IEEE 802.15.4 and ZigBee

Emad Ebeid

Davide Quaglia

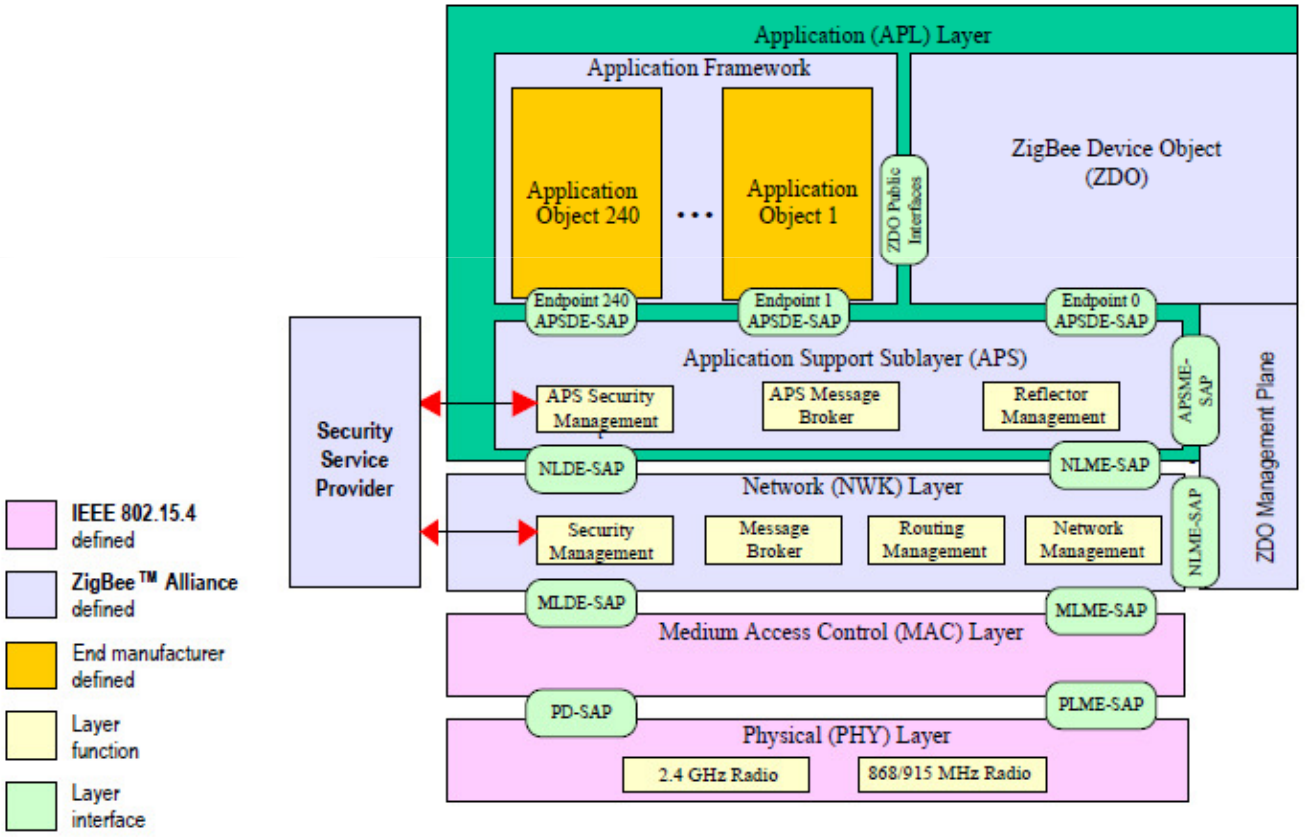
Outline

- Introduction
- Summary of IEEE 802.15.4
- Architecture
- Protocol Stack
- Profiles & Clusters
- Addressing

Introduction

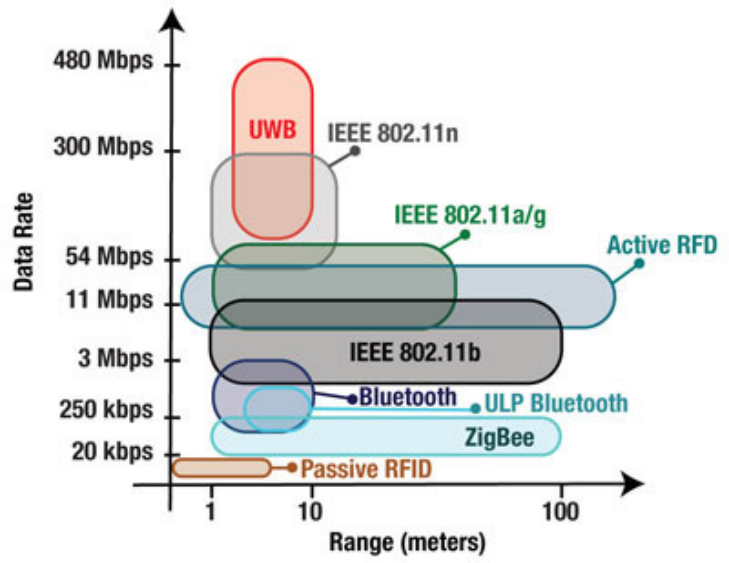
- **ZigBee** stands for " **Z**onal **I**ntercommunication **G**lobal-standard, where **B**attery life was long, which was **E**conomical to deploy, and which exhibited **E**fficient use of resources."
- ZigBee is implemented over IEEE 802.15.4 PHY & MAC
- ZigBee aims:
  - Low data rate
  - Low power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

IEEE 802.15.4/ZigBee stack architecture



802.15.4/ZigBee Frequencies

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



IEEE 802.15.4 vs. other Wireless Technologies

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

History

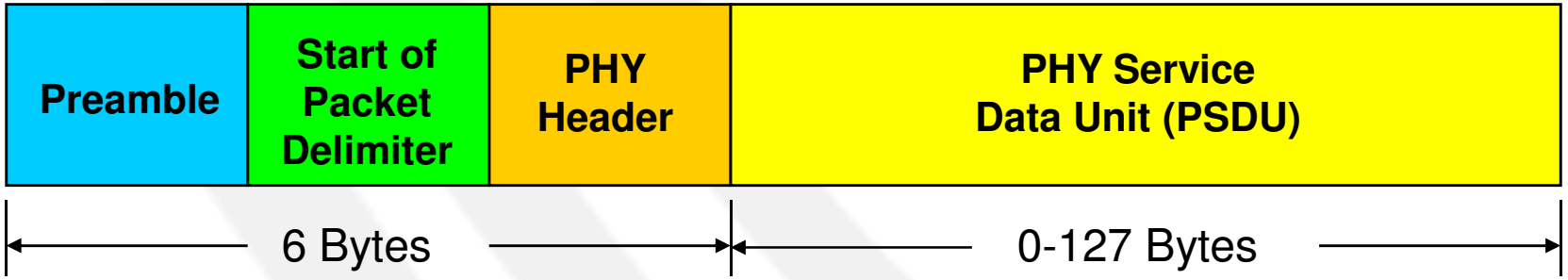
- IEEE 802.15.4
  - 2003
  - 2006
  - 2007 (only for PHY layer for UWB annex)
- ZigBee
  - 2004
  - 2006
  - 2008 (ZigBee Pro)
  - On going for new application profiles

