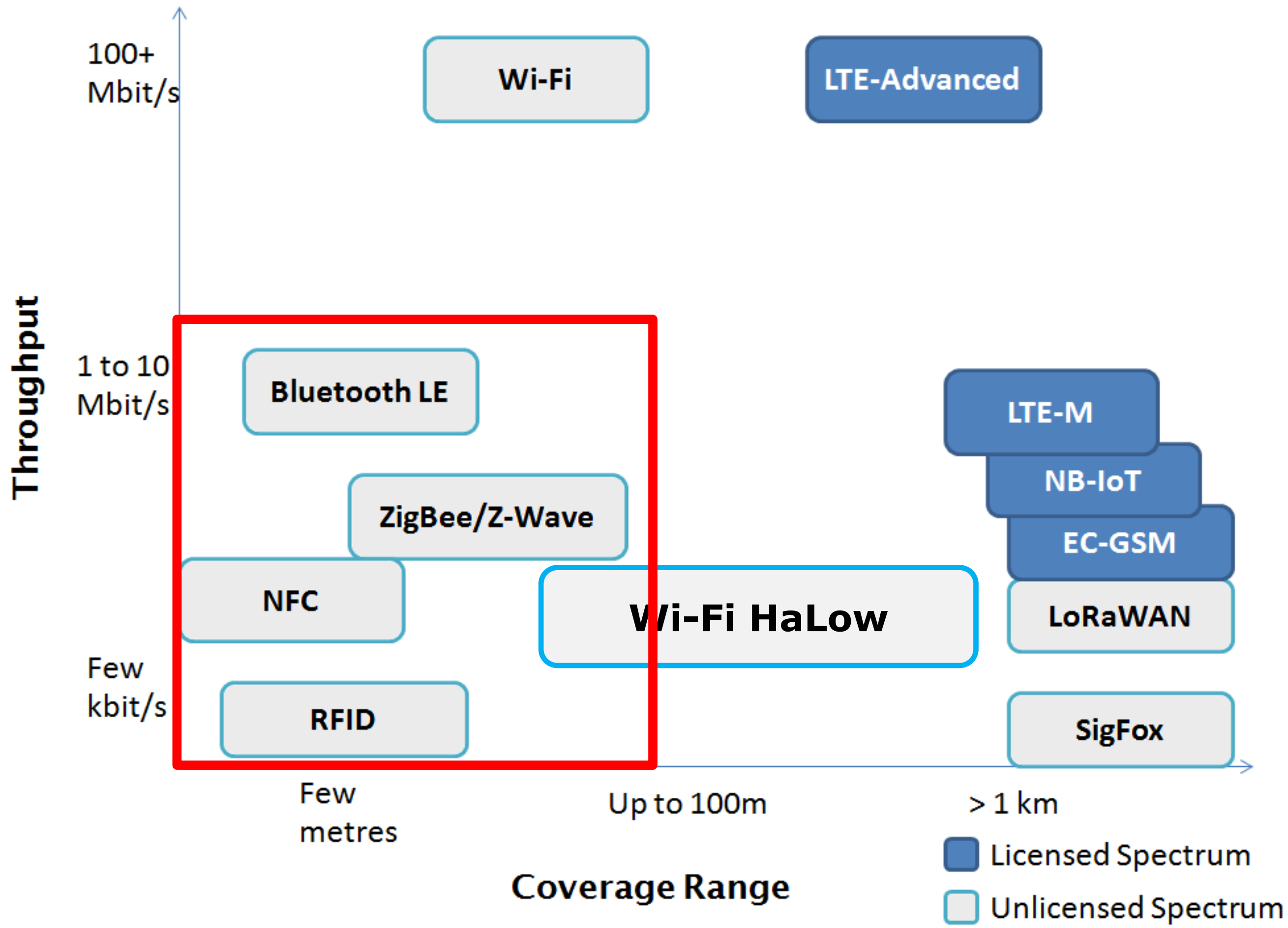
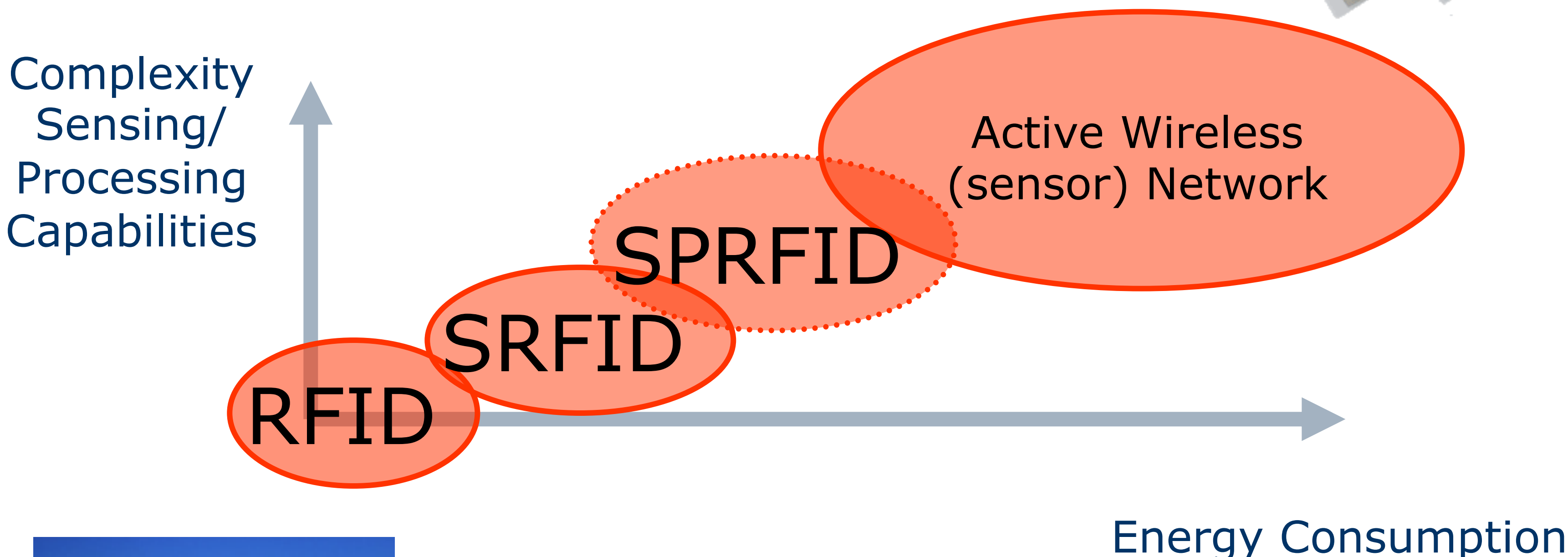
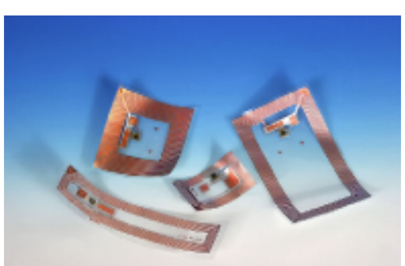
Short Range Communication Technologies and Protocols

Short Range Communication Technologies



Broad Classification of IoT Capillary Technologies





Courtesy of Prof. C. Alippi

Capillary (Multi-Hop) Networks

Standard	Frequency Bands	Max Tx Rate	Max Range	TX Power	Application
ZigBee (802.15.4)	868/915/2450 MHz	250 kbps	100m	1-100mW	Home automation Backhaul for WSN
WI-SUN (802.15.4g)	sub-1GHz, 2.4GHz	1Mpbs	200m	1-100mW	Home automation Backhaul for WSN
ULP (802.15.4q)	868/915/2450 MHz	100kbps	100m	5-15mW	Ultra low power applications
Wireless M-Bus	169/433/868 MHz	100 kbps	300m	1-100mW	Metering
Z-Wave	908 MHz	100 kbps	100m	1-100mW	Home automation
Bluetooth Low Energy (BLE)	2450 MHz	1 Mbps	30m	1-100mW	e-Health, Sport, Multimedia
WiFi Low Power (802.11ah)	Sub-1 GHz	7.8 Mbps	1000m	10mW-1W	Long range WSN Backhaul for WSN

- Highly fragmented technologies/standards/protocols
- Fine for small-scale, hot spot coverage
- The “Gateway Problem”

A New Communication Stack Needed

XML

HTTP / FTP / SNMP

TCP / UDP

IP

Ethernet, 802.3, 802.11

?

Extremely tight to application scenario

Heavy Protocols undesirable

Routing Tiny Disconnected devices

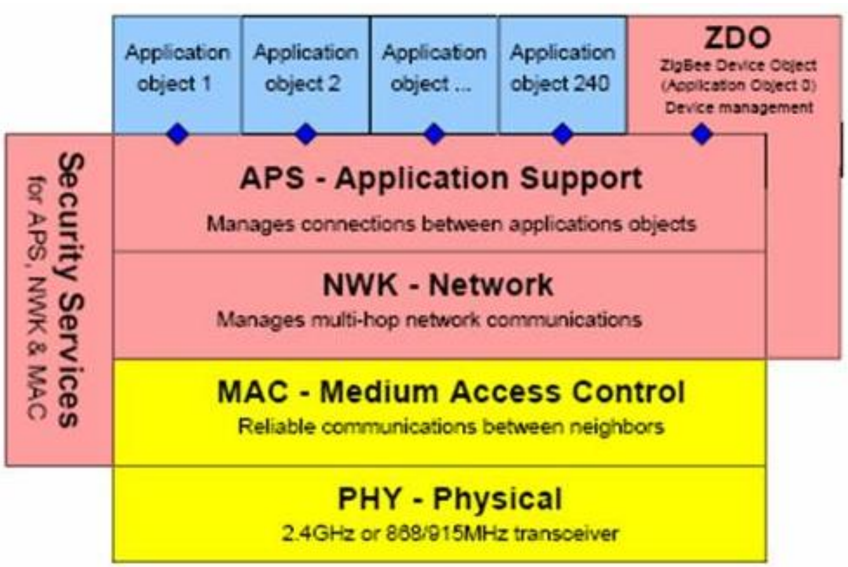
Tight Coupling with PHY- Energy efficiency

