Zigbee, IEEE 802.15.4

Σαράντης Πασκαλής <paskalis@di.uoa.gr>

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν
Πανεπιστήμιον Αθηνών
ΙΔΡΥΘΕΝ ΤΟ 1837

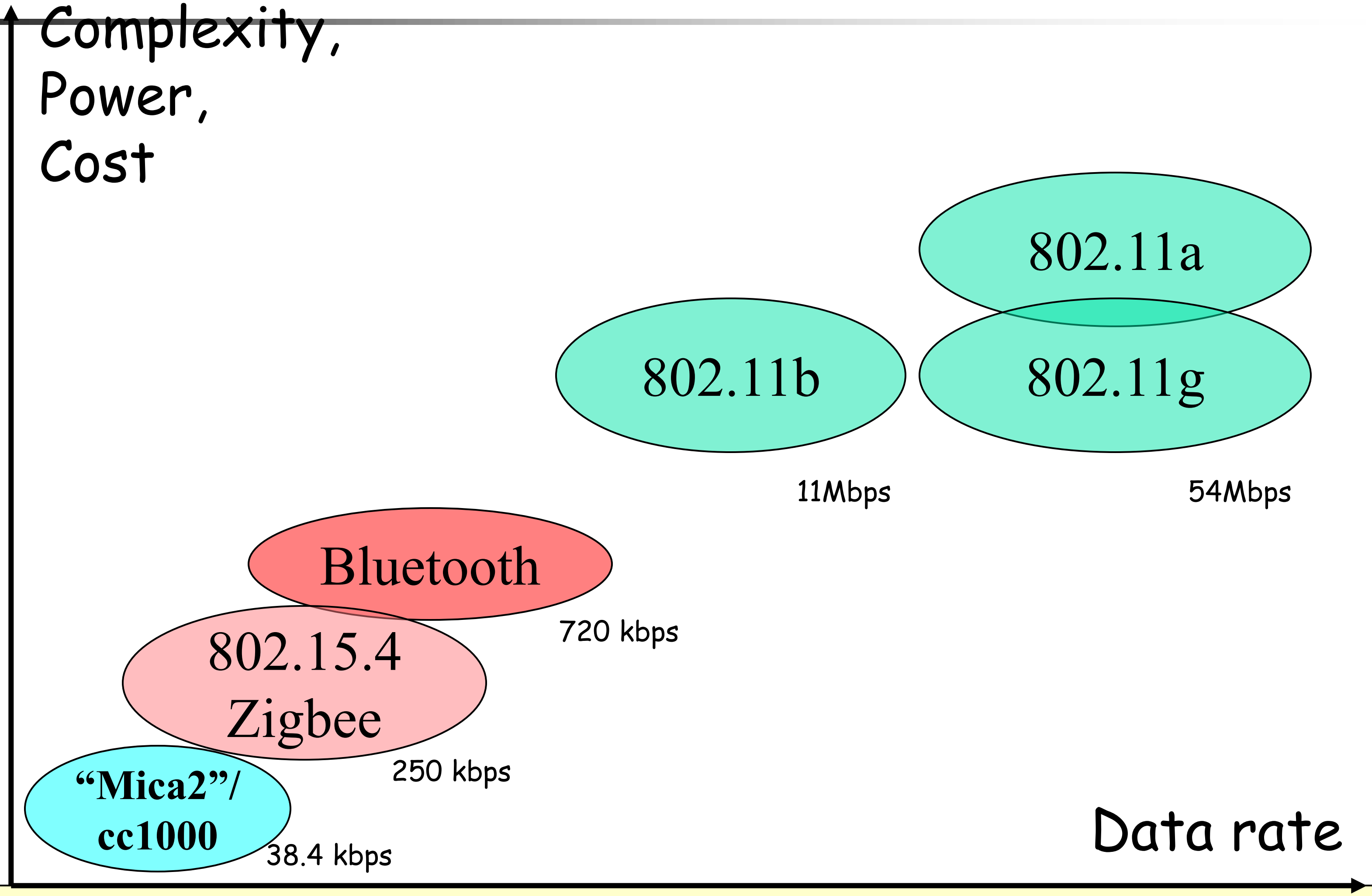
Sensor Network Challenges

- Low computational power
  - Less than 10 MIPS
  - Low memory budget: 4-10 KB
- Limited energy budget
  - AA batteries provide ~2850 mAh
  - LiIon and NiMH batteries provide 800-2500 mAh
  - Solar cells: around 5 mA/cm^2 in direct sunlight
- Communication?

Wireless Communication

- Wireless communication standards:
  - IEEE 802.11 a/b/g
  - Bluetooth
  - GSM
- What makes them unattractive for WSN:
  - Power hungry (need big batteries)
  - Complexity (need lots of clock cycles and memory)
- New protocol for WSN:
  - 802.15.4 and Zigbee (ratified in Dec 14, 2004)

Technology Space



Wireless Standards

	ZigBee™ **802.15.4**	Bluetooth™ **802.15.1**	Wi-Fi™ **802.11b**	GPRS/GSM **1XRTT/CDMA**
Application Focus	Monitoring & Control	Cable Replacement	Web, Video, Email	WAN, Voice/Data
System Resource	4KB-32KB	250KB+	1MB+	16MB+
Battery Life(days)	100-1000+	1-7	.1-5	1-7
Nodes Per Network	255/65K+	7	30	1,000
Bandwidth (kbps)	20-250	720	11,000+	64-128
Range(meters)	1-75+	1-10+	1-100	1,000+
Key Attributes	Reliable, Low Power, Cost Effective	Cost, Convenience	Speed, Flexibility	Reach, Quality

Why NOT 802.11 ?

The Cost of Throughput

- High data rates
  - up to 11Mbps for b and
  - up to 54Mbps for g and a)
- Distance up to 300 feet, or more with special antennas
- High power consumption
  - Sources about 1800mA when transceiver is operational.

IEEE 802.11b example

- Consider running a mote with 802.11b on two AA batteries.
- Consumes 1800mA when transmitting
- Assume NiMH battery capacity 2400mA/h
- Assume transmitting 1/3 of the time

- How long will the batteries last?
- Is the given information sufficient for the question asked?

How About Bluetooth ?