IEEE 802.15.4 MAC overview

Packet Structure

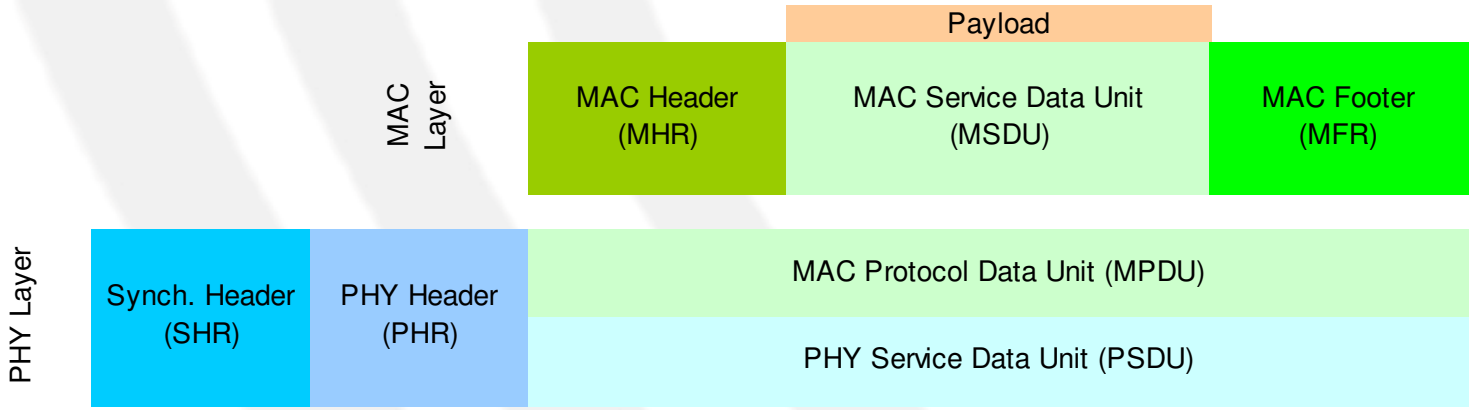
PHY Packet Fields

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



IEEE 802.15.4 MAC overview

General Frame Structure



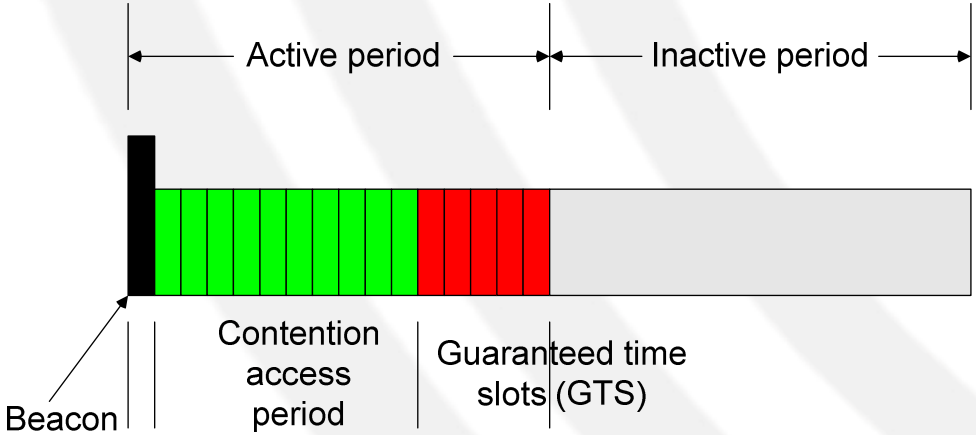
IEEE 802.15.4 MAC overview

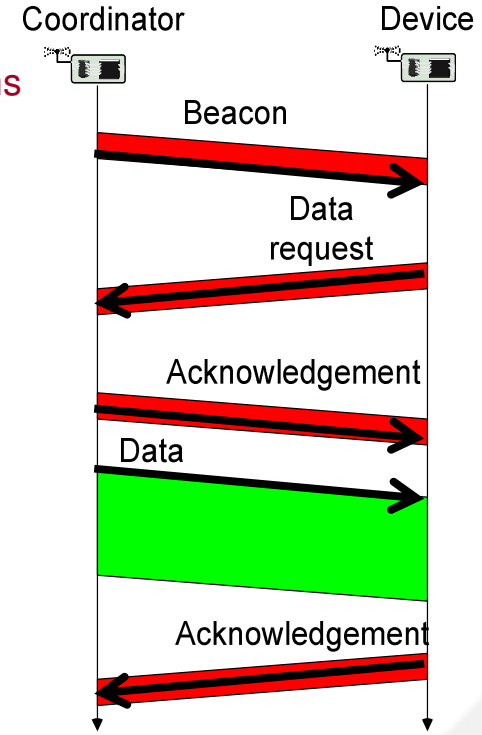
4 Types of MAC Frames:

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

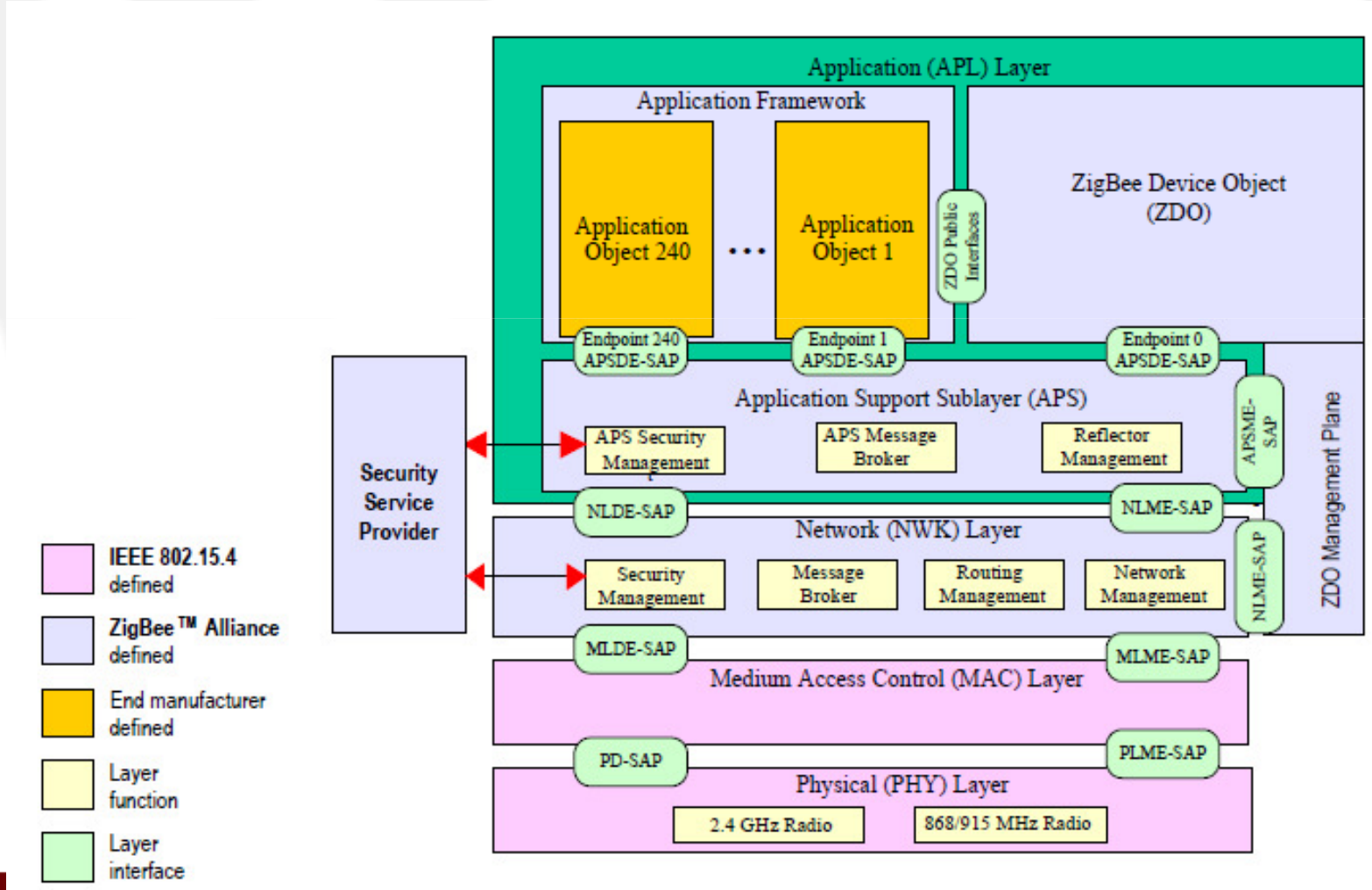
IEEE 802.15.4 MAC overview

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





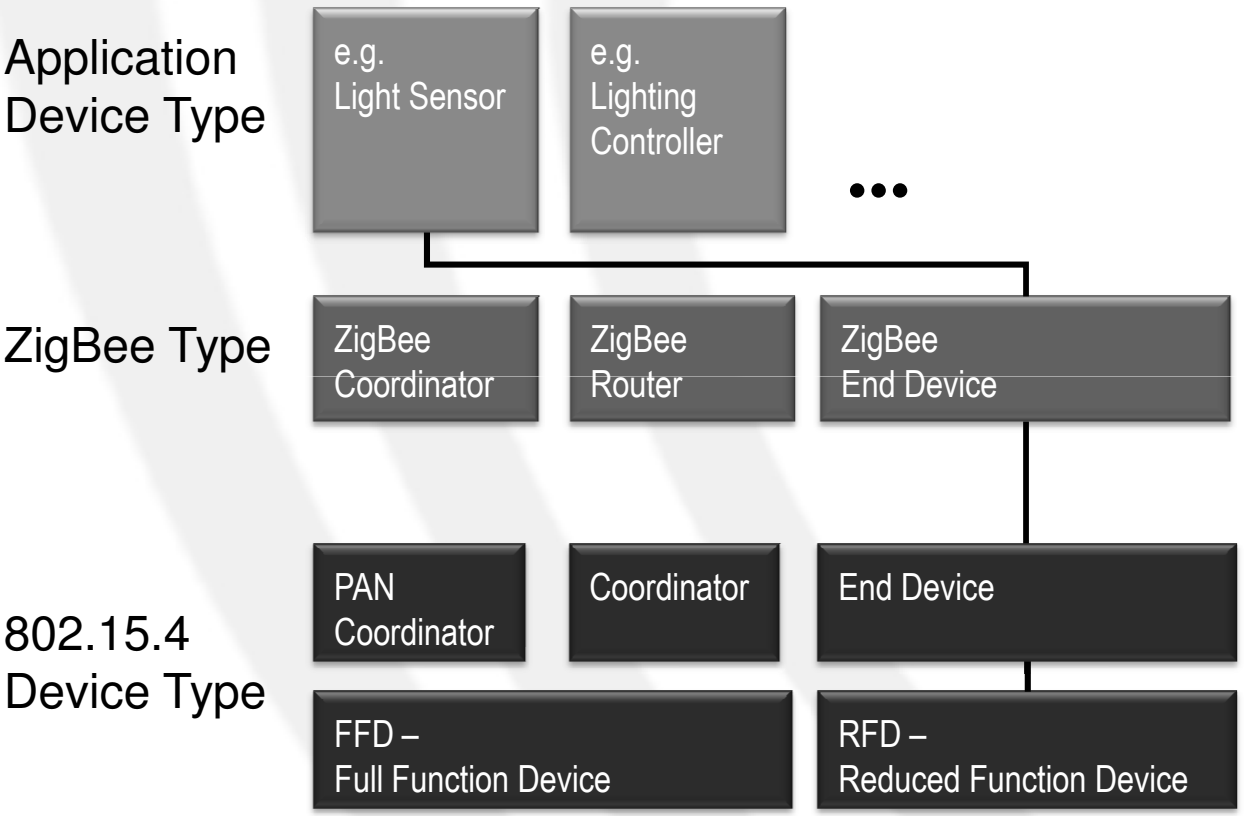
ZigBee stack architecture



ZigBee elements

- Application support sub-layer (APS)
- ZigBee device objects (ZDO)
- ZigBee device profile (ZDP)
- Application framework
- Network layer (NWK)
- ZigBee security services

Device Type Mapping

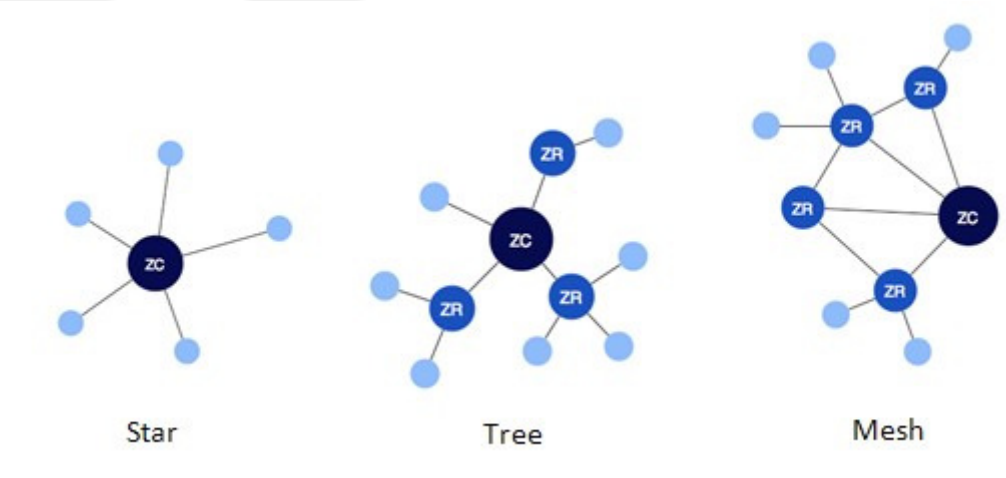


- Distinguishes the type of device from an end-user perspective
- Distinguishes the Logical Device Types deployed in a specific network
- Distinguishes the type of hardware platform

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

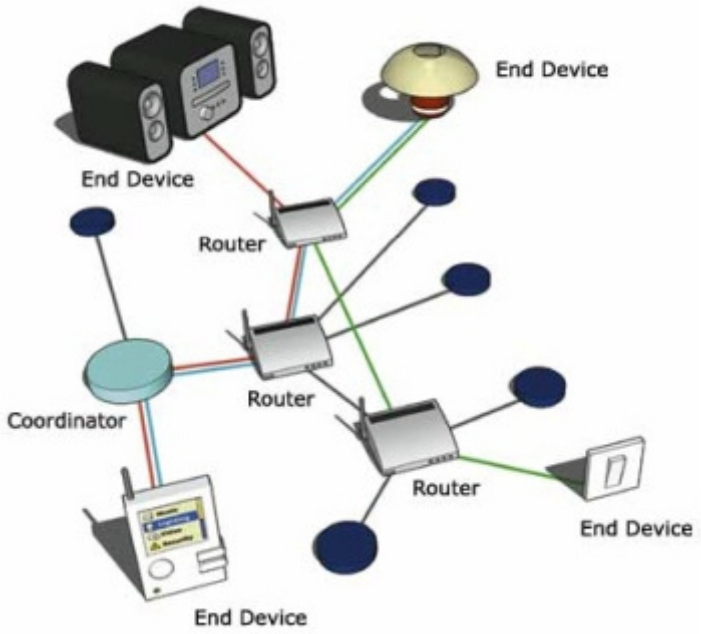
ZigBee architecture

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



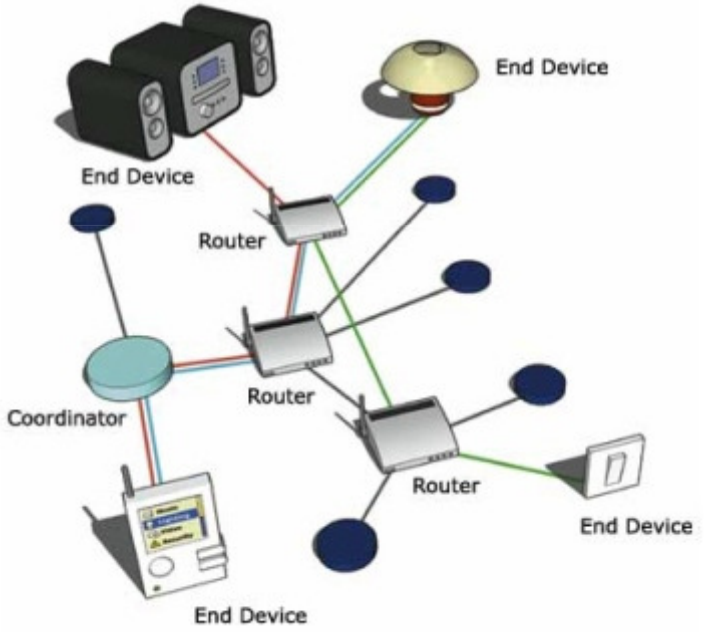
ZigBee Coordinator (ZC)