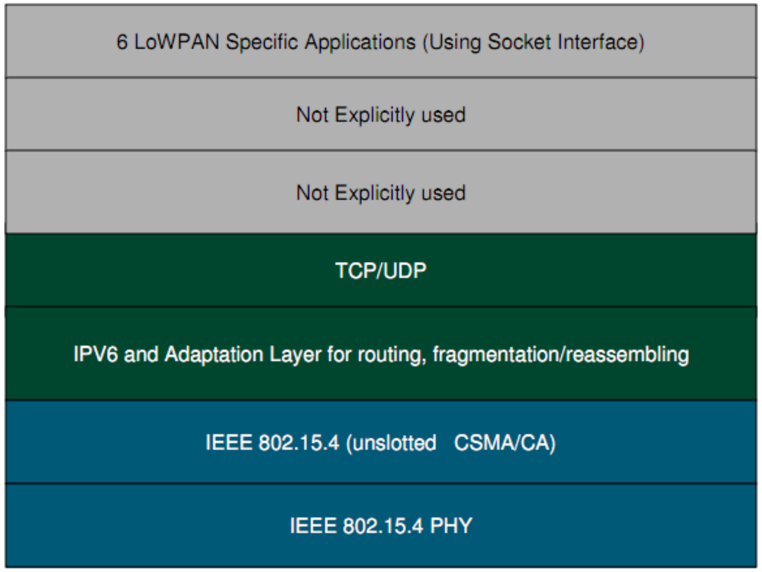
Several Solutions available

- Classification Guidelines
  - **Proprietary** (WirelessHART) vs **open standard** (WiFi, ZigBee, 6LowPAN, THREAD)
  - **Application specific** vs **application agnostic**
    - ZWAVE for home automation, WirelessHART for industrial applications; 6LowPAN/THREAD for everything
  - **IP-compliant** vs **non-IP-compliant**

The Status Quo: ZigBee vs 6LowPAN

- Main (rough) difference:
  - 6LowPAN extends IP to the Internet of Things
  - Zigbee doesn't
- Similarities in the lower layers





ZigBee

Main features

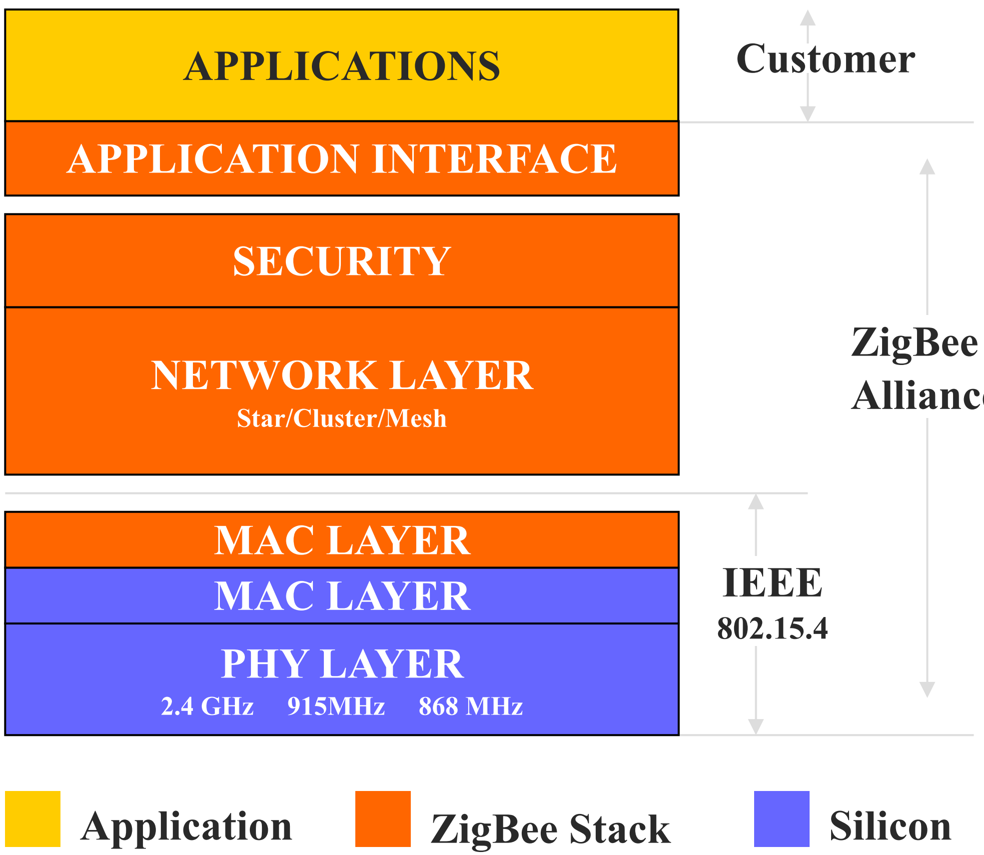
- Low-cost Hardware (2$) and software
- Limited TX range (~10m)
- Low Latency
- High Energy Efficiency!

Towards ZigBee...

- Too many proprietary solutions in the field of IoT (mid 90s)
- Dramatic compatibility/interoperability issues (and high costs)
- WP 4 within IEEE launched in 2001 to have a reference technology
- IEEE 802.15.4 standard published in March 2003.
- The technology is often (misleadingly) referenced as:

ZigBee™

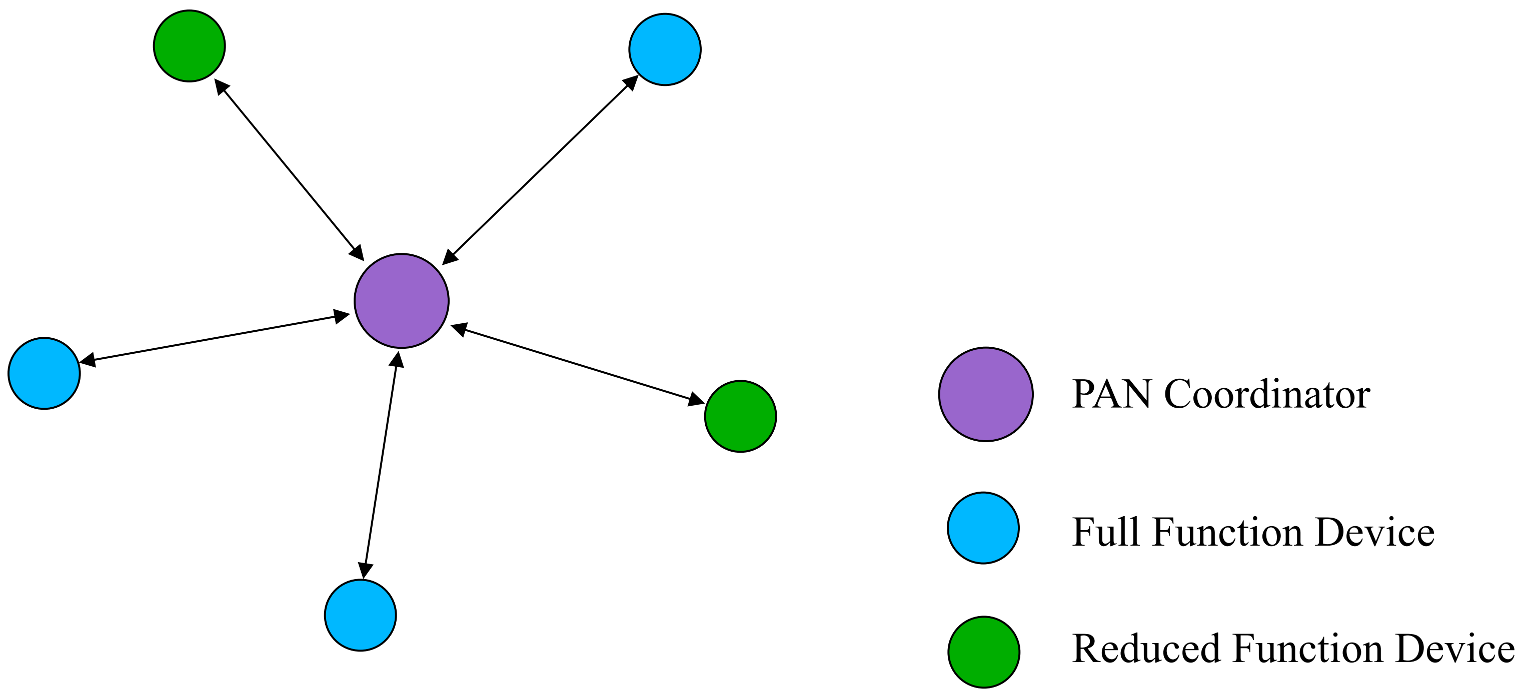
Zigbee: Communication Stack



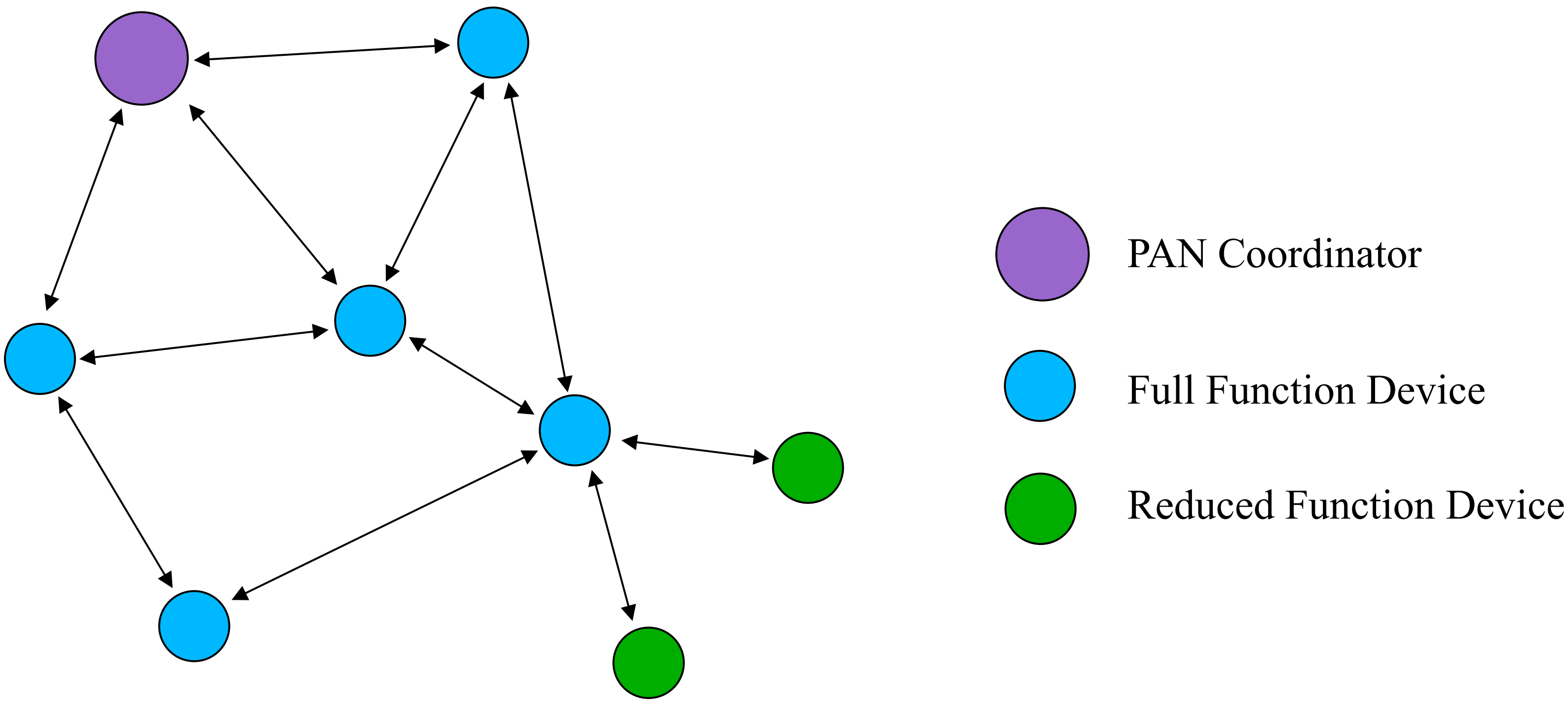
802.15.4: Types of Devices

- **Full Function Device (FFD):**
  - Can send beacons
  - Can communicate with other FFDs
  - Can route frames
  - Can act as PAN coordinator
  - Typically features power supply
- **Reduced Function Device (RFD):**
  - Cannot route frames
  - Cannot communicate with other RFDs
  - Can communicate with FFD
  - Runs typically on batteries
- **PAN Coordinator**
  - Is responsible of a Personal Area Network (PAN)
  - Manages PAN association/de-association

