Overview on 802.15.4/Zigbee

Laura Vanzago
Advanced System Technology – R&D
laura.vanzago@st.com

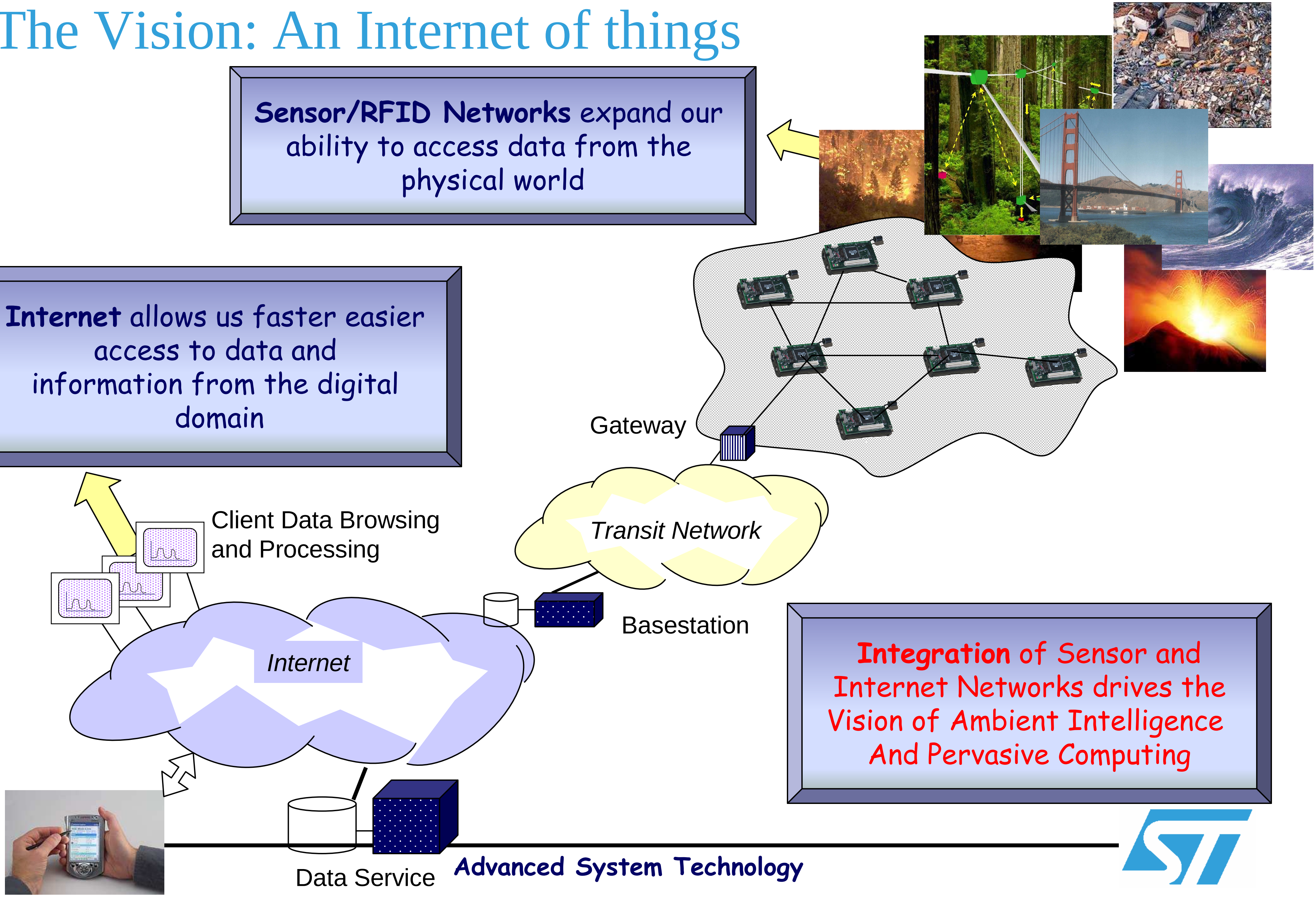
DICO - May 2006

STMicroelectronics

The Vision: An Internet of things

Sensor/RFID Networks expand our ability to access data from the physical world

Internet allows us faster easier access to data and information from the digital domain



Integration of Sensor and Internet Networks drives the Vision of Ambient Intelligence And Pervasive Computing

Outline

- IEEE 802.15.4 Overview
- Zigbee Overview

Many slides from Zigbee official presentations (www.zigbee.org)

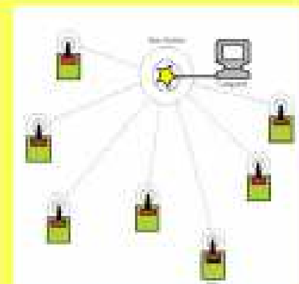
Wireless Networks Evolution

Point to Point

- Simple wire replacement
- Direct Connection between devices
- Limited communication

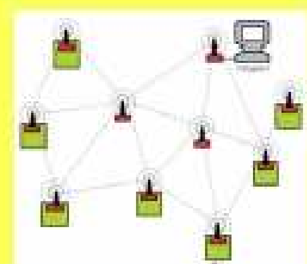
Point to Multi-Point

- Centralized routing and control point
- Examples include: Wi-Fi, GSM, Bluetooth
- All data must flow through “base station”

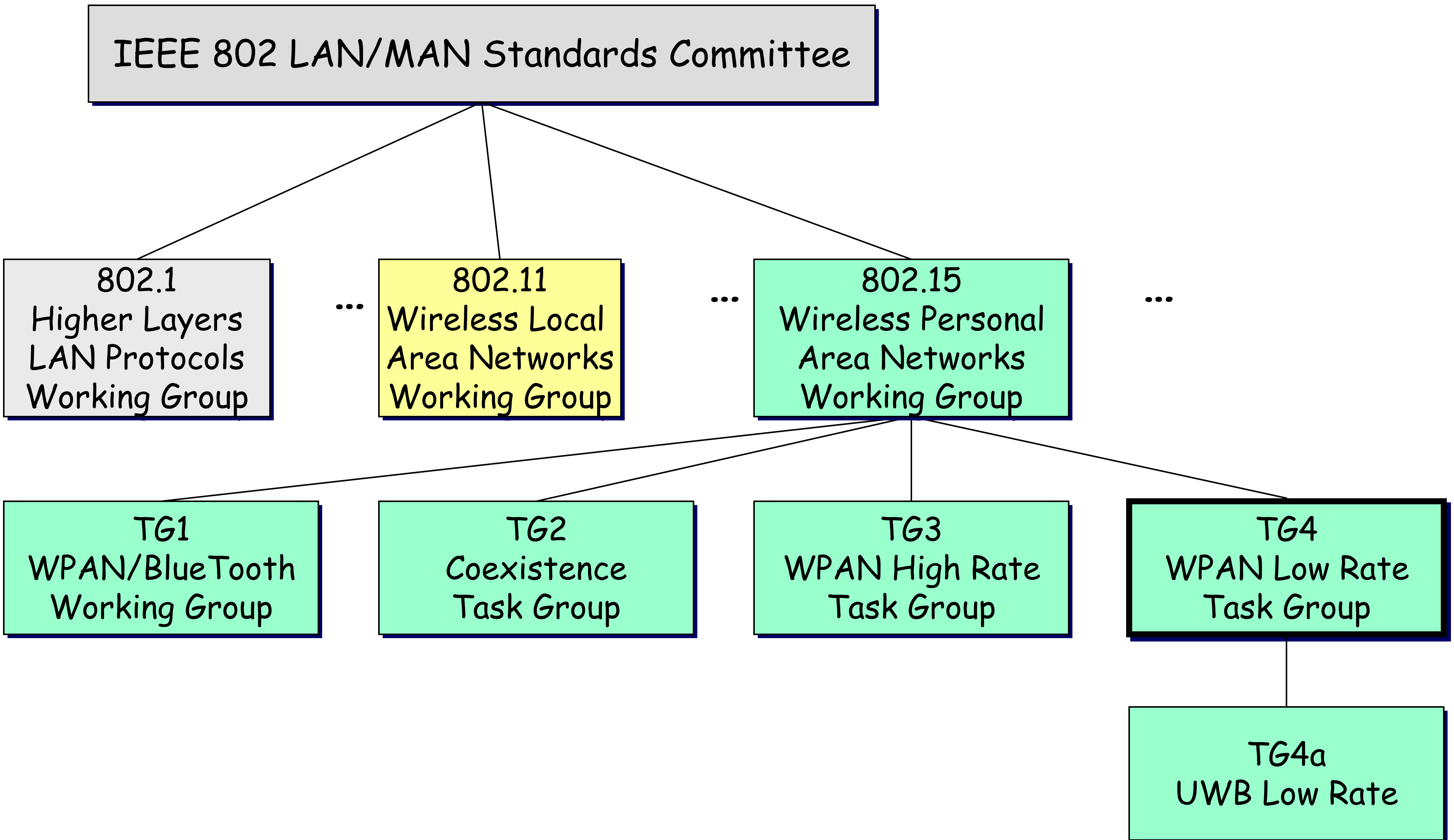


Multi-hop/Mesh

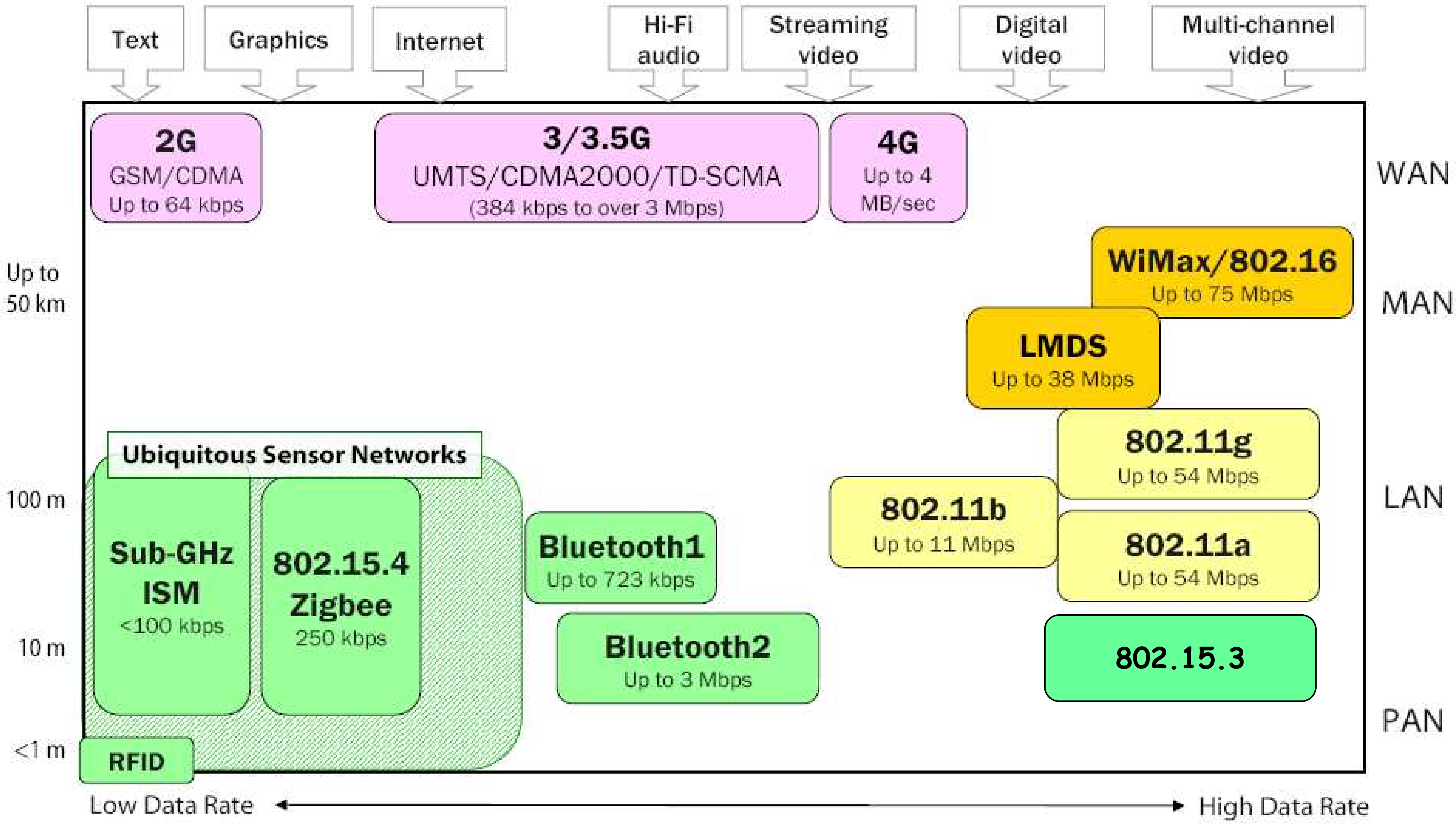
- Full RF redundancy, with multiple data paths
- Self Configuring / Self Healing
- Distributed Intelligence



IEEE Wireless PAN



Wireless Technologies



From *Wireless Sensor Networks* by Feng Zhao and Leo Gubias, 2004.

IEEE 802.15.4 …

- What it is:
  - A WPAN standard optimized for low data throughput applications with simple or no QoS requirements
  - Lower power and lower cost than other WPANs (e.g. Bluetooth)
  - Using Zigbee Alliance for marketing and compliance (like Wi-Fi/802.11b)
  - PHY and MAC layers only (upper layers defined by ZigBee)

- MCU requirements: 8 bit, 4 MHz, 32 kB ROM, 8 kB RAM

Wireless Standard Comparisons

	802.15.4	Bluetooth 802.15.1	Wi-Fi 802.11b	GPRS/GSM 1XRTT/CDMA
Application Focus	Many	Cable Replacement	Web, Video, Email	WAN, Voice/Data
System Resource (Protocol Stack Size)	4KB – 32KB (64KB)	250KB+	1MB+	16MB+
Battery Life (days)	100-1000+	1-7	1-5	1-7
Nodes per Networks	255-65K+	7	30	1
Bandwidth(kbps)	20-250	720	11,000+	64-128+
Range (meters)	1-75+	1-10+	1-100	1,000+
Key Market Attributes	Low Data Rate Low Power Low Cost	Cost, Convenience High QoS Low and Guaranteed latency	Speed, Flexibility	Reach, Quality

IEEE 802.15.4/ZigBee Market Features

1. Low power consumption
2. Low cost
3. Low offered message throughput
4. Reliable Communication
5. Supports large network orders (<= 65 k nodes)
6. Low to no QoS guarantees
7. Selectable levels of security (using AES-128)
    1. Privacy (encryption)
    2. Sender authentication
    3. Message integrity
8. Flexible protocol design suitable for many applications

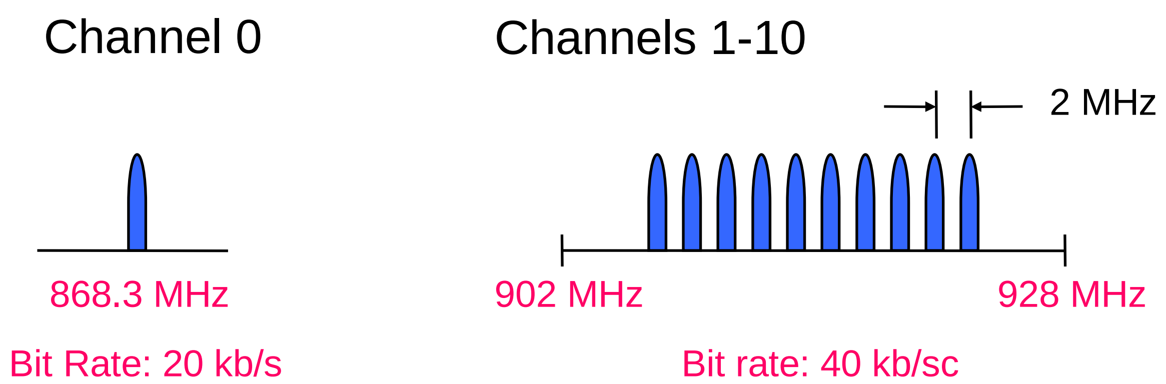
Market News ...