The Cost of Universalism

- Designed for communications between portable and peripheral devices

- 720 kbps, 10m range
- One master and 7 slave devices in each “Piconet”
- Time Division Multiple Access (TDMA)
- Frequency hopping to avoid collisions between Piconets
  - Hop between channels 1600 times a second
  - 79 channels (1MHz each) to avoid collisions

Bluetooth (2)

- Protocol tailored to many different data types: Audio, Text, Raw data
  - Makes the protocol rather complex to accommodate for all data types
  - Needs more memory and clock cycles than we are willing to afford on the Motes
- Zigbee needs only about 10-50% of the software in comparison with Bluetooth and WiFi

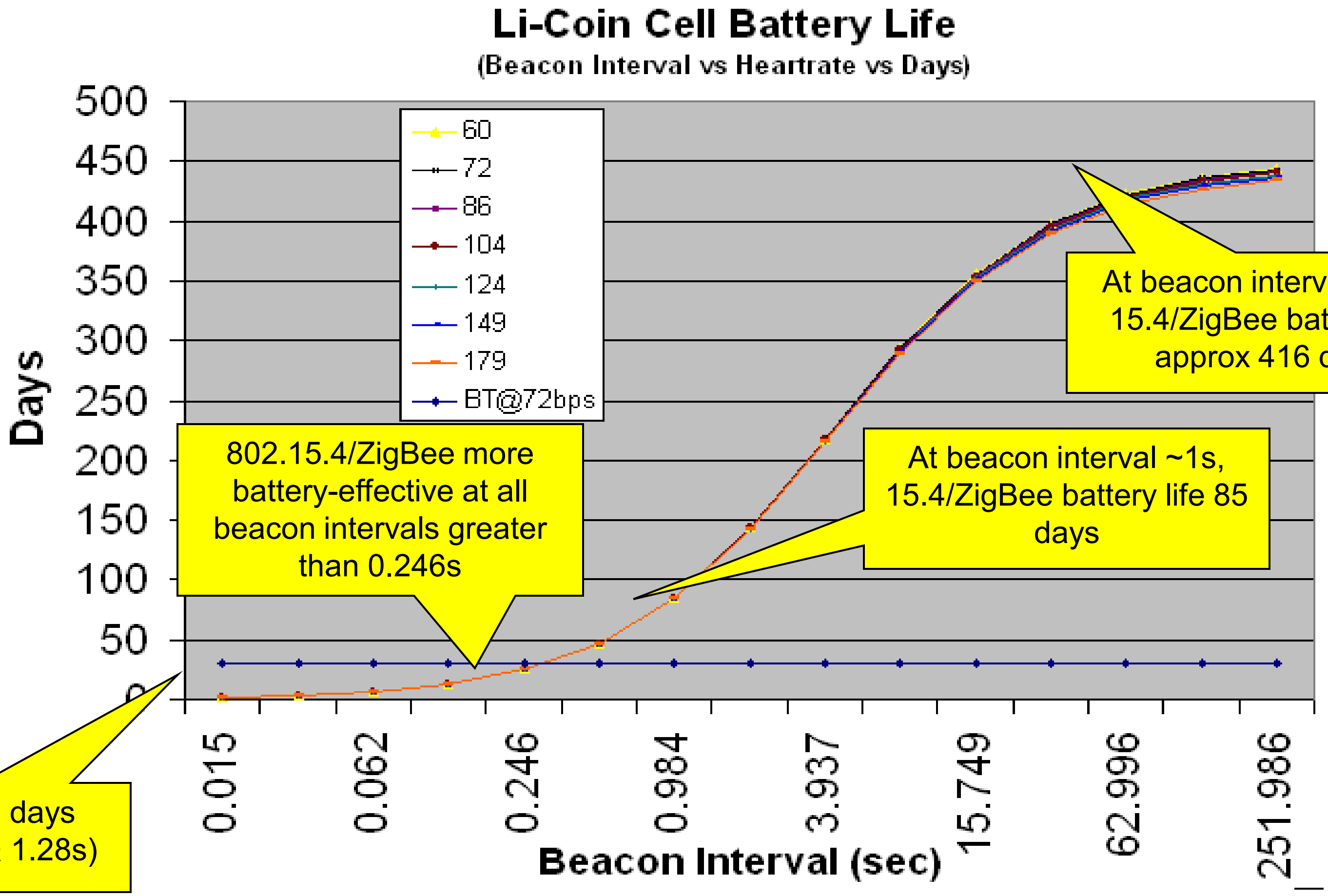
15.4/ZigBee and Bluetooth

- Instantaneous Power Consumption
  - 15.4 Transceivers are “similar” to Bluetooth Transceivers
    - 802.15.4
      - O-QPSK with shaping
      - Max data rate 250kbps over the air
      - 2Mchips/s over the air Direct Sequence Spread Spectrum (62.5ksps*32 spread)
      - -92 dBm sensitivity nominal
      - 40ppm xtal
    - Bluetooth
      - FSK
      - Max data rate 720kbps over the air
      - 1Msps over the air Frequency Hop Spread Spectrum (79 channels @ 1600 hps)
      - -83 to -84 dBm sensitivity nominal
      - 20ppm xtal
- Instantaneous power consumption will be similar for the raw transceivers without protocol
- Bluetooth’s FHSS makes it impractical to create extended networks without large synchronization cost

15.4 Protocol Built for the Mission

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

802.15.4/ZigBee vs Bluetooth



At beacon interval ~60s, 15.4/ZigBee battery life approx 416 days

802.15.4/ZigBee more battery-effective at all beacon intervals greater than 0.246s

At beacon interval ~1s, 15.4/ZigBee battery life 85 days

Bluetooth 30 days (park mode @ 1.28s)

What is Zigbee

- **ZigBee** is a published specification set of high level communication protocols for:
  - Low data rate, low power, low cost wireless systems operating in unlicensed RF domain
- Formely known as
  - *PURLnet*, *RF-Lite*, *Firefly*, and *HomeRF Lite*
- Based on IEEE 802.15.4

ZigBee Applications

- Wireless home security
- Remote thermostats for air conditioner
- Remote lighting, drape controller
- Call button for elderly and disabled
- Universal remote controller to TV and radio
- Wireless keyboard, mouse and game pads
- Wireless smoke, CO detectors
- Industrial and building automation and control (lighting, etc.)

Zigbee General

- Low power
  - battery life multi-month to years
- Multiple topologies
  - star, peer-to-peer, mesh
- Addressing space: 64 bits
  - Question: how many nodes?
- Fully hand-shake protocol (reliability)
- Range: 50m typical
  - 5-500m based on environment