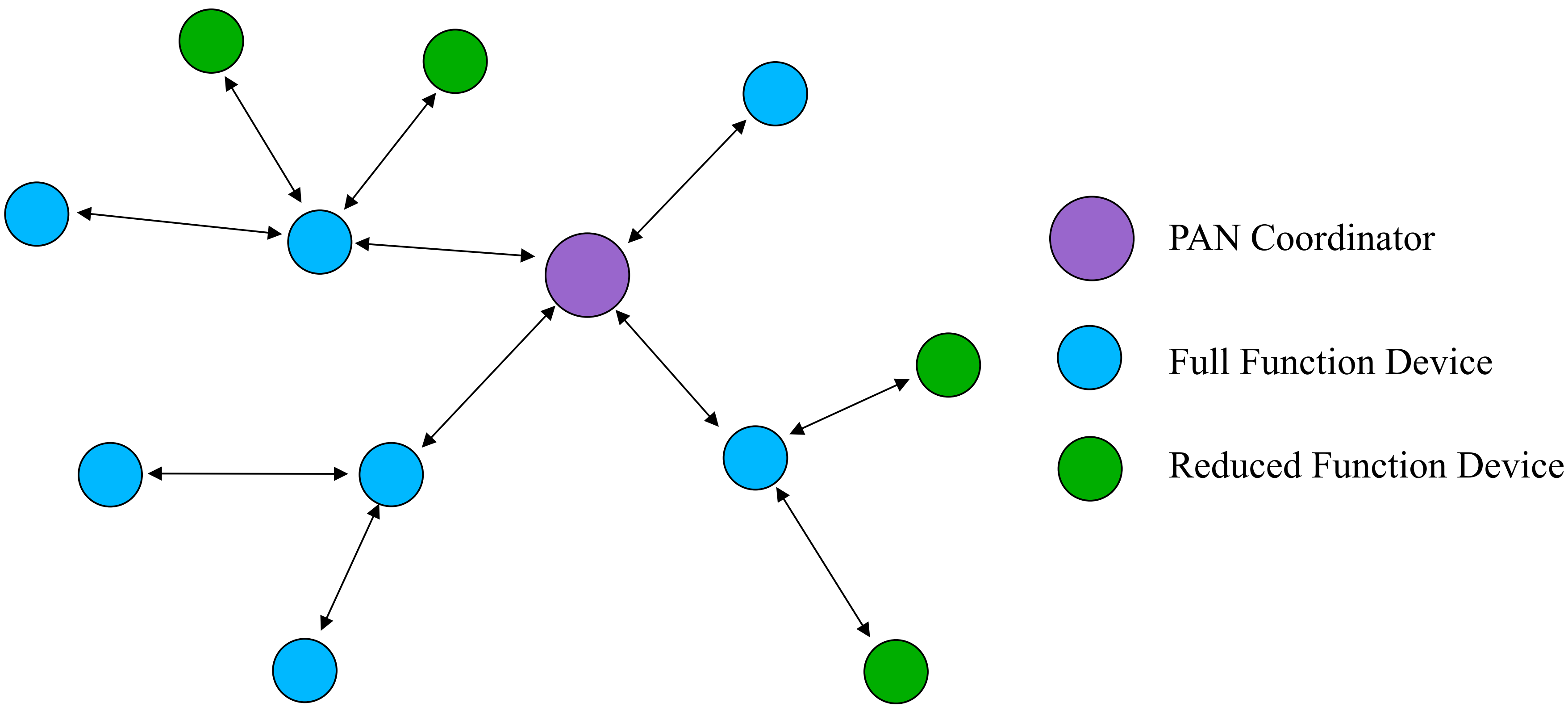
Supported Topology: Stars



Supported Topology: Mesh



Supported Topology: Cluster-Tree (not in 802.15.4 standard)



802.15.4: PHY

- Activation and deactivation of the radio transceiver
- Energy detection (ED) within the current channel
  - Detect energy level for each channel (used to implement scanning functionalities)
- Link quality indicator (LQI) for received packets
- Clear channel assessment (CCA)
  - Used to implement the carrier sense multiple access with collision avoidance (CSMA-CA)
- Channel frequency selection
- Data transmission and reception

802.15.4:PHY

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
868/915 (optional)	868–868.6	400	ASK	250	12.5	20-bit PSSS
	902–928	1600	ASK	250	50	5-bit PSSS
868/915 (optional)	868–868.6	400	O-QPSK	100	25	16-ary Orthogonal
	902–928	1000	O-QPSK	250	62.5	16-ary Orthogonal
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

- 3 channels available in 868MHz bands
- 30 channels available in the 915MHz bands
- 16 channels available in the 2.4GHz bands

PHY: PDU format

		Octets		
		1		variable
Preamble	SFD	Frame length (7 bits)	Reserved (1 bit)	PSDU
SHR		PHR		PHY payload

- *Preamble*: to achieve synchronization
- *SFD*: frame delimiter
- *Frame Length*: length (in octets) of the PHY payload
  - For MAC data frames in the range of [9-127]

MAC Sublayer Tasks

- The features of the MAC sublayer are:
  - beacon management,
  - channel access management,
  - GTS management,
  - Frame validation,
  - acknowledged frame delivery,
  - association, and disassociation,
  - hooks for implementing application-appropriate security mechanisms.

MAC: Functional Description

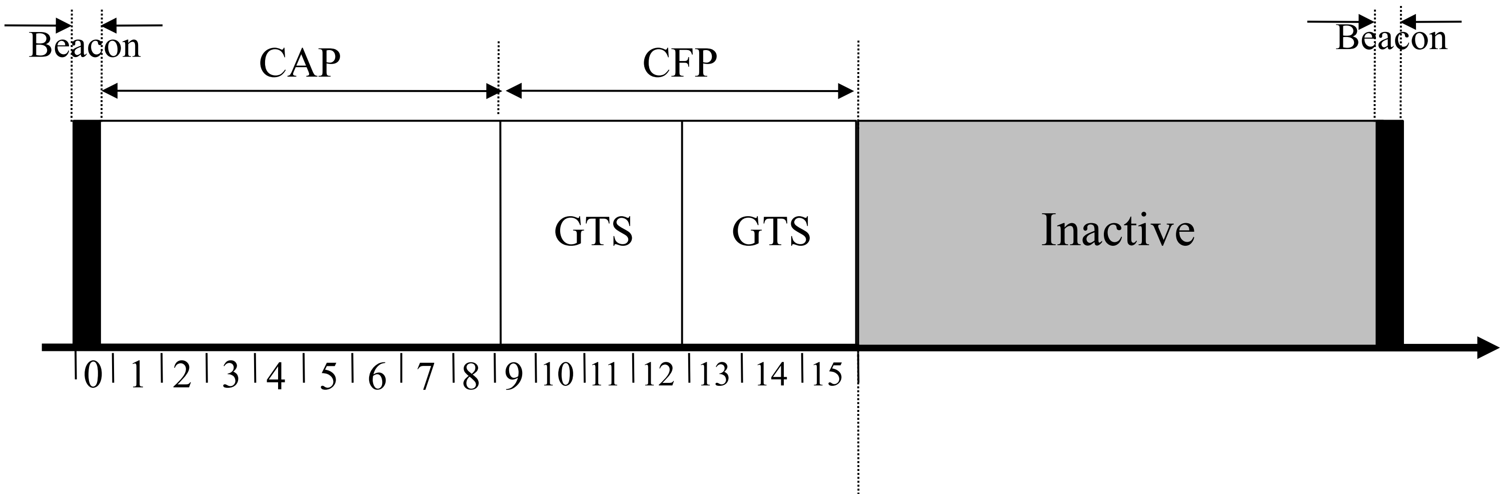
- Two operation modes are defined:
  - **Beacon Enabled**
    - PAN coordinator periodically transmits beacons
    - Usually adopted in star topologies
    - Slotted CSMA/CA + scheduled transmissions
  - **Non Beacon Enabled**
    - Uncoordinated access through unslotted CSMA/CA

802.15.4 Channel Access

- The resource to be shared is time
- A Mixture of Scheduled and Random Access
- Scheduled Access implemented through PAN Coordinator (only beacon-enabled mode)
- Random Access allowed between RFDs and between RFD/FFD and PAN Coordinator (allowed in both operation modes)

Beacon Enabled: functional description

- **Beacon Enabled**



- Frame Length: from 15[ms] to 252[s] (15.38ms*2n where 0 ≤ n ≤ 14)
- RFD associated to PAN coordinator are aligned with the frame structure
- Random access through CSMA/CA in CAP
- *Guranteed Time Slot* statically assigned by PAN coordinator through beacons