New analysis from Frost & Sullivan World UWB & ZigBee Chipset Market, reveals that the market for UWB chipsets that had nil shipments in 2005 shall generate revenues of $950 million in 2009, while the Zigbee chipsets market generated revenues of $11.3 million in 2005 and is likely to reach **$800.0 million in 2009**

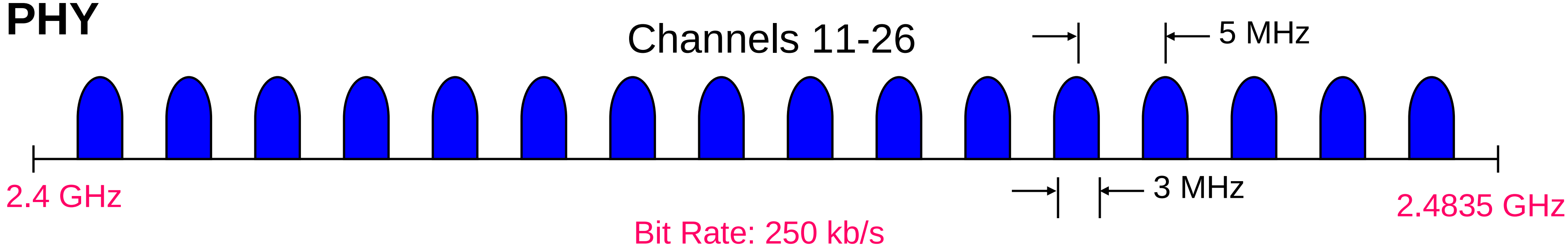
802.15.4 PHY

Operating Frequency Bands

868MHz / 915MHz PHY



2.4 GHz PHY



802.15.4 PHY

Common Parameters

Transmit Power

• Capable of at least 0.5 mW (-3 dBm)

Receiver Sensitivity (Packet Error Rate <1%)

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

Support to Low Duty Cycle

• Minimum beacon packet length 544 us
• Superframes periods [15,36ms, >4minutes]
• Beacon duty cycle [2.3%, 2.16 ppm]
• Adjustable Duty Cycle 1%

Timing

- New Slave Enumeration = 30 ms typically
- Sleeping slave changing to active = 15 ms typically
- Active slave channel access time = 15 ms typically

802.15.4 PHY

PHY Primitives

- Transmitting/ receiving packets across physical medium
- Activation/deactivation of the radio transceiver
  - Duty Cycle
- Clear channel assessment (CCA)
  - CSMA MAC
- Energy detection (ED)
  - Channel selection
- Link Quality Indication (LQI) – byte attached to each received frame
  - Dynamic channel selection, location algorithm, routing based on link quality

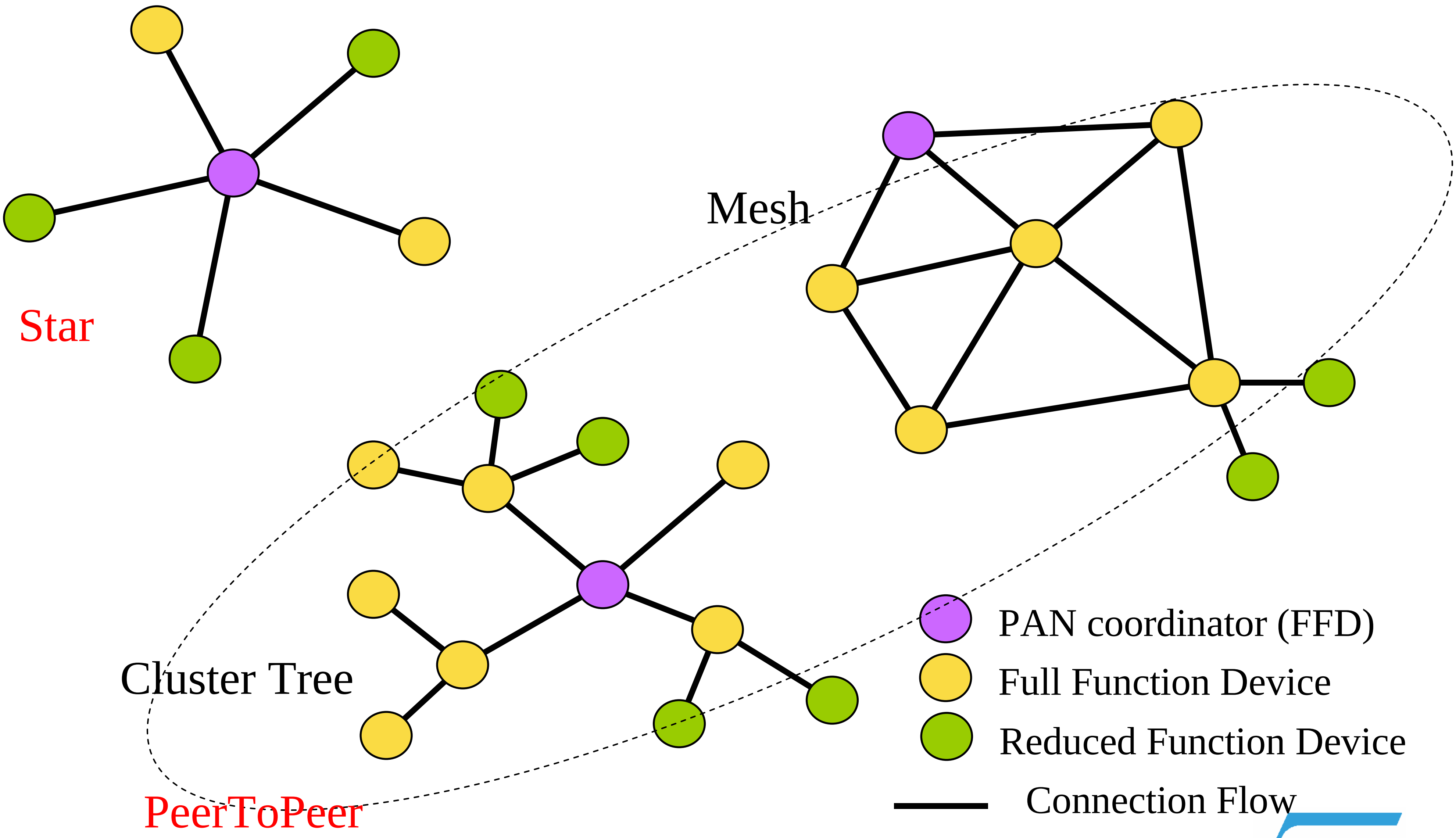
Primitive	Description	Request	Confirm	Response	Indication
PD-DATA	Transmitting/ receiving packets	X	X		X
PLME-GET	Getting PHY PAN information base				
PLME-SET	Setting PHY PAN information base				
PLME-SET-TRX-STATE	Activation/deactivation of the radio transceiver	X	X		
PLME-CCA	Clear channel assessment	X	X		
PLME-ED	Energy detection (ED)	X	X		

802.15.4 Device Types

- PAN coordinator
  - PAN Initiator and PAN Controller
  - Able to transmit beacon and to talk to any other device
- Coordinator
  - Able to transmit beacon and to talk to any other device
- Device
  - Unable to transmit beacon and is able to talk only with coordinators

- Full function device (FFD)
  - PAN coordinator, coordinator, device
  - Memory capabilities sufficient to store routing tables
  - Full MAC implementation
- Reduced function device (RFD)
  - Device
  - Very Low cost device with minimal memory requirements
  - Partial MAC implementation

802.15.4 Supported Topologies



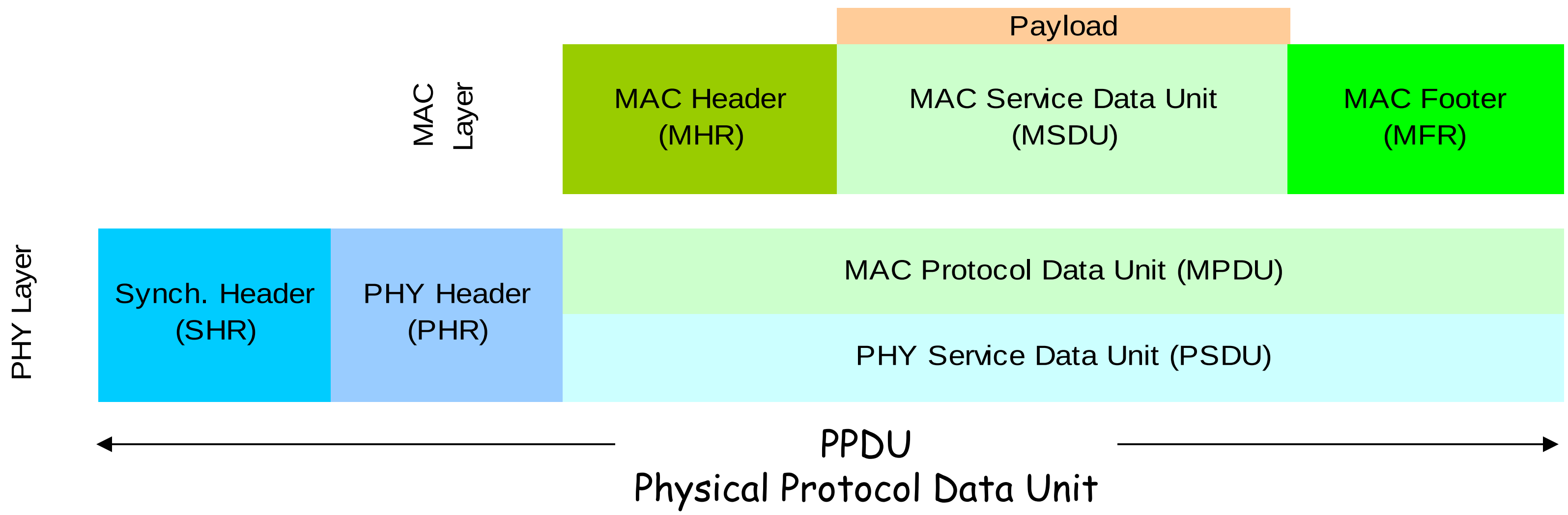
802.15.4 MAC

Addressing

- All devices have IEEE (64 bits) addresses
- Addressing modes:
  - Default Extended (64bit)
    - Used for direct communication in peer-to-peer
  - Optional Short (PanID & 16bit):
    - Allocated by PAN coordinator when the device associates *(64k nodes addressable with reduced overhead)*

802.15.4 MAC

General Frame Structure

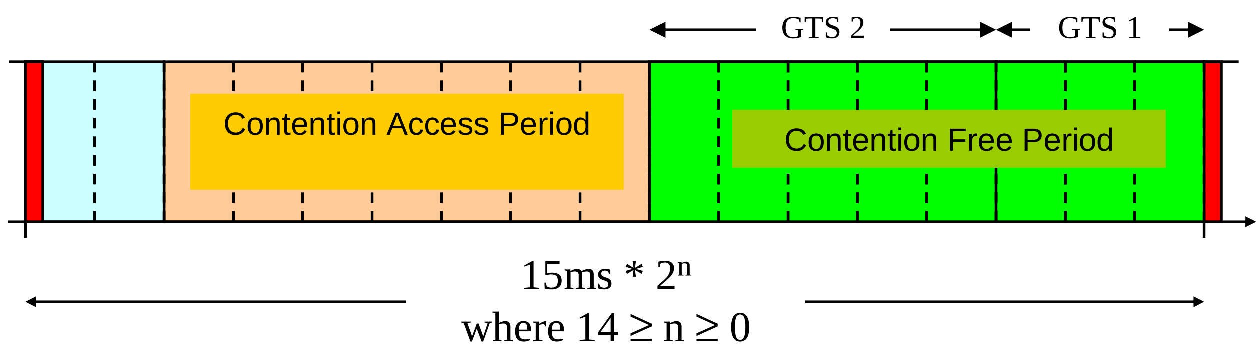


4 Types of MAC Frames:

- Beacon Frame (only implemented in FFD)
  - Superframe boundary marker
  - Frame sync signal
  - Association supervision
- Data Frame
- Acknowledgment Frame (does not contain a MAC payload)
- MAC Command Frame ((Dis)-Association, Orphan notification, Beacon request, ….)

802.15.4 MAC

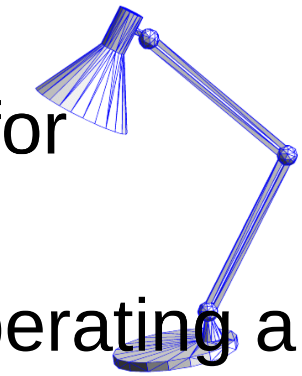
Optional Superframe Structure



Network beacon	Transmitted by network coordinator. Contains network information (sync, period…), frame structure and notification of pending node messages.
Beacon extension period	Space reserved for beacon growth due to pending node messages
Contention period	Access by any node using slotted CSMA-CA
Guaranteed Time Slot	Reserved for nodes requiring guaranteed bandwidth [n = 0].