Zigbee Intended Traffic

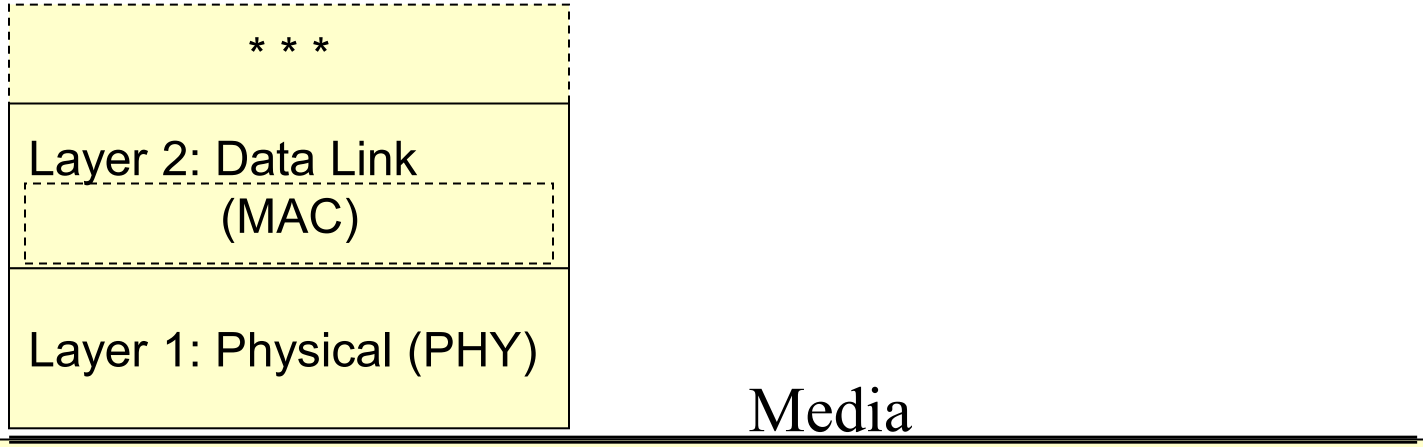
- Periodic data
- Intermittent data
- Application defined rate (e.g., sensors)
- External stimulus defined rate (e.g., light switch)
- Low latency data

ZigBee and OSI Model

	OSI 7-Layer Model	Technology Examples
ZigBee…	Layer 7: Application	SMTP, FTP, Telnet
	Layer 6: Presentation	ASCII, JPEG, BMP
	Layer 5: Session	RPC
	Layer 4: Transport	TCP, UDP
	Layer 3: Network	IP
802.15.4	Layer 2: Data Link • (MAC)	Ethernet, ATM
	Layer 1: Physical (PHY)	CSMA/CD (*Carrier Sensing Multiple Access With Collision Detection*)

Zigbee Protocol Stack

- ZigBee uses the IEEE 802.15.4 – Low Rate Wireless Personal Area Network (WPAN) standard to describe its lower protocol layers: PHY and MAC



Zigbee/IEEE 802.15.4

- Dual PHY: 2.4GHz and 868/915 MHz
- Data rates:
  - 250 kbps @ 2.4GHz
  - 40 kbps @ 915MHz
  - 20 kbps @ 868MHz
    - Q: Why would anyone want this?
    - A: Better penetrates obstacles than @2.4GHz
- CSMA-CA channel access
  - Yields high throughput and low latency for low duty cycle devices

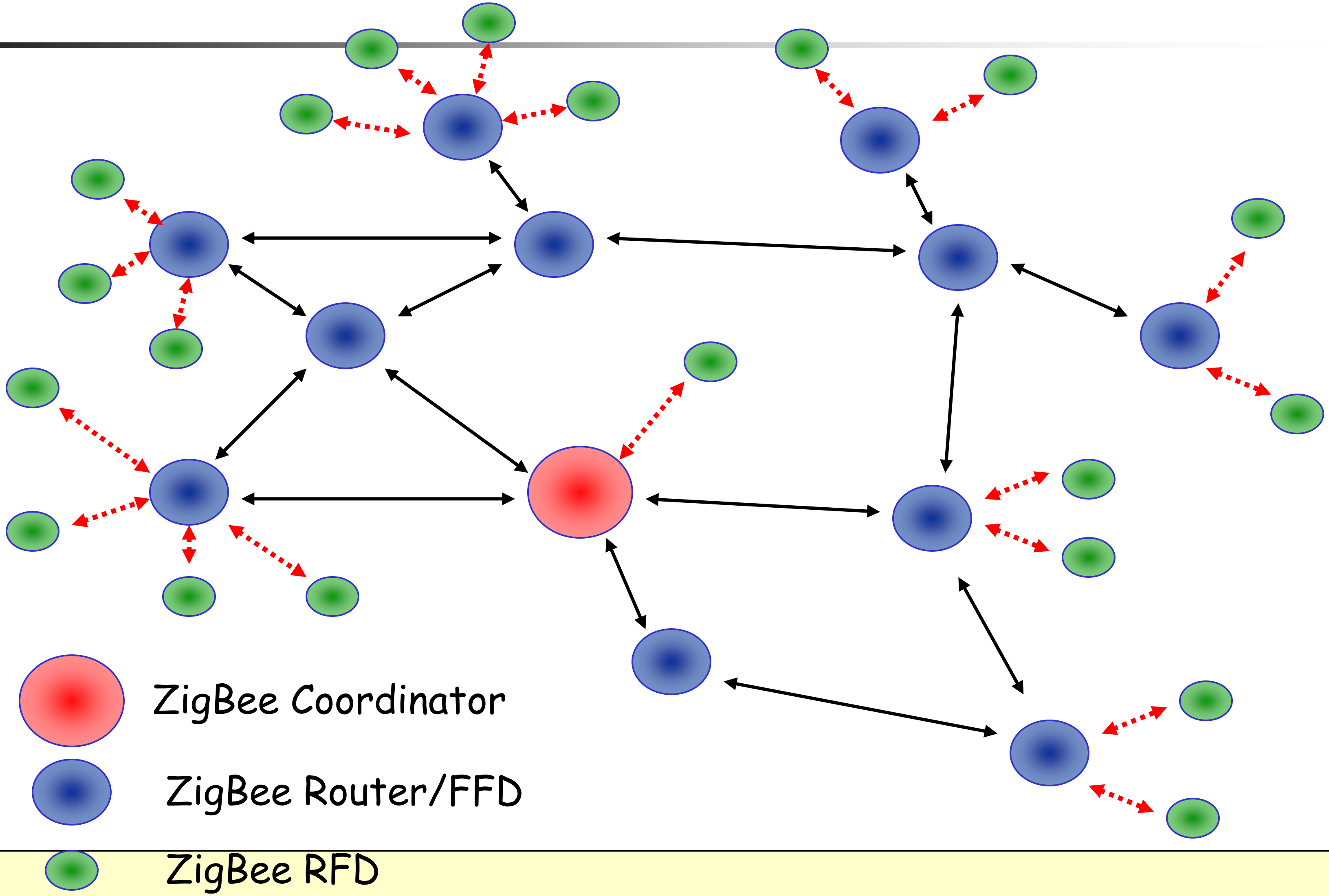
ZigBee: PHY

- The radio uses Digital Spread Spectrum Signaling (DSSS)
  - Conventional DSSS for 868MHz and 915MHz bands
  - Orthogonal Signaling (4 bits per symbol) for 2.4GHz band
- Number of channels
  - 16 channels in the 2.4GHz ISM band
  - 10 channels in the 915MHz
  - one channel in the 868MHz

ZigBee: MAC

- Employs 64-bit IEEE & 16-bit short addresses
- Three device types specified
  - Network Coordinator
  - Full Function Device (FFD)
  - Reduced Function Device (RFD)
- Simple frame structure
- Reliable delivery of data
- Association/disassociation
- AES-128 security
- CSMA-CA channel access
- Optional superframe structure with beacons
- Optional GTS mechanism