- only one in the network
- initiates network
- stores information about the network
- all devices communicate with the ZC
- routing functionality
- gateway towards other networks



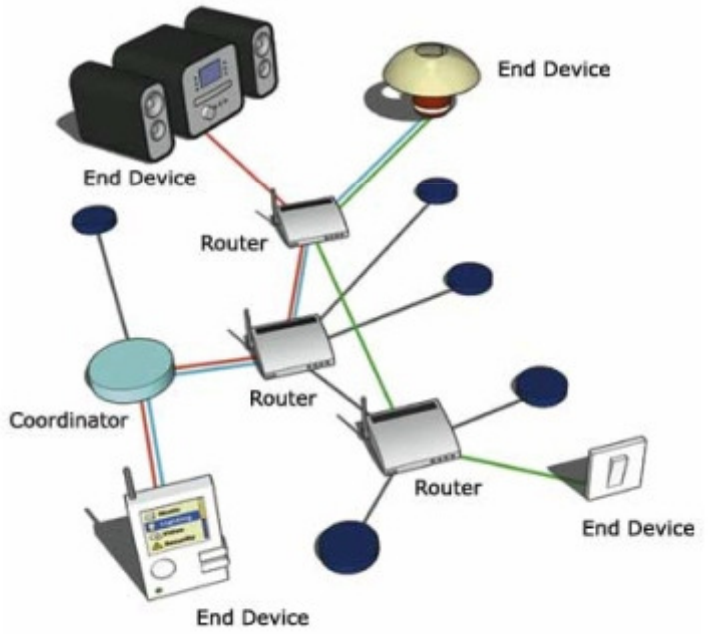
ZigBee Router (ZR)

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



ZigBee End Device (ZED)

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



Summery for ZigBee device types

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

ZC

ZR

ZED

NETWORK LAYER

Network layer overview

- Types of topologies
  - Star
  - Tree
  - Mesh
- Routing
  - Hierarchical in tree topology
  - Ad-hoc routing protocols for mesh topology
- ZigBee covers networks with only 1 PAN ID

APPLICATION FRAMEWORK

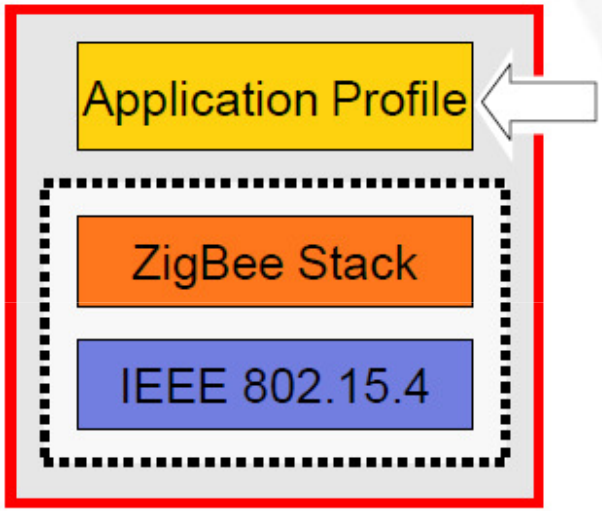
Application framework

- The environment in which application objects are hosted on ZigBee devices
- Up to 240 application objects can be created
  - Identified by Endpoint=1..240
  - Endpoint=0 is for ZDO
  - Endpoint=255 is broadcast address for all application objects

Application Profiles

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

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



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

Application profiles

- Agreements for messages, message formats, and processing actions that enable developers to create an interoperable, distributed application employing application entities that reside on separate devices.
- Application profiles enable applications to send commands, request data, and process commands and requests.
- Defines device types with different capabilities (clusters)
  - Device ID: 2 bytes enumerating device type within the profile
- Profile ID: 2 bytes identification code
  - Assigned by ZigBee Alliance
  - Developers can request private profile IDs for custom applications or use one of ZigBee's published application profiles

Why profiles ?

- Need a common language for exchanging data
- Need a well defined set of processing actions
- Device interoperability across different manufacturers
- Allows solid conformance test programmes to be created
- Simplicity and reliability for the end users
- Realistic application specifications developed through OEM experience

Public profiles

- For generically useful applications
- Developed publicly by members of the ZigBee Alliance
- Managed within the Application Framework Working Group
- Development follows the profile lifecycle
- Enables products to undergo logo certification so that the ZigBee logo can be used

Current public profiles

- ZigBee Building Automation (Efficient commercial spaces)
- ZigBee Remote Control (Advanced remote controls)
- ZigBee Smart Energy (Home energy savings)
- ZigBee Health Care (Health and fitness monitoring)
- ZigBee Home Automation (Smart homes)
- ZigBee Input Device (Easy-to-use touchpads, mice, keyboards, wands)
- ZigBee Light Link (LED lighting control)
- ZigBee Retail Services (Smarter shopping)
- ZigBee Telecom Services (Value-added services)
- ZigBee Network Devices (Assist and expand ZigBee networks)

Private profiles

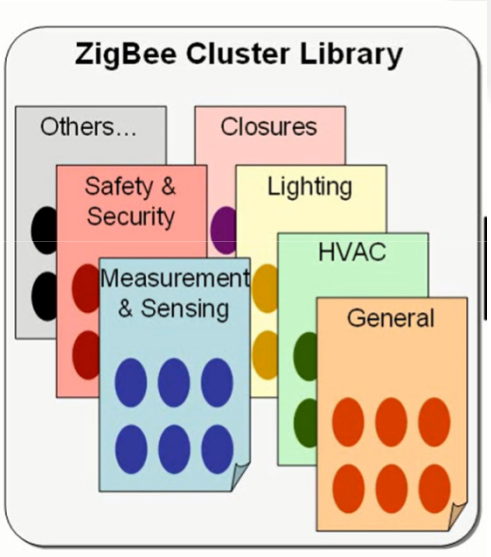
- For manufacturer specific proprietary applications
- Developed privately by individual manufacturers
- Private profiles must use a ZigBee allocated profile identifier
- Commercial products built using private profiles must undergo “no harm” testing