802.15.4 MAC

BeaconLess



- An asymmetrical channel access mode for asymmetrically powered devices
- Textbook case is wireless light switch operating a lamp
  - Lamp has mains power and therefore can be in near-constant receive mode
  - Switch is battery powered, stays in standby until pressed by user, when it transmits
- Unslotted CSMA-CA

802.15.4 MAC Traffic Types

- Periodic data
  - Application defined rate (e.g. sensors)
  - *Can be handled using beaconing*
- Intermittent data
  - Application/external stimulus defined rate (e.g. light switch)
  - *Can be handled in beaconless mode or disconnected fashion*
- Repetitive low latency data
  - Allocation of time slots (e.g. mouse)
  - *Guaranteed Time Slot (GTS) can be allocated by PAN Coordinator only in a Star Topology*

802.15.4 MAC

MAC Primitives

MAC Data Service

- MCPS-DATA – exchange data packets between MAC and PHY

MAC Management Service

- MLME-ASSOCIATE/DISASSOCIATE – network association
- MLME-SYNC / SYNC-LOSS - device synchronization
- MLME-SCAN - scan radio channels
- MLME-GET / -SET– retrieve/set MAC PIB parameters
- MLME-START / BEACON-NOTIFY – beacon management
- MLME-POLL - beaconless synchronization
- MLME-GTS - GTS management
- MLME-ORPHAN - orphan device management
- MLME-RX-ENABLE - enabling/disabling of radio system

Channel Scan

- Energy Detection Scan
  - ED in each of the logical channels specified
- Active Channel Scan
  - Sends a Beacon Request Command in each of the logical channels specified and memorizes the (possible) received PAN descriptors
- Passive Channel Scan
  - Search for beacons in each of the logical channels
- Orphan Channel Scan
  - Sends a “Orphan Notification Command” and waits for a “coordinator realignment command”

Summary of 802.15.4

- Data rates of 250 kb/s (2.4 GHz) , 40 kb/s (915 MHz) and 20 kb/s (868 MHz)
- 16 channels in the 2.4GHz ISM band, 10 channels in the 915MHz ISM band 1 channel in the European 868MHz band
- Star or Peer-to-Peer network topologies supported
- Designed for controllers, sensors, remote monitoring and portable electronics with selectable latency
- Support for low latency devices (Guaranteed Time Slots in Star Networks)
- Multi-level security
  - Access control
  - Data Encryption
  - Frame integrity
  - Sequential Freshness
- CSMA-CA channel access slotted (beacon) and unslotted (beaconless)
- Beaconless operation available
- Dynamic device addressing.
- Fully handshaked protocol for transfer reliability.
- Low power consumption via extremely duty cycle capability

ZigBee name origin

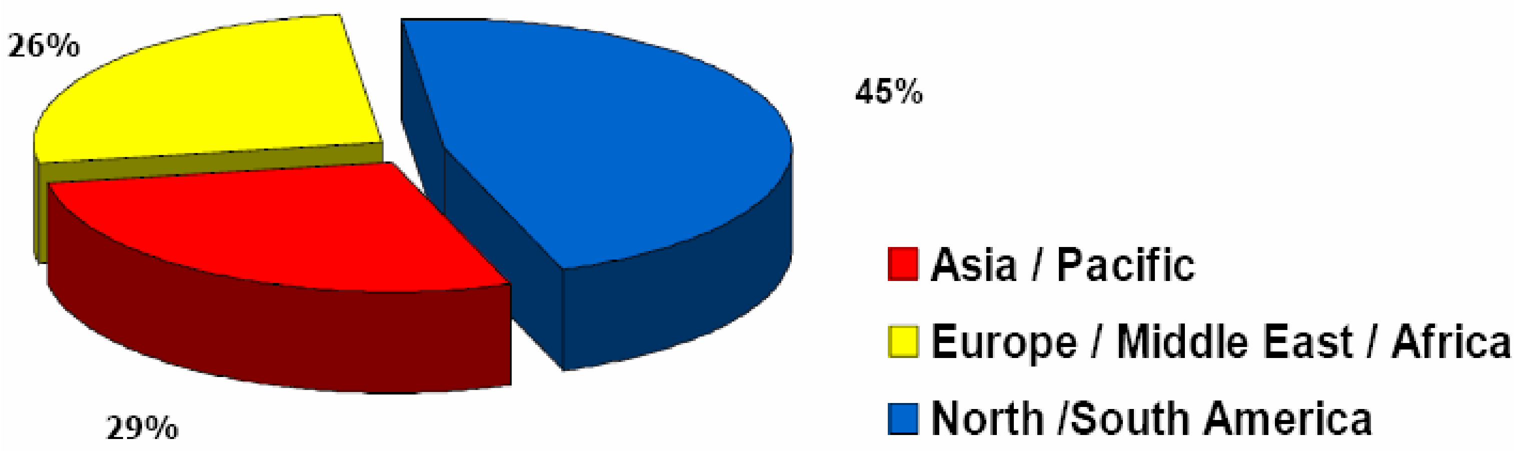
- **ZigBee Principle**
  - Hive's members hierarchically structured
    - a queen, few male drones, and thousands of worker bees
  - The technique used by honey bees to communicate new-found food sources to other members of the colony
    - The bee dances in a zig-zag pattern, sharing information such as the location, distance, and direction of a newly discovered food source

Zigbee Organization

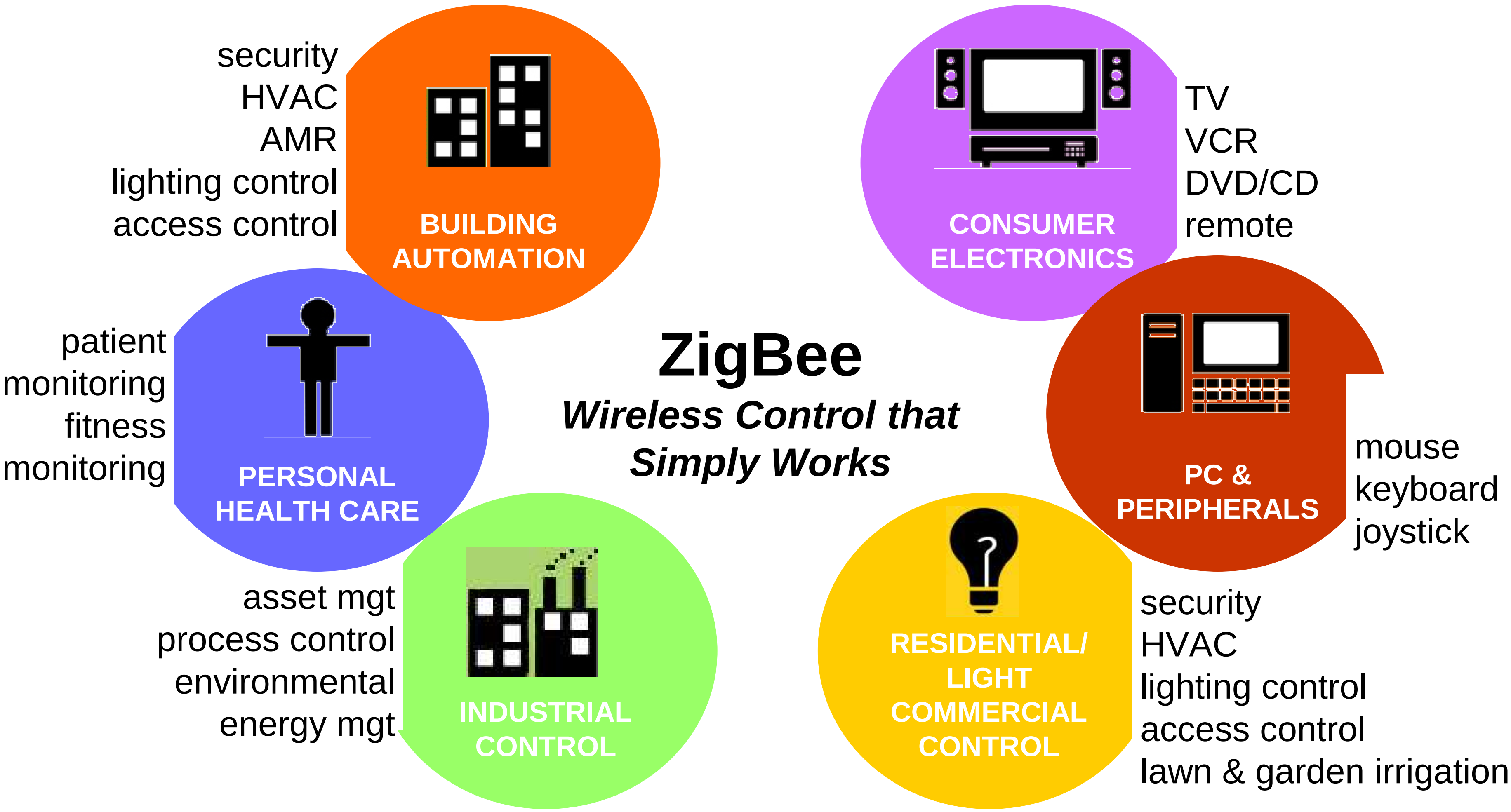
- It's NOT a IEEE standard but a consortium of industries promoting low data rate communication markets
- 8 promoter companies
  - Philips (that holds the brand), Ember, Freescale, Honeywell, Invensys, Mitsubishi, Motorola, Samsung
- Participant list
  - Rapid growling (188 members till now)
  - Industry leaders worldwide committed to provide ZigBee compliant products and solutions
  - include semiconductor manufacturers (**STMicroelectronic too**), wireless IP providers, OEMs and end users
- Version 1.0 of the specification has been ratified in december 2004
- Primary Drivers
  - Low data rate; Simplicity and Low cost; Long battery life; Security and reliability; Networking capabilities (Star, cluster tree and mesh topologies) Interoperable application profiles

Zigbee Member Geographical Distribution

Region (based on primary contact address)	Dec. 2003	Dec. 2004	Dec. 2005	Mar 2006
Asia / Pacific	12 (19%)	21 (19%)	49 (27%)	53 (29%)
Europe / Middle East / Africa	14 (22%)	35 (31%)	52 (28%)	48 (26%)
North/South America	37 (59%)	57 (50%)	84 (45%)	87 (45%)
Total Member Companies	63	113	185	188 With 9 pending