ZigBee as Mesh Networking

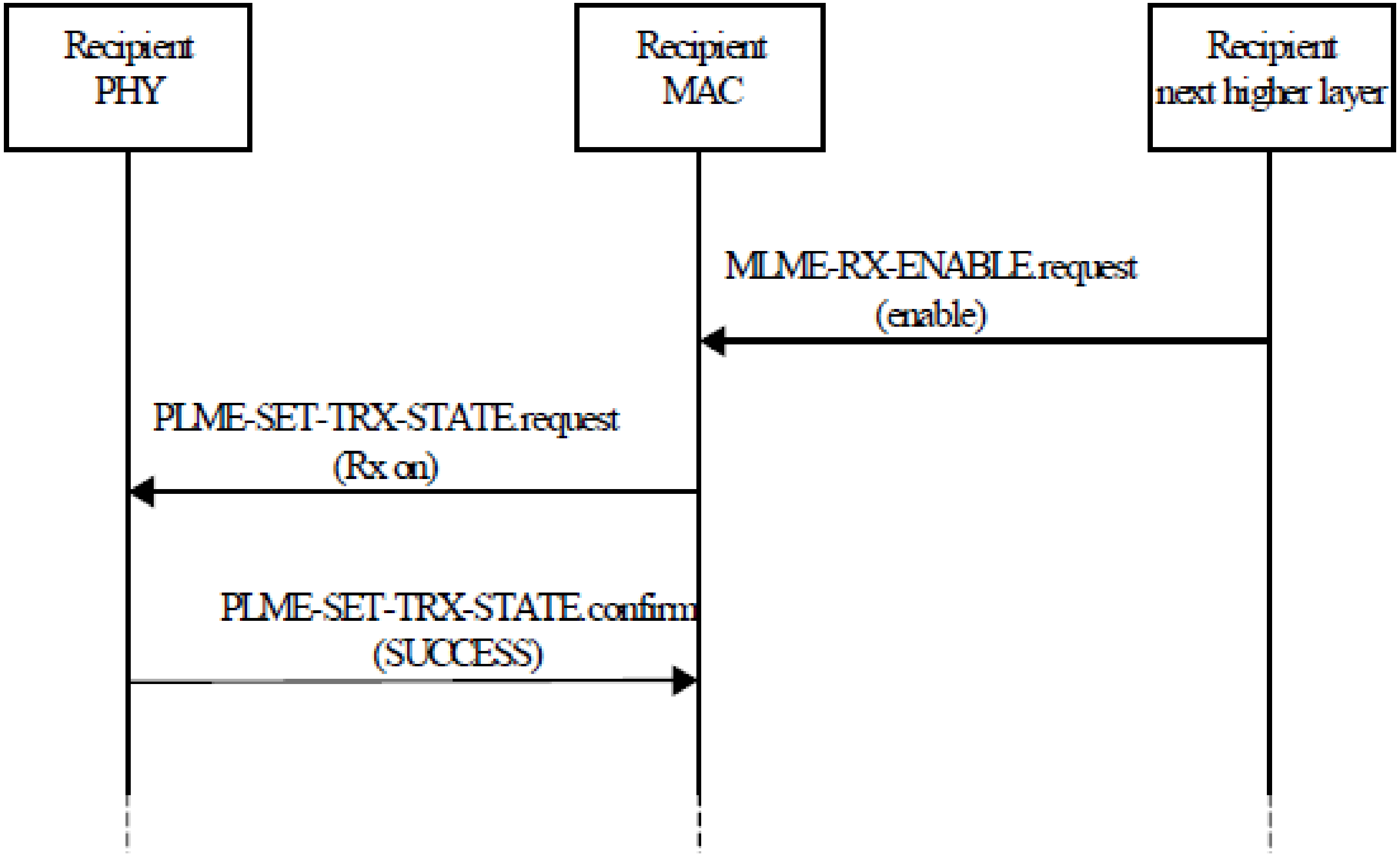


ZigBee Coordinator

ZigBee Router/FFD

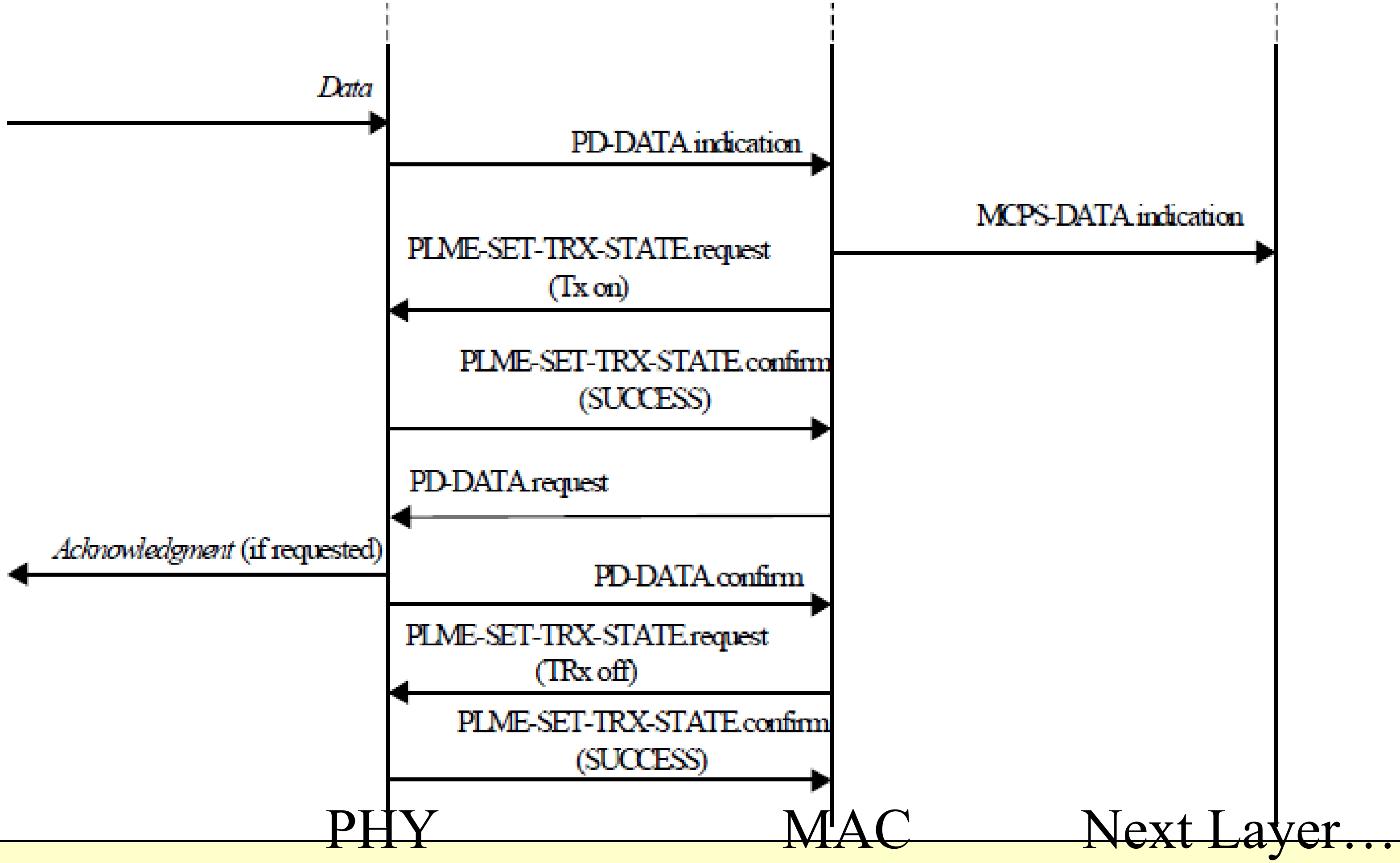
ZigBee RFD

PHY – MAC Interaction Example


Recipient PHY
Recipient MAC
Recipient next higher layer
MLME-RX-ENABLE.request (enable)
PLME-SET-TRX-STATE.request (Rx on)
PLME-SET-TRX-STATE.confirm (SUCCESS)

PHY MAC Next Layer…

PHY – MAC Interaction (2)


Data
PD-DATA.indication
MCPS-DATA.indication
PLME-SET-TRX-STATE.request
(Tx on)
PLME-SET-TRX-STATE.confirm
(SUCCESS)
PD-DATA.request
Acknowledgment (if requested)
PD-DATA.confirm
PLME-SET-TRX-STATE.request
(TRx off)
PLME-SET-TRX-STATE.confirm
(SUCCESS)
PHY
MAC
Next Layer…

ZigBee Upper Layers

- Messaging
- Configurations that can be used
- Security:
  - Key setup and maintenance: Commercial, Residential
  - Defines key types: Master, Link, Network
  - CCM (unified, simple mode of operation)
  - More: Key freshness checks, message integrity, authentication (network and device level)
- Network layer (NWK) supports three topologies:
  - Star
  - Mesh
  - Cluster-Tree (= Star + Mesh)

How A ZigBee Network Forms

- Devices are pre-programmed for their network function
  - Coordinator scans to find an unused channel to start a network
  - Router scans to find an active channel to join, then permits other devices to join
  - End Device will always try to join an existing network
- Devices discover other devices in the network providing complementary services
  - Service Discovery can be initiated from any device within the network
