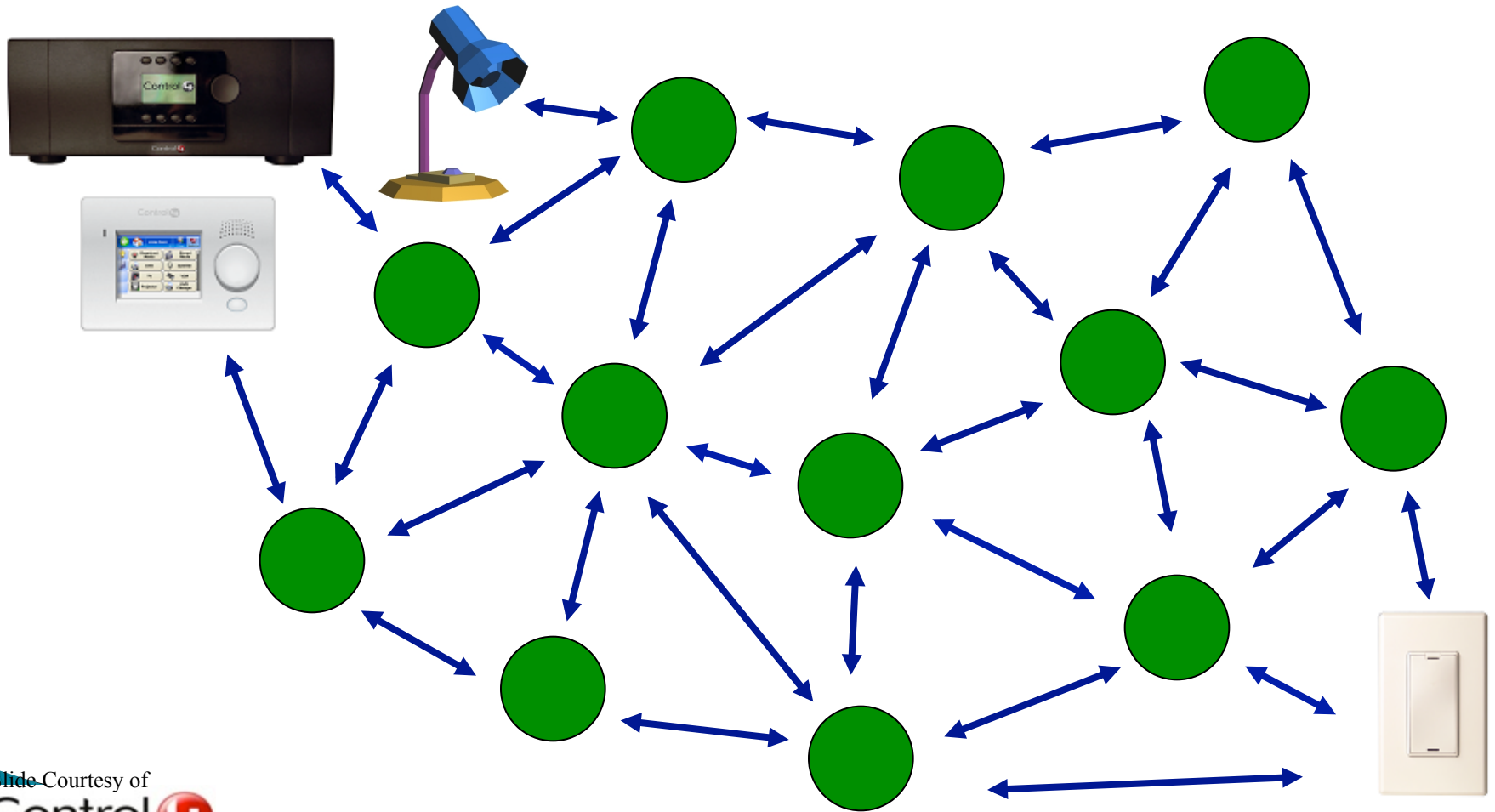
# ZigBee Mesh Networking



Slide Courtesy of

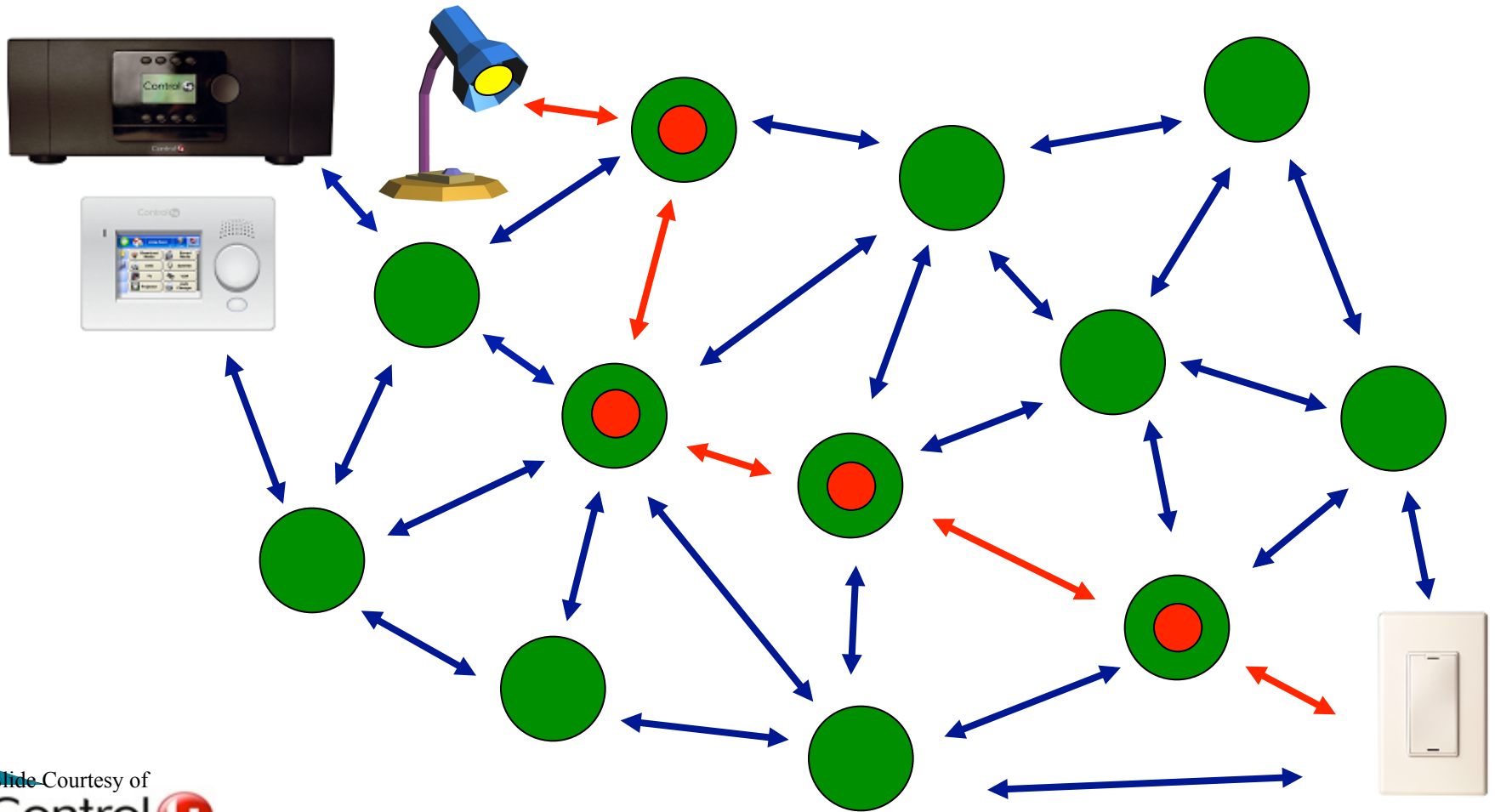


# ZigBee Mesh Networking - Available Routes

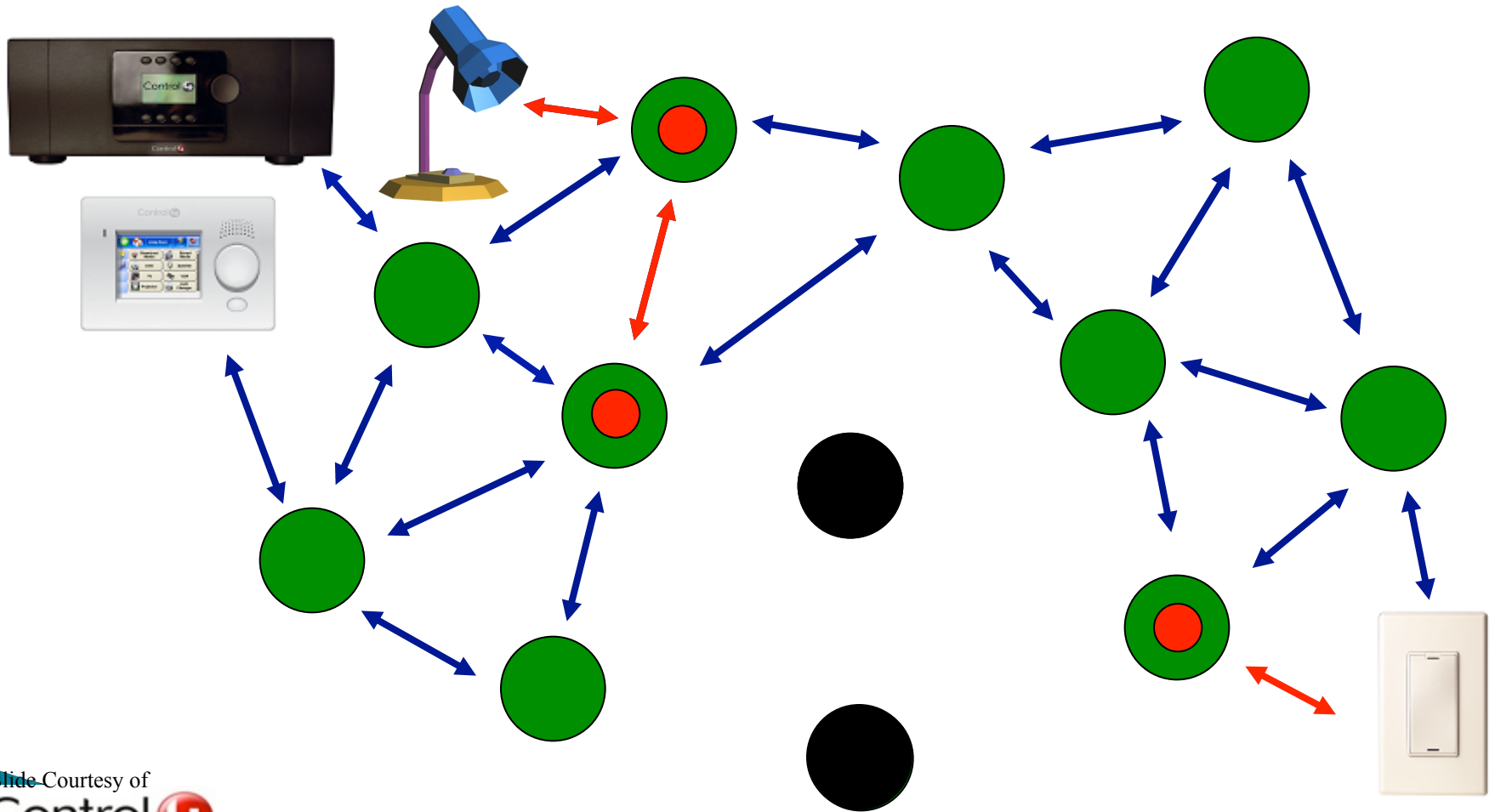


Slide Courtesy of  
**Control4**

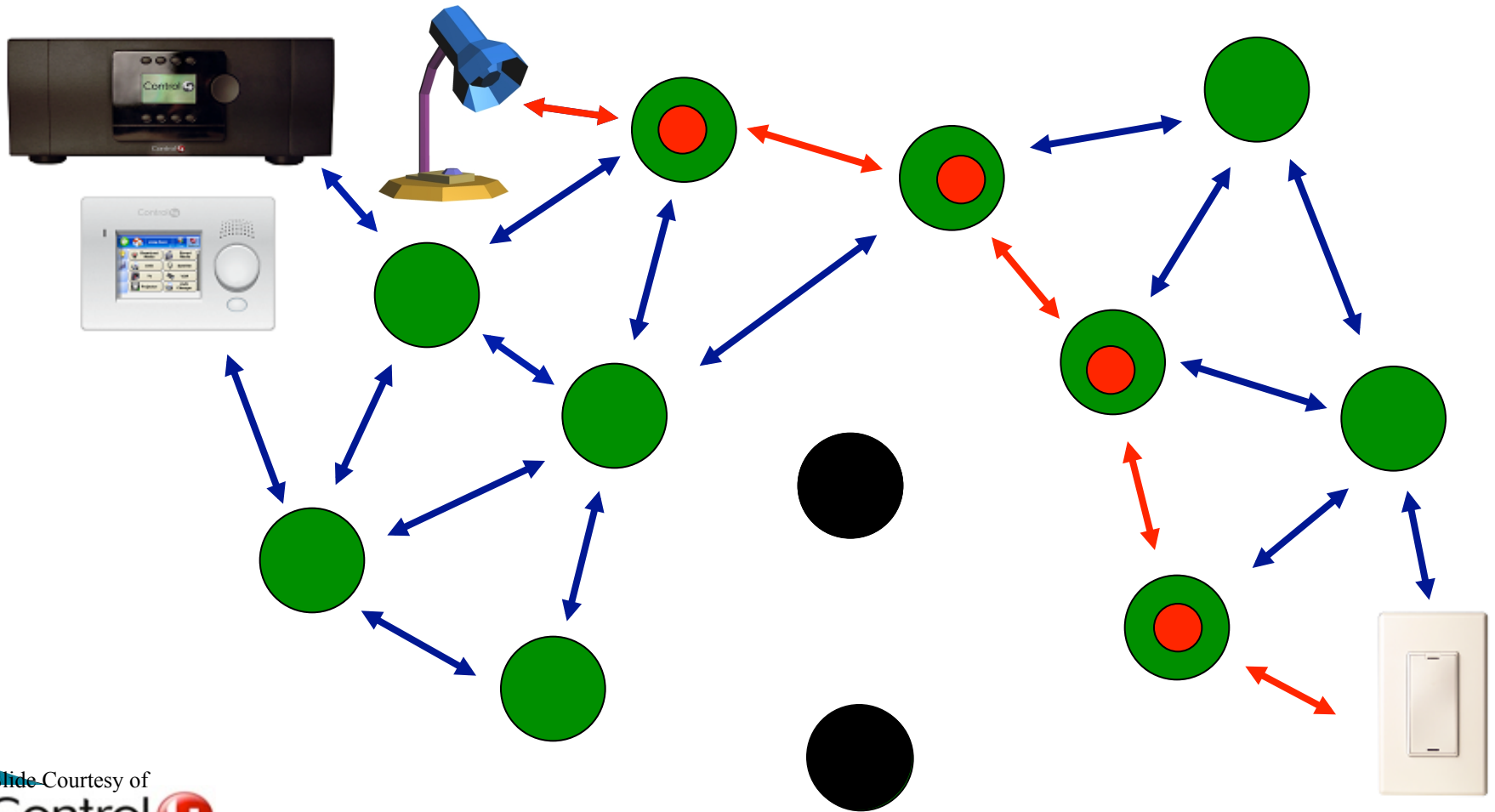
# ZigBee Mesh Networking - Route Selection