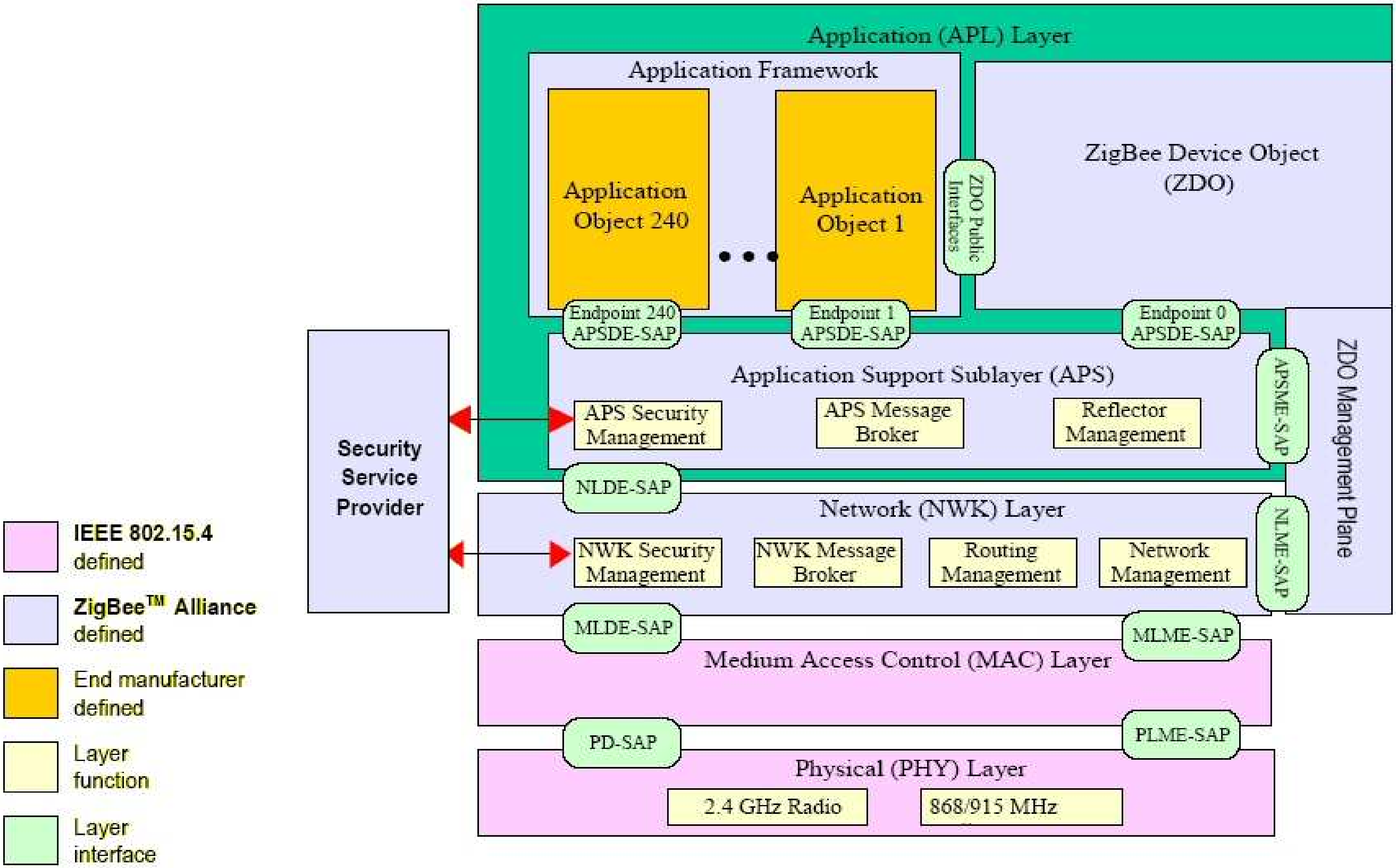


Zigbee Applications



Source: Zigbee

The ZigBee Stack Architecture



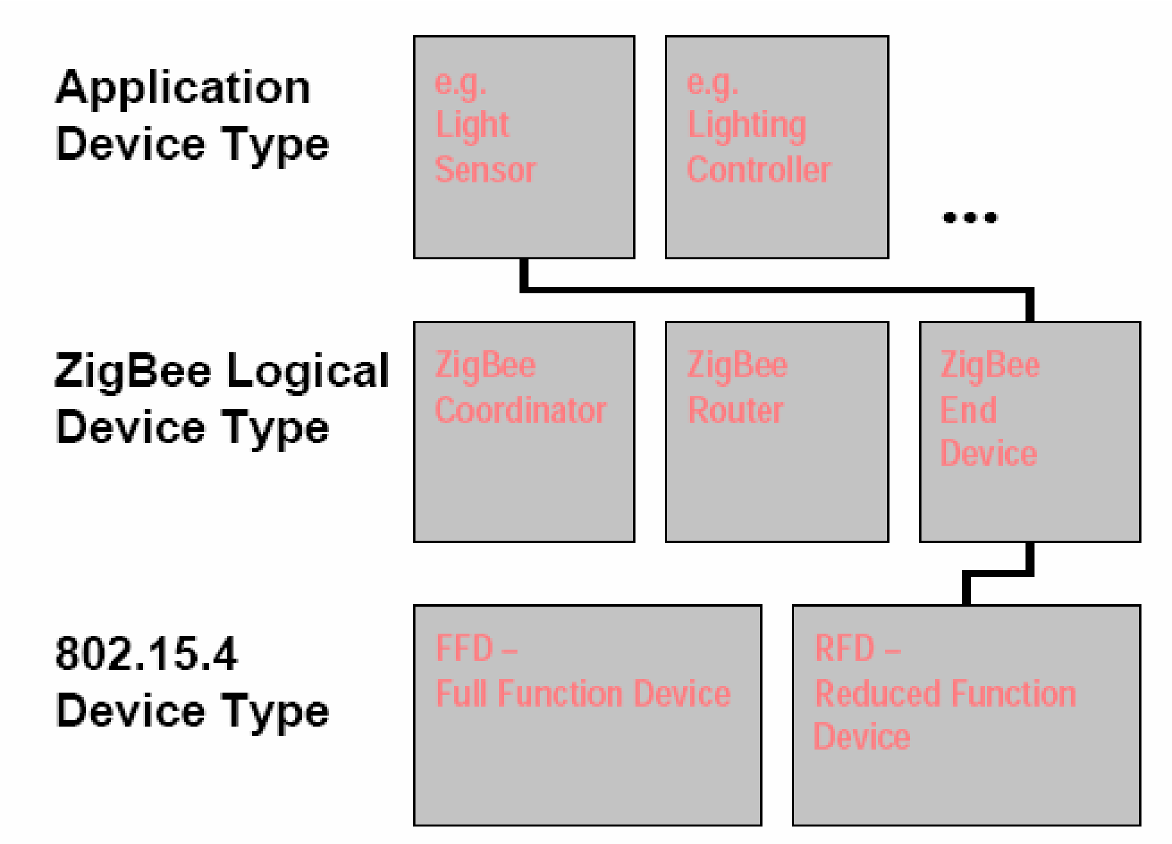
Network Layer Fundamentals

- Uses three different kind of logical devices
- Contains functionalities for
  - Starting a network
  - Joining or leaving a network
  - Addressing
    - Ability of the Zigbee coordinator to assign short (16 bit) address to nodes
  - Data Routing to destination
    - Cluster tree routing
    - After route discovery and maintenance (cost metric based on link quality and hop counts)
  - Security

Application Layer Fundamentals

- Consists of
  - Application Framework (AF)
    - Hosting the manufacturer-defined application objects
    - Providing two data services (Key Value Pair or Messages)
    - Management via ZDO public interface
  - Application Support Sub-layer (APS)
    - Maintaining table for binding (the ability to match two devices together based on their services and their needs) (APSME management services)
    - Forwarding messages between endpoints of bound devices (remote for coordinator) (APSDA data services)
    - Its services are used by the ZDO and by the application framework objects
  - Zigbee Device Object (ZDO)
    - Defining the role of the devices (coordinator, router, end devices)
    - Initiating and or responding to binding requests
    - Establishing a secure relationship between devices
    - Discovering devices and determining which application services they provide
    - Its services are used by the application objects

Zigbee Devices Type Model



Distinguishes the type of device from an end user perspective

Distinguishes the logical device types deployed in a specific Zigbee network

Distinguishes the type of Zigbee hardware Platform

Zigbee Logical Device: Coordinator (ZC)

- One and only one required for each ZigBee network
  - First one on the scene
- Initiates network formation
  - Selects the time and place (Channel, PANId, Stack Profile)
- Acts as IEEE 802.15.4 PAN coordinator (FFD)
- Also performs as router once network is formed
- Not necessarily a dedicated device can perform an application too
- One extra function: Acts as Bind Request Controller

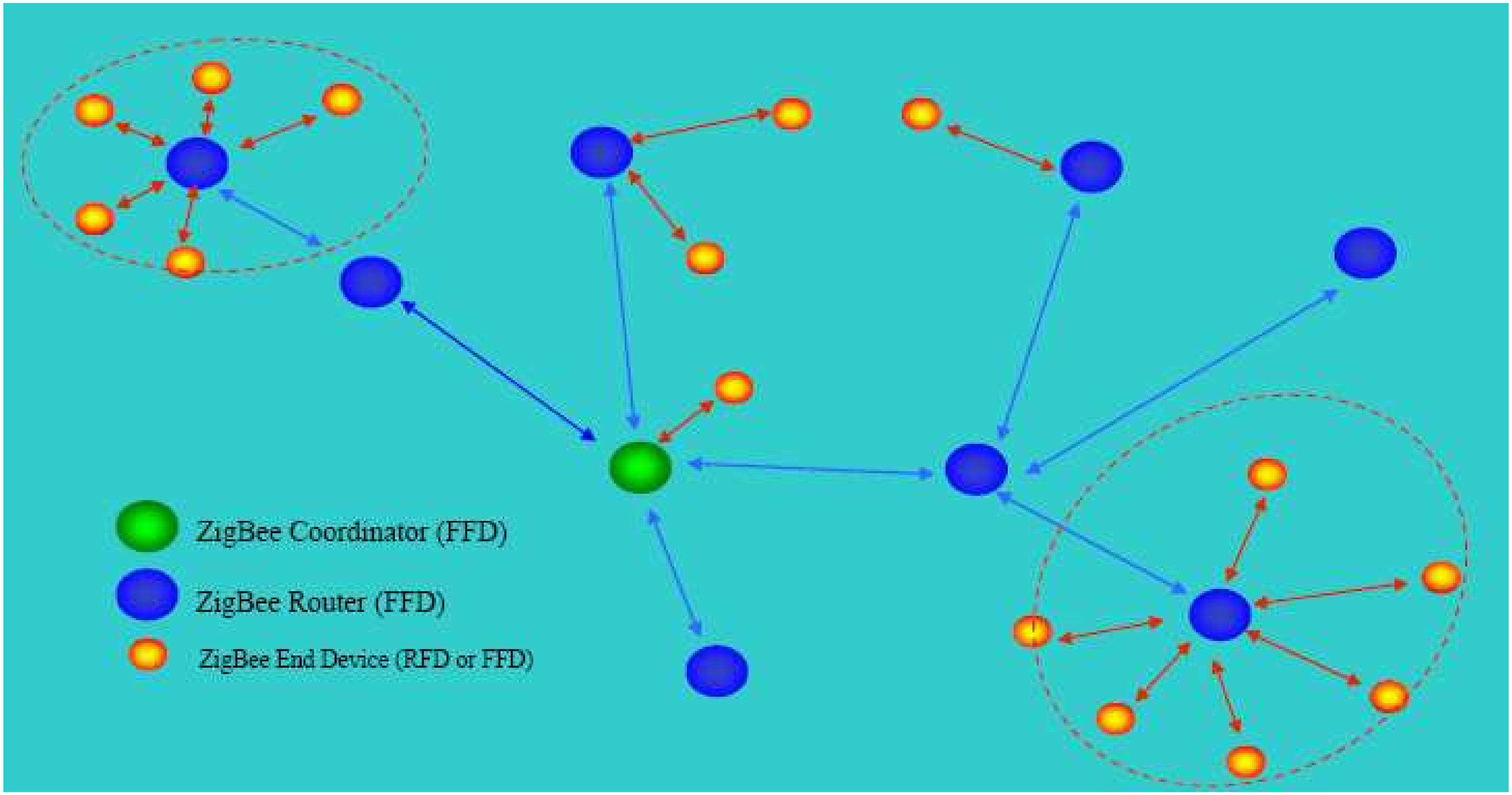
Zigbee Logical Device: Router (ZR)

- Optional network component
- Discovers and associates with ZC or ZR
  - Extends the network coverage
- Acts as IEEE 802.15.4 coordinator or device (FFD)
- Manages local address allocation / de-allocation
- Participates in multi-hop / mesh routing of messages.
- Maintains Neighbor Table to allow Neighbor Routing

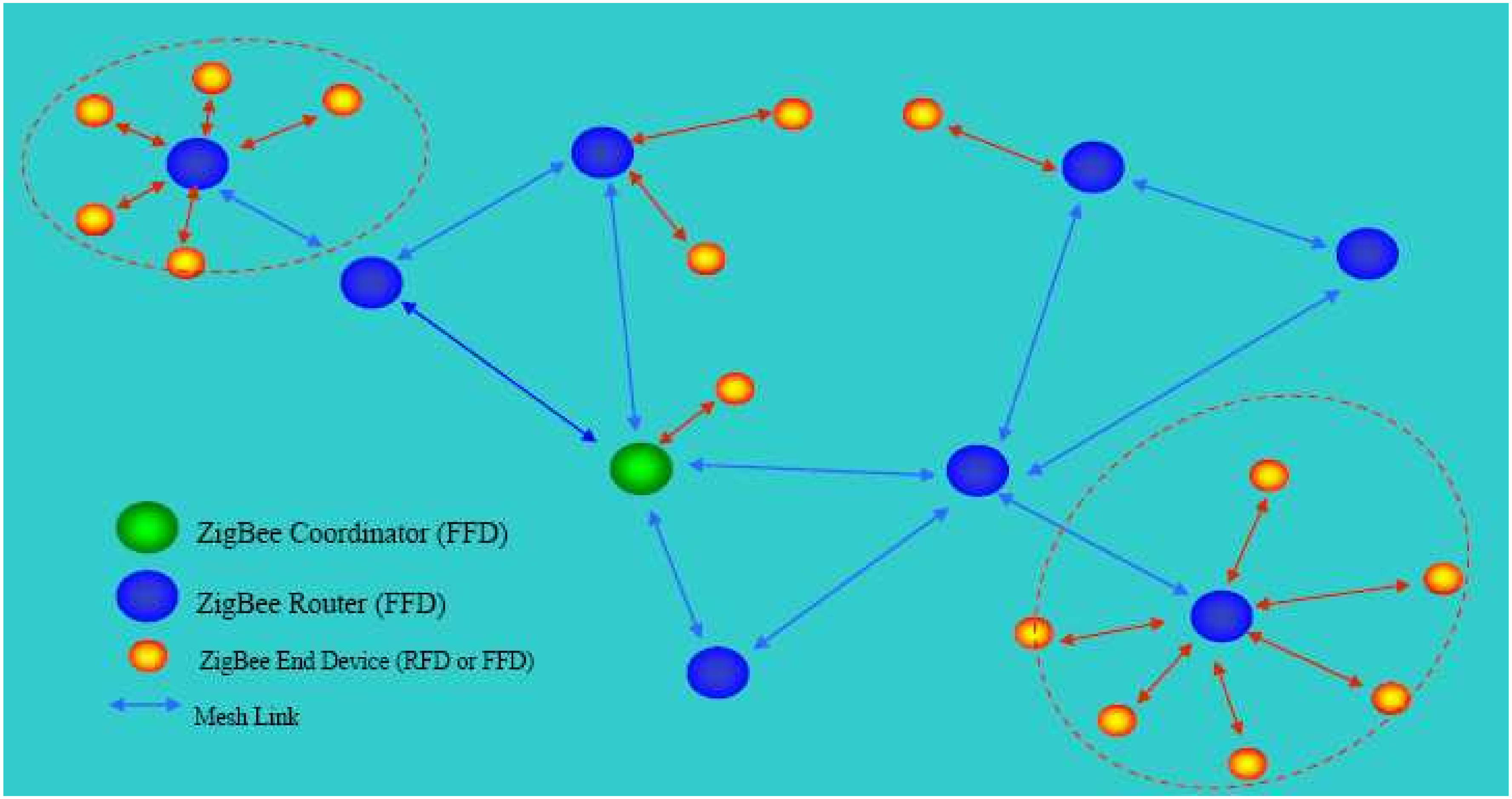
Zigbee Logical device: End Device (ZED)

- Optional network component
- Discovers and associates with ZC or ZR
- Acts as IEEE 802.15.4 device (RFD)
- Can be optimized for very low power operation
- Relies on its parent to let it sleep
- Shall not allow association
- Shall not participate in routing

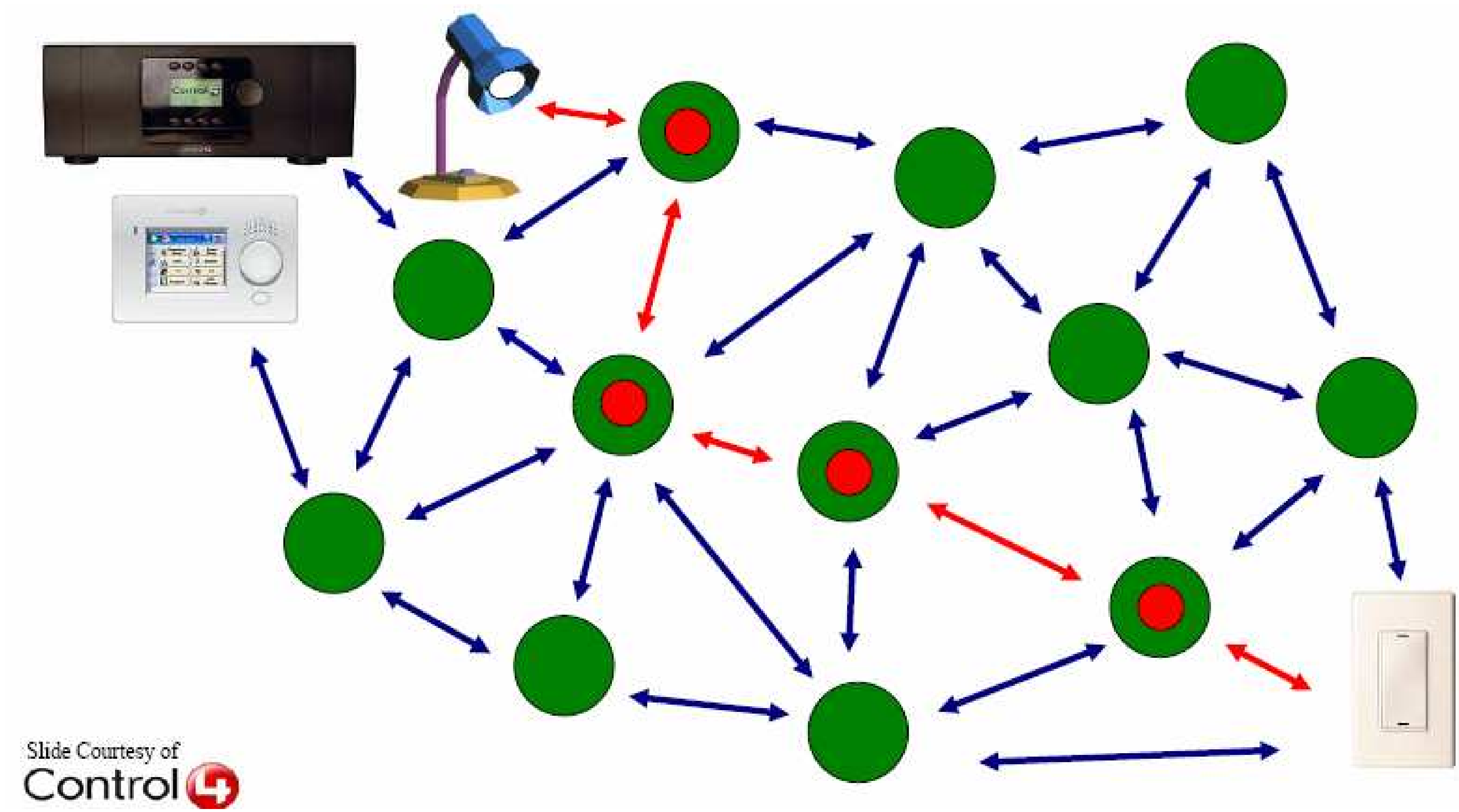
Zigbee Network Communication Model (Cluster Tree)