- Devices can be bound to other devices offering complementary services
  - Binding provides a command and control feature for specially identified sets of devices

ZigBee Stack Architecture: Addressing

- Every device has a unique 64 bit MAC address
- Upon association, every device receives a unique 16 bit network address
- Only the 16 bit network address is used to route packets within the network
- Devices retain their 16 bit address if they disconnect from the network, however, if they leave the network, the 16 bit address is re-assigned

ZigBee Stack Architecture: Addressing (2)

- NWK broadcast implemented above the MAC:
  - NWK address 0xFFFF is the broadcast address
  - Special algorithm in NWK to propagate the message
  - “Best Effort” or “Guaranteed Delivery” options
  - Radius Limited Broadcast feature

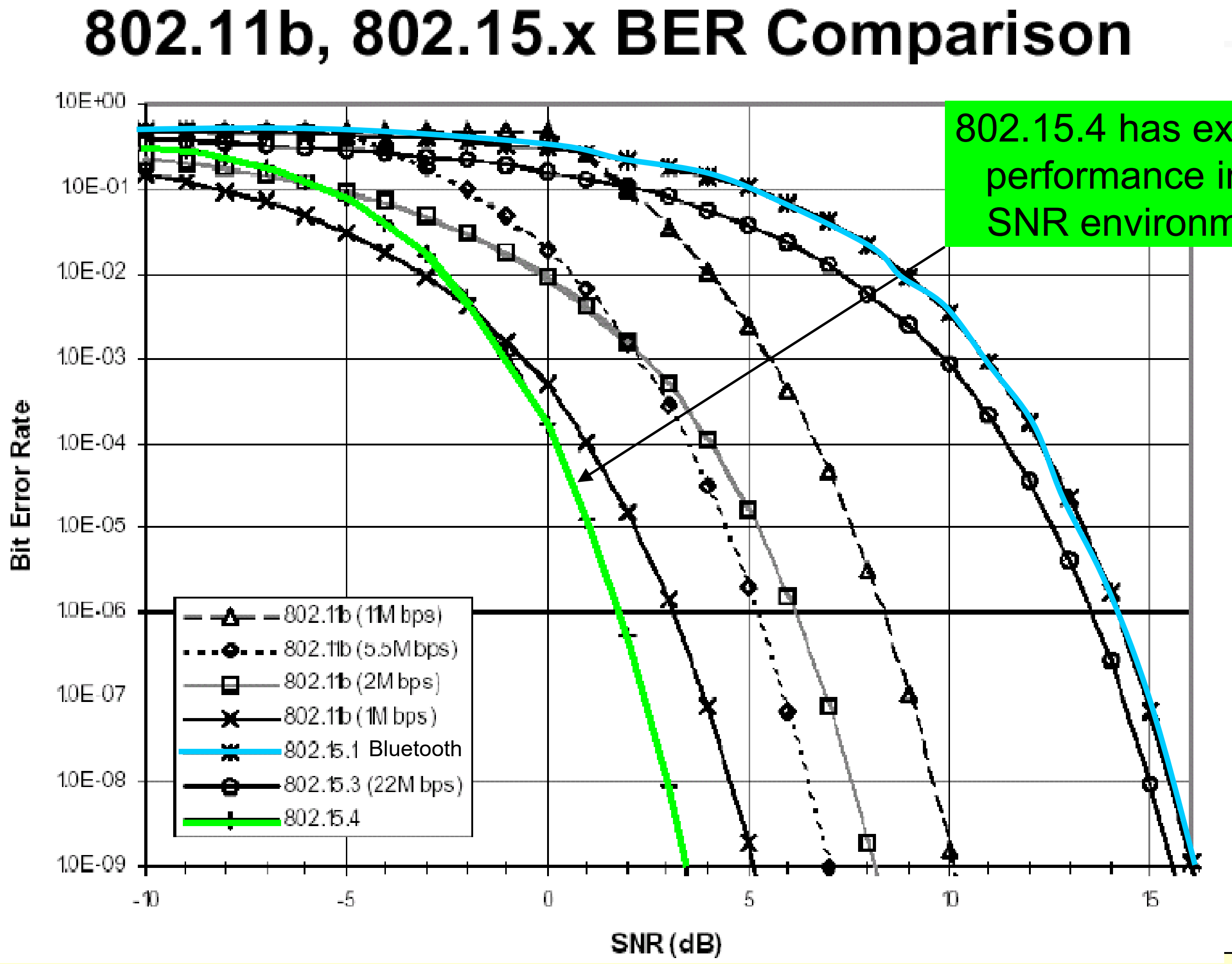
ZigBee Routing

- Routing table entry:
  - Destination Address (2 bytes)
  - Route status (3 bits)
  - Next Hop (2 bytes)
- Route request command frame:
  - FrameID, Options, RequestID, Destination Address, Path cost
- Route reply command frame:
  - FrameID, Options, Req.ID, Originator Addr, Responder Addr, Path cost
- A device wishing to discover or repair a route issues a route request command frame which is broadcast throughout the network
- When the intended destination receives the route request command frame it responds with at least one route reply command frame
- Potential routes are evaluated with respect to a routing cost metric at both source and destination