CSMA/CA

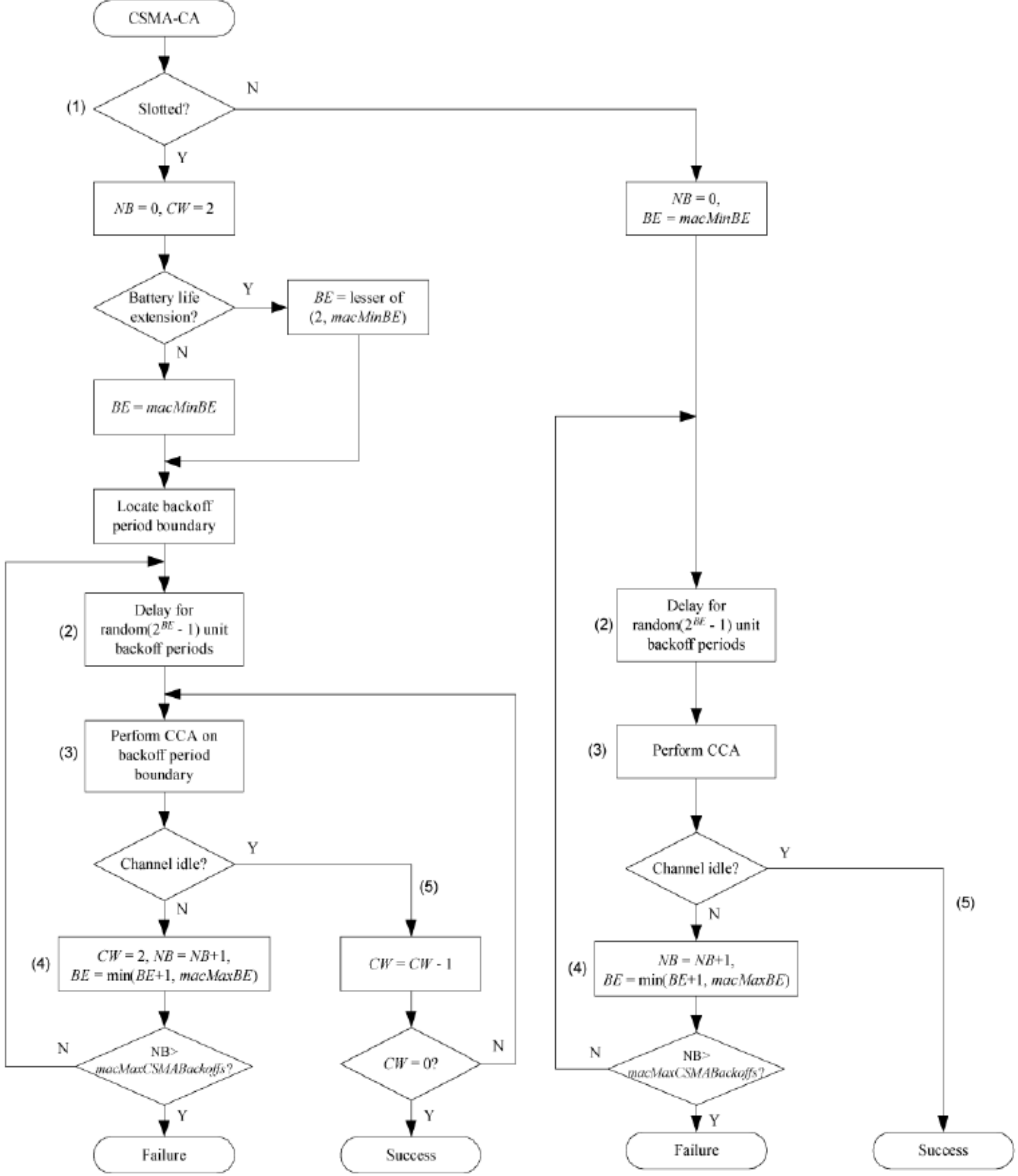
- Each device shall maintain three variables for each transmission attempt: NB, CW and BE.
  - ***NB*** is the number of times the CSMA-CA algorithm was required to backoff (initialized to zero before each new transmission attempt)
  - ***CW*** is the contention window length, defining the number of backoff periods that need to be clear of channel activity before the transmission can commence (initialized to 2, only for slotted CSMA-CA).
  - ***BE*** is the backoff exponent, which is related to how many backoff periods a device shall wait before attempting to assess a channel.
- Backoff period: duration of 20 symbols

CSMA Procedure at a Glance

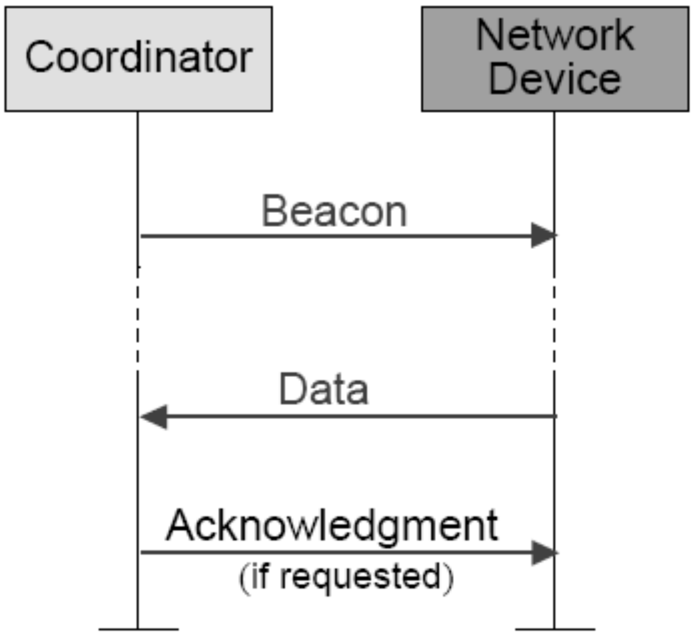
- A transmitting node delays for a random number of backoff periods in $[0, 2^{BE}-1]$
- If clear channel assessments (CCA) is idle for ***CW*** consecutive backoff periods, the node starts the transmission and waits for an ACK.
- If the channel is busy, the exponent ***BE*** and the number of backoff attempts, ***NB***, are incremented and the procedure is repeated
- After "too many" (NB_{max}) failed retries, the packet is discarded

CSMA Further Nits

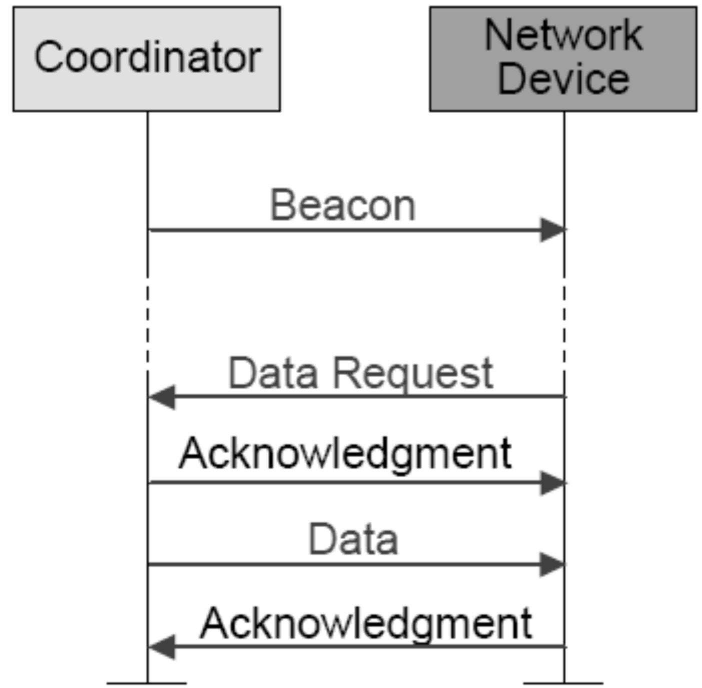
- Transmission procedure (including ACK) must end within a CAP
- Classical unslotted CSMA/CA without synchronization
- CSMA not applied to beacons and ACKs
- In case of collision (ACK does not come back), the procedure restarts


CSMA-CA
(1)
Slotted?
N
Y
NB = 0, CW = 2
NB = 0,
BE = macMinBE
Battery life extension?
Y
BE = lesser of (2, macMinBE)
N
BE = macMinBE
Locate backoff period boundary
(2)
Delay for random(2^BE - 1) unit backoff periods
(3)
Perform CCA on backoff period boundary
Channel idle?
Y
(5)
N
(4)
CW = 2, NB = NB+1,
BE = min(BE+1, macMaxBE)
CW = CW - 1
N
NB> macMaxCSMABackoffs?
CW = 0?
Y
Failure
Success
(2)
Delay for random(2^BE - 1) unit backoff periods
(3)
Perform CCA
Channel idle?
Y
(5)
N
(4)
NB = NB+1,
BE = min(BE+1, macMaxBE)
N
NB> macMaxCSMABackoffs?
Y
Failure
Success

Data Transfer Modes: Beacon Enabled (slotetd CSMA/CA)

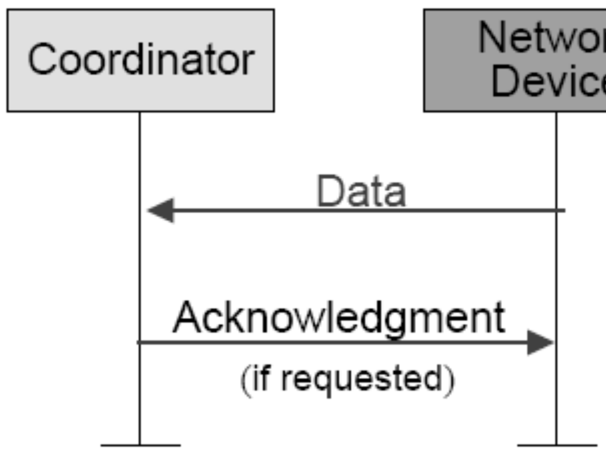


From device

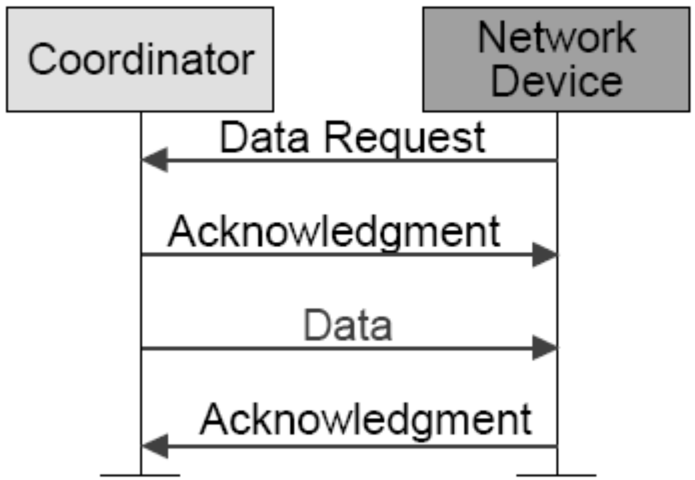


From Coordinator

Data Transfer Modes: non-beacon enabled (unslotted CSMA/CA)



From device



From coordinator

MAC Sublayer: Frame Format

Octets: 2	1	0/2	0/2/8	0/2	0/2/8	0/5/6/10/14	variable	2
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	Source PAN Identifier	Source Address	Auxiliary Security Header	Frame Payload	FCS
		Addressing fields						
MHR							MAC Payload	MFR