# ZigBee Mesh Networking - Power Loss



# ZigBee Mesh Networking – Reroute (self-healing)



Slide Courtesy of  
**Control 4**

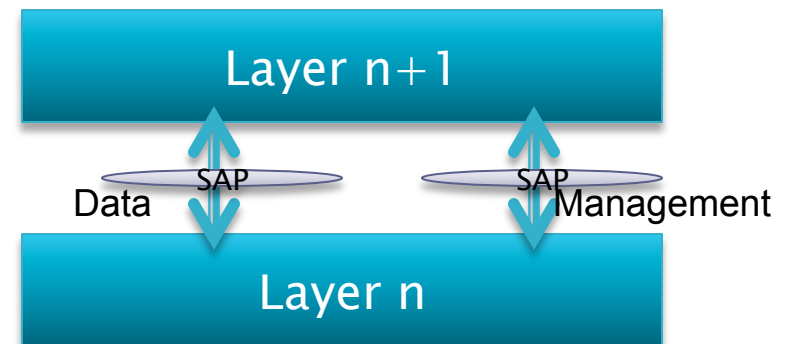
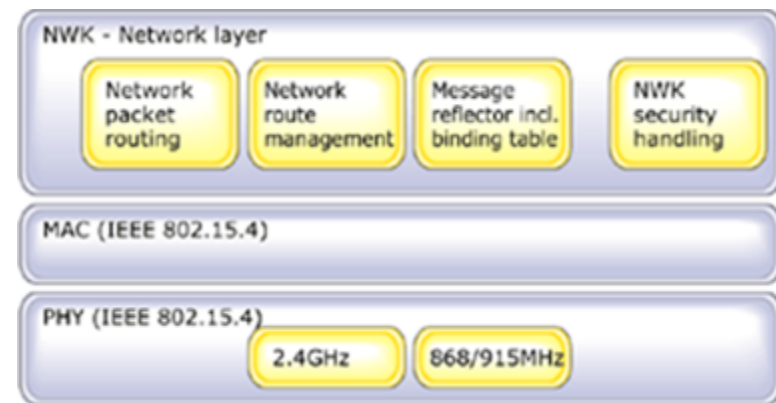


# Introduction to ZigBee – Part 2

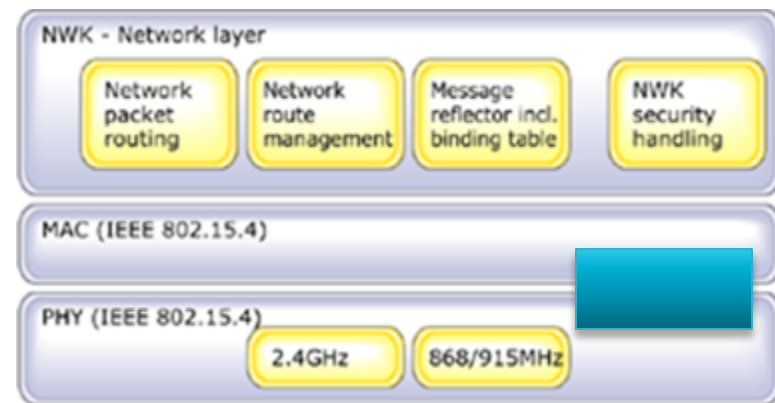
- ▶ **Physical Layer**
  - Services
  - Channel Assignment
  - Sensitivity
  - Jamming
  - Power Efficiency
  - dBc
- ▶ **MAC Services**
  - Functionalities
  - Channel Access
    - CSMA-CA
    - GTS
  - Addressing
    - Addressing Mechanism
    - Example
  - Data Transfer (continue→)
- Device to Coordinator
  - Coordinator to Device
  - Frame Format
  - Header and addressing
  - Services
- ▶ **Network Layer**
  - Communication modes
  - Functionalities
  - Routing

# Zigbee & IEEE 802.15.4 Protocols Layers

- ▶ Each layer can
  - Provide services to the upper layer
  - Request services from lower layer
- ▶ Each layer communicates with adjacent layers
  - **Management Entity** (to request for services)
  - **Data Entity** (to pass the data)
- ▶ The communication between the layers is performed through **Service Access Points (SAP)**
  - SAP – Management Entity
  - SAP – Data Entity (data Service)
- ▶ SAP uses primitives (function calling)
  - 4 distinct primitives:
    - Request / confirm
    - Indication / Response
  - Requests starts from higher layer
  - Indication originates from lower layer



# PHY Services: Data & Management



## ▶ Data Services

- Evoked between MAC and PHY
- MAC requests transmission
- The state of the radio (TCVR ON/ TCVR OFF/TCVR BUSY) is reported to MAC
- Tells the MAC about new data arrival
- As data is handed down overhead is added

## ▶ PHY Management Services

- Perform CCA (clear channel assessment)
- Perform ED (energy detection)
- Generate an LQI (link quality indicator) for packets

# PHY Management Services – Clear Channel Assessment (CCA)

- ▶ Performed by the PHY layer at the request of MAC
- ▶ Check available frequencies
- ▶ There are three CCA modes:
  - Energy level (ED) using a threshold
  - 802.15.4 channel compliance (CC)
  - Logical relation between mode 1 and 2
    - (ED AND/OR CC)

# PHY Management Services – Link Quality Indicator (LQI)

- ▶ Received Signal Strength Indicator (**RSSI**)
  - Determines the total energy of the signal
  - Higher RSSI → more signal energy
  - Higher RSSI → less packet error ratio (PER)
- ▶ **LQI** measurement is performed per packet
  - Provides 8 distinct levels
  - The results are reported to the higher layers (used for routing decisions)

# IEEE 802.15.4 PHY Layer Specifications

## Channel Assignment & Typical Parameters

### Transmit Power

- Capable of at least 1 mW

### Transmit Center Frequency Tolerance




- $\pm 40$  ppm

### Receiver Sensitivity (packet error rate <1%)

- -85 dBm @ 2.4 GHz band
- -92 dBm @ 868/915 MHz band

### RSSI Measurements

- Packet strength indication
- Clear channel assessment

	Channel	Center Frequency (MHz)	Availability
868 MHz Band	0	868.3	 <i>Europe</i>
915 MHz Band	1	906	 <i>Americas</i>
	2	908	
	3	910	
	4	912	
	5	914	
	6	916	
	7	918	
	8	920	
	9	922	
	10	924	
2.4 GHz Band	11	2405	 <i>World Wide</i>
	12	2410	
	13	2415	
	14	2420	
	15	2425	
	16	2430	
	17	2435	
	18	2440	
	19	2445	
	20	2450	
	21	2455	
	22	2460	
	23	2465	
	24	2470	
	25	2475	
	26	2480	

# IEEE 802.15.4 PHY Layer Specifications

## Transmission Power

- ▶ 802.15.4 Transceivers
  - **Minimum** amount of energy needed to transmit is  $-3\text{dBm}$ , ( $0.5\text{ mW}$ ) –  $P_{\text{dBm}} = 10 \times \log(P_{\text{mW}} / 1\text{ mW})$
  - **Minimum** sensitivity in the receiver is  $-92\text{dBm}$  ( $6.3 \times 10^{-10}\text{ mW}$ ) –  $P_{\text{mW}} = 10^{(P_{\text{dBm}} / 10)}$
- ▶ **Reception sensitivity**, the XBee shows  $-92\text{dBm}$  ( $6.3 \times 10^{-10}\text{ mW}$ ) and  $-100\text{ dBm}$  ( $1 \times 10^{-10}\text{mW}$ ) the XBee-Pro flavor
- ▶ Some radio module have a variable transmission power strength
  - $0\text{dBm}$  ( $1\text{mW}$ ) in XBee 802.15.4 OEM
  - $20\text{dBm}$  ( $100\text{mW}$ ) in the XBee-Pro 802.15.4 OEM
    - both values are higher than the minimum set in the 802.15.4 Standard

Note: OEM (original equipment manufacturer) refers to the implementation! E.g., XBee/XBee-PRO 802.15.4 OEM RF Modules by Digi

# IEEE 802.15.4 PHY Layer Specifications

## Receiver Sensitivity & Freq. Shift

- ▶ Lowest received signal power with acceptable error ratio: PER < 1%
- ▶ Zigbee requires -85dBm @ 2.4GHz -95dBm @ 868/915 MHz (BPSK)
- ▶ With -85 dBm sensitivity

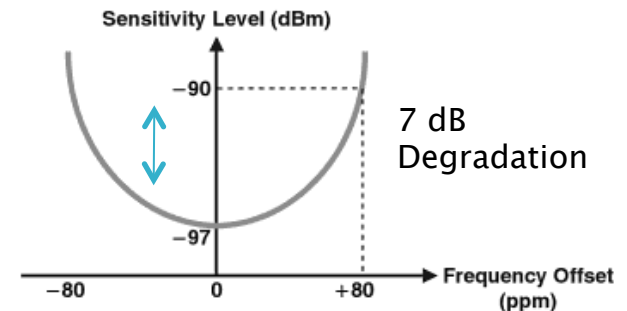
- Acceptable received signal power: 3.16pW
- Root-mean-square (rms) voltage =  $\sqrt{P \times R}$ ;
- R= Impedance of the antenna (50 ohm)
- →Acceptable received signal voltage: 12.6 uV -

- ▶ Receiver Sensitivity changes as frequency shifts

- In the presence of frequency shift → sensitivity will be degraded

- ▶ **Example:** Assume the min required sensitivity is -85 dBm when Zigbee is operating on channel 20

- What is +80 ppm freq. offset?
- What kind of sensitivity is expected?



80 ppm → 196,000 Hz →  
2450,000,000 + 196,000 = 2450,196,000

Note:

Channel 20 → 2450

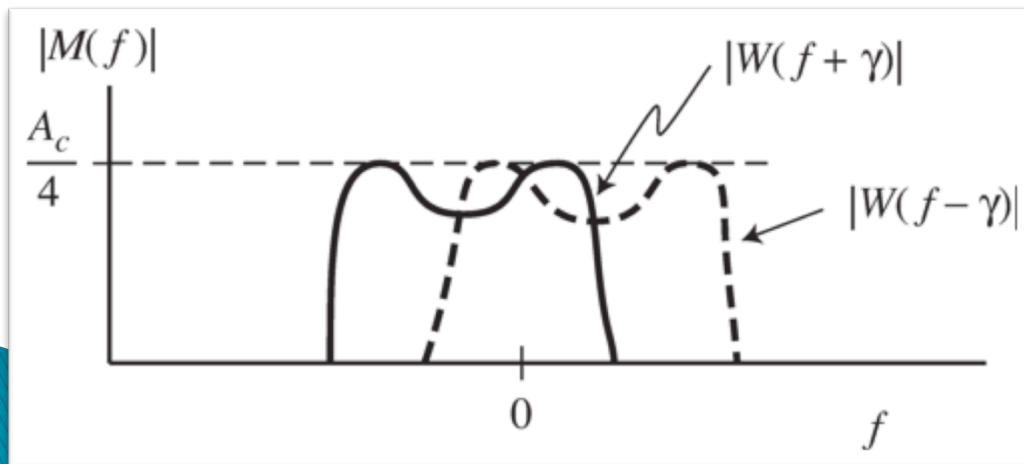
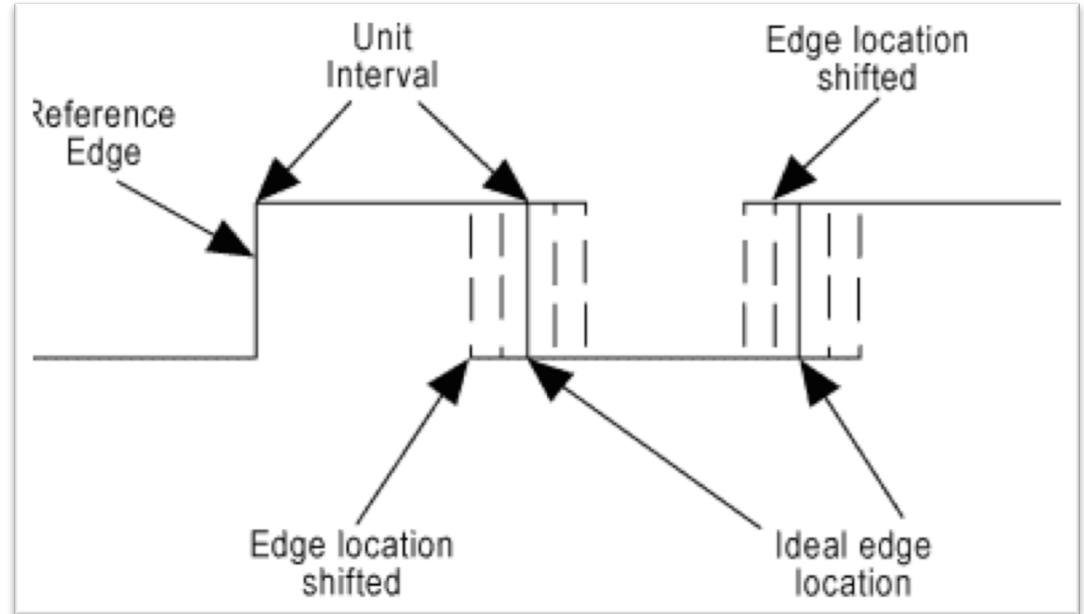
Channel 21 → 2455

Thus, at 2450,196MHz  
Required Sensitivity will  
be  
 $-85 + 7 = -78$  dBm



# IEEE 802.15.4 PHY Layer Specifications

## Jitter and Frequency offset



# IEEE 802.15.4 PHY Layer Specifications

## Jitter and Frequency offset

### ▶ Example:

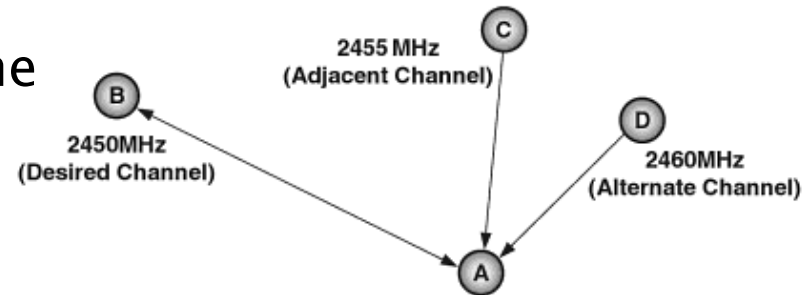
- A clock could have high offset and low jitter, as in the case of a 156.3281 MHz clock with perfect edge placement (+500 ppm from nominal frequency of 156.25 MHz, and no jitter).
- A clock could have low offset and high jitter, as in the case of a 156.25 MHz clock whose edges deviate from their ideal positions in time by  $+/-200$  ps.