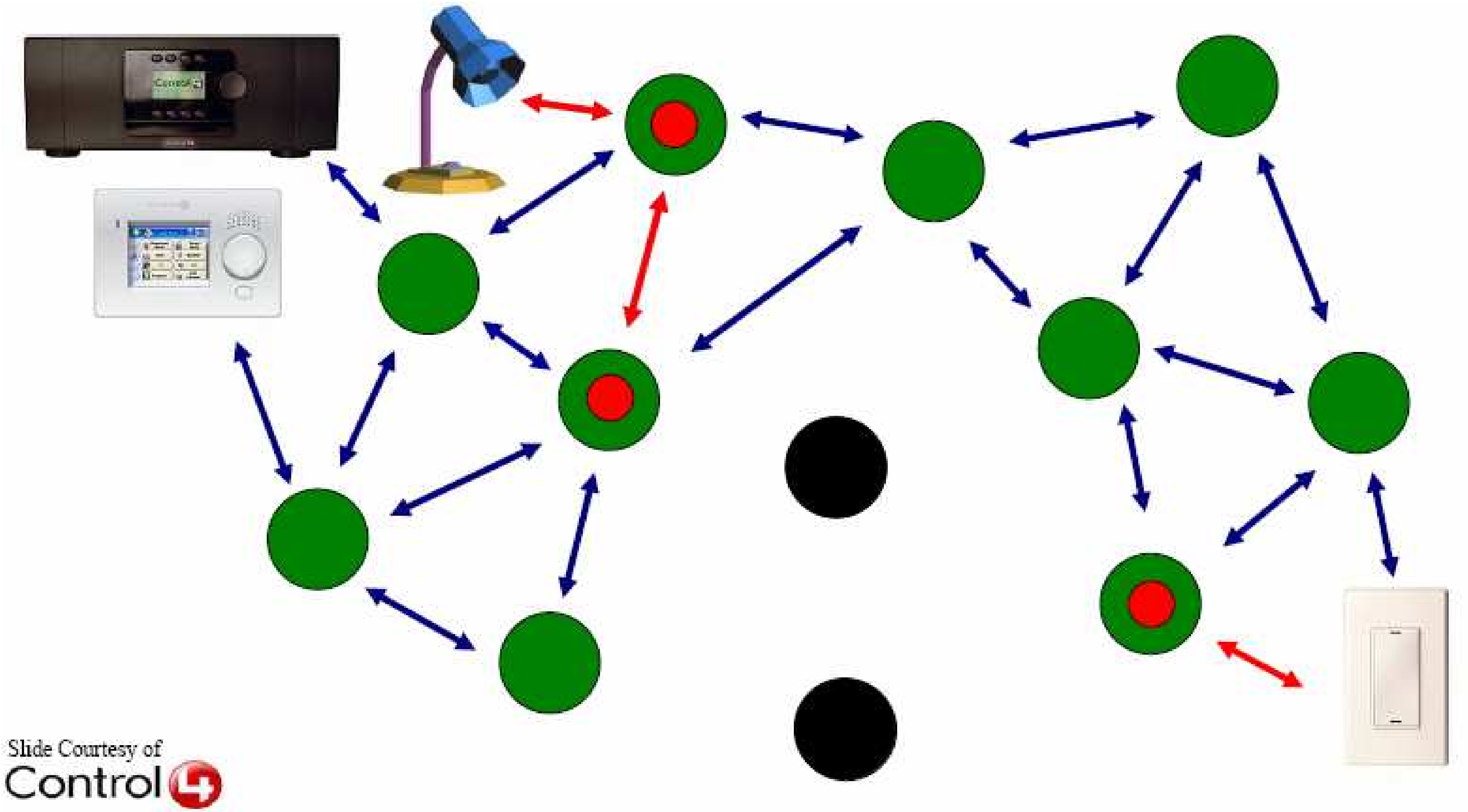
Zigbee Network Communication Model (Mesh)



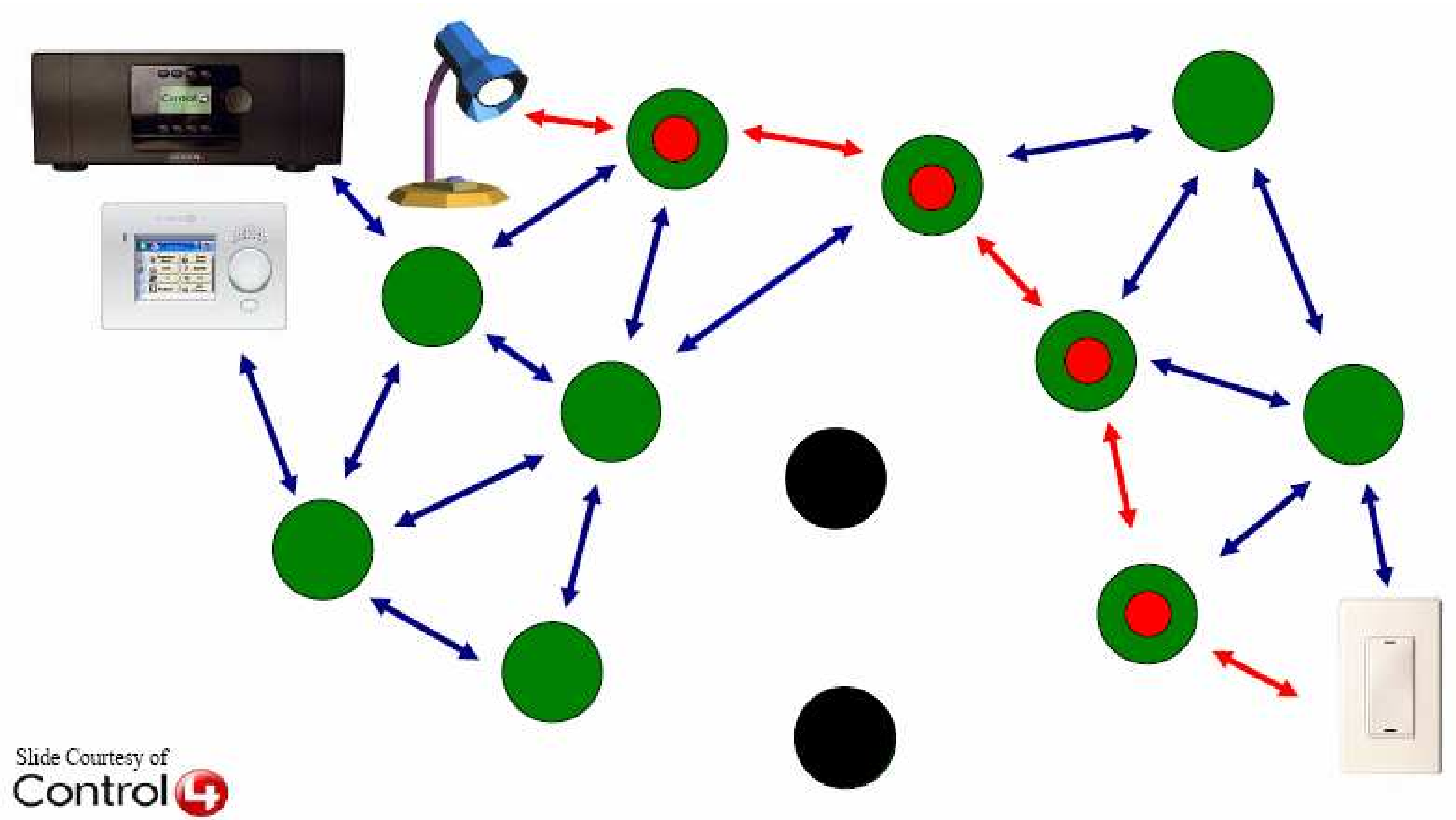
Mesh Behavior



Mesh Behavior



Mesh Behavior



Architecture: Stack Profile

- A Stack Profiles Defines
  - Network Topology
  - Application Services
  - Device Compatibles
  - Security Services
  - And many more
    - Table sizes
    - Timeouts
    - Route Cost Calculation Algorithm

Current stack profiles:

- Home Controls (mesh)
  - Supports Home Controls Lighting and Home Automation application profiles
- Commercial, Industrial and Institutional (mesh)
  - Supports Commercial Building Automation, HVAC and Industrial Plant Monitoring application profiles
- Stack profile identifier supplied in beacon payload. Devices join appropriate networks supporting desired stack profile.

Network Initiation: ZC

- NLME_NETWORK_FORMATION.request
- Performs an Energy Detect Scan
  - Looks for other wireless devices on the channel
- Performs an Active Scan
  - Looks for other 802.15.4 networks on the channel
- Selects the *"nicest"* channel
  - Weights up channels based on noise level and PANs
- Selects an unused PANId
- Starts a network

Network Discovery: ZR and ZED

- NLME_NETWORK_DISCOVERY.request
- Performs an Active Scan
  - Looks for other ZigBee networks on the channel
- Selects a compatible network
  - Based on Stack Profile ID matching

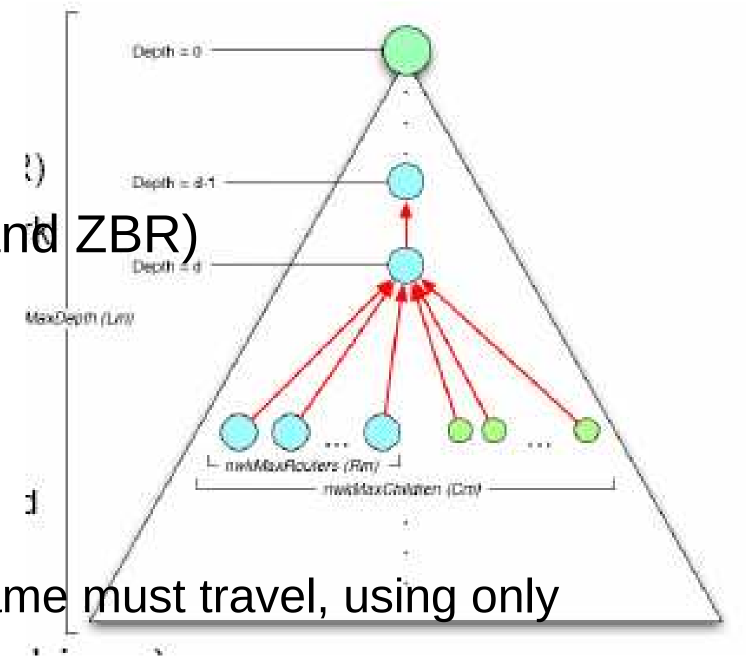
Network Association: ZR & ZED

- NLME_JOIN.request
- Selects the highest acceptable router
  - Link Quality, with addressing capacity
- Associates with the router
- Allocated an address on the network
- Device authenticates with network

Network Association: ZR (cont)

- NLME_START_ROUTER.request
- Updates Beacon Payload
  - Depth, Address Capacity
- Starts a router
- Updates Association Permit Status

Distributed Address Assignment



- Target
  - Addresses Distributed assignment (by ZBC and ZBR)
  - Unique address within a particular network
  - Tree topology support
- Features
  - Every device has an associated depth
    - the minimum number of hops a transmitted frame must travel, using only parent-child links, to reach the ZBC
- ZBC tuning knobs (application-driven defined by the Stack Profile)
  - nwkMaxDepth: maximum depth – **Lm**
  - nwkMAxChildren: maximum number of children for each parent - **Cm**
  - nwkMAxRouters: maximum number of routers for each parent - **Rm**

Addressing: Tree structured Address Assignment

- CSkip based address assignment
- Address determined from tree location
- For each ZBR is assigned an address sub-block
  - Its size, ***Cskip,*** depends on the ZBR's depth

$$Cskip(d) = \begin{cases} \dfrac{1 + Cm - Rm - Cm \cdot Rm^{Lm-d-1}}{1 - Rm} & if\ Rm \neq 1 \\ 1 + Cm \cdot (Lm - d - 1) & if\ Rm = 1 \end{cases}$$

- Only ZBR with Cskip(d) > 0 shall accept child devices
- Different address's assignment mechanisms for the children if they are router-capable device or not.