Bits: 0–2	3	4	5	6	7–9	10–11	12–13	14–15
Frame Type	Security Enabled	Frame Pending	Ack. Request	PAN ID Compression	Reserved	Dest. Addressing Mode	Frame Version	Source Addressing Mode

Beacon Frame format

Octets: 2	1	4/10	0/5/6/10/14	2	variable	variable	variable	2
Frame Control	Sequence Number	Addressing fields	Auxiliary Security Header	Superframe Specification	GTS fields (Figure 45)	Pending address fields (Figure 46)	Beacon Payload	FCS
MHR				MAC Payload				MFR

Octets: 1	0/1	variable
GTS Specification	GTS Directions	GTS List

Octets: 1	variable
Pending Address Specification	Address List

- ***Addressing Field***: only source PAN identifier + source address (short or long)
- ***Superframe Specification***: to define the length and structure of the superframe (see next slide)

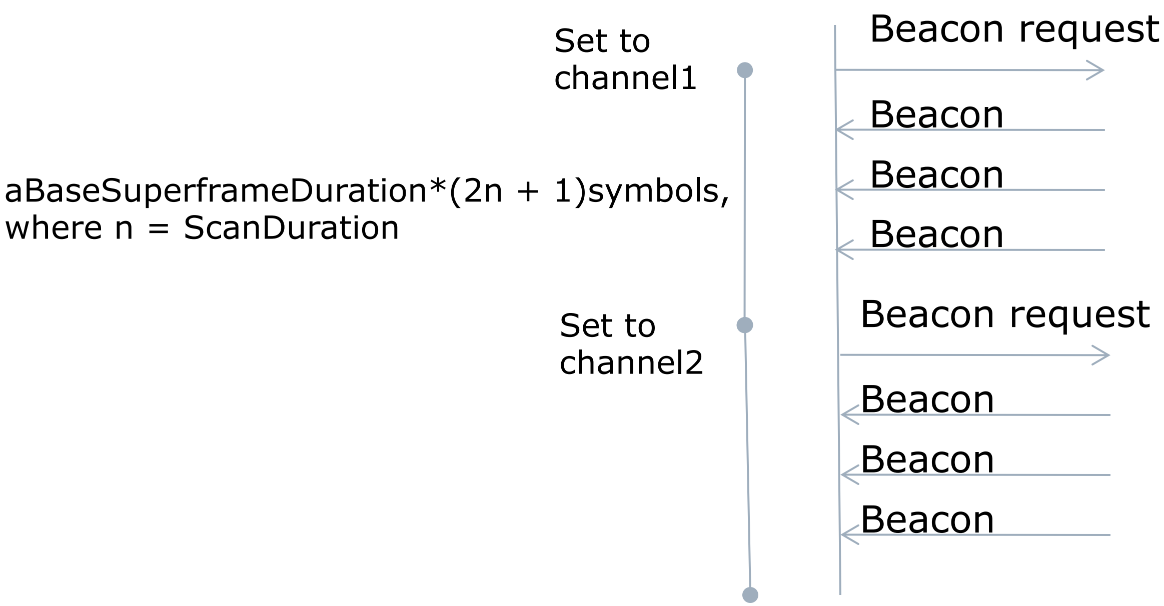
Superframe Specification

Bits: 0–3	4-7	8-11	12	13	14	15
Beacon Order	Superframe Order	Final CAP Slot	Battery Life Extension (BLE)	Reserved	PAN Coordinator	Association Permit

- *Beacon Order (BO):* defines the *Beacon Interval (BI)*
  - BI = aBaseSuperframeDuration*2^{BO} symbols
- *Superframe Order (SO)* : defines the *Superframe Duration (SD)*
  - SD = aBaseSuperframeDuration*2^{SO} symbols
- aBaseSuperframeDuration=16 slots x 60 symbols

Network Formation: Scanning

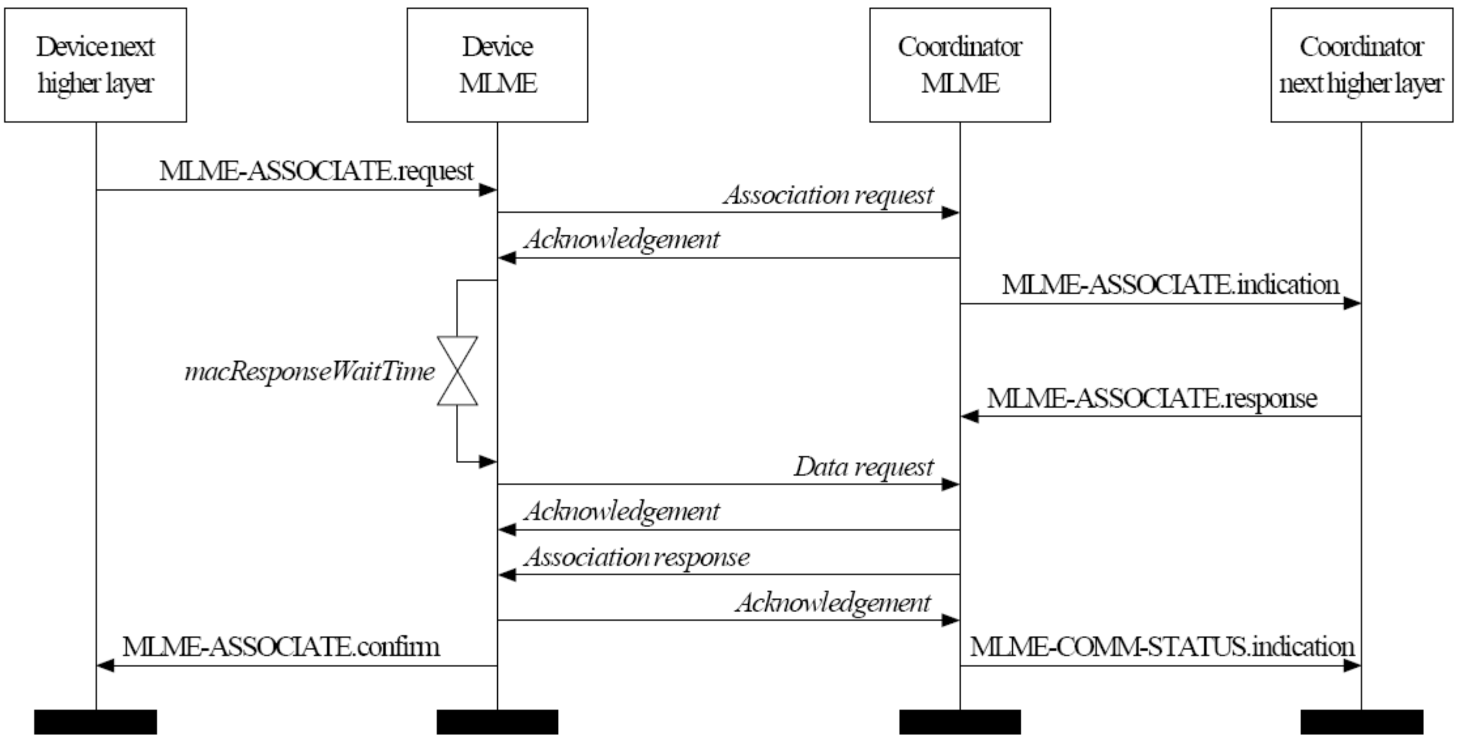
- Active Scanning (only for FFDs):
  - a beacon request message is sent out to trigger beacon transmission



  - Upon termination of the scanning procedure a PAN ID is chosen

- Passive Scanning (for FFDs and RMDs): similar to Active Scanning but without explicit *Beacon Request* messages

Network Formation: Association



IEEE802.15.4 Extensions

- IEEE 802.15.4e
  - Slotted channel access
- IEEE 802.15.4g
  - Amendement for smart utility applications
- IEEE 802.15.4k
  - Amendement for critical infrastructure monitoring

Network Layer

Network Layer Functionalities

- ***Configuring a new device***: this is the ability to sufficiently configure the stack for operation as required.
- ***Starting a network***: this is the ability to establish a new network.
- ***Joining, rejoining and leaving a network***: this is the ability to join, rejoin or leave a network as well as the ability of a ZigBee coordinator or ZigBee router to request that a device leave the network.
- ***Addressing***: this is the ability of ZigBee coordinators and routers to assign addresses to devices joining the network.
- ***Neighbor discovery***: this is the ability to discover, record, and report information pertaining to the one-hop neighbors of a device.
- ***Route discovery***: this is the ability to discover and record paths through the network, whereby messages may be efficiently routed.
- ***Reception control***: this is the ability for a device to control when the receiver is activated and for how long, enabling MAC sub-layer synchronization or direct reception.
- ***Routing***: this is the ability to use different routing mechanisms such as unicast, broadcast, multicast or many to one to efficiently exchange data in the network

Zigbee Routing: overview

- Zigbee Specification (7/2005)
- Three Types of Devices:
  - *ZB Coordinator (FFD)*
  - *ZB Router (FFD)*
  - *ZB End-Device (RFD o FFD)*
- ZigBee Routing Integrates:
  - *Ad-hoc On-demand Distance Vector (AODV)*
  - *Cluster Tree Algorithm*