ZigBee NWK Parameters

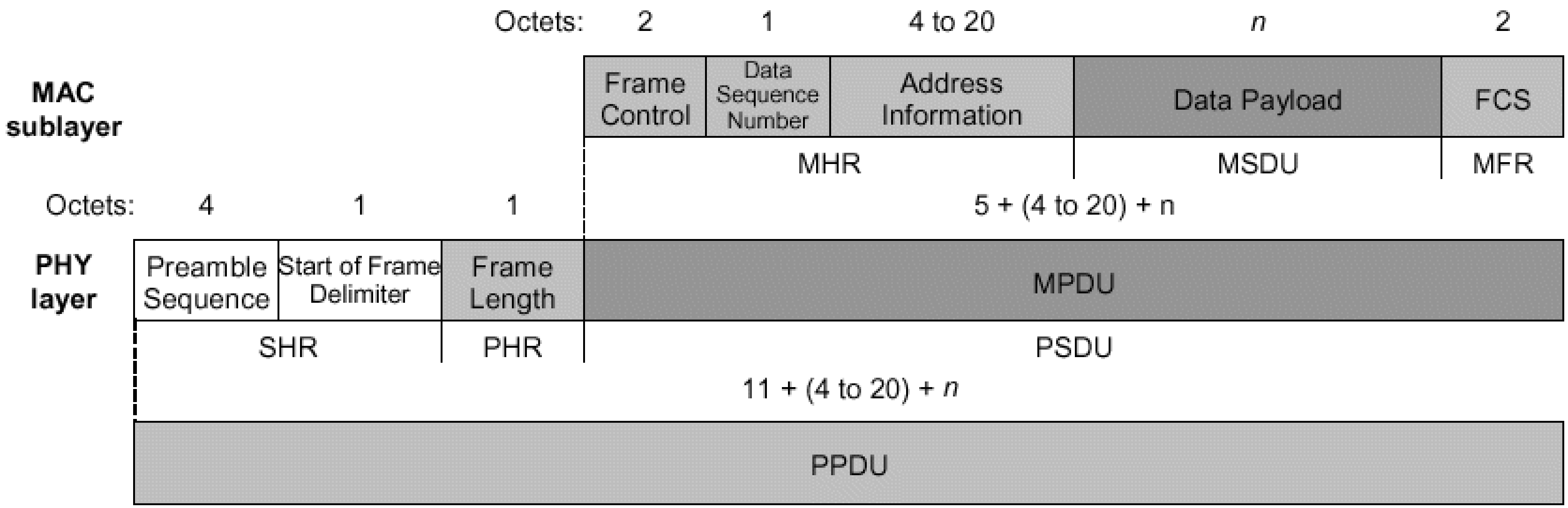
- *nwkMaxDepth* and *nwkMaxChildren*
- *nwkMaxRouters*
- Size of the routing table
- Size of neighbor table
- Size of route discovery table
- Number of reserved routing table entries
- How many packets to buffer pending route discovery
- How many packets to buffer on behalf of end devices
- Routing cost calculation
- *nwkSymLink*
- *nwkUseTreeRouting*