Address Assignment

- ZBC's network address is *0*
- Given a ZBR *K* with the assigned address *Aparent* at depth *d*
  - For rth router-capable child device of *K*
    - $Achild = Aparent + r \times Cskip(d) + 1$ with $0 <= r <= (Rm-1)$
  - For nth end child device of *K*
    - $Achild = Aparent + Cskip(d) \times Rm + n$ with $1 <= n <= (Cm-Rm)$

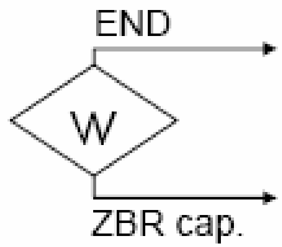
Address Assignment Example

nwkMAxChildren = 8

nwkMaxRouters = 3

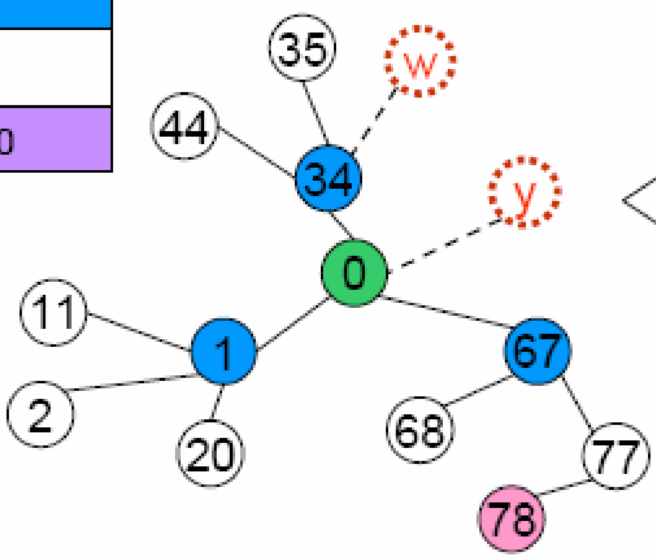
nwkMaxDepth=3

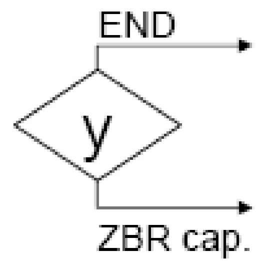
Depth	Cskip
0	33
1	9
2	1
3	<0



$$Aw = Aparent + Cskip(d) \cdot Rm + n = $$
$$= 34 + 9 \cdot 3 + 1 = \mathbf{62}$$

$$Aw = Aparent + r \cdot Cskip(d) + 1 = $$
$$= 34 + 2 \cdot 9 + 1 = \mathbf{53}$$





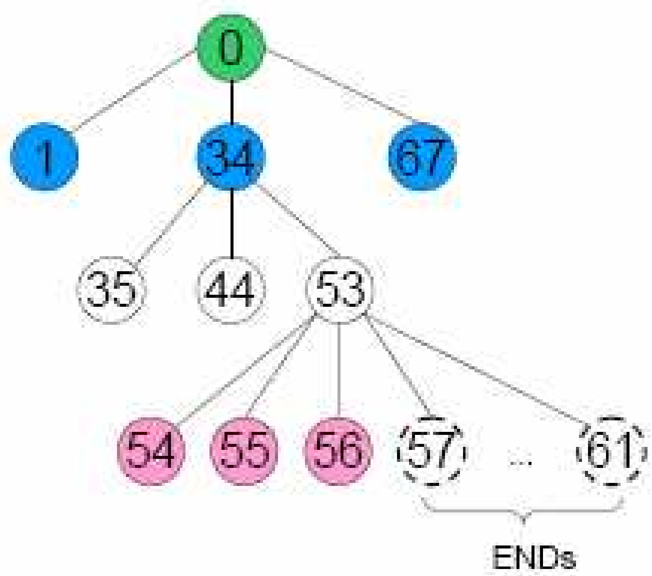
$Aw = 100$

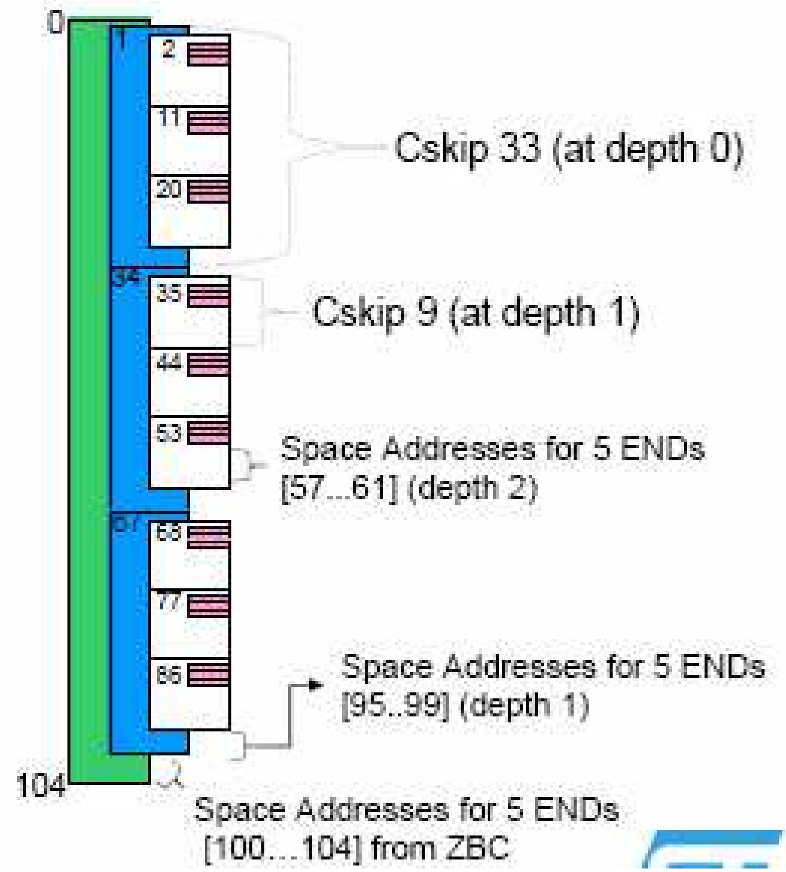
None ZBR address free

Affiliate with another ZBR or as END

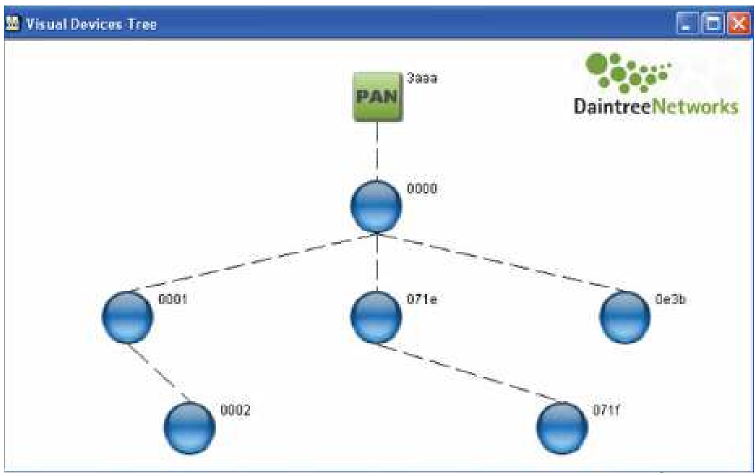
Address Assignment Example

nwkMAxChildren = 8
nwkMaxRouters = 3
nwkMaxDepth=3

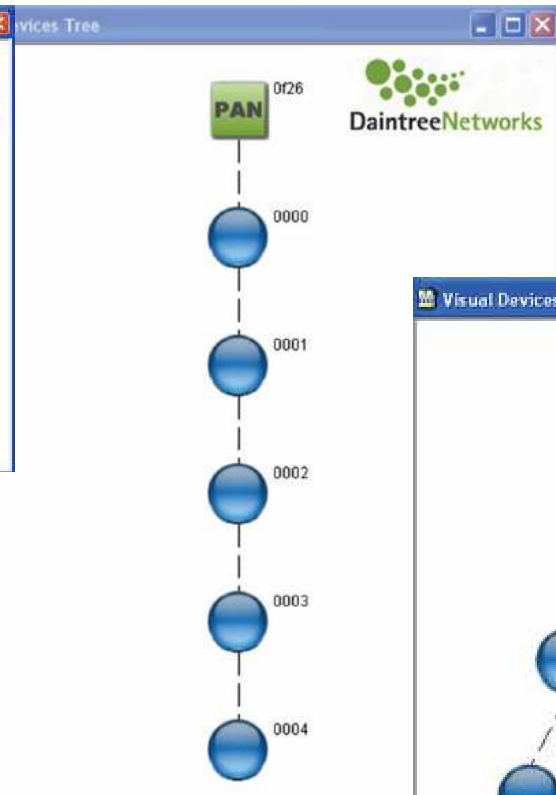




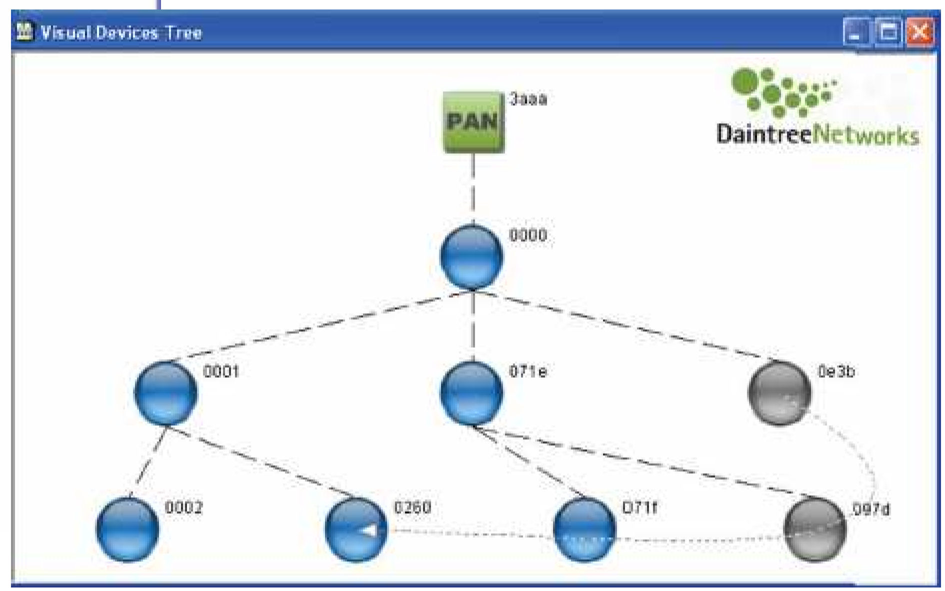
Network Topologies (Examples)



- nwkMaxDepth=7
- nwkMaxChildren=5
- nwkMaxRouters =3



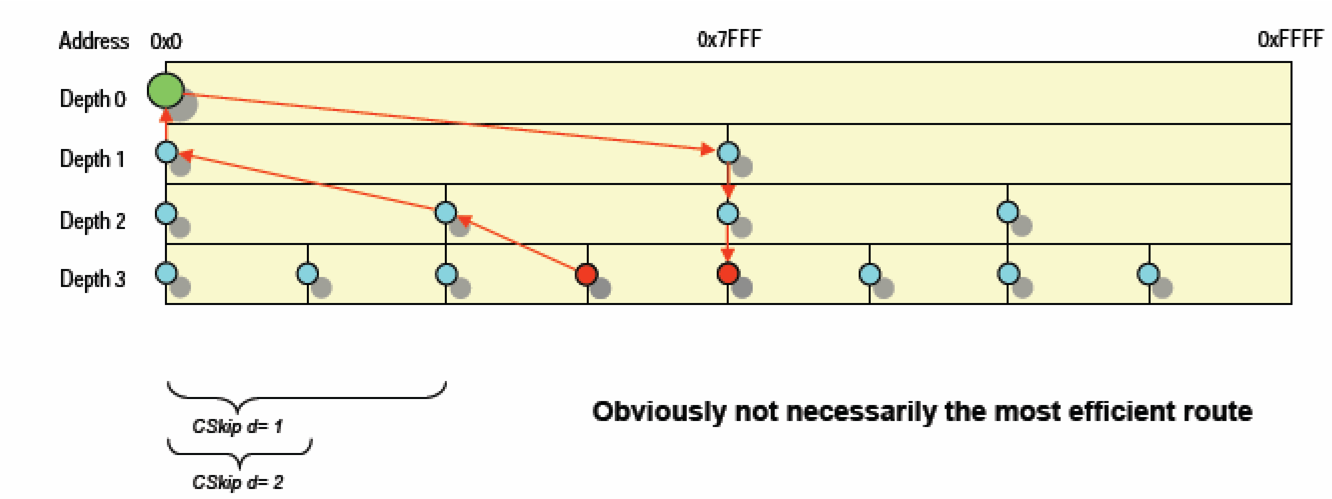
- nwkMaxDepth=10
- nwkMaxChildren=1
- nwkMaxRouters =1



- Reassociations causing Topology Changes

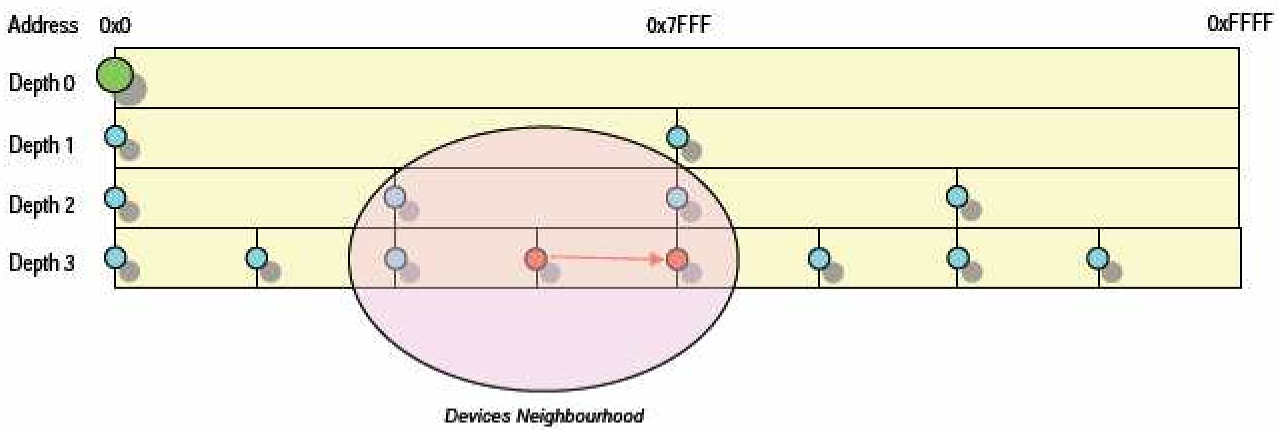
Tree Routing

- The address tells you where the destination is
- Simple equation gives ‘route up’ or ‘route down’
- If *LocalAddr< DestAddr< LocalAddr+ CSkip(d-1)* Route Down
- Else Route Up



Neighbour Routing

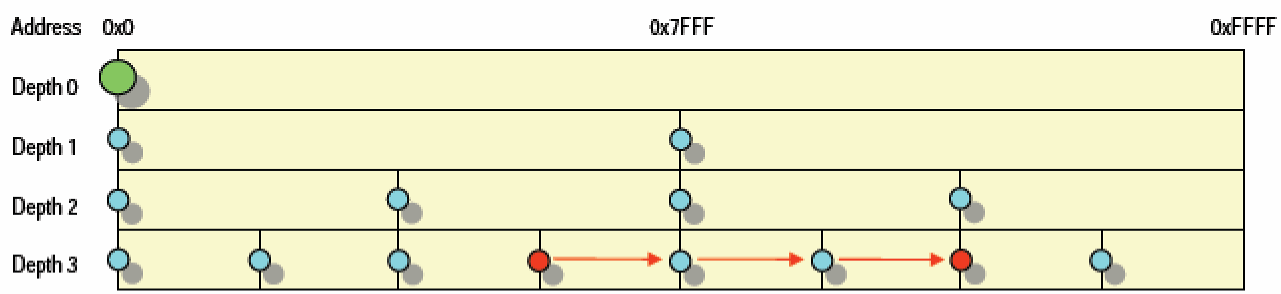
- A ZC or ZR maintains a table of devices in its neighbourhood
- If the target device is physically in range it can send the message directly.



But what happens if the destination is not in the local neighbourhood?