Cluster

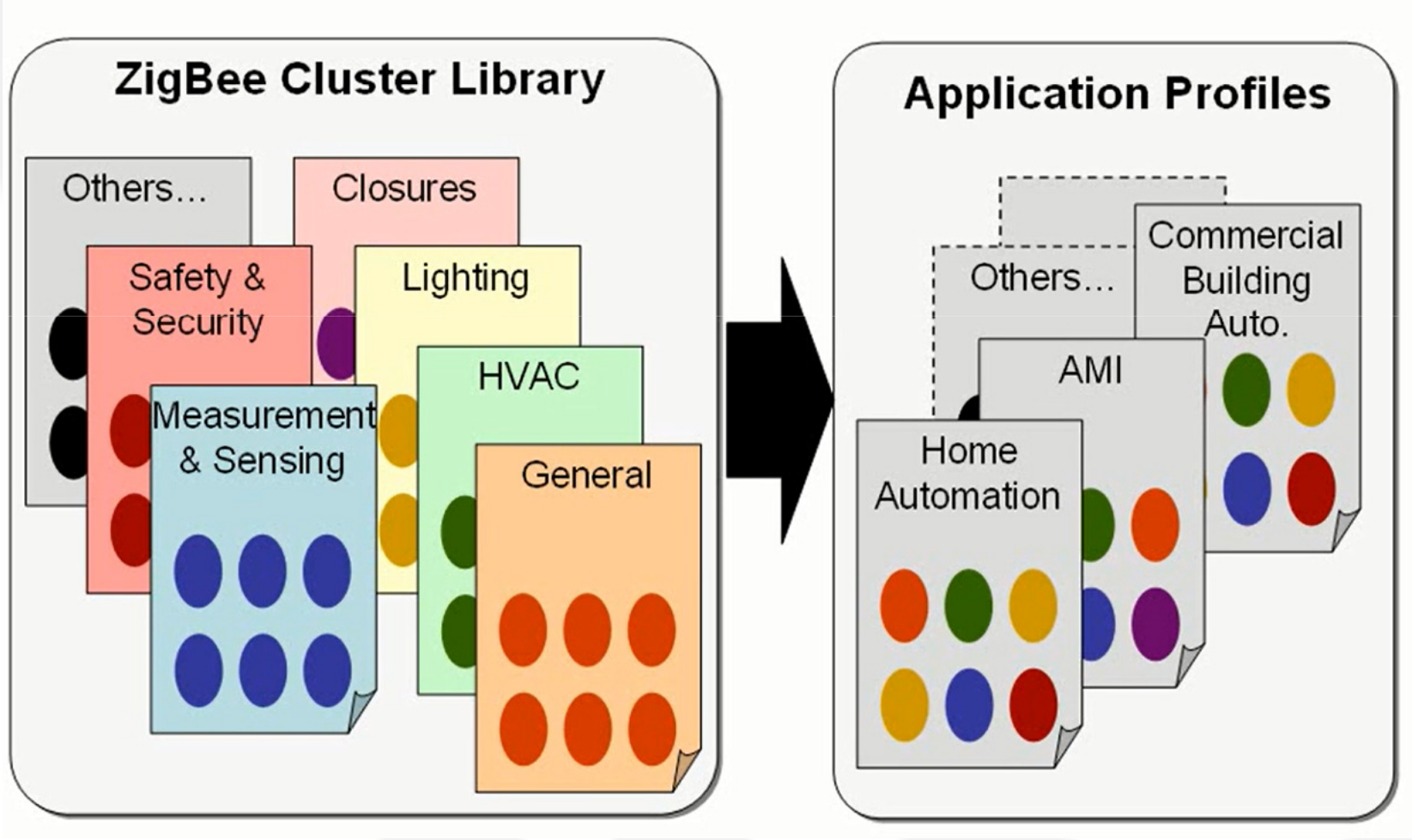
- Clusters are identified by a cluster identifier, which is associated with data flowing out of, or into, the device.
- Cluster identifiers are unique within the scope of a particular application profile.

ZigBee clusters

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



ZigBee clusters



ZIGBEE DEVICE OBJECT (ZDO)

ZigBee Device Object

- Provides an interface between the application objects, the device profile, and the APS.
- The ZDO is located between the application framework and the application support sub-layer.
- It satisfies common requirements of all applications operating in a ZigBee protocol stack.

ZDO responsibilities

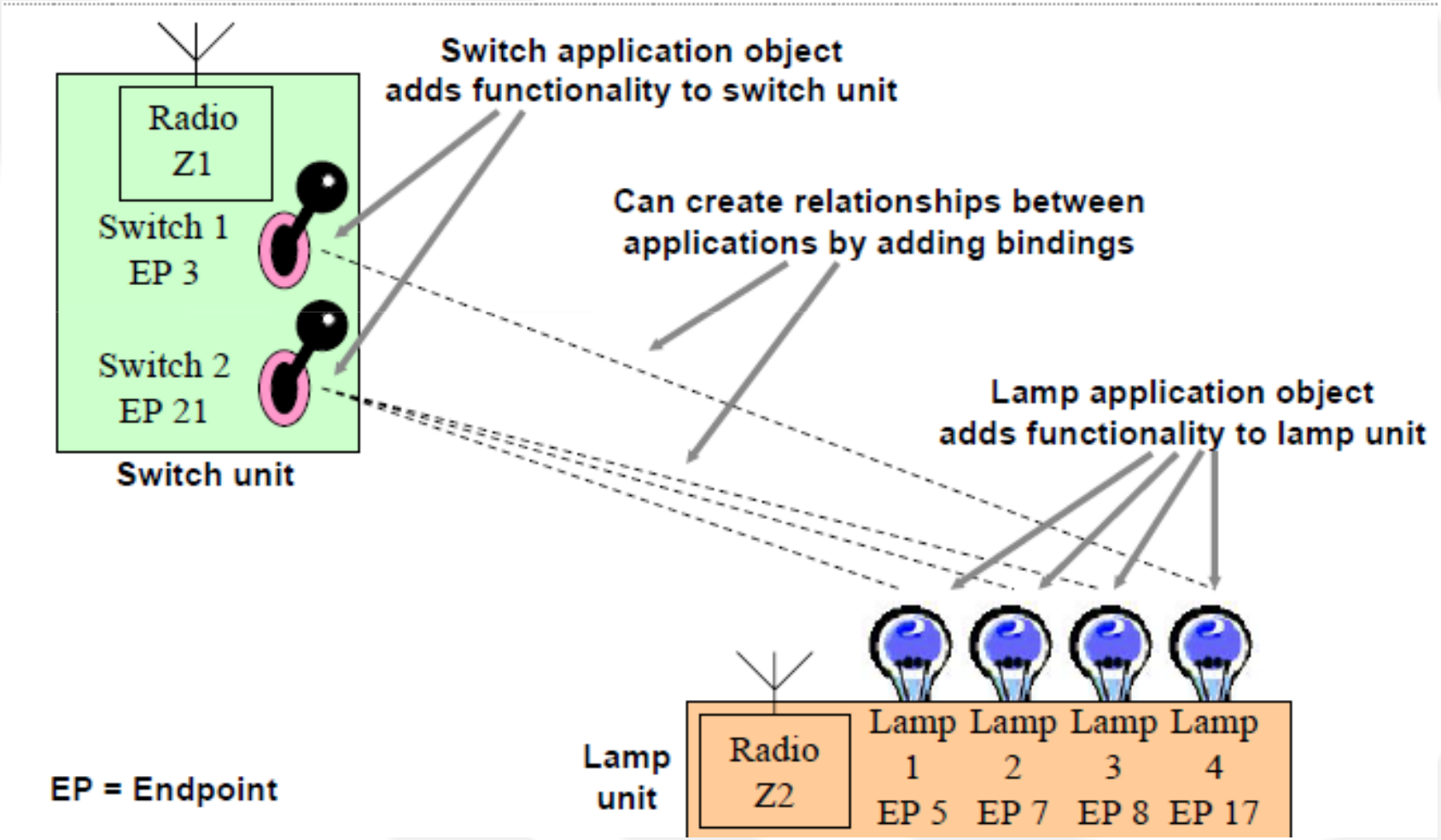
- Initializing the application support sub-layer (APS), the network layer (NWK), and the Security Service Provider.
- Assembling configuration information from the end applications to determine and implement discovery, security management, network management, and binding management.
- The ZDO presents public interfaces to the application objects in the application framework layer for control of device and network functions by the application