500 ppm of 156.25 MHz clock is 78,125 → MAX freq =  
 $156250000 + 78,125 = 156,328,125$  Hz

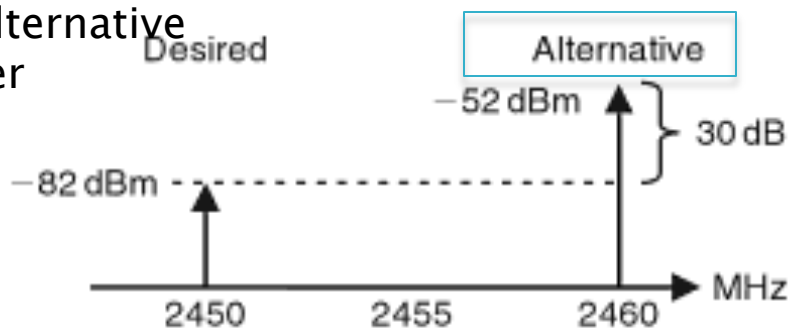
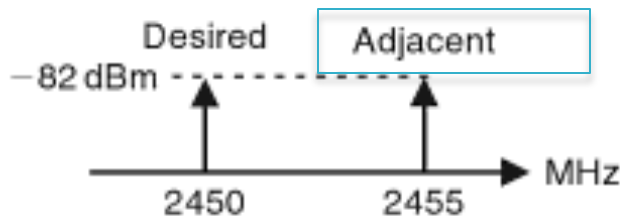
# IEEE 802.15.4 PHY Layer Specifications

## Jamming Resistance

- ▶ What happens to the receiver SNR in the presence of adjacent and alternative channels?
- ▶ The minimum required resistance to signals from 802.15.4 devices operating other channels, called the jamming resistance
- ▶ IEEE 802.15.4 Standard requirement:
  - **Adjacent Channel Rejection** is 0 dB – meaning the signal can be received even if the adjacent channel has the same signal strength
  - **Alternative Channel Rejection** is 30 dB – meaning the signal can be received even if the alternative channel has signal strength 30 dB larger



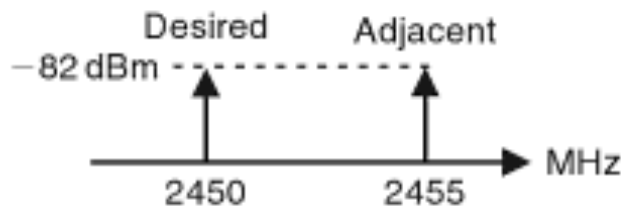
Multiple Nodes Communicating with the Base Station



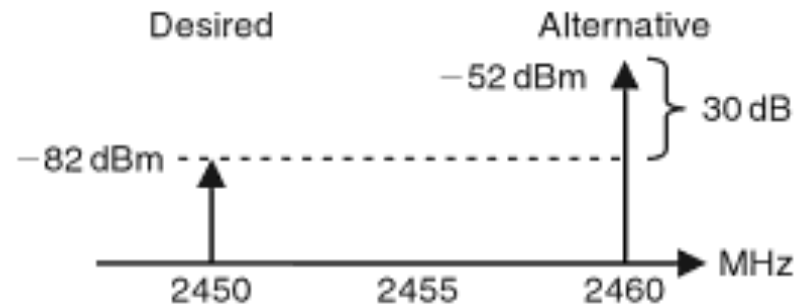
# IEEE 802.15.4 PHY Layer Specifications

## Jamming Resistance

- ▶ Resistance of a receiver in the presence of adjacent or alternative channels
- ▶ IEEE 802.15.4 Standard requirement:
  - Maintain PER  $< 1\%$  under the following conditions:



When desired and interferer signals are at  $-82\text{dBm}$   $\rightarrow$  PER  $< 1\%$

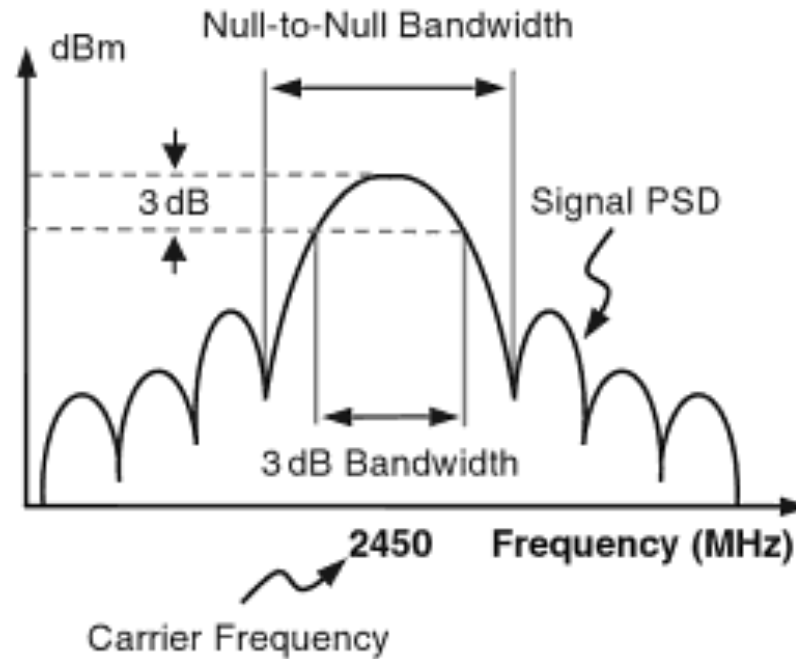


When desired signal is at  $-82\text{dBm}$  and interferer signal is at  $-52\text{dBm}$   $\rightarrow$  PER  $< 1\%$

# IEEE 802.15.4 PHY Layer Specifications

## Bandwidth

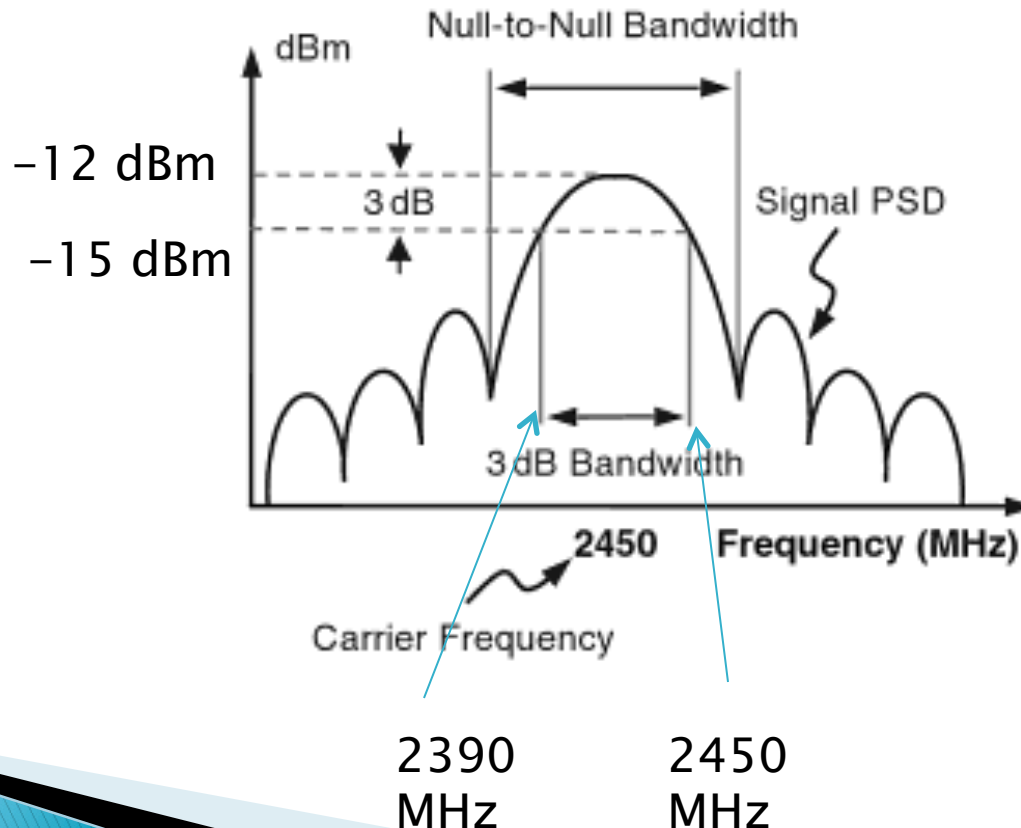
- ▶ 3-dB bandwidth representation
- ▶ Also called null-to-null bandwidth



# IEEE 802.15.4 PHY Layer Specifications

## Bandwidth – Example

- ▶ Calculate 3dB BW
- ▶ Which is larger 3-dB or Null-to-Null BW?

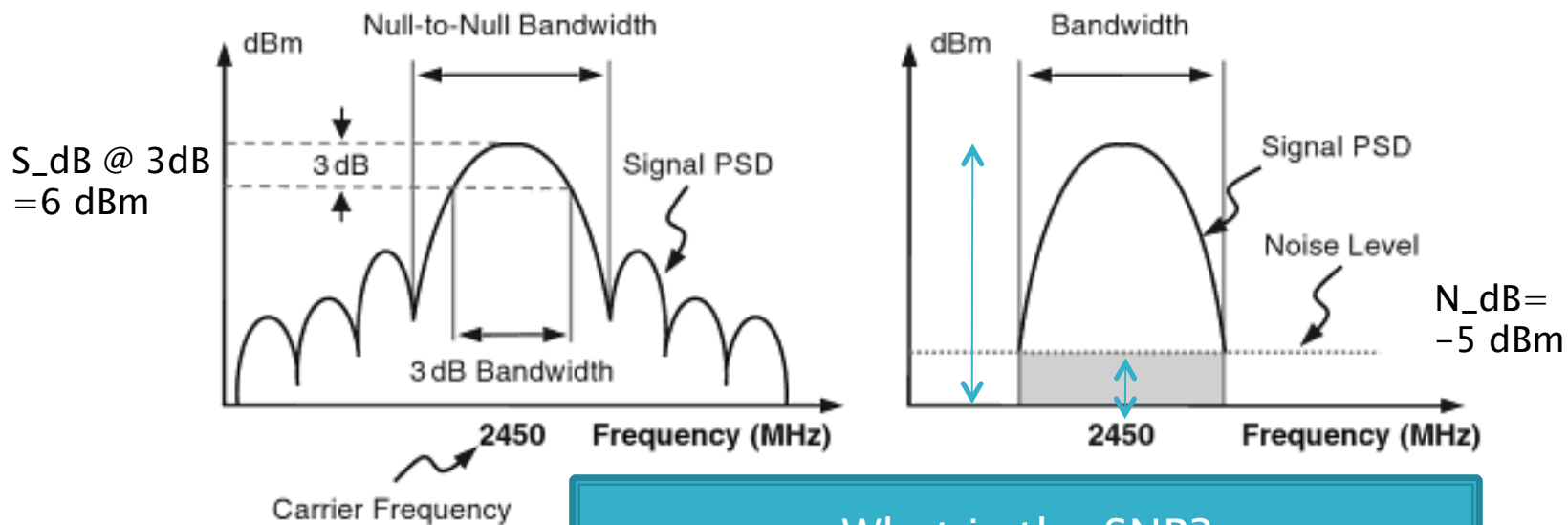




# IEEE 802.15.4 PHY Layer Specifications

## Signal-to-Noise Ratio – Example

- ▶ Bandwidth and power spectral density (PSD)
- ▶ SNR is defined as the ratio of total signal power to noise power
  - Increasing SNR improves PER (packet error ratio)



What is the SNR?

$$S_{dB} - N_{dB} = 6 - (-5) = 11 \text{ dB}$$



# IEEE 802.15.4 PHY Layer Specifications – Power Efficiency

- ▶ Low duty cycle
  - Ratio of active time to the total time
  - Typically less than 1% to ensure long battery life
- Duty-cycle control using superframe structure
- Indirect data transmission
- Devices may sleep for extended period over multiple beacons
- Allows control of receiver state by higher layers

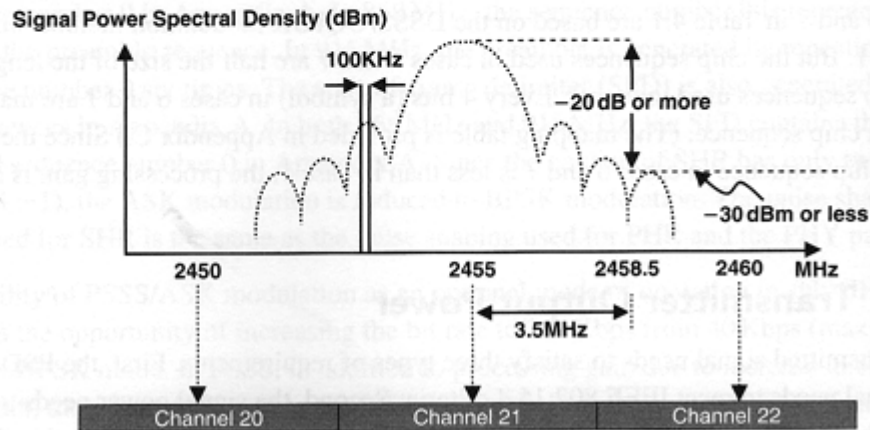
Calculate the duty cycle if the TX is ON only 20 msec every minute.

# IEEE 802.15.4 PHY Layer Specifications

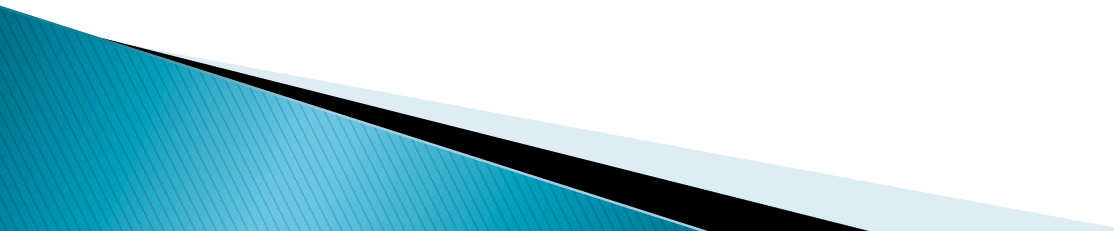
## PDS Limits in 802.15.4

- ▶ dBc is decibels relative to the carrier
- ▶ Where is the 3dB BW?