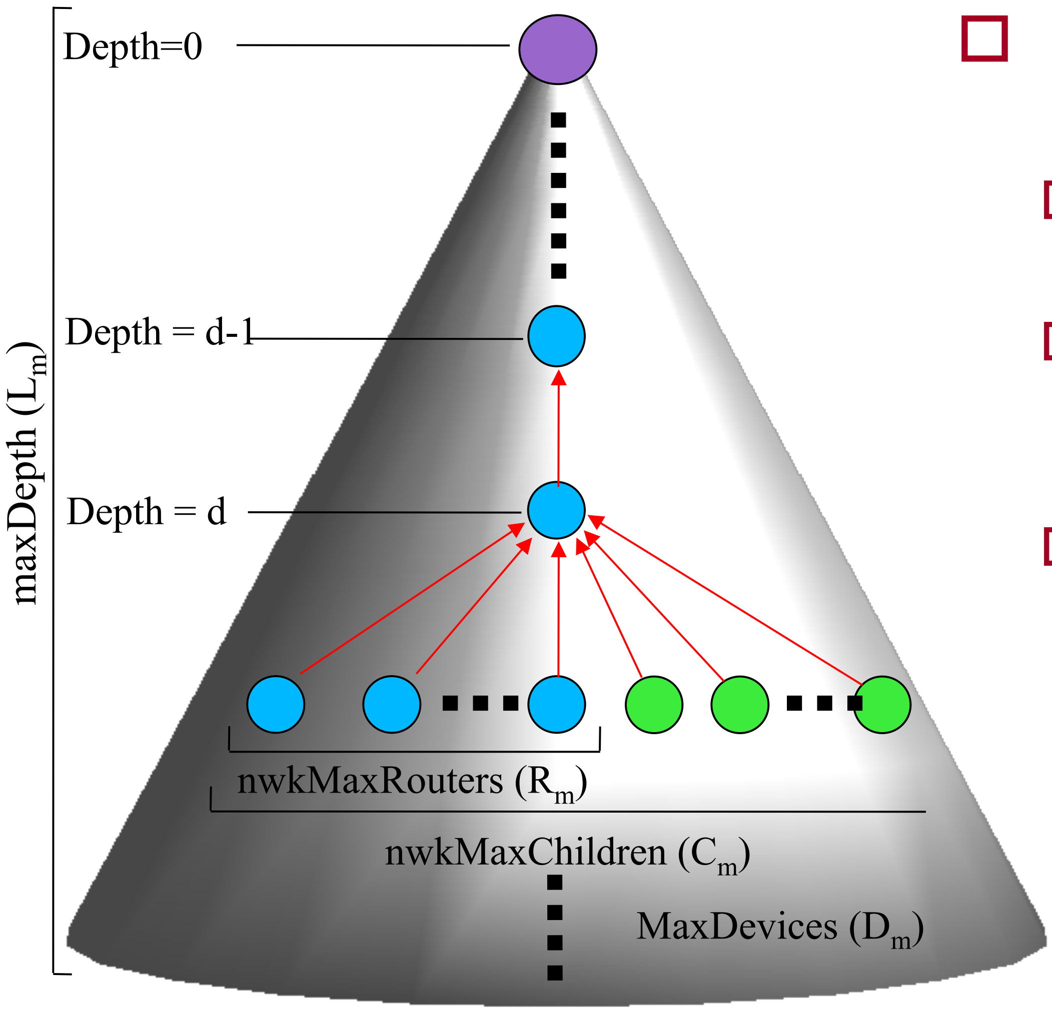
Cluster Tree Algorithm: Tree Formation

- A FFD kicks off the procedure:
  - It scans the available channels through the proper functionalities at the lower layers
  - Chooses a channel (e.g., the least interfered)
  - Sets the PAN identifier
  - Sets its own Network Address to 0 (Coordinator)
- Other devices may now associate to the coordinator through the lower-layer association procedures
- Associated devices may be:
  - ZB Router (only FFD): may let other devices to associate to the network
  - ZB End-Device
- Address Assignment (16 bits short addresses) is performed jointly with association
- Each parent device (PAN coordinator, ZB router) assigns groups of addresses to its children (other ZB routers, ZB end devices)

Cluster Tree Formation: principles

- On the basis of its depth in the tree, a newly joined router is assigned a range of consecutive addresses (16-bit integers).
- The first integer in the range becomes the node address while the rest will be available for assignment to its children (routers and end-devices).

Cluster Tree Algorithm: Tree Creation



- The ZigBee coordinator fixes
  - the maximum number of routers (R_m)
  - end-devices (D_m) that each router may have as children and
  - the maximum depth of the tree (L_m).

Address Assignment Rule

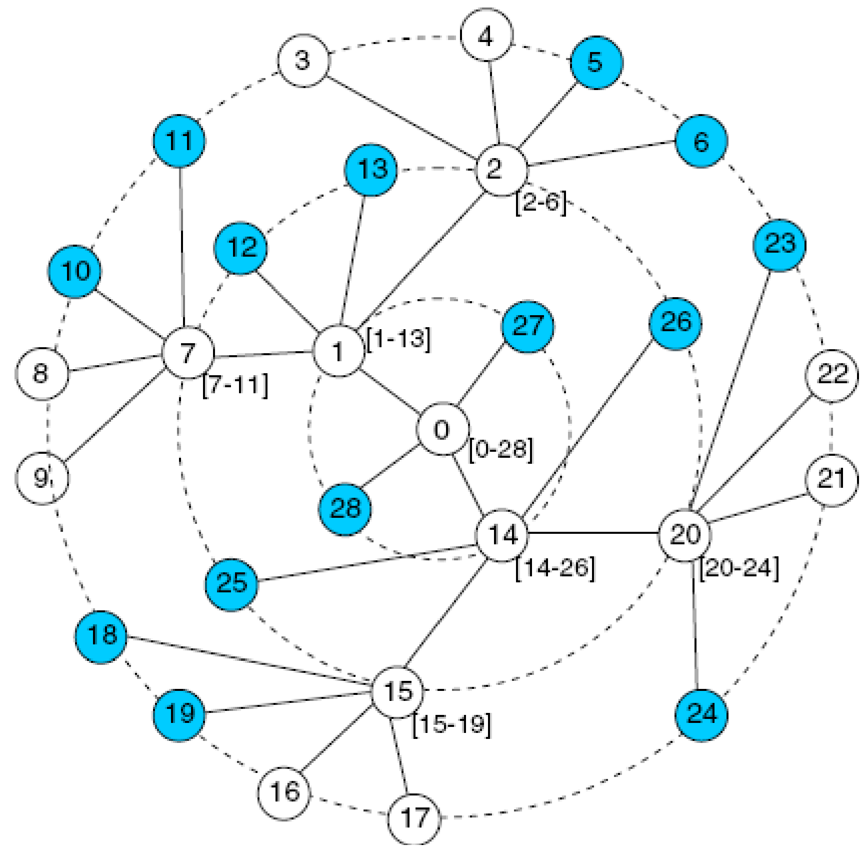
- The size A(d) of the range of addresses assigned to a router node at depth $d < L_m$ is defined by:

$$A(d) = \begin{cases} 1 + D_m + R_m & \text{if } d = L_m - 1 \\ 1 + D_m + R_m A(d+1) & \text{if } 0 \leqslant d < L_m - 1 \end{cases}$$

- Nodes at depth L_m and end-devices are assigned a single address.
- Simple Assignment Rule:
  - A mote at level *d* is assigned addresses in range [x,x + A(d)-1]
  - It will assign
    - *[x+(i-1)A(d+1)+1,x+iA(d+1)]* to its i-th router child ($1 \leq i \leq R_m$)
    - $x+R_mA(d+1)+j$ to its jth end-device child ($1 \leq j \leq D_m$).

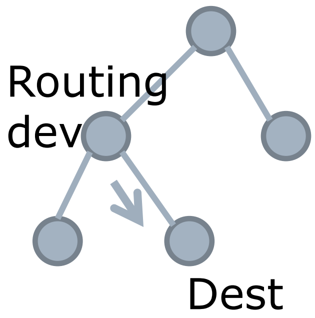
An Example

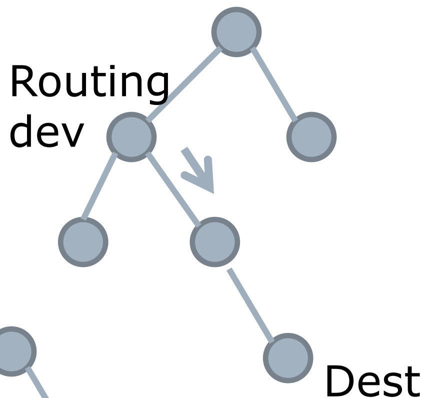
- Address allocations for $R_m = 2$, $D_m = 2$ and $L_m = 3$.
  - A(2)=2+2+1=5
  - A(1)=1+2+2A(2)=13
  - A(0)=1+2+2A(1)=29
  - PAN Coordinator can assign addresses in the range [0,28]

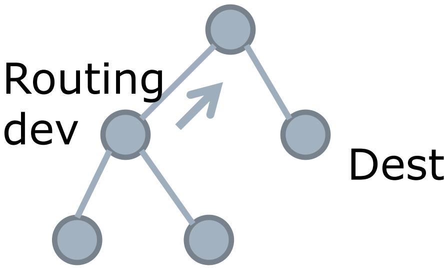


Tree-Based Routing: Principles

- Routing Along the Tree:
  - If destination address is one of children end devices:
    - route directly
  - Else if destination address belongs to one of children routers' addresses set:
    - send to corresponding children router
  - Else
    - Send to parent node