Service discovery

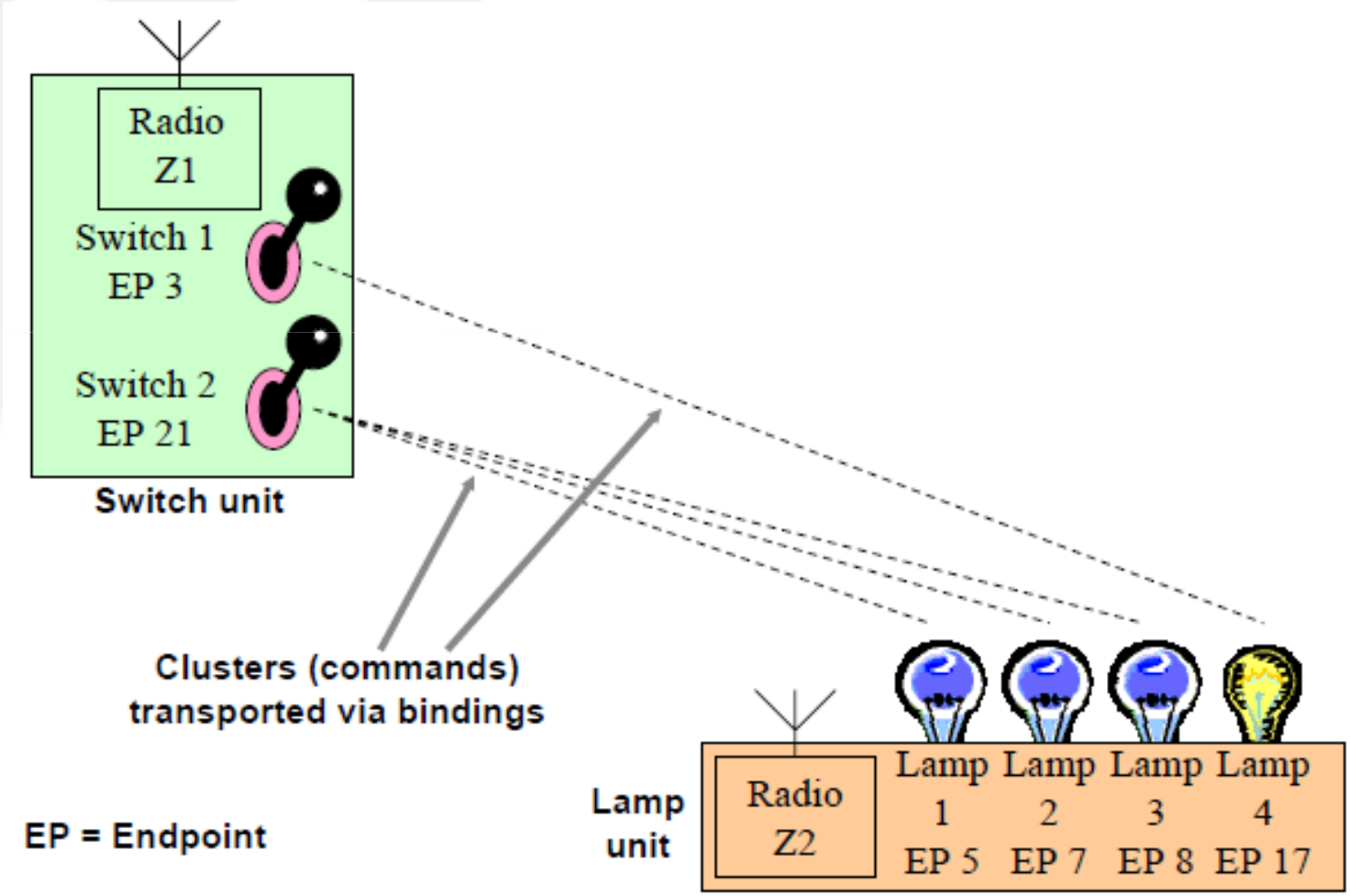
- It is the process whereby the capabilities of a given device are discovered by other devices.
- Service discovery can be accomplished by issuing a query for each endpoint on a given device or by using a match service feature (either broadcast or unicast).
- The service discovery facility defines and utilizes various descriptors to outline the capabilities of a device.

APPLICATION SUPPORT SUB-LAYER (APS)

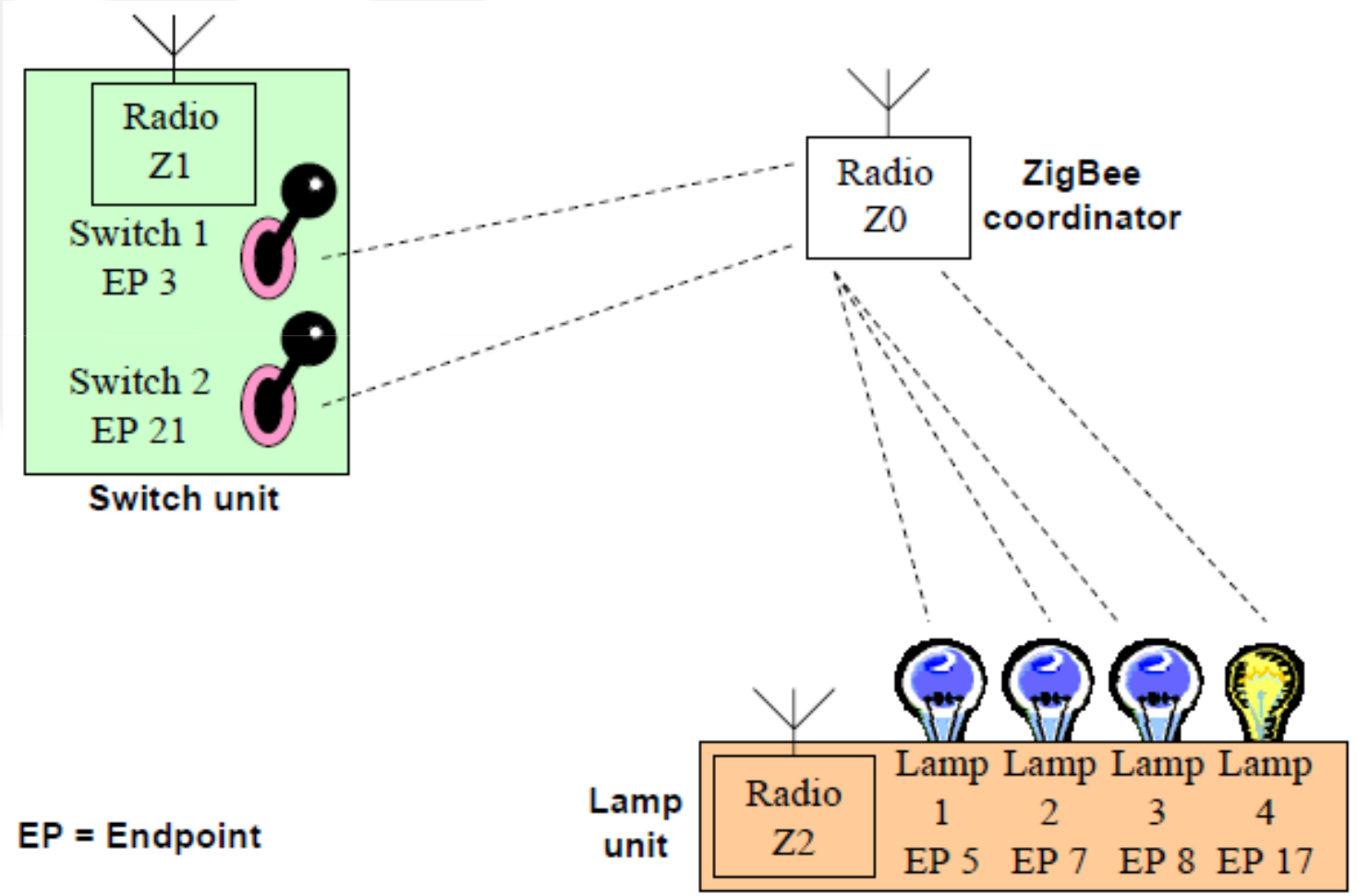
Addressing and Binding



Transporting clusters



Indirect transmission



Binding table

The binding table forms the mapping:

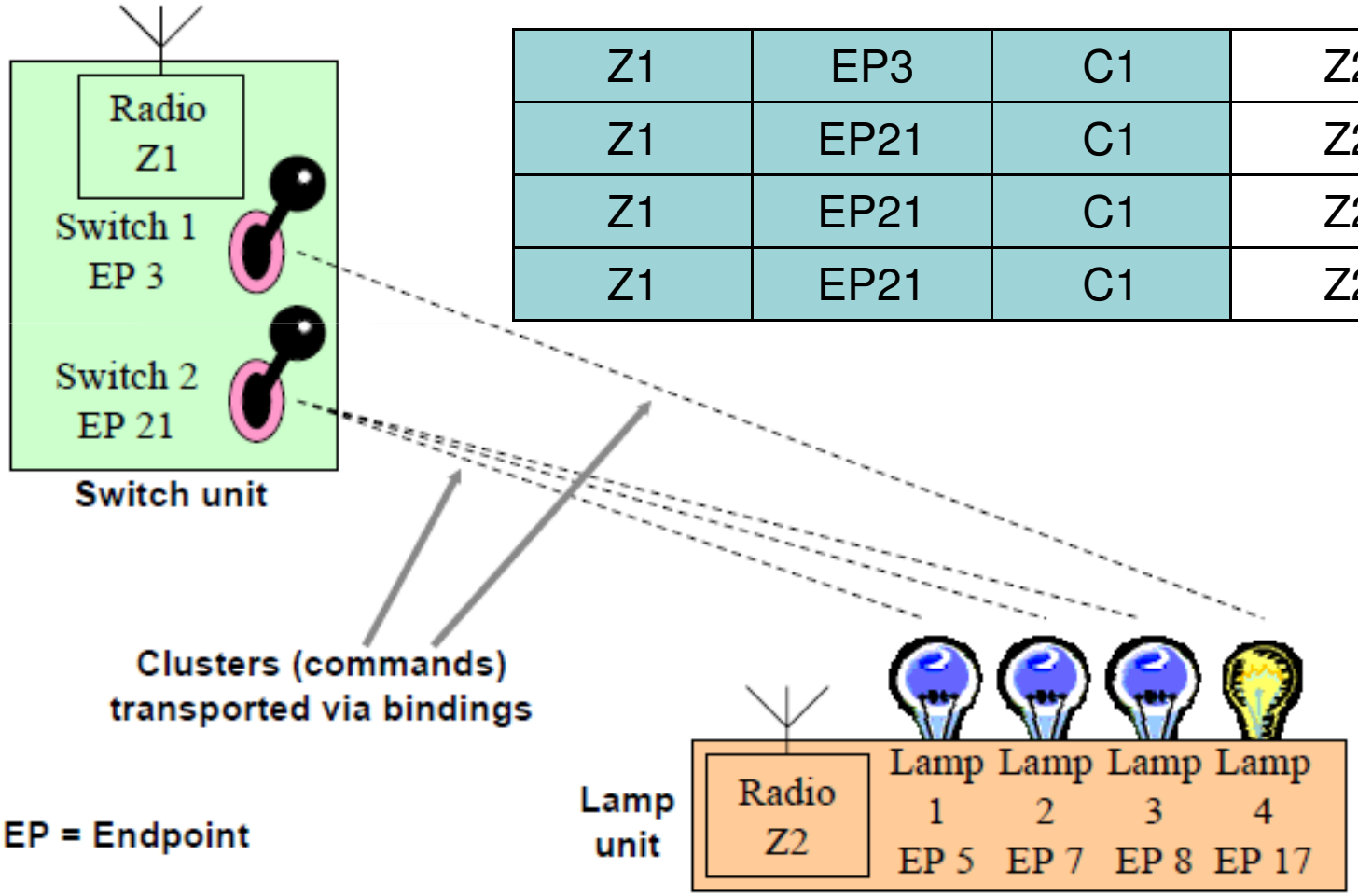
$$(a_s, e_s, c_s) = \{ (a_{d1}, e_{d1}), (a_{d2}, e_{d2}), \ldots, (a_{dn}, e_{dn}) \}$$

Where

- a_s = the address of the device as the source of the binding link
- e_s = the endpoint identifier of the device as the source of the binding link
- c_s = the cluster identifier used in the binding link
- a_{di} = the i^{th} address of the device as the destination of the binding link
- e_{di} = the i^{th} endpoint identifier of the device as the destination of the binding link