Frequency Band	Frequency Offset	Relative Limit	Absolute Limit
2.4 GHz	$ f - f_c  > 3.5\text{MHz}$	-20 dBc	-30 dBm
915 MHz	$ f - f_c  > 1.2\text{MHz}$	-20 dBc	-20 dBm
868 MHz	N/A	N/A	N/A



# IEEE 802.15.4 MAC Layer



# IEEE 802.15.4 MAC Layer Main Functionalities

- ▶ **Generate Beacons**
  - Coordinator uses for
    - sync.
    - Data is pending from the device
  - Received beacon information is passed to NWK layer
    - NWK makes sure the device is sync. (make sure no beacon is missing)
- ▶ **Synchronize to beacons**
  - NWK requests synch.
- ▶ **Channels Access**
  - ▶ **Implements CSMA/CA**
    - Request performing Clear Channel Assessment before transmission
  - ▶ **Manage GTS (Guaranteed time slot) channel access**
    - Deny GTS
    - Request from coordinator
    - Take away from device
- ▶ **MAC security**
- ▶ **Channel Scanning**
- ▶ **Perform PAN association and disassociation**

# Channel Access Methods

- ▶ Contention-based channel access
  - In CSMA-CA the first channel that get access starts transmitting (misbehave?)
  - Two channels can send at the same time → contention!
- ▶ Contention-free channel access
  - Guaranteed time slot (GTS)

ZigBee uses both GTS and CSMA-CA

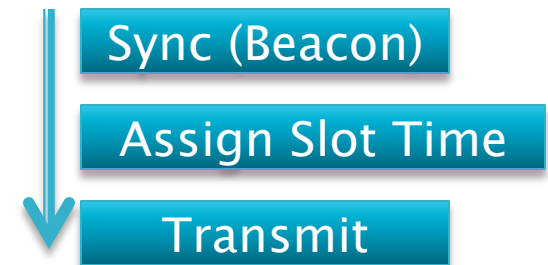
# Channel Access Methods – CSMA

- ▶ CSMA-CA
  - Contention-based channel access
  - 802.15.4 implements Carrier Sense Multiple Access with Collision Avoidance
    - When the device wants to send something it performs a Clear Channel Assessment (CCA)
      - This is done through **Channel Energy Scan**
    - Then, it starts sending
- ▶ Alternative methods to check if channel is busy:
  - **Spectral Energy**
    - This is called going into **Receive Mode** and performing **Energy Detection (ED)**
    - It doesn't matter if it is caused by other ZigBee nodes or by another technology or noise
    - Just reports if the spectrum is being used
    - Only when the value received is below a certain threshold we will transmit
  - **Carrier Sense (CS)**
    - Scan the medium and report if there are 802.15.4 transmissions
    - Only when the channel is free we will transmit
  - **CS + Energy:**
    - Scan the medium and report if there are 802.15.4 transmissions above the energy threshold specified
    - If not we will use the channel

# Channel Access Methods

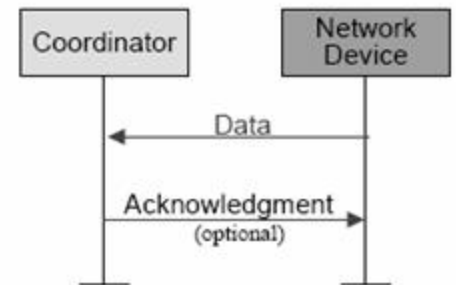
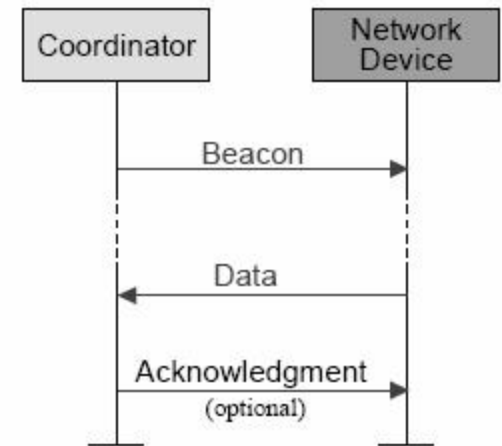
## Guaranteed Time Slot (GTS)

- ▶ Contention-free channel access
- ▶ A centralized node (**PAN coordinator**) first makes sure all the devices in the network are synchronized
  - Beacon messages are used
  - Referred as **beacon-enabled PAN** (beacon networking)
  - The disadvantage longer duty cycle (more power busy responding to the beacon)
- ▶ PAN gives slots of time to each node so that any knows when they have to transmit
- ▶ There are 16 possible slots of time
  - A node must send to the PAN coordinator a GTS request message
  - The PAN will send a beacon message containing the slot allocated and the number of slots assigned
- ▶ A device with an allocated GTS will start transmitting without using the CSMA-CA
- ▶ Nonbeacon network is not capable of using GTS
  - Not contention-free
  - Better battery power
  - The device **wakes up** less often!



# Data Transfer Methods – Device to the coordinator

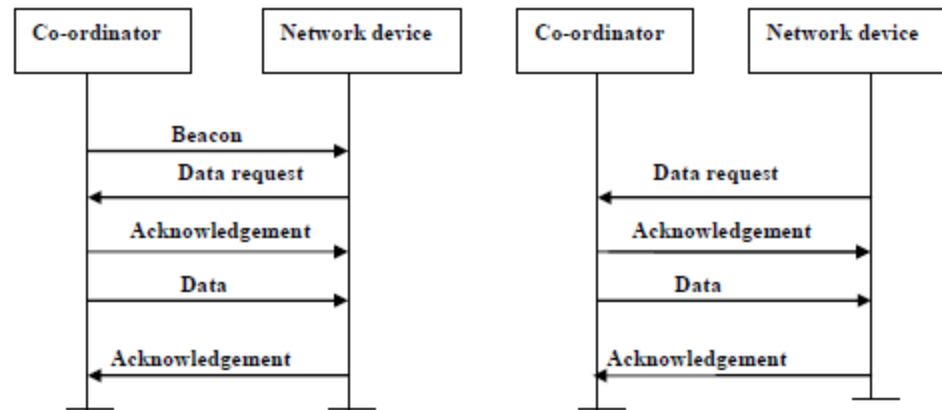
- ▶ Beacon-enabled
  - Coordinator sends beacon
  - Device sends data
  - Coordinator sends ACK
- ▶ Non-beacon enabled
  - The device just sends the data (CSMA-CA)
  - The Coordinator sends back an ACK





# Data Transfer Methods – Coordinator to Device

- ▶ Beacon-enabled
  - Coordinator sends beacon saying he has data to send
  - The device sends a data request message
- ▶ Non-beacon enabled
  - The coordinator waits until the device requests for data



(a) Beacon Enabled

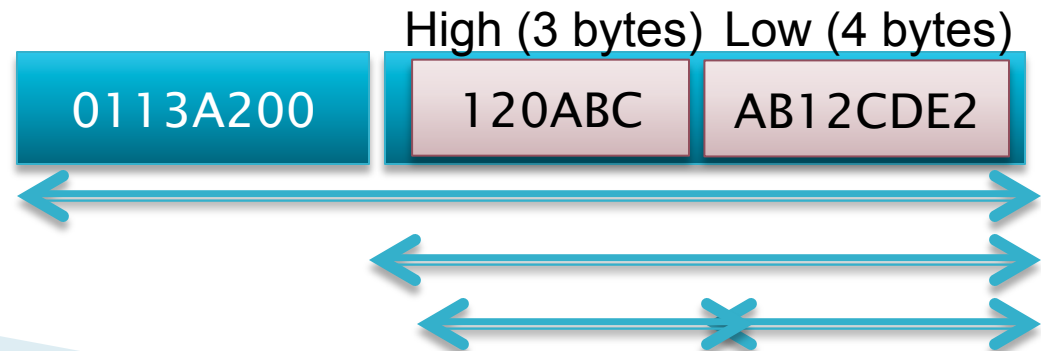
(b) Nonbeacon Enabled

# Network Addressing

## 802.15.4



- ▶ Strictly speaking, 802.15.4 supports 16-bit and 64-bit addressing
  - 64-bit unique serial number (radio address)
    - 00113A200 + xxxxxxxx (High + Low)
    - 00113A200 Identifies Digi XBEE Coordinators
  - 16-bit dynamic address
    - PAN ID
    - Within each PAN we can have multiple node ID addresses which are only unique to the PAN
- ▶ To establish connection, each network must operate under a unique channel number
  - All embedded PANs must operate within the same frequency

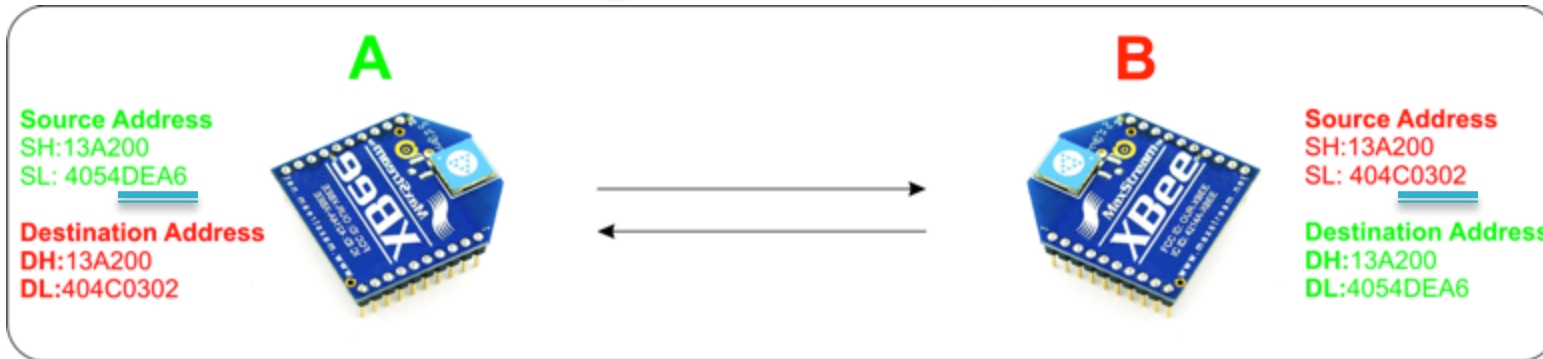


# Network Addressing

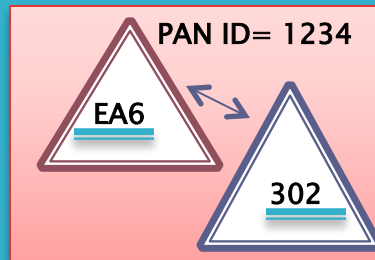
## 802.15.4 & ZigBee

- ▶ ZigBee in turn provides a Network Layer Address
  - -16-bit address
  - It maps 64-bit address of the radio to NWK address
- ▶ Channels must be the same within a network for nodes to communicate with one another
  - Wireless links under 802.15.4 can operate in 27 different channels
  - PHY layer should be able to tune its transceiver into a certain channel upon receiving the request from MAC sub-layer
  - Channel selection can be performed automatically

# Addressing Example (1)



Channel 12



X-CTU [COM12] Module A

Remote Configuration

Modem Parameters and Firmware: Read Write Restore Clear Screen Save Load

Modem: XBEE-PRO Function Set: ZNET 2.5 ROUTER/END DEVICE AT Version: 1247

Networking

- [FFFF] MY - Operating PAN ID
- [234] ID - PAN ID
- [1FFE] SC - Scan Channels
- [3] SD - Scan Duration
- [FF] NJ - Node Join Time
- [0] JV - Channel Verification

Addressing

- [FFFF] MY - 16-bit Network Address
- [13A200] SH - Serial Number High
- [4054DEA6] SL - Serial Number Low
- [13A200] DH - Destination Address High
- [404C0302] DL - Destination Address Low
- [0] ZA - ZigBee Addressing
- [E8] SE - Source Endpoint
- [E8] DE - Destination Endpoint
- [11] CI - Cluster ID
- [ ] NI - Node Identifier
- [0] BH - Broadcast Radius

Change networking settings:

COM12 9600 8N-1 FLOW:NONE XBEP24-B Ver:1247

X-CTU [COM12] Module B

Remote Configuration

Modem Parameters and Firmware: Read Write Restore Clear Screen Save Load

Modem: XBEE-PRO Function Set: ZNET 2.5 COORDINATOR AT Version: 1047

Networking

- [12] CH - Operating Channel
- [234] OP - Operating PAN ID
- [234] ID - PAN ID
- [1FFE] SC - Scan Channels
- [3] SD - Scan Duration
- [FF] NJ - Node Join Time

Addressing

- [0] MY - 16-bit Network Address
- [13A200] SH - Serial Number High
- [404C0302] SL - Serial Number Low
- [13A200] DH - Destination Address High
- [4054DEA6] DL - Destination Address Low
- [0] ZA - ZigBee Addressing
- [E8] SE - Source Endpoint
- [E8] DE - Destination Endpoint
- [11] CI - Cluster ID
- [COM8] NI - Node Identifier
- [0] BH - Broadcast Radius
- [FF] AR - Aggregation Route Broadcast Time

Set/read the lower 32 bits of the 64 bit destination extended address. 0x0000000000000000 is the broadcast address for the PAN. 0x0000000000000000 can be used to address the Pan Coordinator.

RANGE: 0-0xFFFFFFFF

COM12 9600 8N-1 FLOW:NONE XBEP24-B Ver:1047

# Addressing Example (2)

802.15.4 ZigBee Module Pair Utility

Device 1  
Port Name: COM7  
Baud Rate: 9600

Device 2  
Port Name: COM8  
Baud Rate: 9600

**MY (Xbee ID) is set to Zero**

Parameter	Device 1 Value	Device 2 Value
AP	01	01
Baudrate	br_9600	br_9600
DH	0013A200	0013A200
DL	4092F15C	4033DD15
MY	0000	0000
NI		
PanID	3333	3333
CH	0C	0C
FirmwareID	10ED	10EC
SH	0013A200	0013A200
SL	4033DD15	4092F15C

**DL/DH 64 bits**

**Same PAN ID**

**64 Bits**

**DL**  
The lower 32 bits of the 64 bit destination extended address. 0x000000000000FFFF is the broadcast address for the PAN. 0x0000000000000000 can be used to address the Pan C...

**Read** **Write** **4** **Copy To Device2** **Read** **Write** **Copy To Device1** **3**

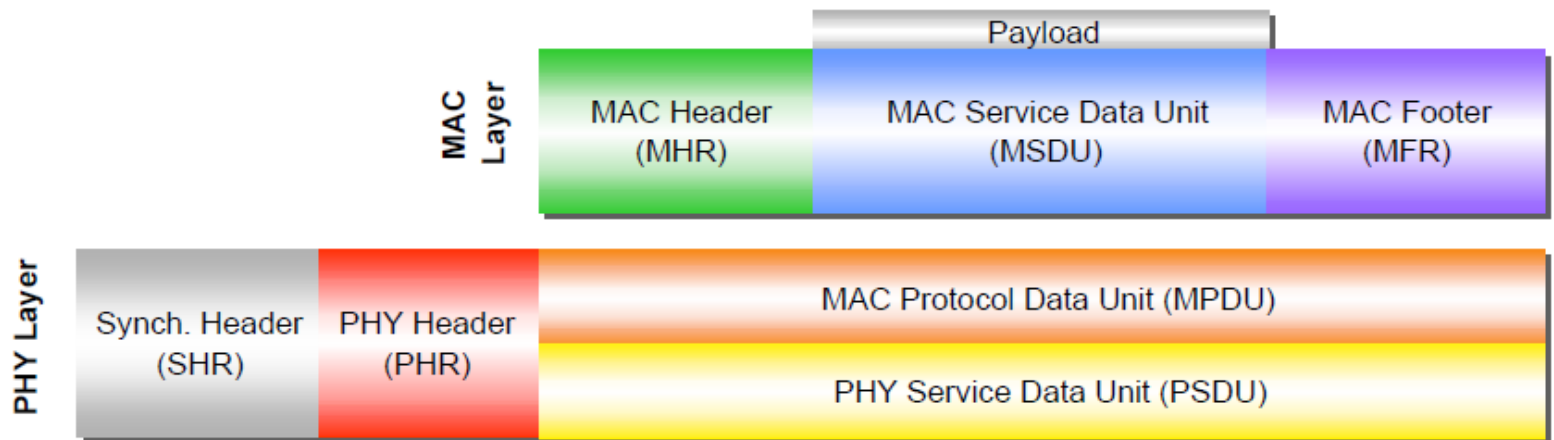
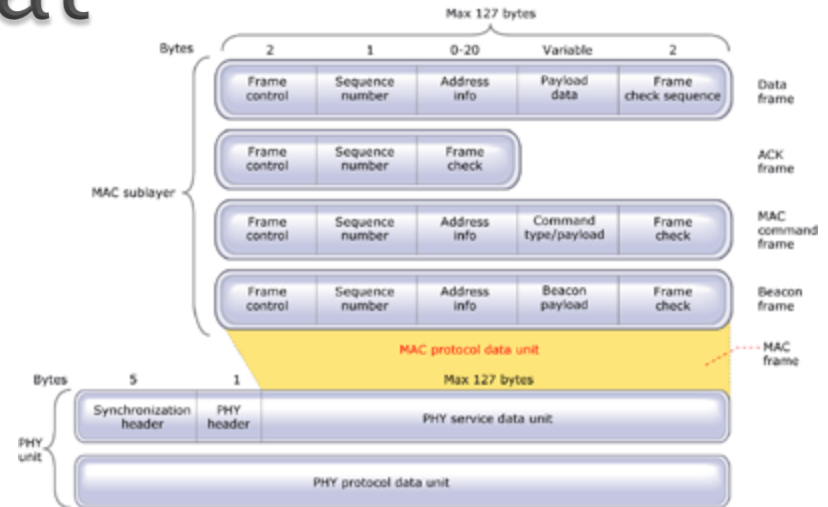
# IEEE 802.15.4 MAC Layer Channel Scanning