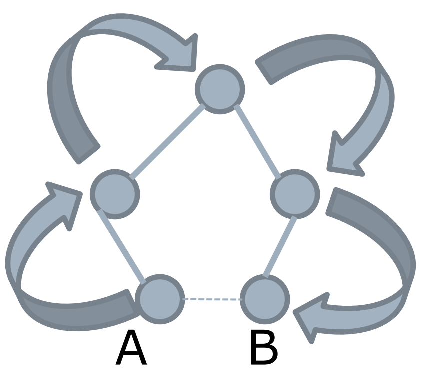




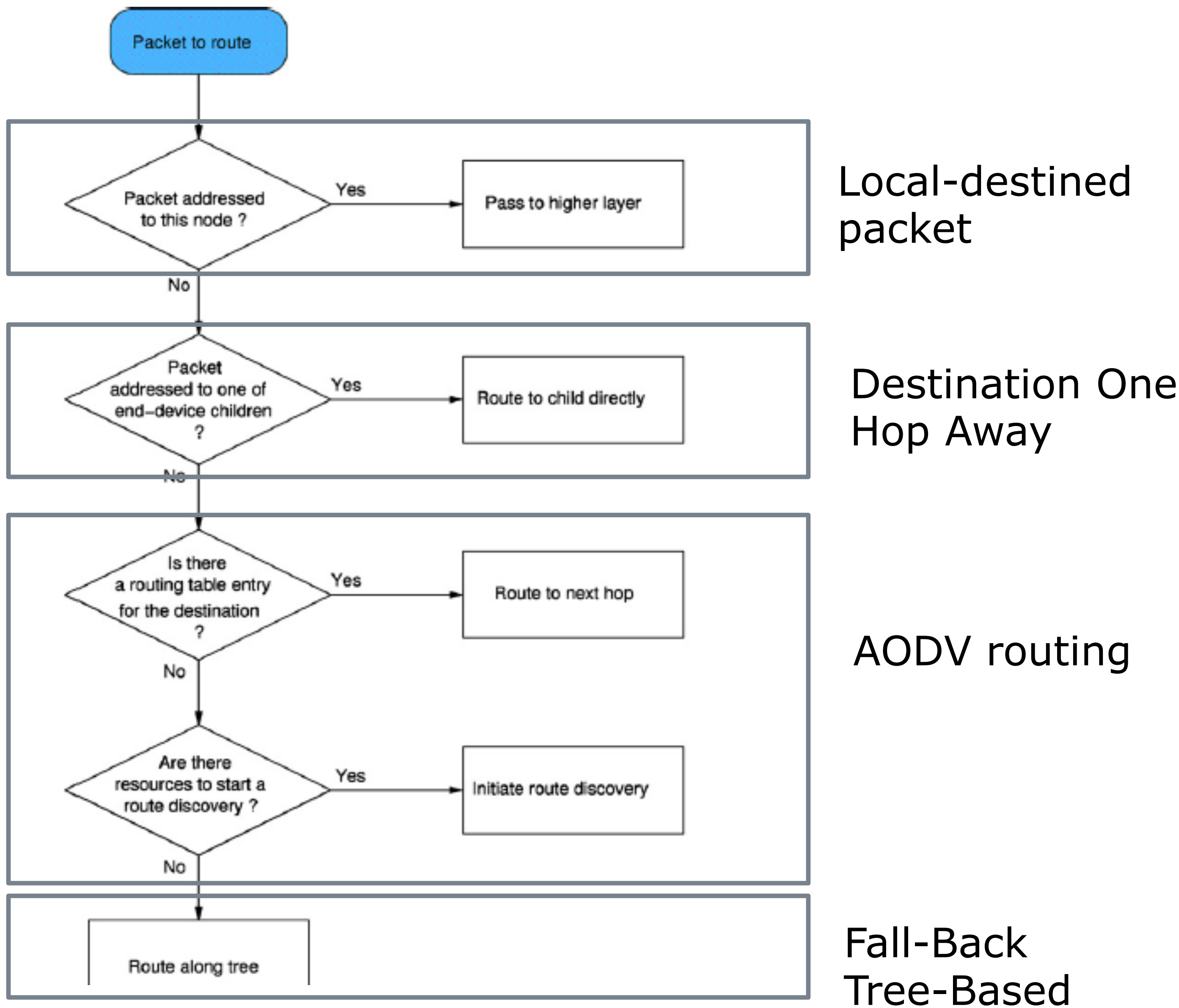


Routing Along the Tree: Shortcomings

- Routing may be not optimized
  - Route always along the tree
  - Routing is “quality-agnostic”
  - E.g.: A wants to send to B



ZigBee Routing Revealed



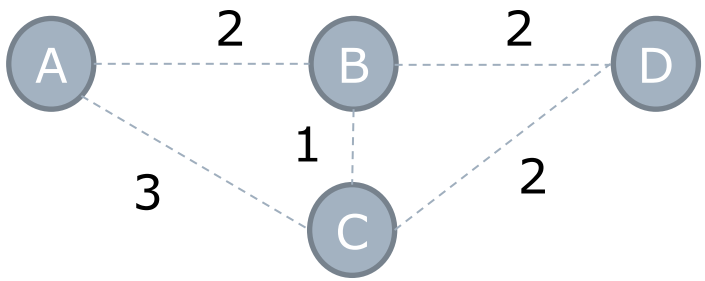
AODV Routing

- A node willing to send to a destination broadcast a *Route Requests (RREQ)* message
  - aka shout ”where’s the destination”
- RREQ messages are flooded by receiving nodes
  - relay shouting
- When a node re-broadcasts a *Route Request*, it sets up a reverse path pointing towards the source
  - stores “who shouted at me”
- When the intended destination receives a Route Request, it replies by sending a Route Reply
  - Shouts back “It’s me”
- Route Reply travels along the reverse path set-up when Route Request is forwarded
  - Shouting travels back the same route

ZigBee Implementation of AODV

- Routing Table
  - ***Destination Address***: 16-bit network address of the destination
  - ***Next-hop Address***: 16-bit network address of next hop towards destination
  - ***Entry Status***: One of Active, Discovery or Inactive
- Routing Discovery Table
  - ***RREQID Unique ID*** (sequence number) given to every RREQ message being broadcasted
  - ***Source Address:*** Network address of the initiator of the route request
  - ***Sender Address:*** Network address of the device that sent the most recent lowest cost RREQ
  - ***Forward Cost:*** The accumulated path cost from the RREQ originator to the current device
  - ***Residual Cost***: The accumulated path cost from the current device to the RREQ destination
- Entries of RT and RDT have validity time-outs

Example



A

DEST	NEXT	STATUS
D	?	Disc

ID	SOURCE	SENDER	FWD COST	RES COST
432	A	A	null	inf

B

DEST	NEXT	STATUS

ID	SOURCE	SENDER	FWD COST	RES COST

C

DEST	NEXT	STATUS

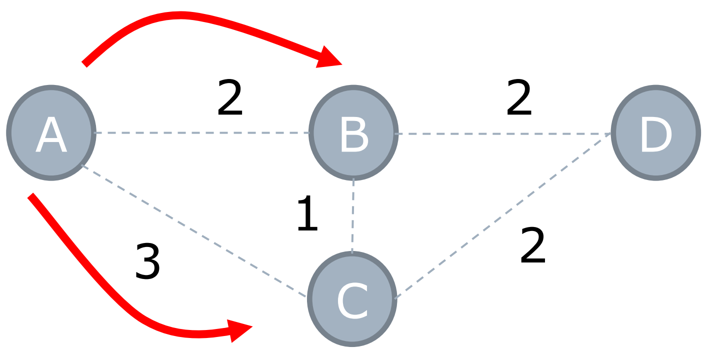
ID	SOURCE	SENDER	FWD COST	RES COST

D

DEST	NEXT	STATUS

ID	SOURCE	SENDER	FWD COST	RES COST

Example



RREQ A-B: cost 2
RREQ A-C: cost 3

A

DEST	NEXT	STATUS
D	?	Disc

ID	SOURCE	SENDER	FWD COST	RES COST
432	A	A	null	inf

B

DEST	NEXT	STATUS
D	?	Disc

ID	SOURCE	SENDER	FWD COST	RES COST
432	A	A	2	inf

C

DEST	NEXT	STATUS
D	?	Disc

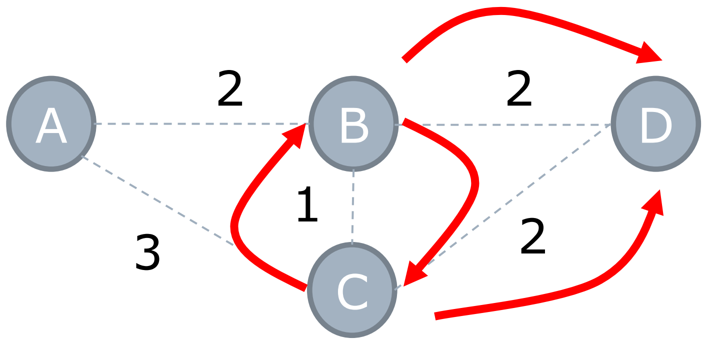
ID	SOURCE	SENDER	FWD COST	RES COST
432	A	A	3	inf

D

DEST	NEXT	STATUS

ID	SOURCE	SENDER	FWD COST	RES COST

Example



RREQ B-C: fw cost 3 DROPPED
RREQ C-B: fw cost 4 DROPPED
RREQ B-D: fw cost 4
RREQ C-D: fw cost 5

A

DEST	NEXT	STATUS
D	?	Disc

ID	SOURCE	SENDER	FWD COST	RES COST
432	A	A	null	inf

B

DEST	NEXT	STATUS
D	?	Disc

ID	SOURCE	SENDER	FWD COST	RES COST
432	A	A	2	inf

C

DEST	NEXT	STATUS
D	?	Disc

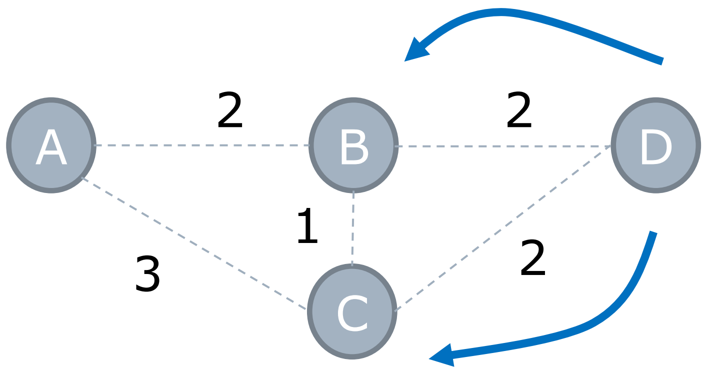
ID	SOURCE	SENDER	FWD COST	RES COST
432	A	A	3	inf

D

DEST	NEXT	STATUS

ID	SOURCE	SENDER	FWD COST	RES COST
432	A	B	4	inf

Example



RREP D-B: res=0, fwd=4
RREP D-C: res=0, fwd=5

A

DEST	NEXT	STATUS
D	?	Disc

ID	SOURCE	SENDER	FWD COST	RES COST
432	A	A	null	inf

B

DEST	NEXT	STATUS
D	D	Disc

ID	SOURCE	SENDER	FWD COST	RES COST
432	A	A	2	2

C

DEST	NEXT	STATUS
D	D	Disc

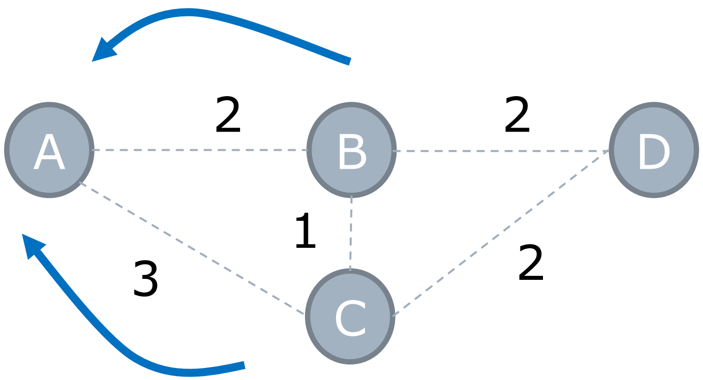
ID	SOURCE	SENDER	FWD COST	RES COST
432	A	A	3	2