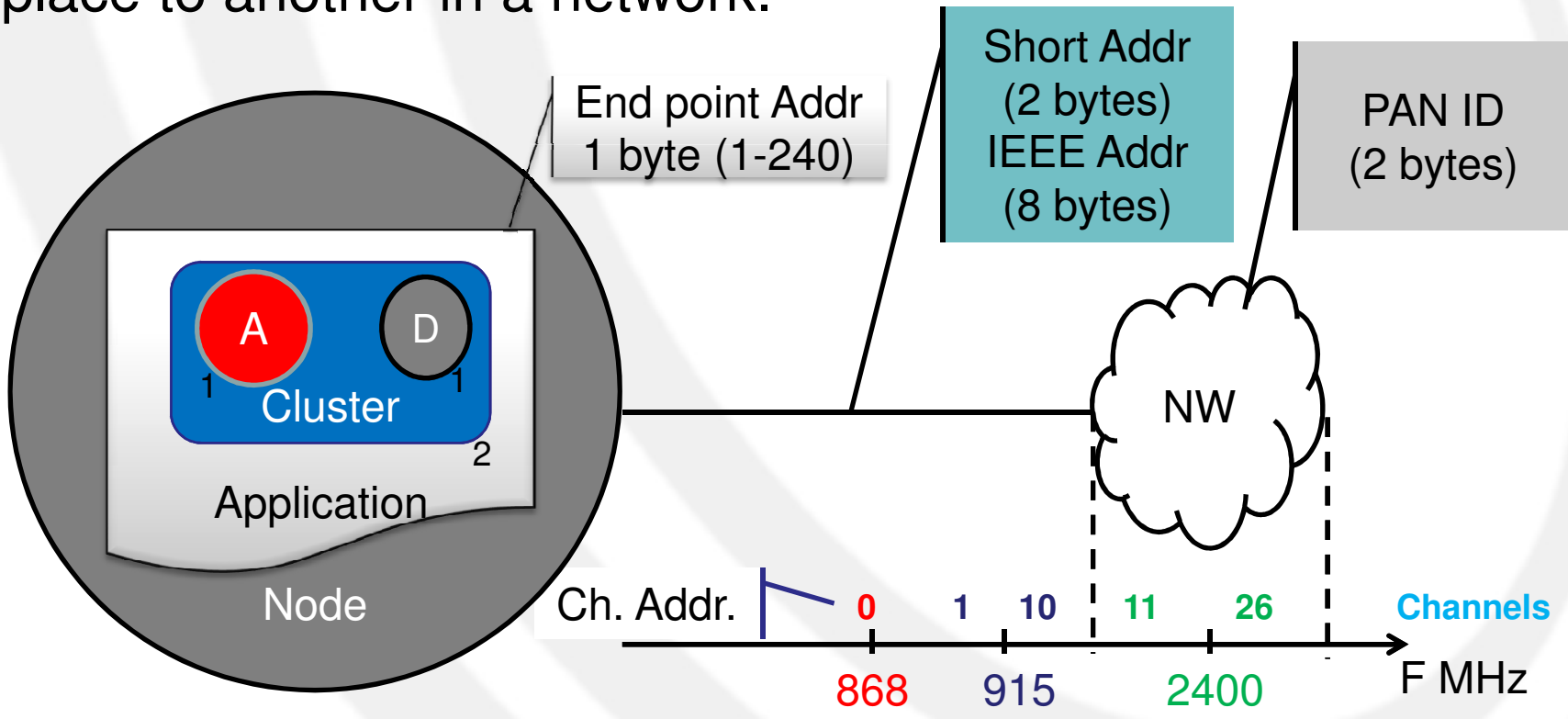
Binding table example

Z1	EP3	C1	Z2	EP17
Z1	EP21	C1	Z2	EP5
Z1	EP21	C1	Z2	EP7
Z1	EP21	C1	Z2	EP8



Summary on ZigBee addressing

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



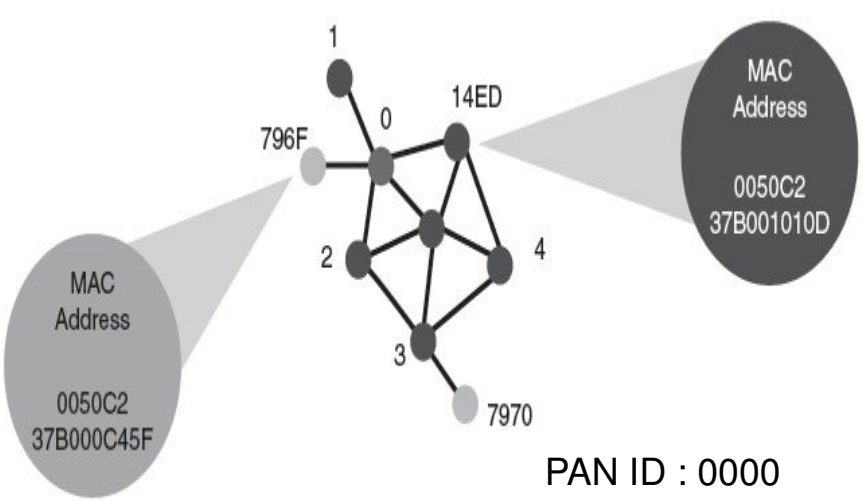
Summary on ZigBee addressing

- For 2.4 GHz

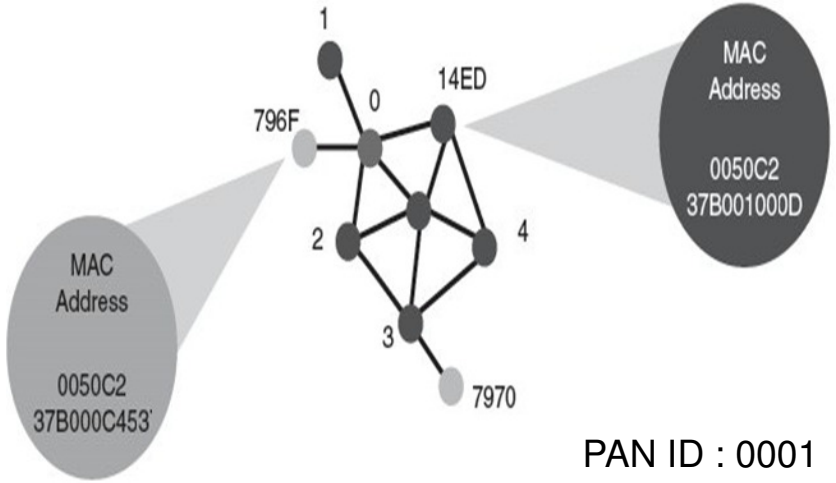
Name	Range	Description
Channel	11–26	A physical portion of the RF spectrum
PAN ID	0x0000–0x3fff	The address of a network within a channel
NwkAddr	0x0000–0xfff7	The address of a node within a network
Endpoint	1–240	The address of an application within a node
Cluster	0x0000–0xffff	The object within the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

Summary on ZigBee addressing

- The MAC address, also called IEEE address, long address, or extended address, is a 64bit number that uniquely identifies this board from all other IEEE 802.15.4 boards in the world



PAN ID : 0000



PAN ID : 0001

APS data transmission

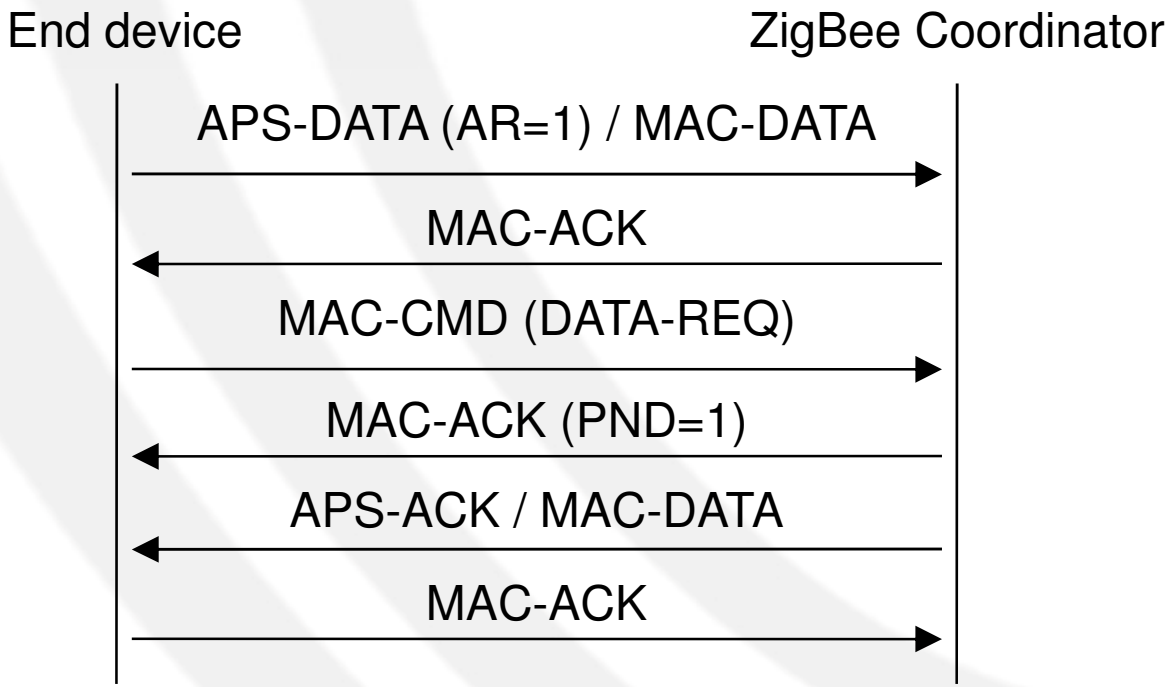
- Endpoint numbers as APS addresses
- Stop&wait ack/re-tx can be used
- Fragmentation
  - If an APS PDU is larger than an IEEE 802.15.4 payload

ACK and retransmission

- APS PDU (both DATA and ACK) has a field named “counter”, a source endpoint and a destination endpoint
- Source APS requests ack through the AR bit set to 1 in the APS-DATA PDU
  - The received ack is valid if the counter has the same value and source/destination endpoints are switched.

APS-ACK and MAC-ACK

- The APS ack is a IEEE 802.15.4 DATA PDU
- Example:



Fragmentation

- All the blocks have the same sequence number
- Specific fields are used to indicate
  - The number of blocks
  - Block order in the sequence
- Definition of a “transmission window” grouping up to 8 blocks
  - An acknowledgement is sent when the last block of the window is received either to confirm that all blocks in the transmission window have been successfully received or to request retransmission of one or more unreceived blocks.