- ▶ A service requested by the network layer (NWK)
- ▶ Two basic types
  - Passive
    - Energy in each channel is measured using the ED service provided in PHY
    - Only the receiver is on (no beacons)
  - Active
    - Used by the coordinator interested to create its own network
    - Sends beacon to find all active PAN ID and channels
    - Used to find a unique PAN ID and available channel
    - Promiscuous mode to read all the devices (who is available)
  - Orphan
    - A node disconnected (disjoint) from the coordinator
    - The orphan sends a notification on each channel **within its POS** to find the coordinator so he can join the network

# MAC Frame Format

## 4 Types of MAC Frames:

- Data frame
- Beacon frame
- Acknowledgment frame
- MAC command frame



# MAC Frame Types

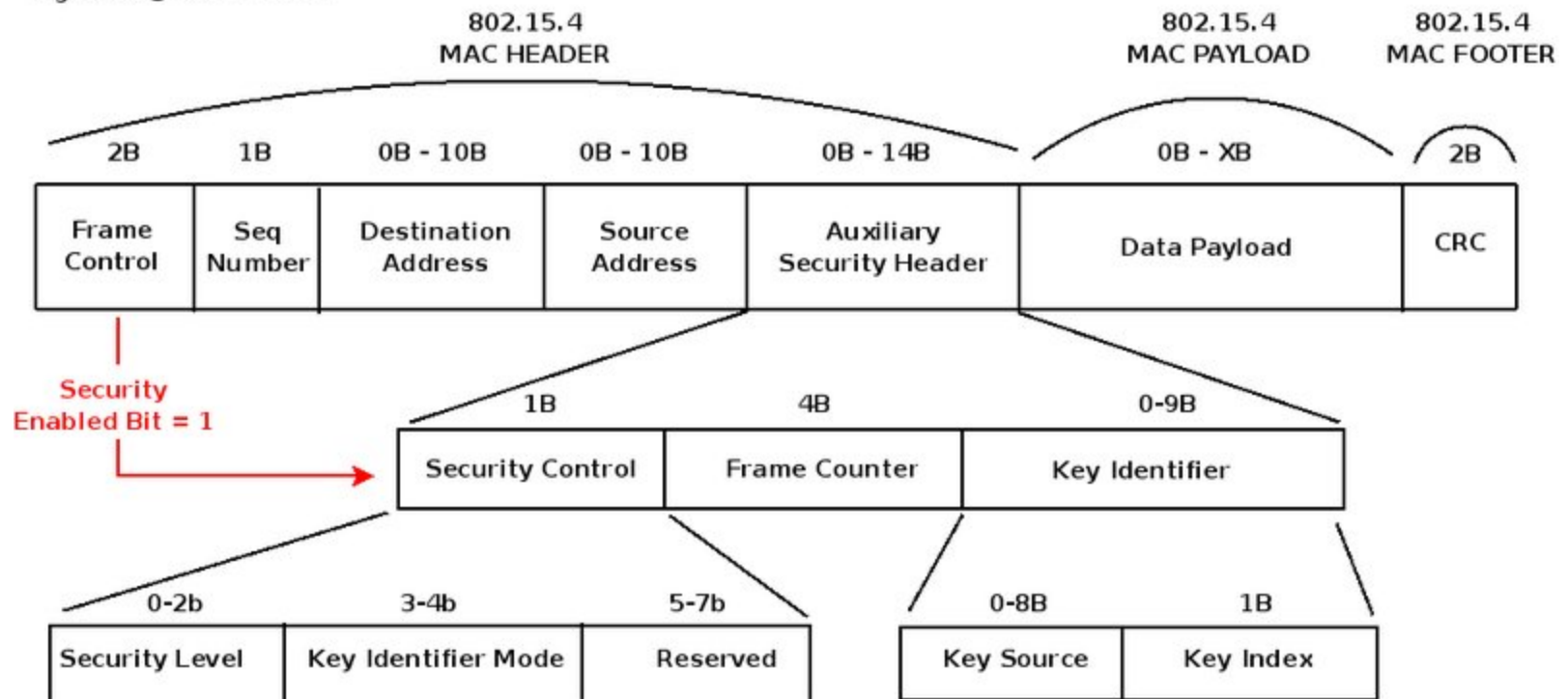
- ▶ Data
  - Payload provided by NWK
- ▶ Beacon Frame
  - Establish GTS (a list is GTS users is created)
    - How often beacons are generated (the end device needs to know for synch.)
  - Establish retransmission (seq. number)
  - There is pending data for end devices
- ▶ ACK
  - Success of reception
- ▶ MAC Command
  - Command to the recipient
  - Association and disassociation
  - Data request (from the coordinator who announced there is pending data)



# MAC Header Structure

Security in the IEEE 802.15.4 MAC FRAME  
<http://www.sensor-networks.org>

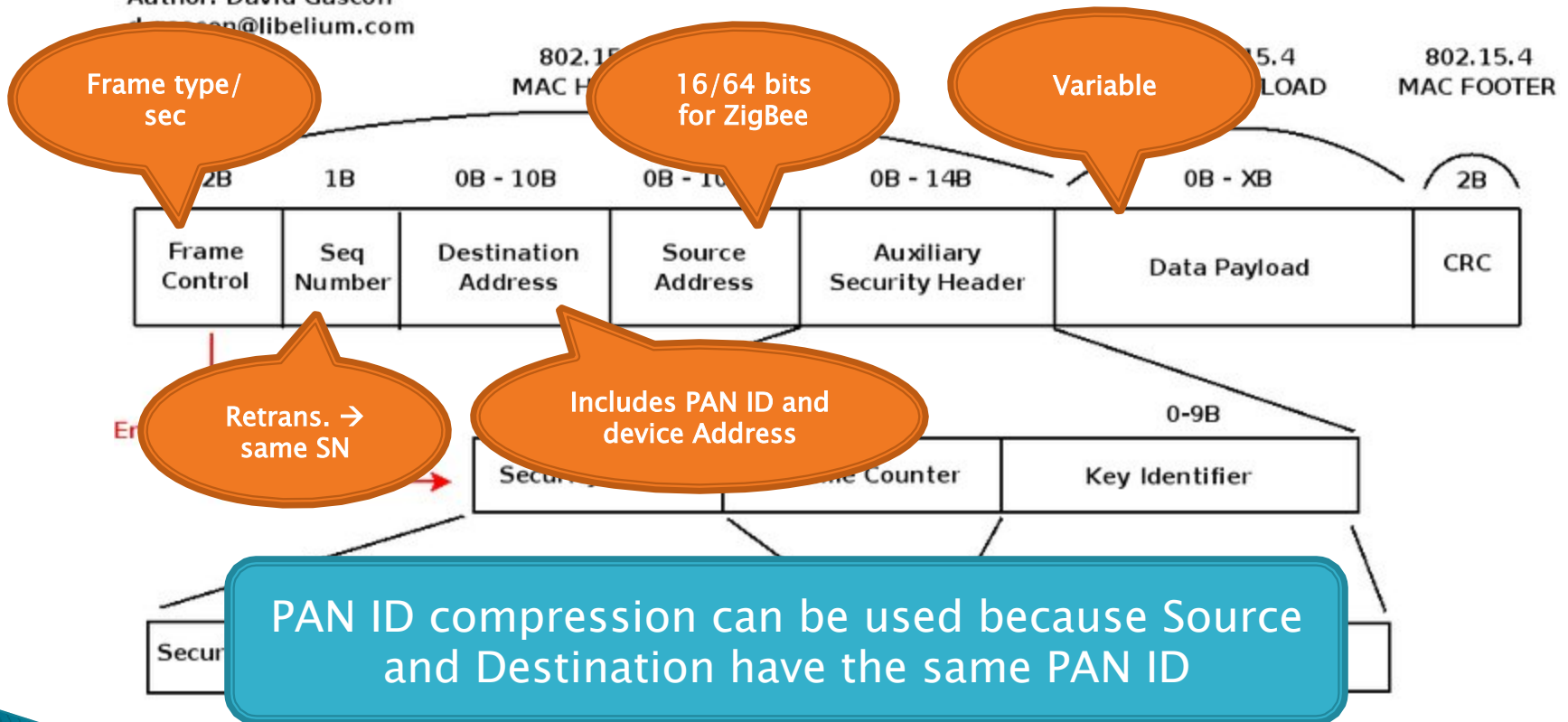
Author: David Gascón  
d.gascon@libelium.com



# MAC Header Structure

Security in the IEEE 802.15.4 MAC FRAME  
<http://www.sensor-networks.org>

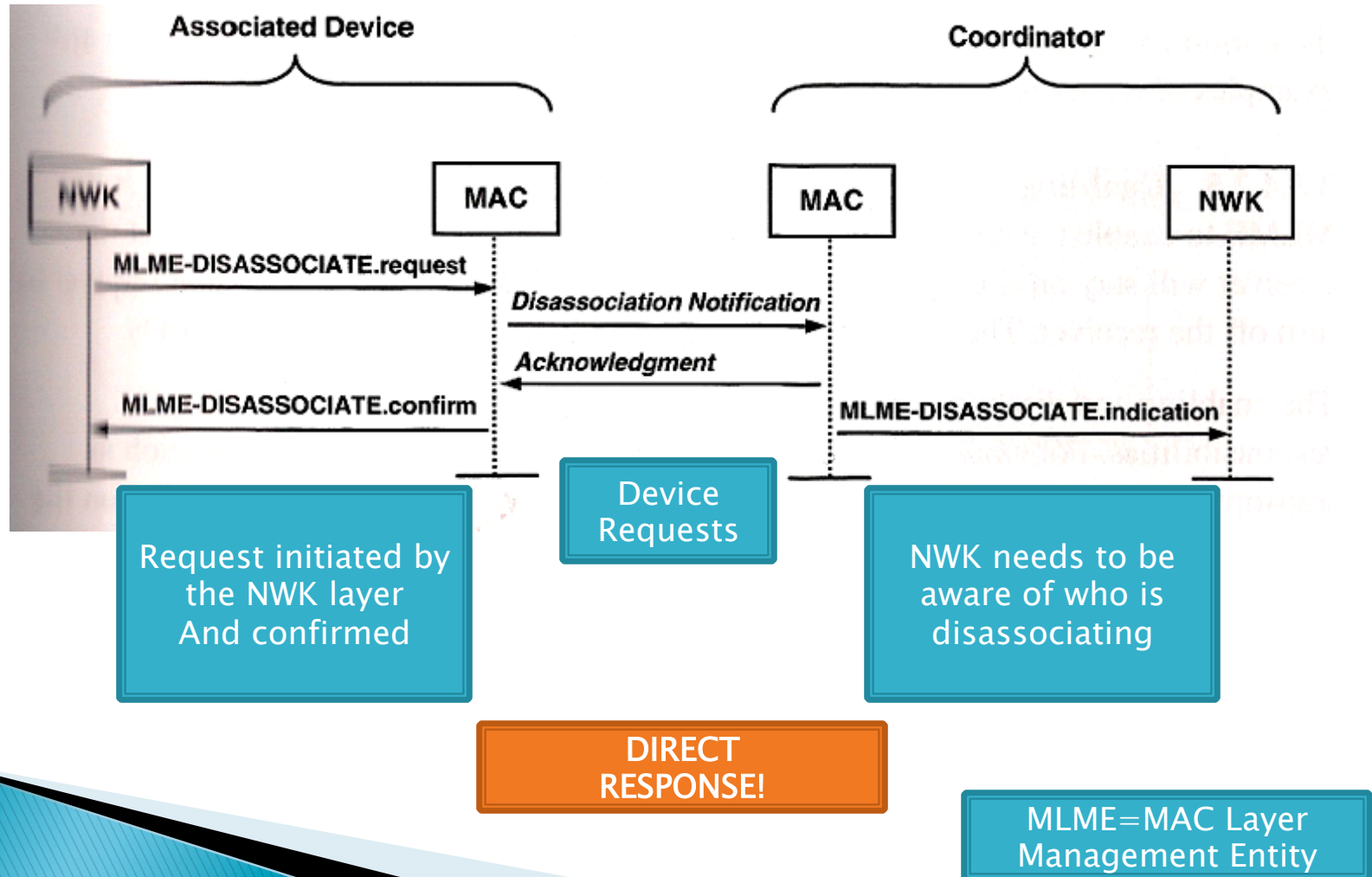
Author: David Gascón  
d.gascón@libelium.com