Mesh Routing

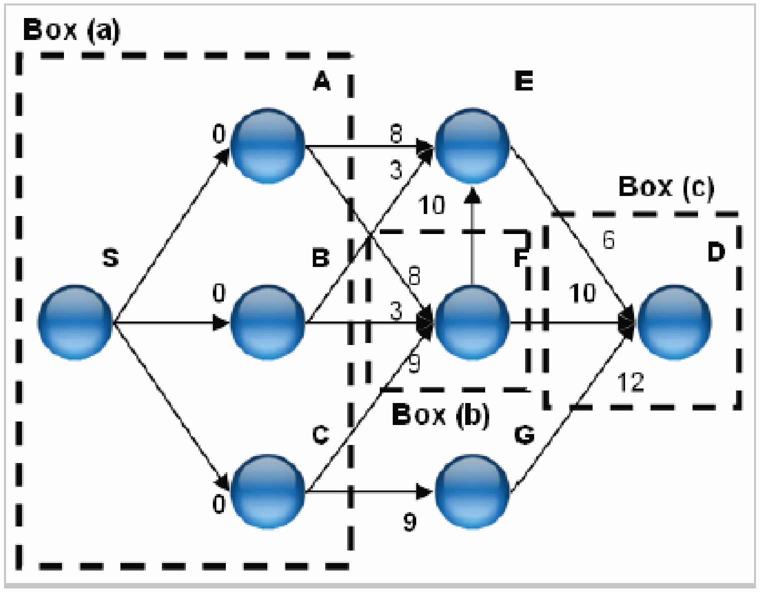
- ZC or ZR maintains a routing table of next hop addresses
- If the target device has a routing table entry then the message can be sent using this route.



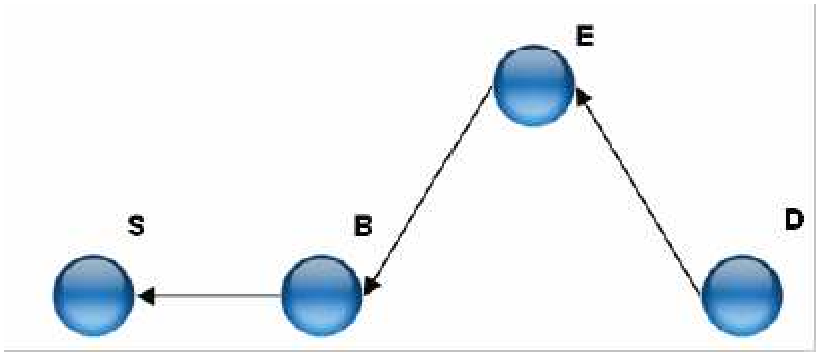
That's great, but where do the routing table entries come from?

Routing: Route Discovery

- Route discovery uses AODV routing algorithm
  - Route Request broadcast message
  - Route Reply unicast message
- Potential routes are evaluated with respect to a routing cost metric in both directions (source to destination and viceversa).
  - Link Cost (probability to deliver a packet along a link) & Path Cost (sum of Link Costs along a multihop way)



Route Request



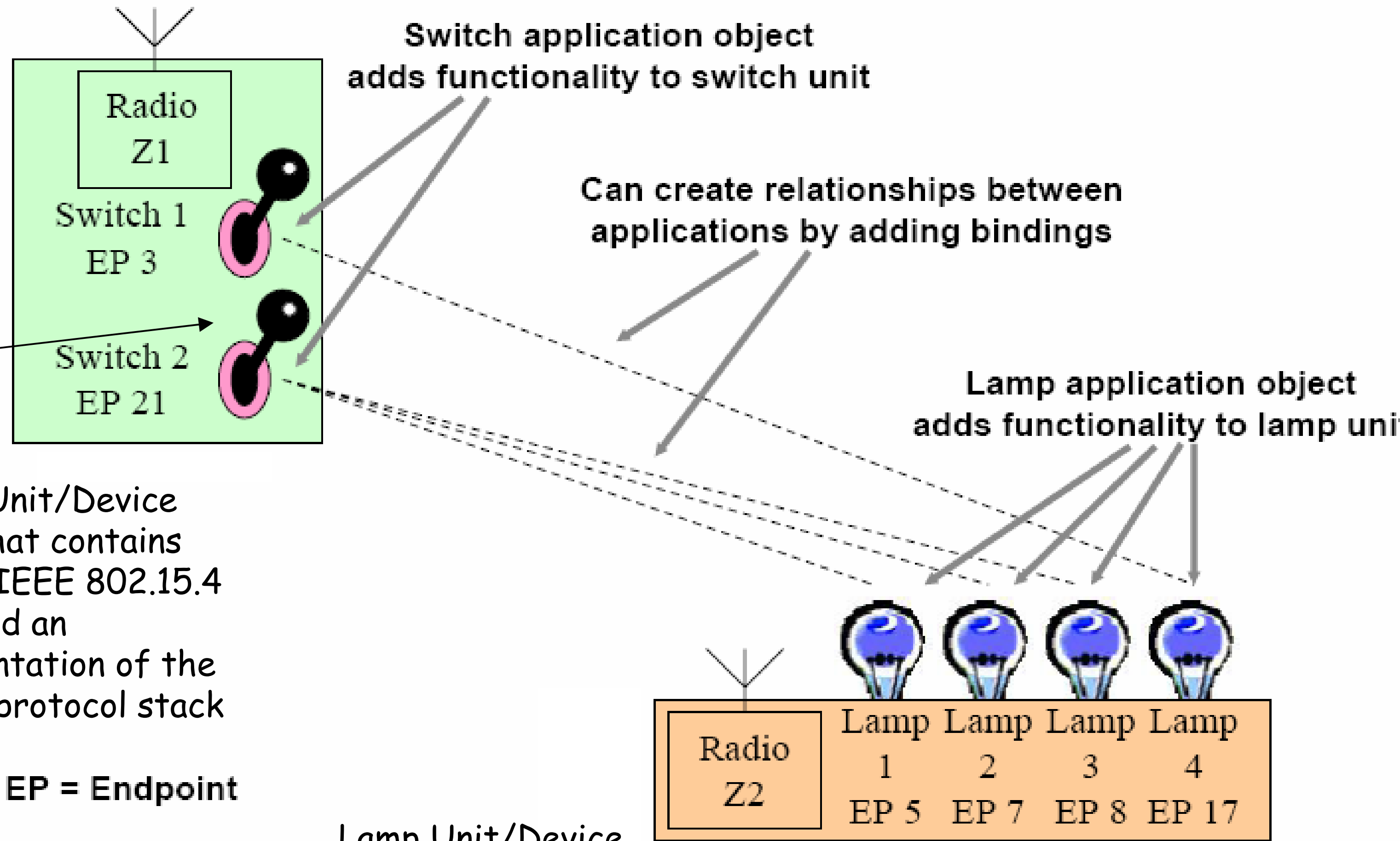
Route Response

To Summarize the Network Layer

- Has 3 device types; ZC, ZR and ZED
- Performs network discovery and formation
- Performs address allocation
- Performs message routing
- Configured by the stack profile
- Provides network wide security
- Allows low power devices to maximize their battery life

ZigBee turns 802.15.4 into a low power multi-hop mesh network.

Application Overview: Addressing and Binding



Component/
SubUnit
Consists of a
physical
object

Switch Unit/Device
entity that contains
a single IEEE 802.15.4
radio and an
implementation of the
ZigBee protocol stack

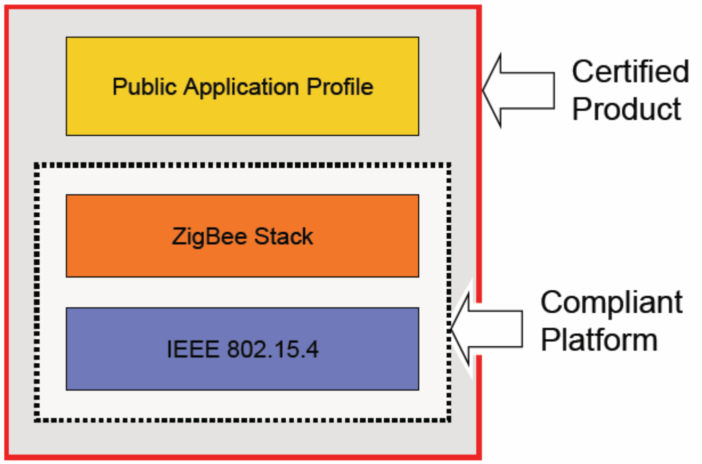
EP = Endpoint

Lamp Unit/Device

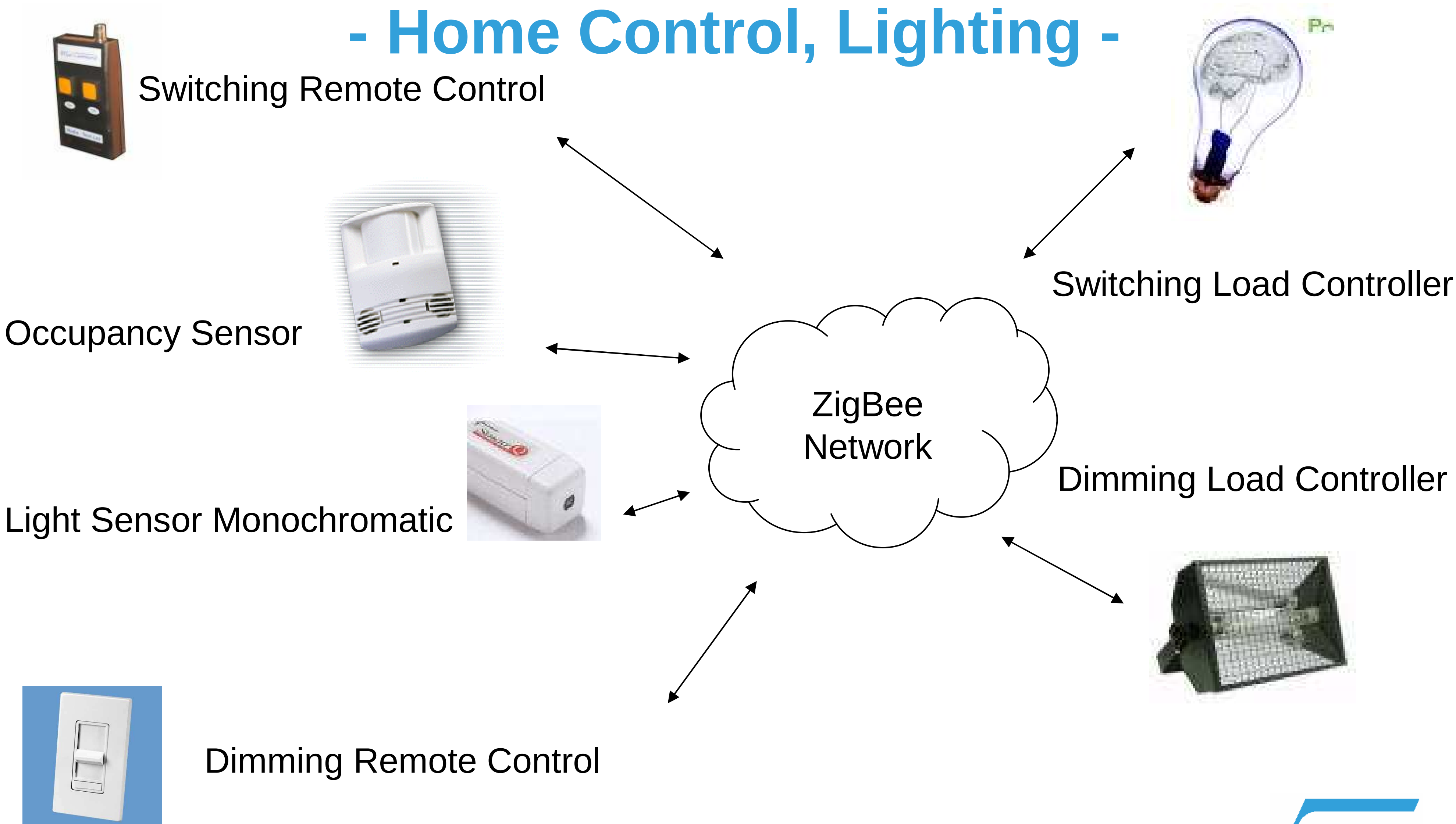
Each node is given a 16-bit **short address** when it joins the ZigBee network
For each Node there can be more **subunits**

Application Profiles

- Application Profiles
  - are an agreement on a series of messages defining an application space (for example, “Home Controls-Lighting”)
  - Define compatible sets of devices for specific market areas
  - It’s identified by a Profile identifier that is uniquely assigned by the Alliance
  - Defines
    - Device and Cluster descriptions
    - Service types (KVP or MSG)
- Public (Standard)
  - Fully Defined and ratified by the Zigbee Alliance through the Application Framework Working Group (AFG) and a Profile Task Groups (PTG)
  - ZigBee certified products
- Non-Public (Private)
  - Profile ID issued by the ZigBee Alliance, However the details of The profile are not necessarily made public by the vendor



An example of Application Profile
- Home Control, Lighting -



Current and Future Profiles

Current Profiles

- Commercial building automation
  - Complete building control, monitoring and energy management
- Heating, ventilation, air conditioning
  - HVAC systems for improved efficiency and lower installation cost
- Home automation
  - Low to high end residential systems for control of devices around the home
- Home control, lighting (example, included in ZigBee specification)
  - Residential lighting control allowing basic control and dimming
- Industrial plant monitoring
  - Monitoring time varying attributes related to operating environment and machinery conditions
- Wireless sensor applications
  - Environmental monitoring, asset tracking and structural monitoring

Future Standard Profiles

- Telecom applications
  - File/data transfer
  - Applications controllers
- Automatic Meter Reading
  - Residential & commercial utility systems
- Medical & personal health care
  - Body area networks
  - Fitness monitoring: home, gym, on-the-move
  - Patient monitoring
- Automotive
  - In vehicle control: vehicular & entertainment
  - Status monitoring
- Others identified by ZigBee members

Clusters/Attributes

- For each Profile Identifier there are:
  - A pool of device descriptions described by a 16-bit value
  - A pool of cluster Identifiers described by an 8-bit value
    - Each Cluster Identifier supports a pool of attributes described by 16-bit value
- Cluster
  - is a container for one or more attributes
  - is identified by **Cluster Identifier**, unique within the scope of each profile (Application Domain segment)
  - for each device description there is one or more ClusterID.
- Attribute
  - Is a data entity, which represents a physical quantity or state. The data is communicated to other devices using commands.