D

DEST	NEXT	STATUS

ID	SOURCE	SENDER	FWD COST	RES COST
432	A	B	4	inf

Example



RREP B-A: res=2, fwd=4
RREP C-A: res=2, fwd=5

A

DEST	NEXT	STATUS
D	B	Active

ID	SOURCE	SENDER	FWD COST	RES COST
432	A	A	null	4

B

DEST	NEXT	STATUS
D	D	Disc

ID	SOURCE	SENDER	FWD COST	RES COST
432	A	A	2	2

C

DEST	NEXT	STATUS
D	D	Disc

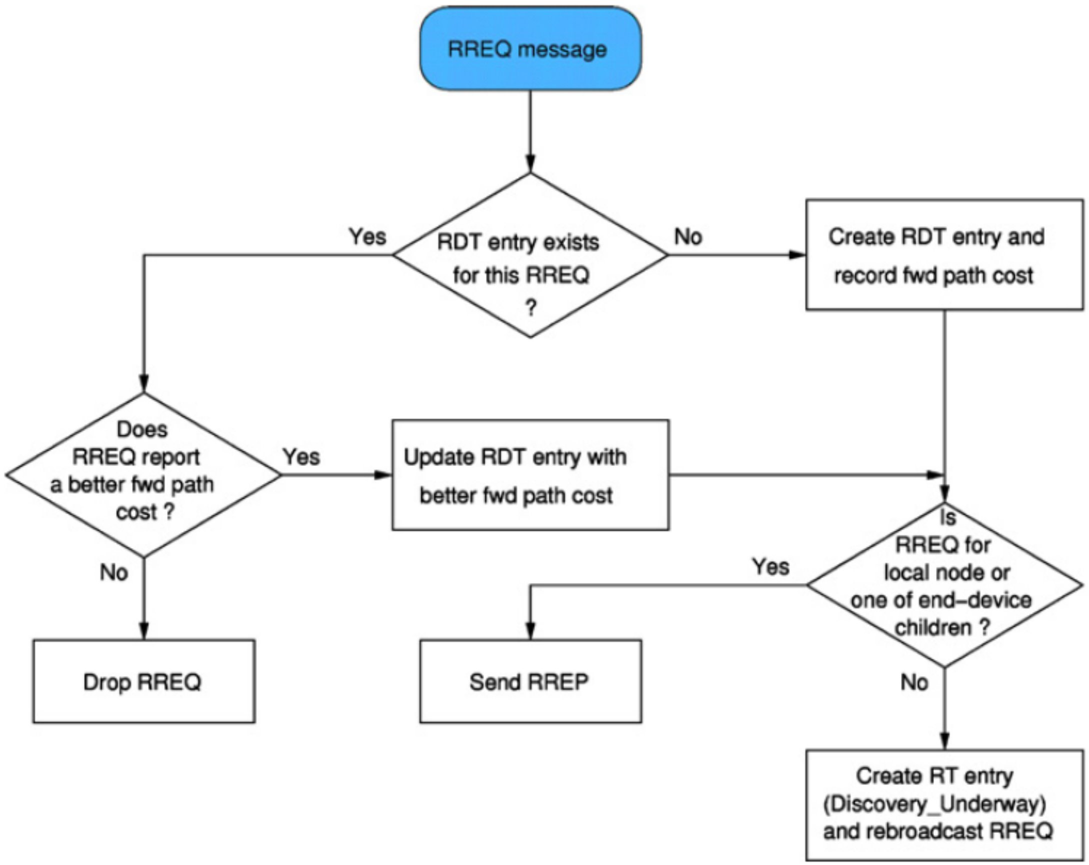
ID	SOURCE	SENDER	FWD COST	RES COST
432	A	A	3	2

D

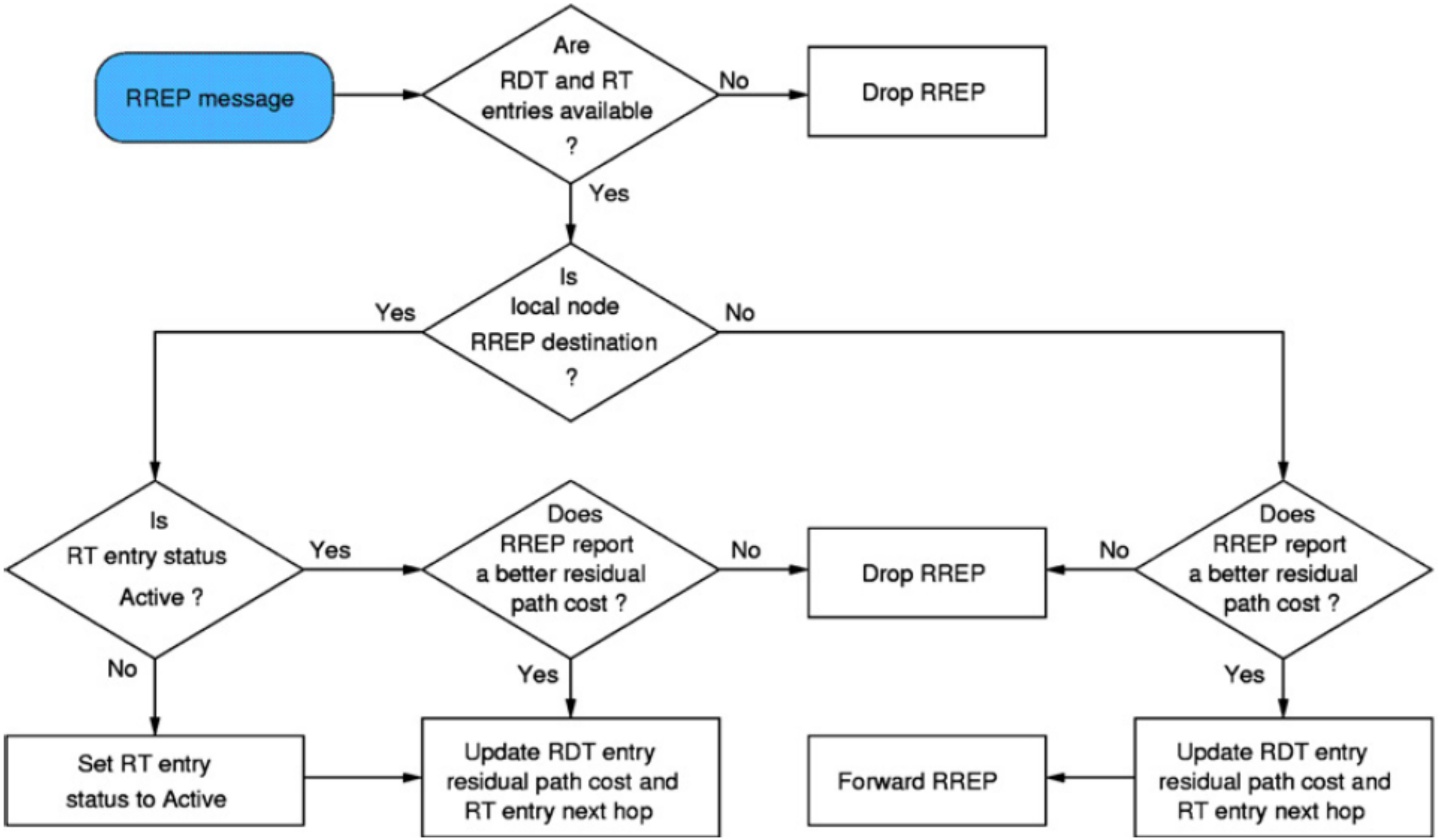
DEST	NEXT	STATUS

ID	SOURCE	SENDER	FWD COST	RES COST
432	A	B	4	inf

RREQ Transmission



Route Set Up


RREP message
Are RDT and RT entries available ?
No
Drop RREP
Yes
Is local node RREP destination ?
Yes
No
Is RT entry status Active ?
Yes
Does RREP report a better residual path cost ?
No
Drop RREP
No
Does RREP report a better residual path cost ?
No
Yes
Yes
Set RT entry status to Active
Update RDT entry residual path cost and RT entry next hop
Forward RREP
Update RDT entry residual path cost and RT entry next hop

Routing Cost

- The cost for path *P* composed of *L-1* links is defined as:

$$C\{P\} = \sum_{i=1}^{L-1} C\{[D_i, D_{i+1}]\}$$

- ZigBee standards “suggests” the following form for the cost of the generic link *l*

$$C\{l\} = \begin{cases} 7, \\ \min\left(7, \mathrm{round}\left(\frac{1}{p_l^4}\right)\right) \end{cases}$$

- P_l is the packet reception rate over link *l*

Network Layer: Frame format

16 bit Addresses

2 Bytes	2 Bytes	2 Bytes	1 Byte	1 Byte	Variabile
FRAME CONTROL	Destination Address	Source Address	Broadcast Radius	Broadcast Sequence Number	FRAME PAYLOAD
	Routing				
NWK Header					NWK Payload

Frame Type, route discovery indication

Max Hop count

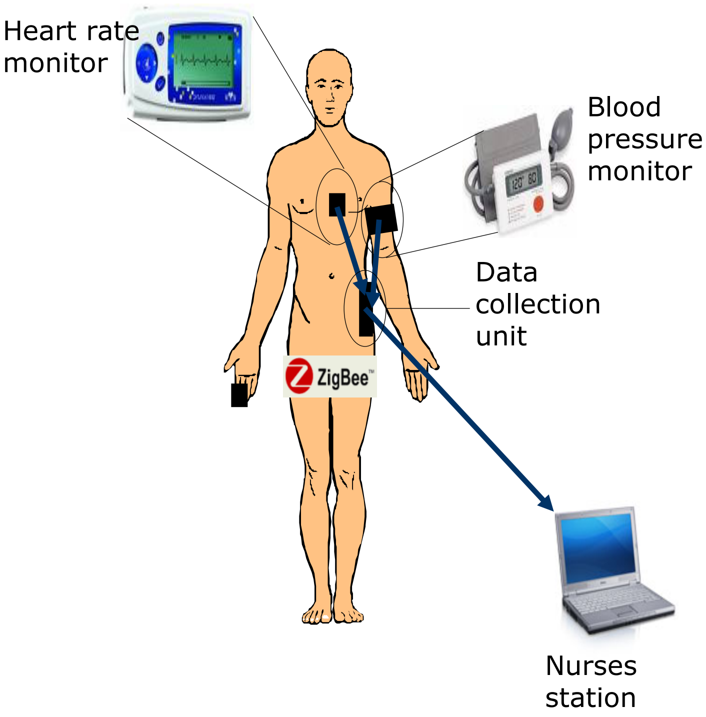
ZigBee Application Profiles

- Needs:
  - A common language for exchanging data
  - A well defined set of processing actions
  - Device interoperability across different manufacturers
  - Simplicity and reliability for the end users

- Profile Definition (9 Profile Libraries Currently Specified)
  - A set of devices required in the application area
  - A set of clusters to implement the functionality
    - A set of attributes to represent device state
    - A set of commands to enable the communication
  - Specification of which clusters are required by which devices
  - Specific functional description for each device

Profile Components

- E.g.: Personal Health Care Profile
- Data Collection Unit
  - The Data Collection Unit (DCU) gathers the data from the different on-body medical and non-medical devices and delivers it to a gateway.
- Electrocardiograph
  - This is a device that records and measures the electrical activity of the heart over time.
- Pulse Monitor
  - A pulse monitor measures a proxy value for the heart rate.
- Sphygmomanometer
  - A sphygmomanometer (blood pressure meter) is a device that measures the blood pressure.



Profiles Snapshot