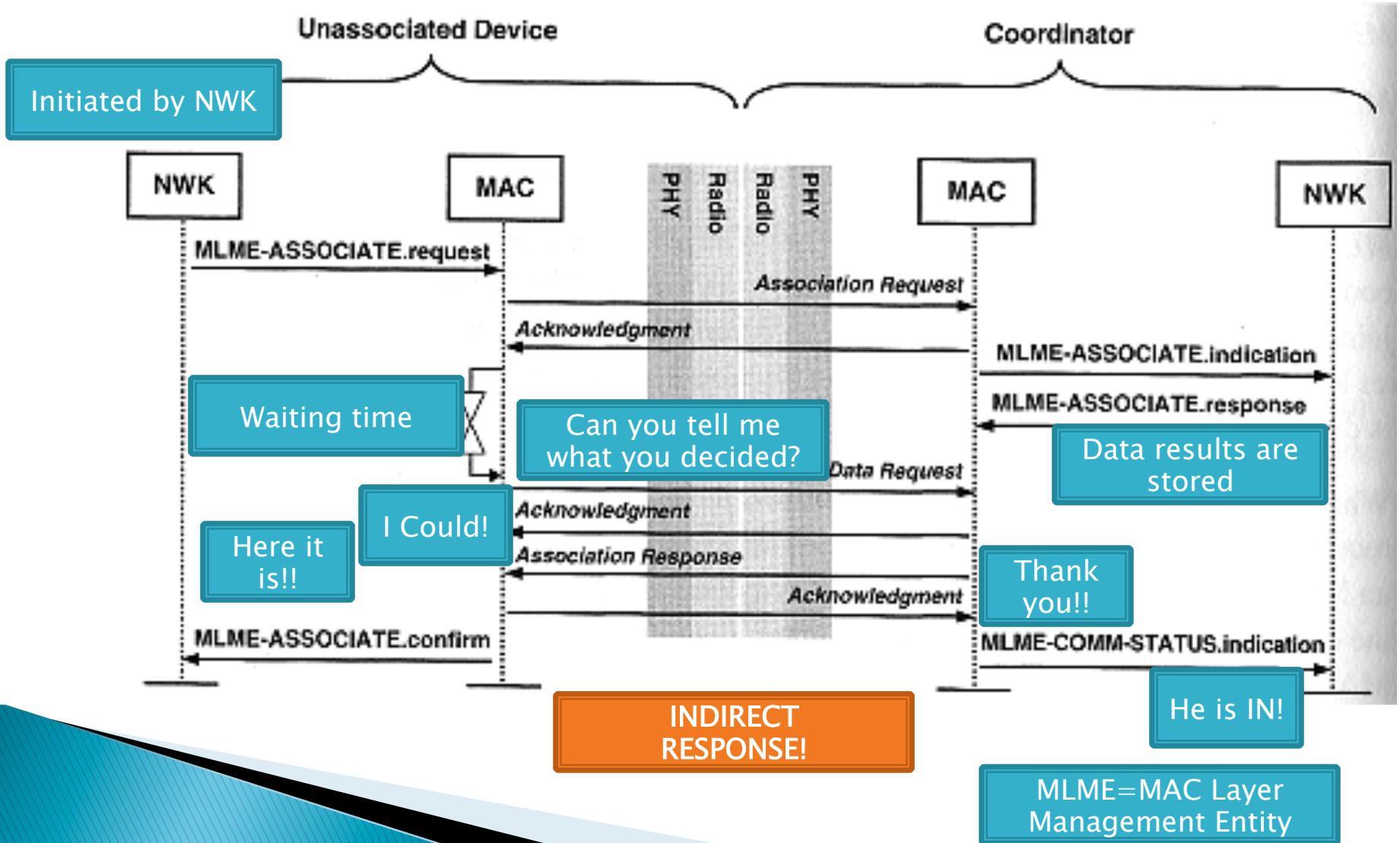
# MAC Management Service – Association and Disassociation

- ▶ A part of MAC management service offered to **NWK layer**
  - NWK of the coordinator uses this information to manage the network
  - NWK of the device uses this information to dis/join the network
- ▶ Association: Joining the network
  - Request to join the coordinator
  - Primitives: Request (device) & confirm (by coordination)
- ▶ Disassociation: Leaving the network

# MAC Management Service – Disassociation: Initiated by the device

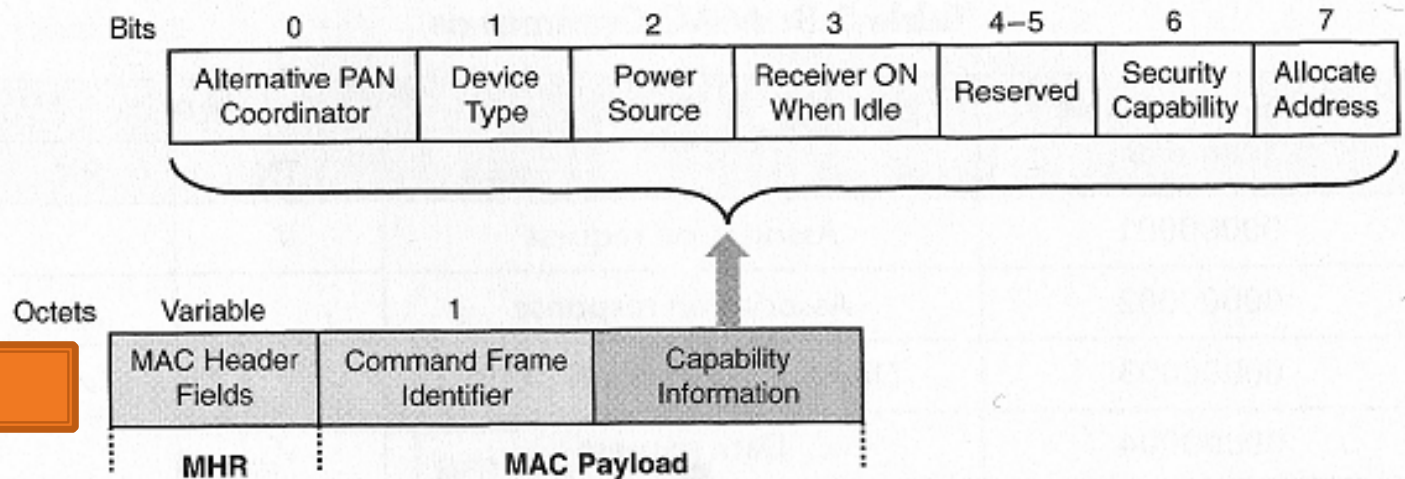


# MAC Management Service – Association: Initiated by the device (1)

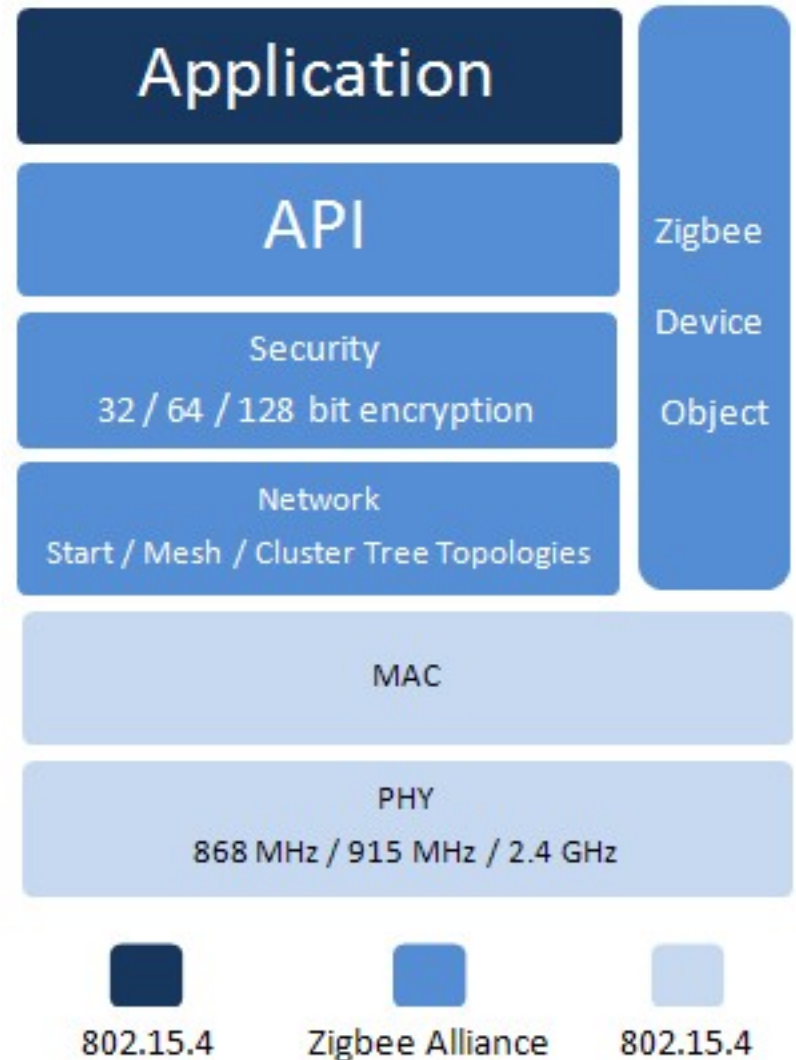


# MAC Management Service – Association: Initiated by the device (2)

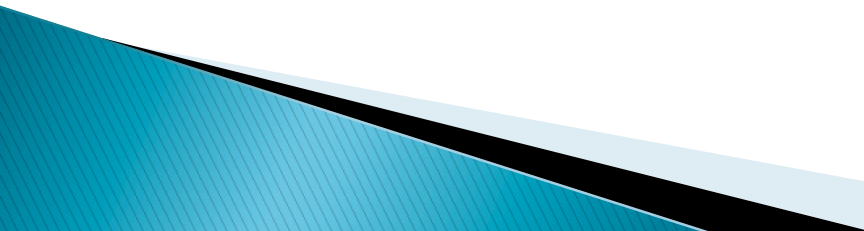
- ▶ *Association Request* Frame Structure
  - The device must tell the coordinator about his status



# Network Layer



# Network Layer – Functionalities

- ▶ Configure the device (end device, router, coordinator)
  - ▶ Starts a network
  - ▶ Allows joining or leaving
  - ▶ Apply network layer security
  - ▶ Perform routing and route discovery
  - ▶ Support various communication modes
  - ▶ Support different topologies
- 



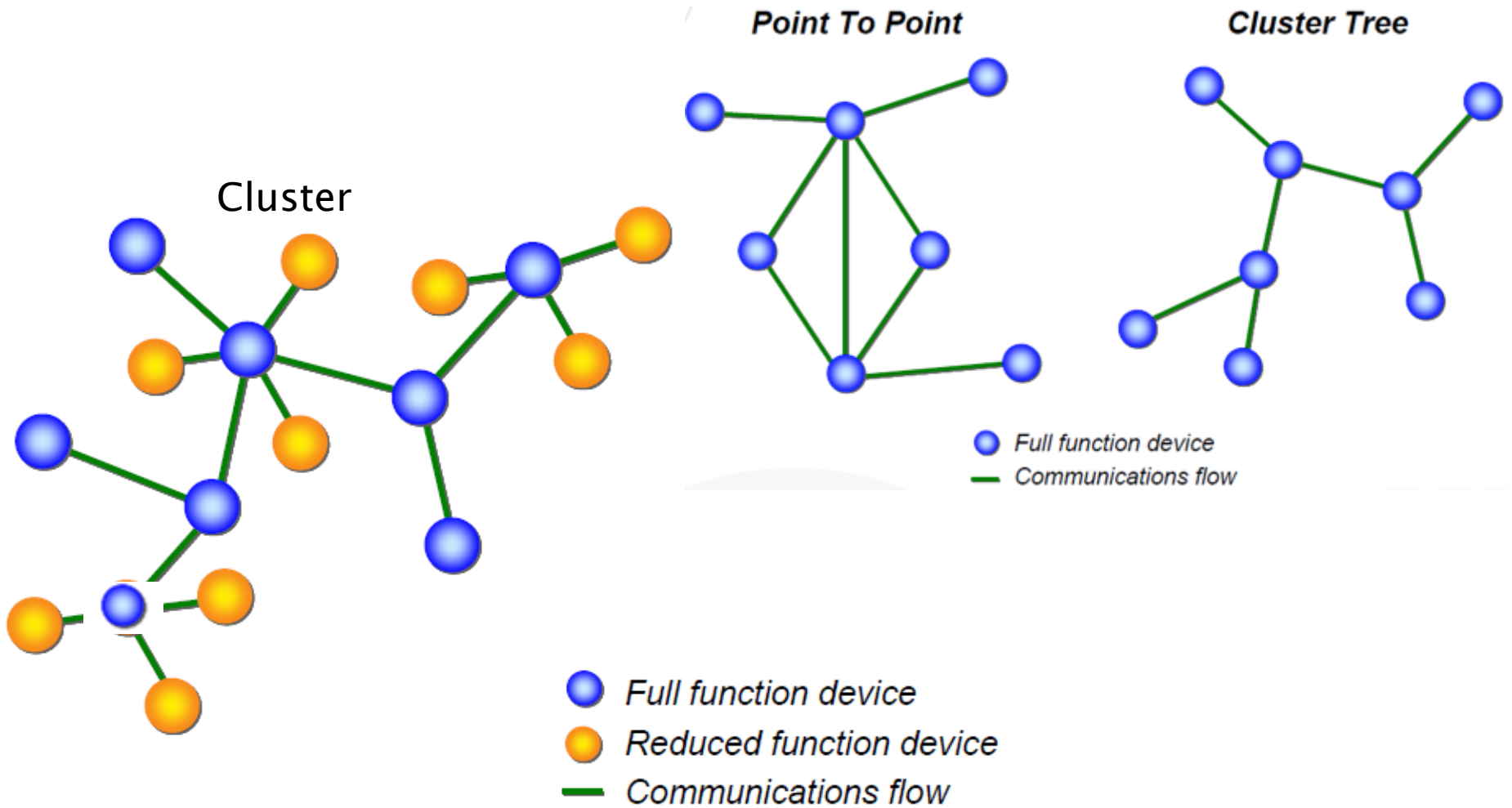
# Network Layer – Communication Modes

- ▶ **Broadcasting**
  - Selects a frequency channel (network)
  - The PAN ID=0xFFFF (16-bit short addressing)
- ▶ **Multicasting**
  - A group of devices are the destination (e.g., a number of lights in the room)
  - Any node on the network can initiate it (member or non-member)
- ▶ **Unicasting**
- ▶ **Many-to-one**
  - A Single sink node receiving all the traffic

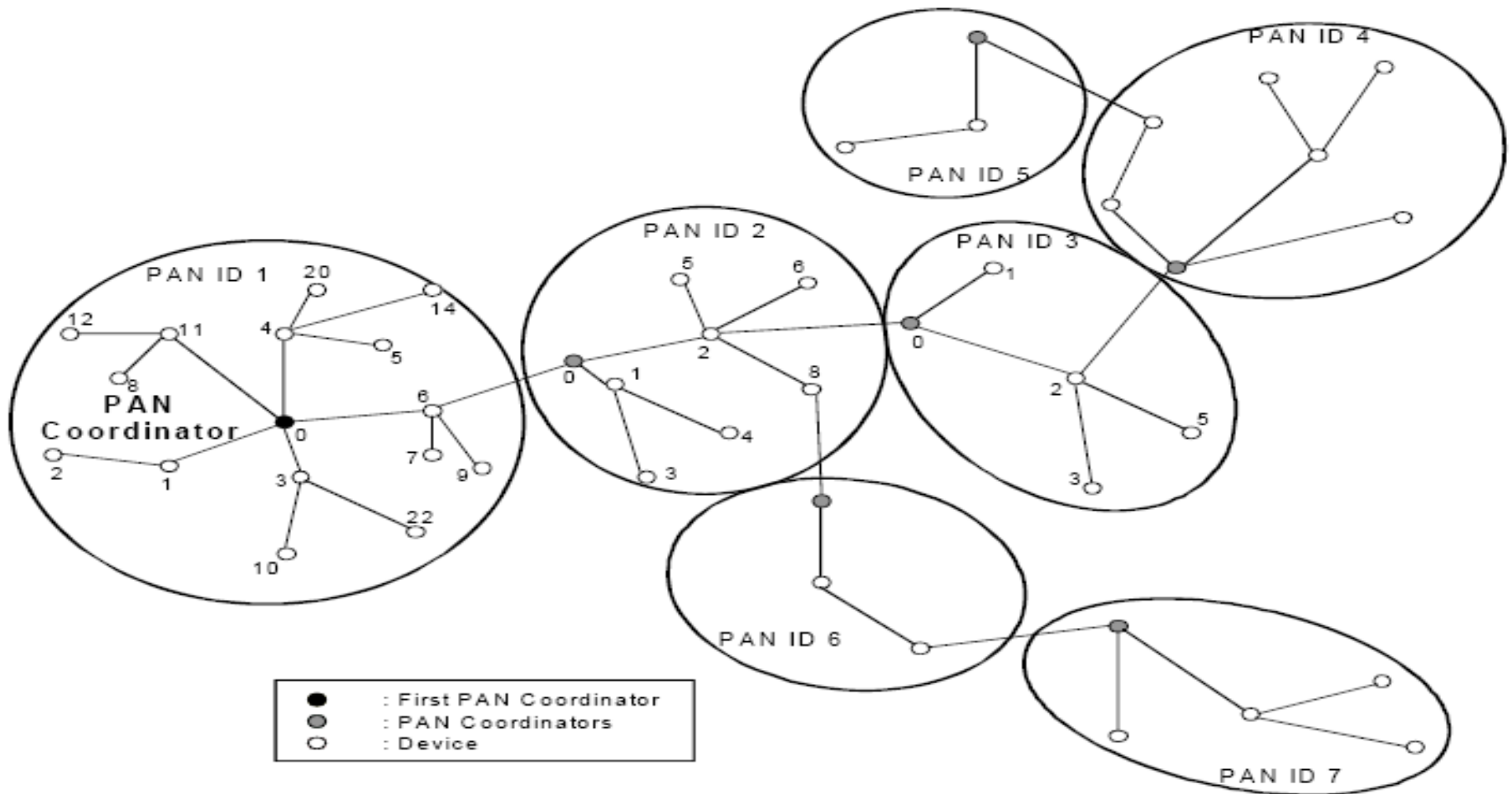
# ...Creating a Network

- ▶ The Application layer sets the Coordinator
  - Self-forming network
- ▶ The network is coordinated by the Coordinator
  - Coordinator is selected
  - Scans the channels (all other networks)
    - Active or passive
  - Select an available channel and a PAN ID
    - Make sure there is no channel/PAN conflict (if it receives a beacon with the same ID)