PHY Performance



802.15.4 has excellent performance in low SNR environments

Data Frame format



MAC sublayer

Octets: 2 | 1 | 4 to 20 | *n* | 2

Frame Control | Data Sequence Number | Address Information | Data Payload | FCS

MHR | MSDU | MFR

PHY layer

Octets: 4 | 1 | 1 | 5 + (4 to 20) + n

Preamble Sequence | Start of Frame Delimiter | Frame Length | MPDU

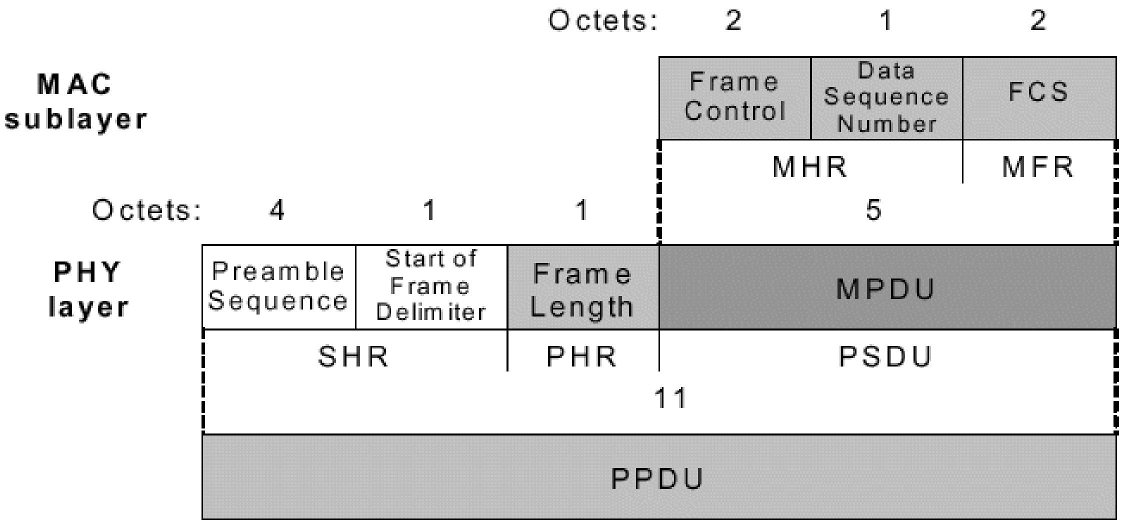
SHR | PHR | PSDU

11 + (4 to 20) + *n*

PPDU

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

Acknowledgement Frame Format



Octets: 2 1 2

MAC sublayer

Frame Control

Data Sequence Number

FCS

MHR

MFR

5

Octets: 4 1 1

PHY layer

Preamble Sequence

Start of Frame Delimiter

Frame Length

MPDU

SHR

PHR

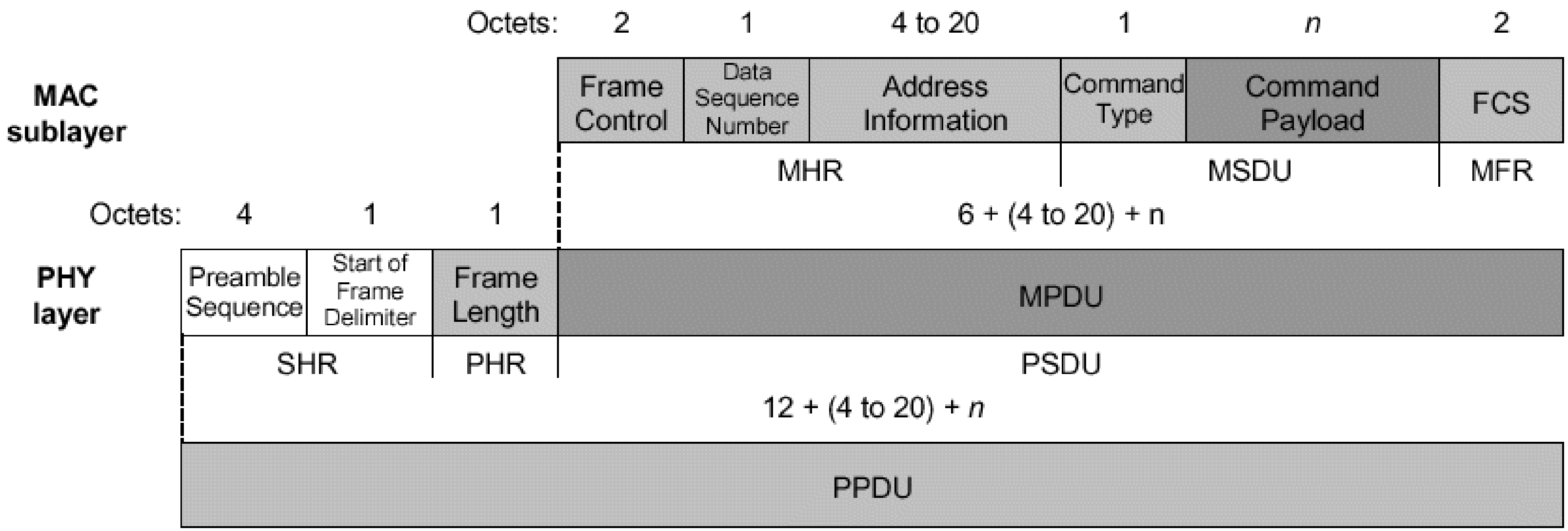
PSDU

11

PPDU

- The other most important structure for 15.4
- 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



MAC sublayer

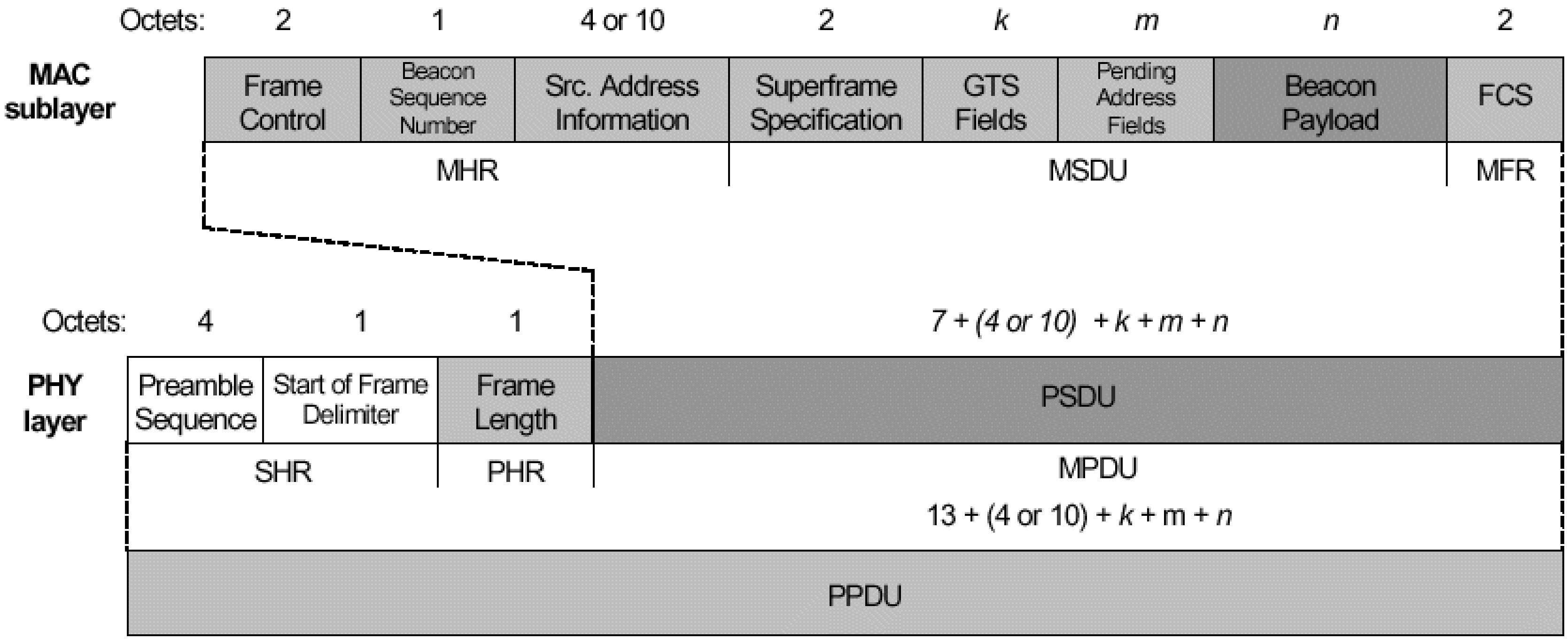
Octets:	2	1	4 to 20	1	*n*	2
	Frame Control	Data Sequence Number	Address Information	Command Type	Command Payload	FCS
	MHR			MSDU		MFR

PHY layer

Octets:	4	1	1	6 + (4 to 20) + n
	Preamble Sequence	Start of Frame Delimiter	Frame Length	MPDU
	SHR		PHR	PSDU
	12 + (4 to 20) + *n*			
	PPDU			