AF Frame Format

General frame format

Bits: 4	4	Variable	Variable	Variable
Transaction count	Frame Type	Transaction 1	...	Transaction n

Bits:8	Variable
Transaction seq. number	Transaction data

Enables an applications to manipulate attributes

KVP

Bits:4	4	16	0/8	Variable
Command type identifier	Attribute data type	Attribute identifier (KEY)	Error code	Attribute data

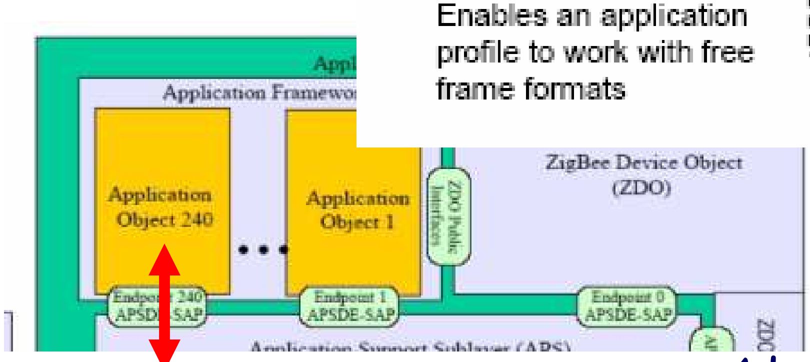
Set , Event
Get, Set and Event with ACK
Get, Set and Event response

Success, Invalid Endpoint, Unsupported attribute, Invalid command type,...

Enables an application profile to work with free frame formats

MSG

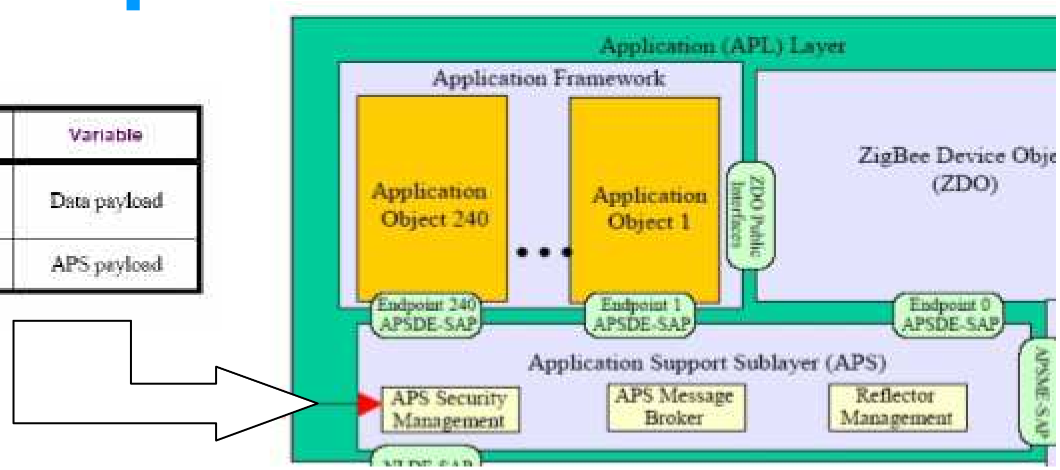
Bits:8	Variable
Transaction Length	Transaction data



Endpoints

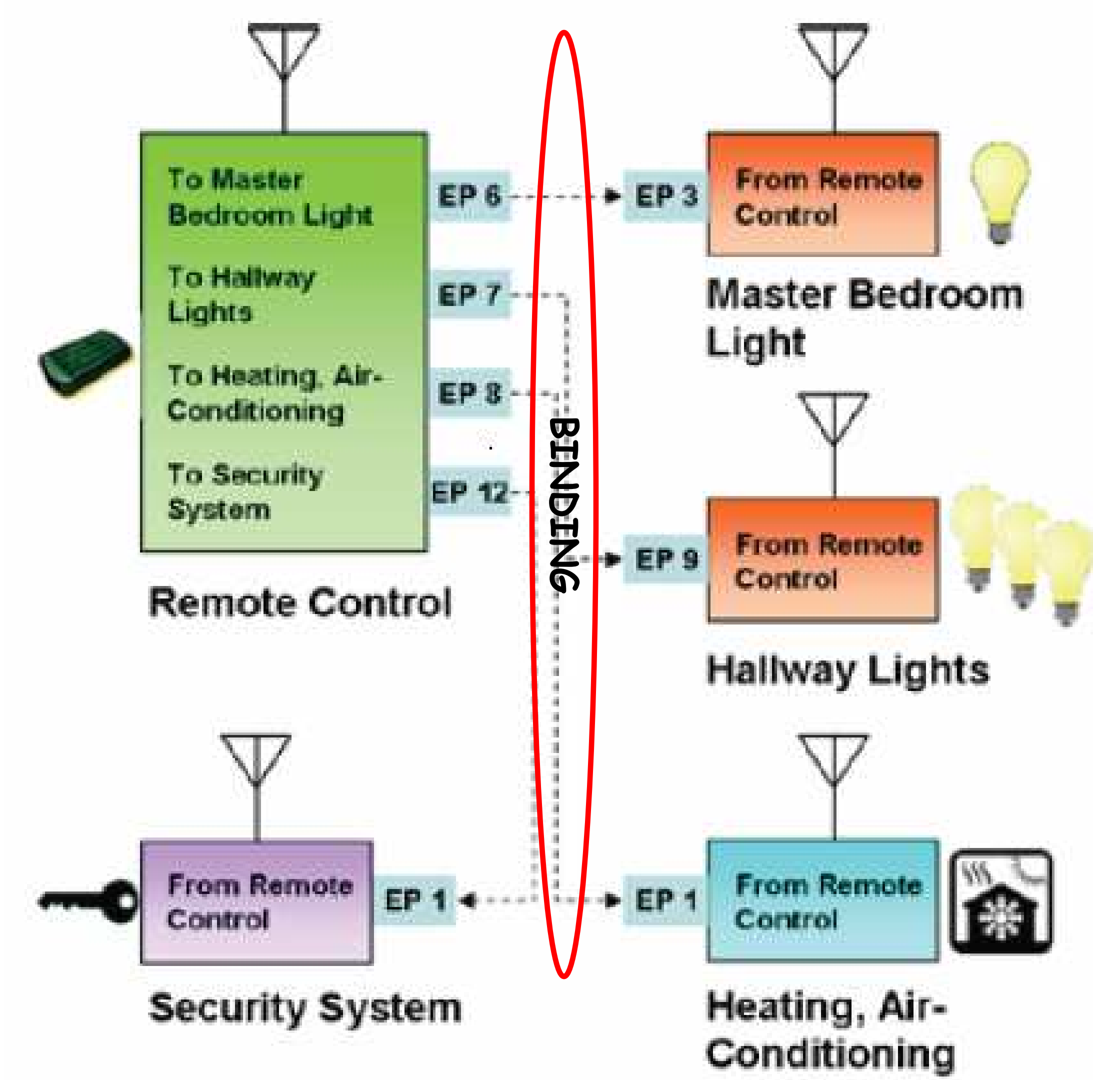
Octets: 1	0/1	1	0/2	1	Variable
Frame control	Destination endpoint	Cluster Id	ProfileId	Source endpoint	Data payload
APS header					APS payload

Data frame format



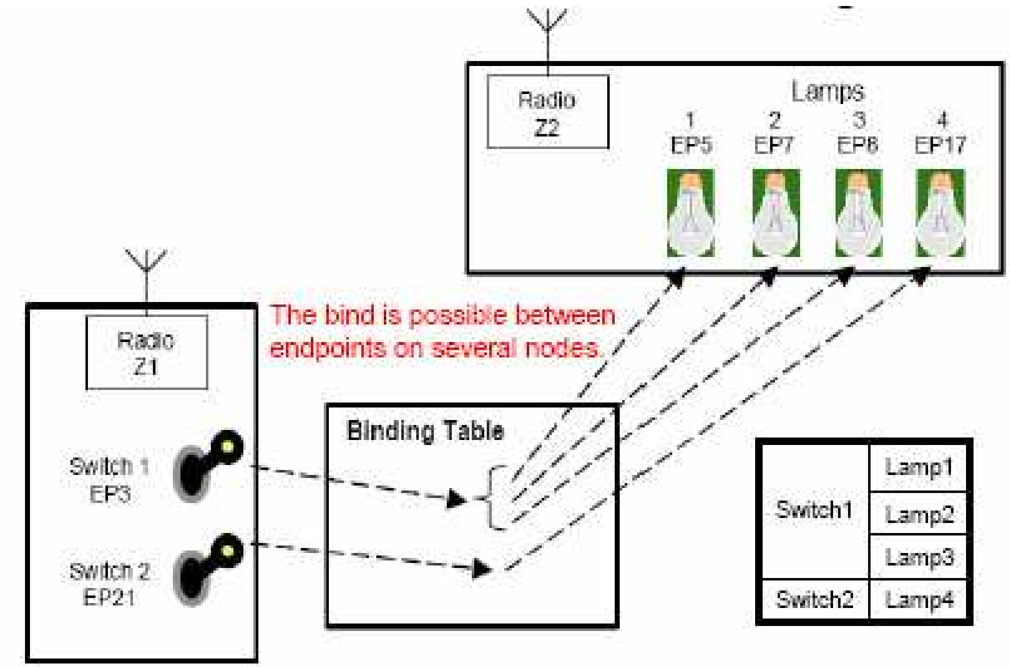
- Endpoints
  - Endpoints are a logical extension added to a single ZigBee radio which permits support for multiple applications, addressed by the Endpoint number (1-240)
  - To each subunit is assigned its own specified endpoint in the range [1-240]
  - The Endpoint 0x00 is reserved for device management (ZDO) and is used to address the descriptors in the node
  - The Endpoint 0xFF is used to address all active endpoints (broadcast endpoint) on a given node
  - For each endpoint there is a **Device Description**
    - Es. “the light sensor monochromatic”

Zigbee Scenario Example



Binding

- Logical links between complementary application devices and endpoints
  - Es. “Thermostat” binds with “furnace controller”.
- The binding table stores the information of clusters bounded among nodes.



1. Direct Binding (source binding)
   - Binding info in the source
2. Indirect Binding (Binding Cashing)
   - (Binding info in ZR o ZC)

Device and Service Discovery

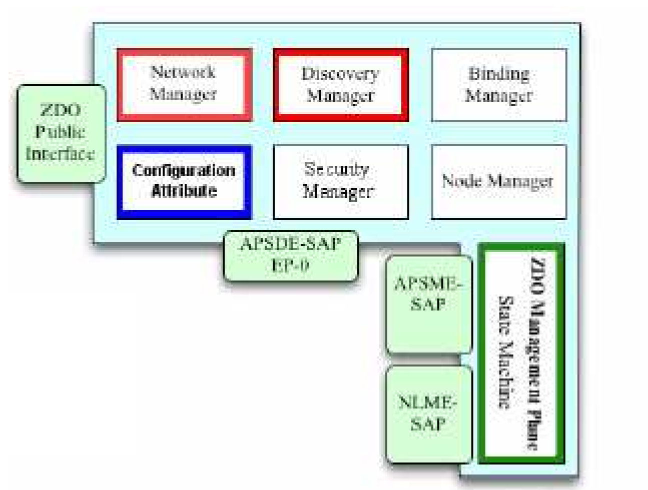
- Device discovery (other ZigBee device by query)
- Service discovery
  - Discovery of the services available on endpoints
    - By query for each endpoint on a given device
    - By using a match service feature (broadcast or unicast)
    - By having devices announce themselves
- Utilizes the complex, user, node, or power descriptors

ZigBee Descriptors

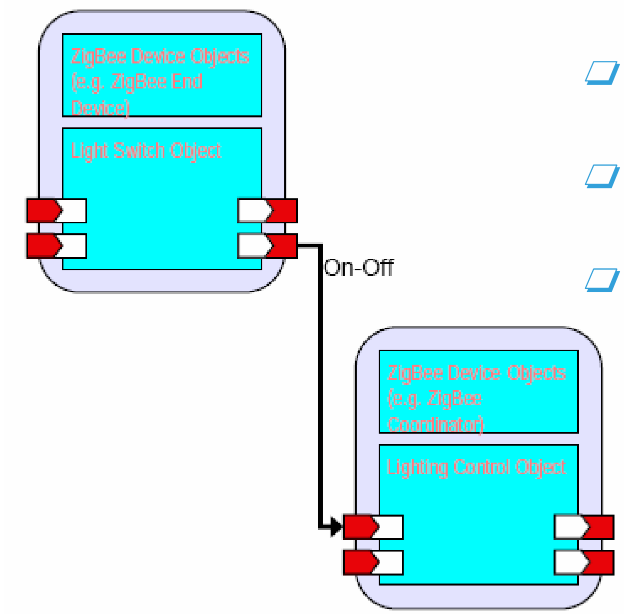
- Used to describe the ZigBee device
  - Mandatory
    - Node
      - Contains infos about the capabilities of the ZigBee node (one per device)
      - (Logical type, APS flag, frequency band, MAC flag, Manufacturer code, max buffer and transfer sizes)
    - Node power
      - Gives Node dynamic indication of the power status of the node (one per device)
      - (Current power, available power sources, current power sources, current power source levels)
    - Simple
      - Contains information specific to each endpoint contained in the node (one per active endpoint)
      - (Endpoint, ProfileID, Device ID and version, input cluster count and list, output cluster count and list)
  - Optionals
    - Complex
      - Extended infos for each device descriptors contained in the node (one per active endpoint)
      - (manufacturer name, model name, serial number, Device URL, Icon URL..)
    - User
      - User-definable information
      - (contains information that allows the user to identify the device by using user-friendly character string

ZigBee Device Profile

- ZDP
  - Scope
    - To describe how general ZigBee device features such Binding, Device Discovery and Service Discovery are implemented within ZDOs.
    - The Device Descriptions and Clusters defined here, define capabilities that shall be supported in all ZigBee devices
  - Services
    - Device and Service Discovery (Mandatory)
    - End Device Bind, Bind and Unbind
    - Network Management (Mandatory)
    - Node management
    - Security management



Summary of ZigBee Application Model



- Devices are modeled through Application Objects that are associated to the Endpoints
- Application Objects communicate through the exchange of Clusters and Attributes
- Each Profile Object can contain single or multiple Clusters and Attributes
- Binding mechanism between endpoints ensures interoperable exchange of Clusters/Attributes
- Messaging is
  - Direct addressing
    - Knowledge of the address, endpoint of the target device is required.
    - Binding is not a prerequisite
  - Indirect addressing
    - Binding management is required.
    - Indirect addressing is specified via APSDE-SAP
  - Broadcast addressing
    - Broadcast to all endpoints on a given destination address (**application broadcast**)
    - Broadcast flag is set in APS frame control field
- Generic ZigBee device functions are provided through ZigBee Device Objects

Left Behind

- Many features on PHY, MAC, Network and Application Layers
- Security Features (@ MAC, Network and Application Layers)
- Support Tools
  - Application Profile Editors
  - Commissioning Tools
- New Features for next version