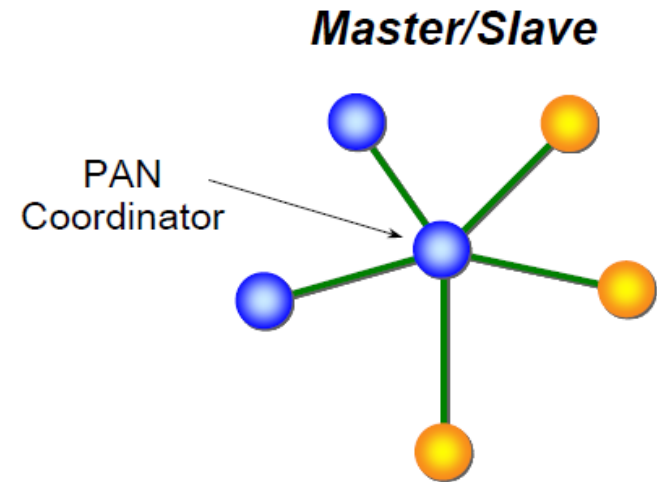
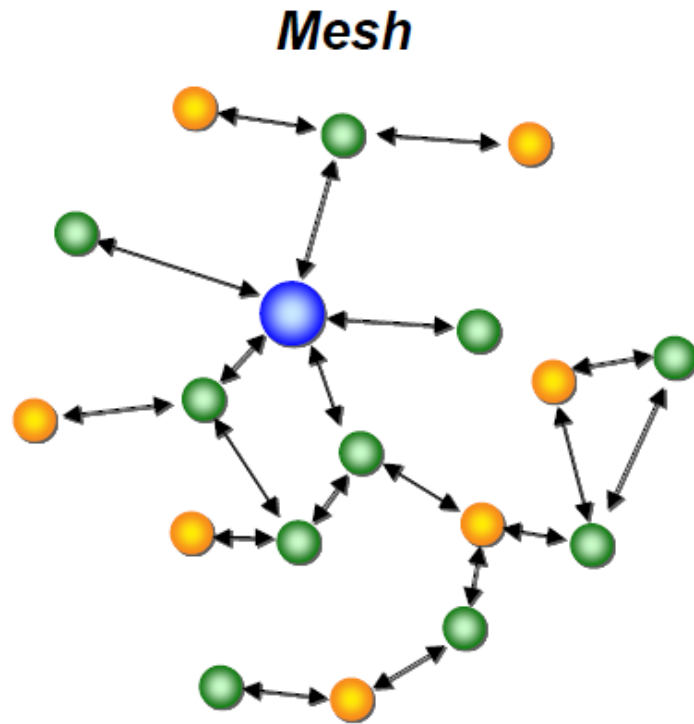
# MAC Peer-to-Peer






# Cluster Tree Network



# MAC Star and Mesh Topologies

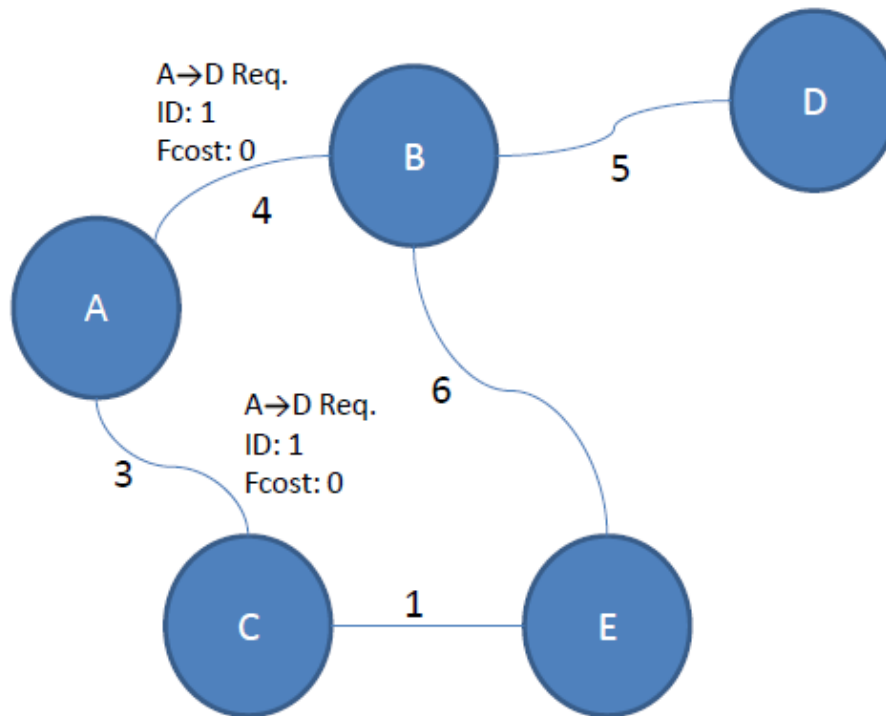


-  Full function device
-  Reduced function device
-  Communications flow

# Routing

- ▶ Performed by the coordinator and router on behalf of the end-device
- ▶ Routing is based on NEXT-HOP routing
  - What is the next hop (s,d) addressing is required
- ▶ Based on finding the *best* link
  - Link with the lowest cost
    - Energy efficient, least probability of error, etc.
- ▶ **Path cost** is sum of all link costs

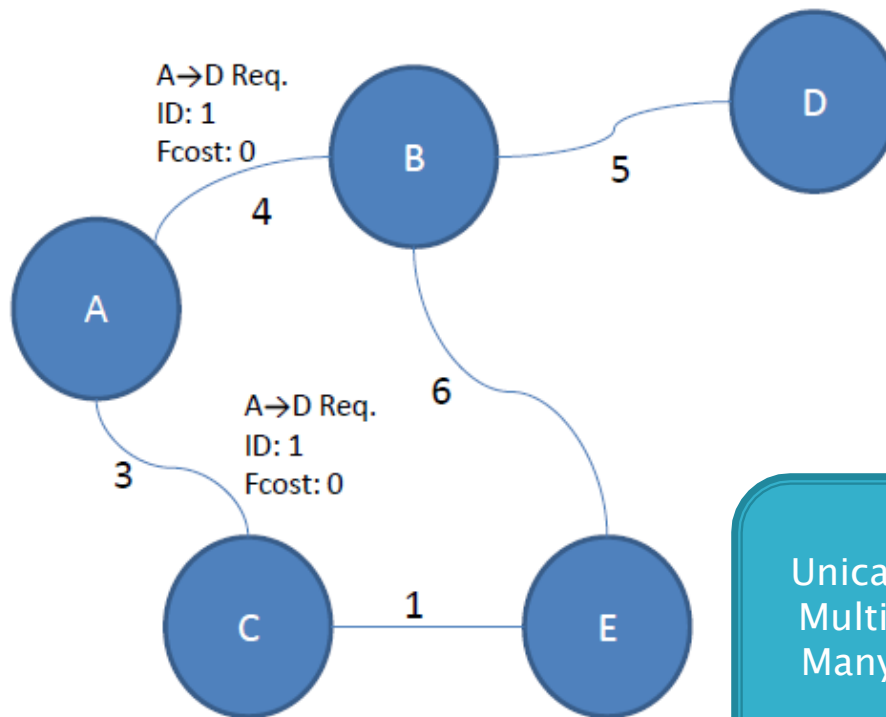
# Path Cost



Path cost from A→D  
Can be:  
9 or 15  
But which one?

*Note:* Numbers beside links are link costs

# Path Discovery



*Note:* Numbers beside links are link costs

Path discovery requires checking all networks members channels on POS (personal operation space)



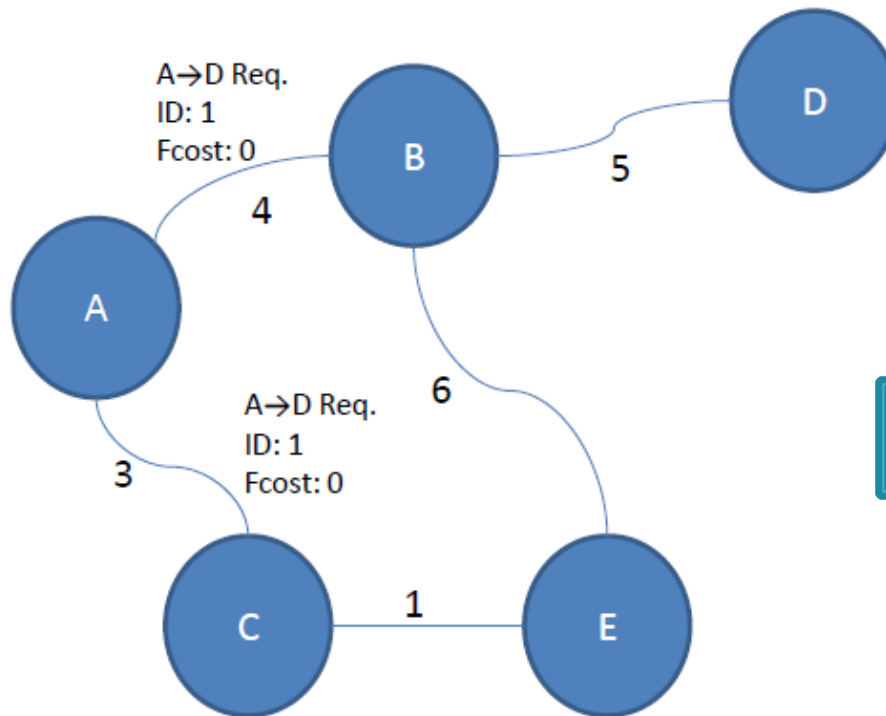
MAC has to perform channel scanning

Path discovery:

Unicast: Starting from node A ending at D  
Multicast: Broadcast to a multicast group  
Many-to-one: the destination will be the sink device



# Path Discovery



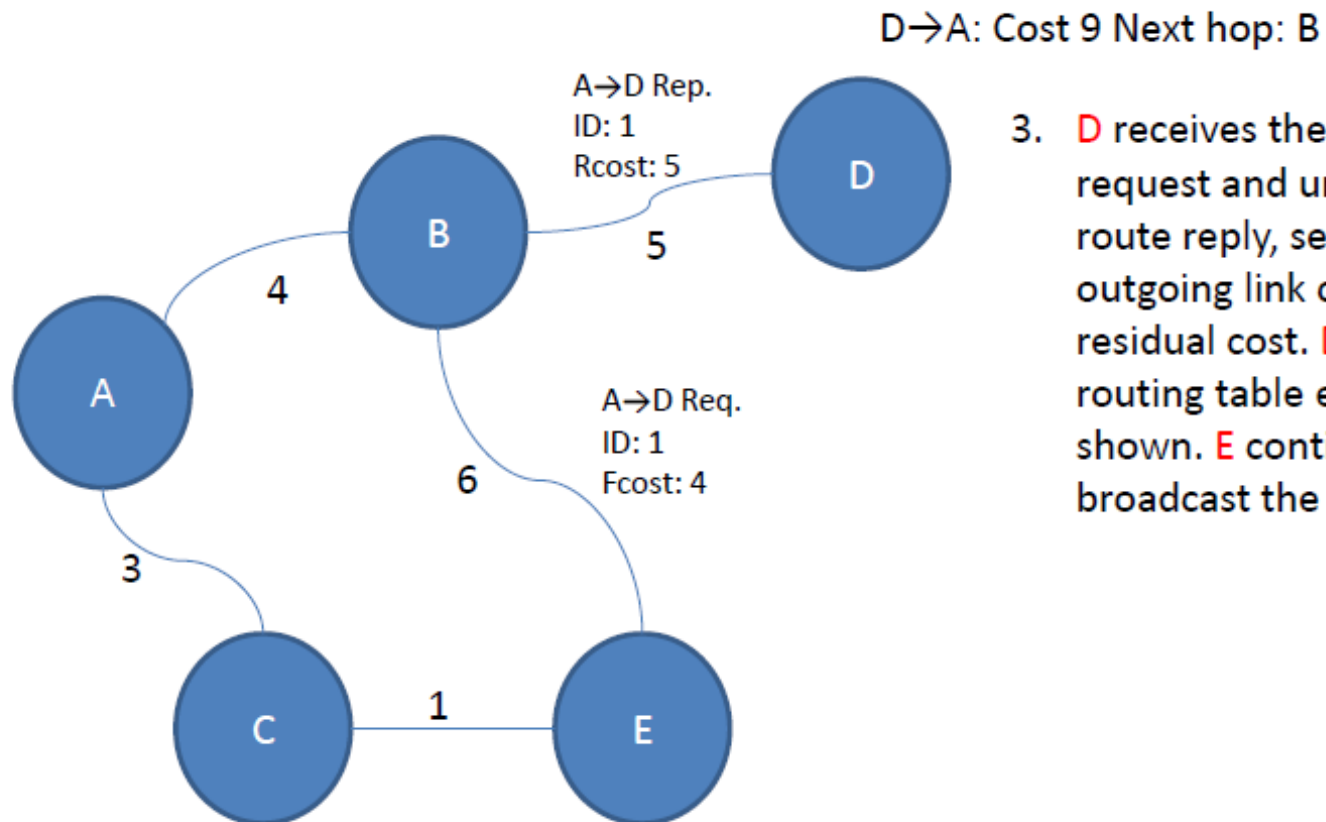
A wants to talk to D, but never met him before