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

Beacon Frame format

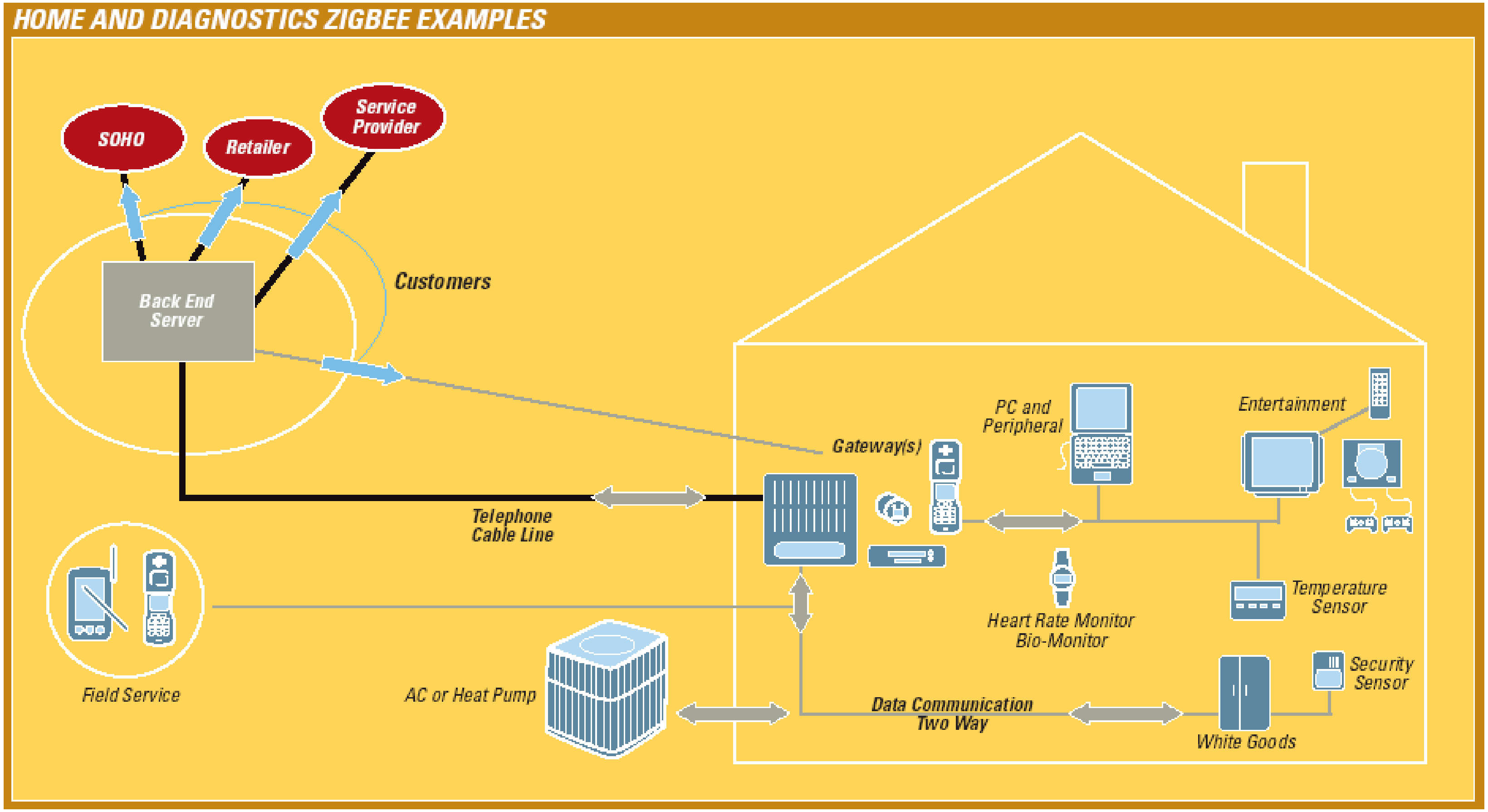


Octets:	2	1	4 or 10	2	*k*	*m*	*n*	2
MAC sublayer	Frame Control	Beacon Sequence Number	Src. Address Information	Superframe Specification	GTS Fields	Pending Address Fields	Beacon Payload	FCS
	MHR			MSDU				MFR

Octets:	4	1	1	*7 + (4 or 10) + k + m + n*
PHY layer	Preamble Sequence	Start of Frame Delimiter	Frame Length	PSDU
	SHR		PHR	MPDU 13 + (4 or 10) + *k* + m + *n*
	PPDU			

- 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

Home/Light Commercial Spaces



Industrial/Commercial Spaces

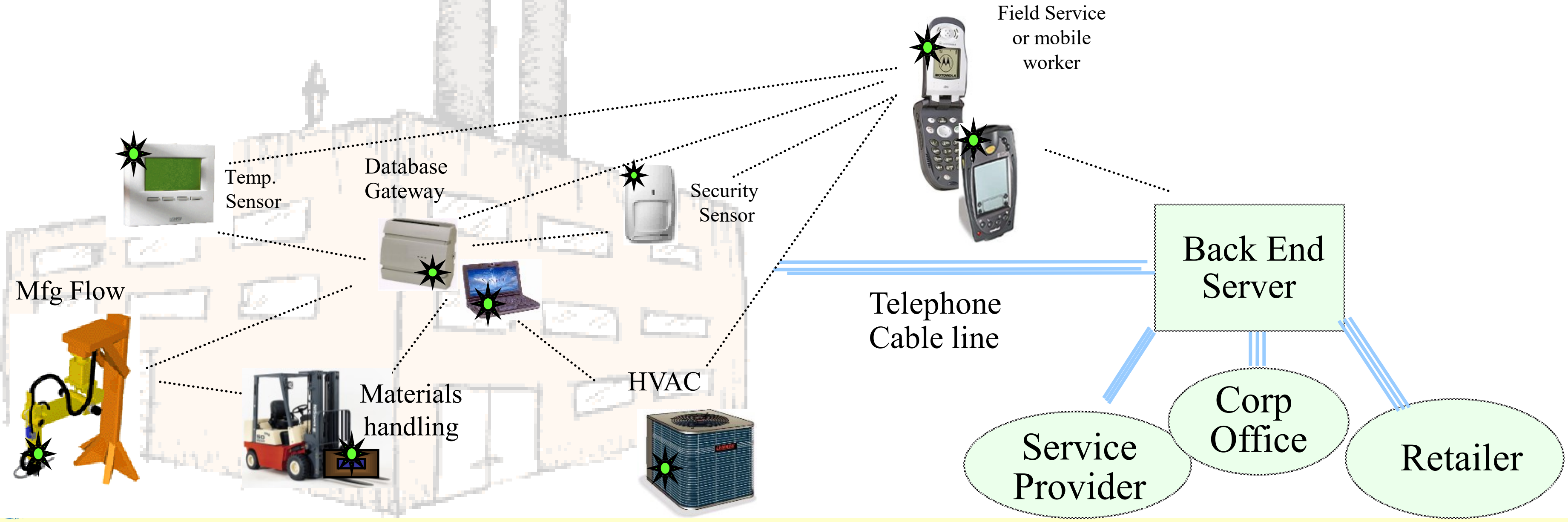
- Warehouses, Fleet management, Factory, Supermarkets, Office complexes
- Gas/Water/Electric meter, HVAC
- Smoke, CO, H_2O detector
- Refrigeration case or appliance
- Equipment management services & Preventative maintenance
- Security services
- Lighting control
- Assembly line and work flow, Inventory
- Materials processing systems (heat, gas flow, cooling, chemical)

Energy, diagnostics, e-Business services

- **Gateway or Field Service links to sensors & equipment**
  - Monitored to suggest PM, product updates, status changes

Nodes link to PC for database storage

- PC Modem calls retailer, Service Provider, or Corp headquarters
- Corp headquarters remotely monitors assets, billing, energy management


Field Service or mobile worker
Temp. Sensor
Database Gateway
Security Sensor
Mfg Flow
Materials handling
HVAC
Telephone Cable line
Back End Server
Corp Office
Service Provider
Retailer