1. A broadcasts a route request to its neighbors.

Unicast Rout Discovery  
A—B and A→C

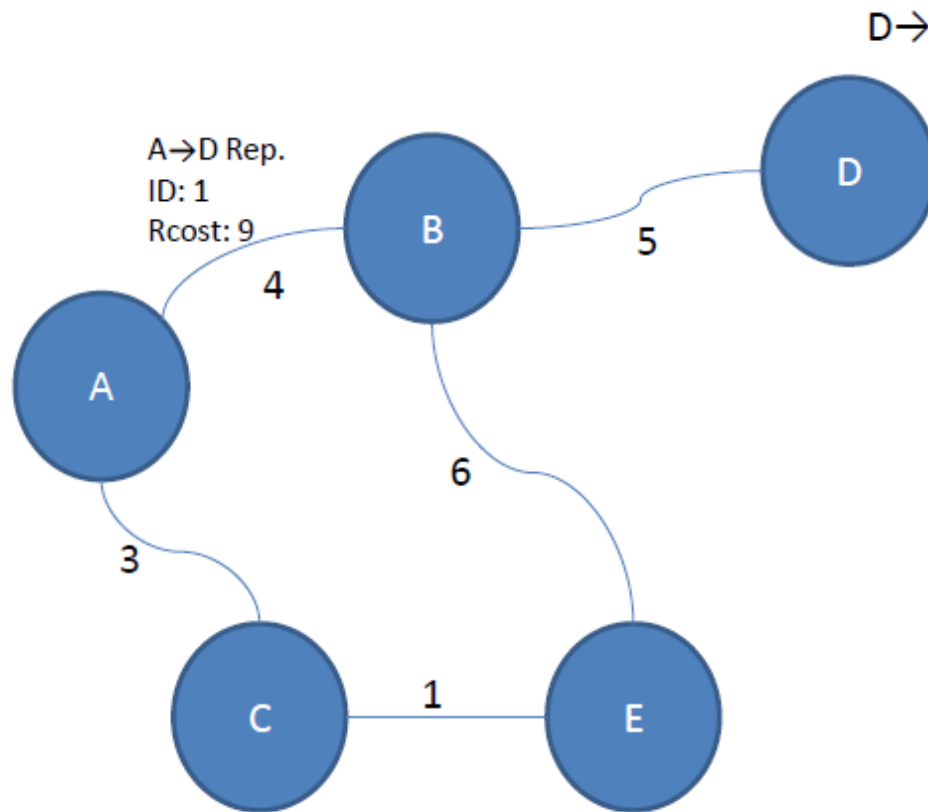
*Note:* Numbers beside links are link costs

# Path Discovery



3. **D** receives the route request and unicasts a route reply, setting the outgoing link cost as a residual cost. **D**'s new routing table entry is shown. **E** continues to broadcast the request.

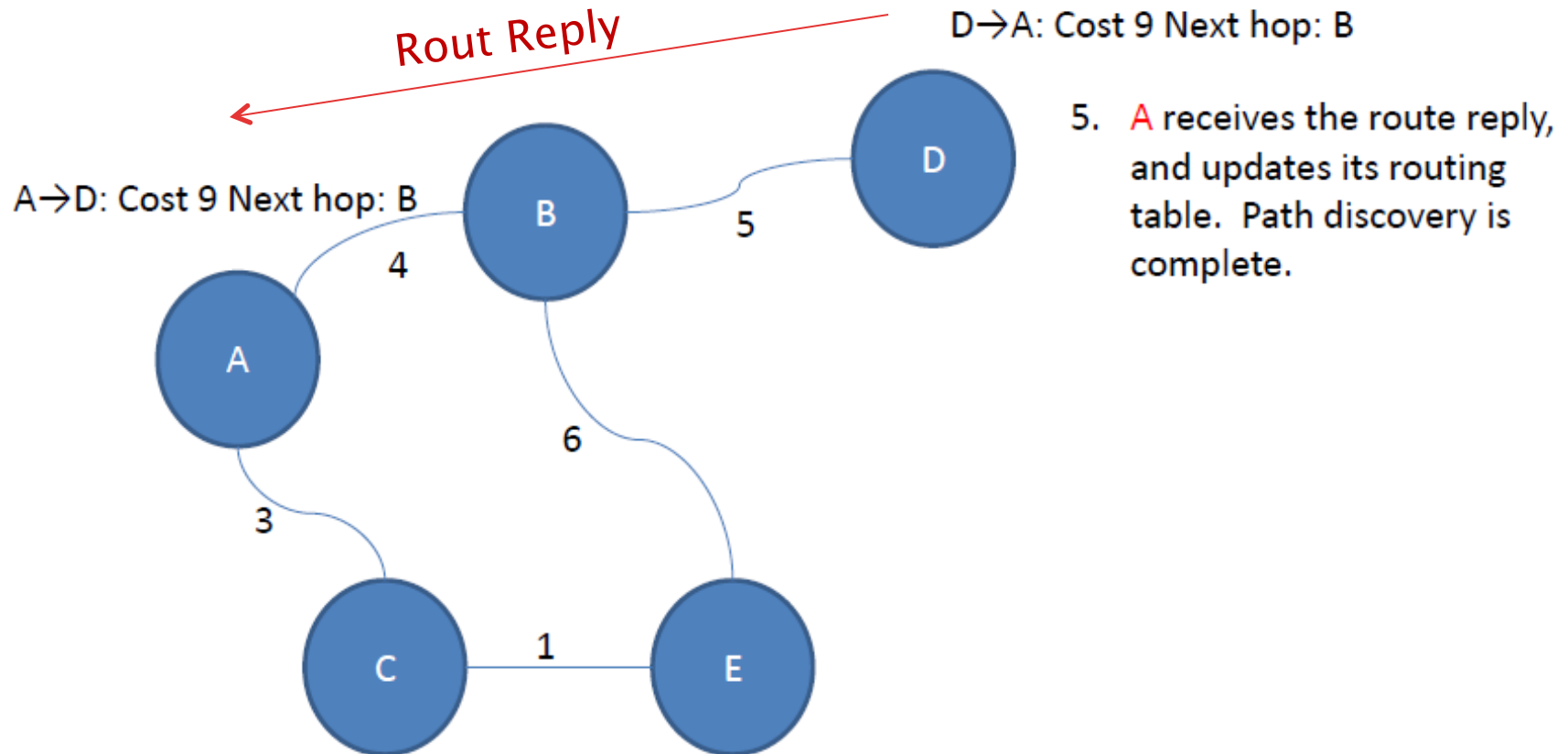
# Path Discovery



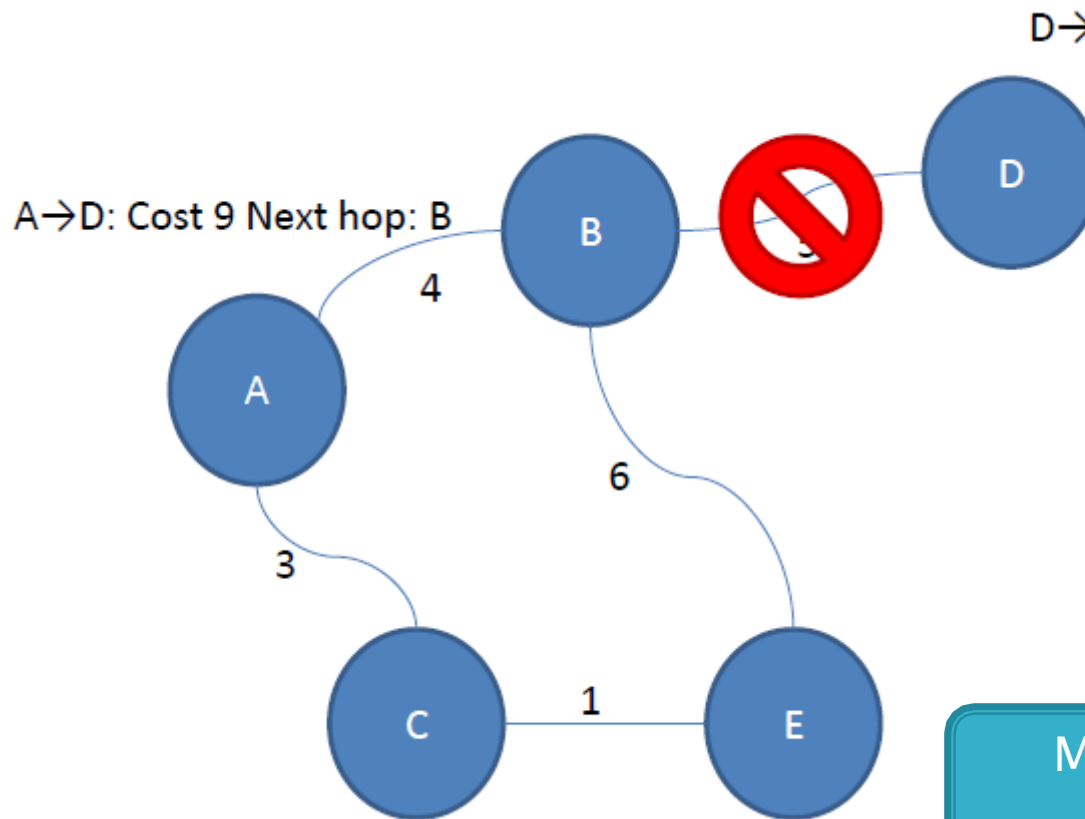
D→A: Cost 9 Next hop: B

4. E's route request is dropped by B since B has seen a lower cost. B unicasts the route reply to A, updating the residual cost.

# Path Discovery



# Path Discovery



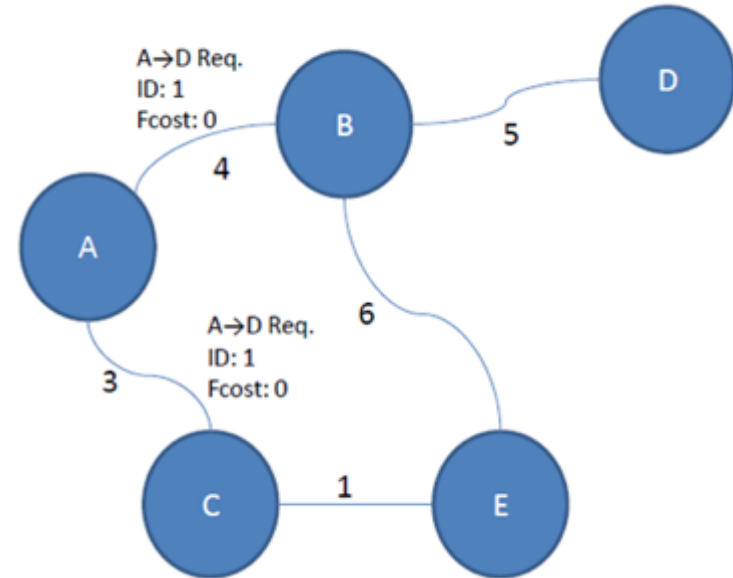
What if the link between **B** and **D** breaks, and **A** tries to send again?

- **A** sends a packet to **D**, first sending to **B** as its routing table suggests
- **B** notices the link failure, and tells **A**
- **A** deletes **D**'s entry in the routing table

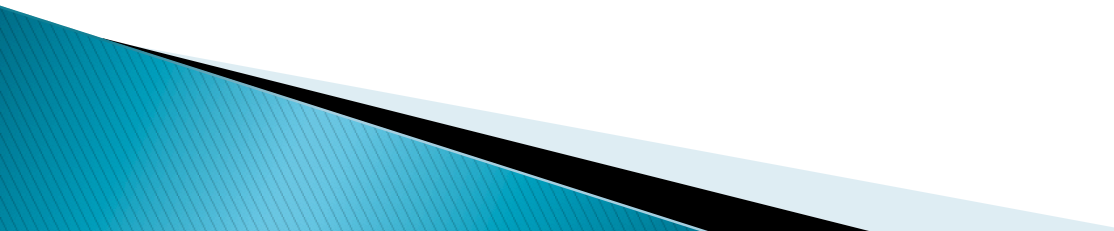
Modify the routing table!  
**Self-healing Feature**

# Forward vs. Backward Routing

- ▶ From A → D Forward routing
- ▶ From D → A backward routing
- ▶ If **symmetric routing** then forward routing and backward routing are the same
  - Otherwise backward route has to be discovered again



# Future ....

- ▶ API stuff
  - ▶ A few more set up and test
  - ▶ Using the network analyzer
  - ▶ Changing the channel and viewing it through the network analyzer
  
  - ▶ More on frequency ext.
- 

# Some References

- ▶ <http://www.zigbee.org/en/about/faq.asp>
- ▶ <http://www.zigbee.org/en/resources/#SlidePresentations>
- ▶ [http://computing.arizona.edu/networkmasterplan/tech\\_hpe\\_0703.pdf](http://computing.arizona.edu/networkmasterplan/tech_hpe_0703.pdf)
- ▶ <http://www.santafe.cc.fl.us/~faeds/presentations/2004%20Educational%20Tech%20Landscape.ppt#11>
- ▶ [http://danielneamu.rdscv.ro/cutenews/images/gartner\\_hype\\_cycle\\_4.jpg](http://danielneamu.rdscv.ro/cutenews/images/gartner_hype_cycle_4.jpg)
- ▶ <http://www.embedded.com/shared/printableArticle.jhtml?articleID=52600868>
- ▶ [http://www.technologyreview.com/articles/04/08/wo\\_brown081904.asp](http://www.technologyreview.com/articles/04/08/wo_brown081904.asp)
- ▶ [http://www.wisegeek.com/what-is-zigbee.htm?referrer=adwords\\_campaign=zigbee\\_ad=013761&\\_content\\_kw=what%20is%20zigbee](http://www.wisegeek.com/what-is-zigbee.htm?referrer=adwords_campaign=zigbee_ad=013761&_content_kw=what%20is%20zigbee)
- ▶ [http://www.emba.uvm.edu/~jfrolik/papers/chris\\_prop.pdf](http://www.emba.uvm.edu/~jfrolik/papers/chris_prop.pdf)
- ▶ <http://bmc.ub.uni-potsdam.de/1743-0003-2-6/1743-0003-2-6.pdf>
- ▶ <http://www.oki.com/en/otr/200/downloads/otr-200-R08.pdf>
- ▶ [http://www.ece.uah.edu/~milenska/docs/dc\\_ssst05\\_synch.pdf](http://www.ece.uah.edu/~milenska/docs/dc_ssst05_synch.pdf)
- ▶ <http://www.merl.com/reports/docs/TR2005-029.pdf>
- ▶ [http://www.zigbee.org/resources/documents/IWAS\\_presentation\\_Mar04\\_Designing\\_with\\_802154\\_and\\_zigbee.ppt](http://www.zigbee.org/resources/documents/IWAS_presentation_Mar04_Designing_with_802154_and_zigbee.ppt)
- ▶ <http://en.wikipedia.org/wiki/ZigBee>
- ▶ [http://www.zigbee.org/imwp/idms/popups/pop\\_download.asp?ContentID=7092](http://www.zigbee.org/imwp/idms/popups/pop_download.asp?ContentID=7092)
- ▶ [http://www.zigbee.org/en/spec\\_download/download\\_request.asp](http://www.zigbee.org/en/spec_download/download_request.asp)



- ▶ <http://www.drdobbs.com/embedded-systems/192202114>