Zigbee / IEEE 802.15.4 Standard

Presenter: Dusan Stevanovic

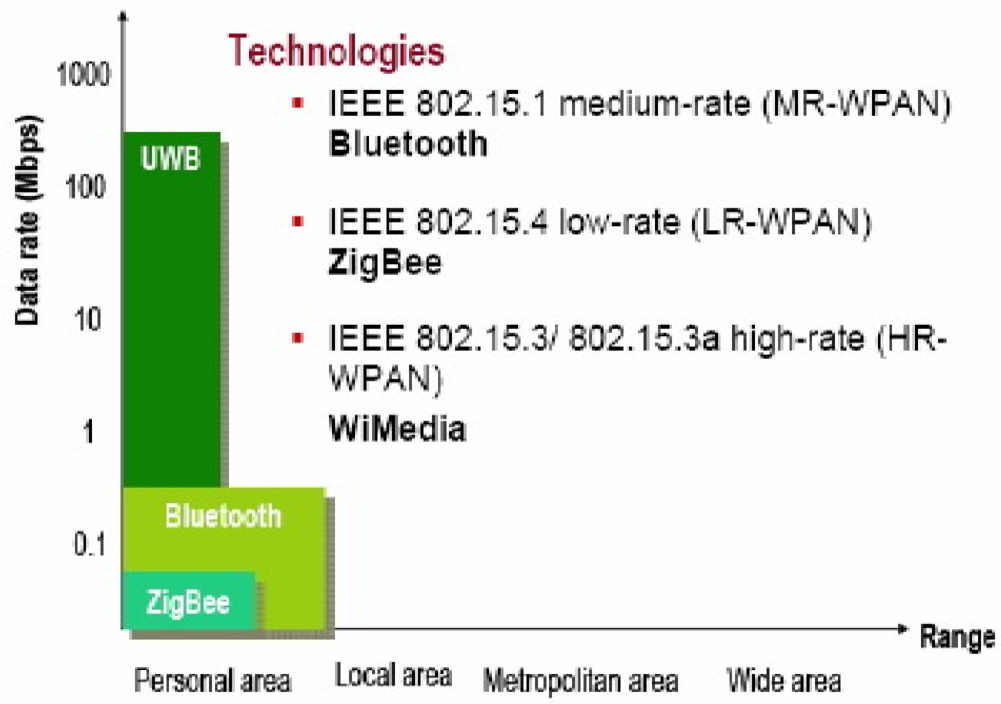
June 20, 2007

Outline

- Introduction
- IEEE 802.15.4 Standard
  - PHY Layer
  - MAC Layer
- Zigbee Protocol Stack
  - Network Layer
    - Network Formation and Address Assignment
    - Routing and Route Discovery
  - Application Layer
    - Application Objects and Application Profile
    - Zigbee Device Objects and Device Profile
- Conclusion and Future Work

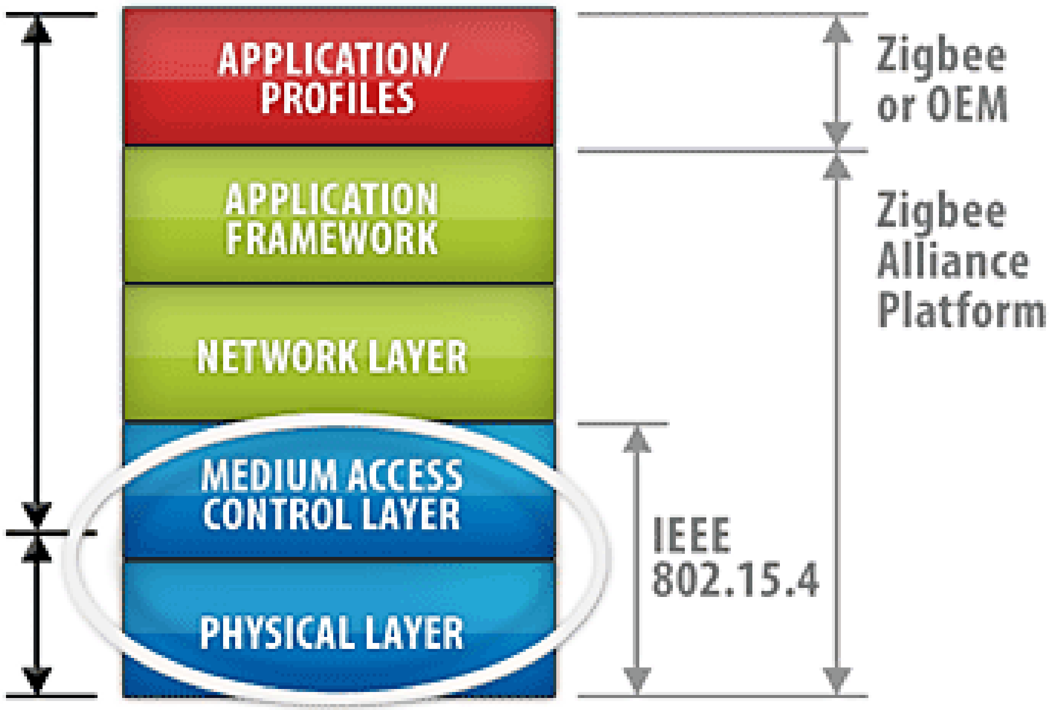
Introduction

- Various in-home applications are driving the need for communications
- Internet, multi-PC connectivity, home automation, energy conservation and security
- Some applications demand low-rate, low power consumption protocol stacks
- **Solution**: In 2000, IEEE New Standards Committee (NesCom) introduced a low-rate wireless personal area network (LR-WPAN) standard, called 802.15.4
- In 2003, Zigbee Alliance introduced Zigbee standard protocol



Introduction

- IEEE 802.15.4 standard defines the characteristics of the physical and MAC layers for LR-WPANs
- Zigbee builds upon the IEEE 802.15.4 standard and defines the network layer specifications and provides a framework for application programming in the application layer



ZigBee, WiFi™, and Bluetooth™ compared

NAME	ZIGBEE	WiFi	BLUETOOTH
Standard	802.15.4	802.11a,b,g	802.15.1
Application	Monitoring and control	Web, e-mail, video	Cable replacement
System resources	50 to 60 Kbytes	> 1 Mbyte	> 250 Kbytes
Battery life (days)	100 to > 1000	1 to 5	1 to 7
Network size	65, 536	32	7
Bandwidth (Kb/s)	20 to 250	11,000	720
Maximum transmission range (m)	100+	100	10
Success metrics	Reliability, power, cost	Speed, flexibility	Cost, convenience

IEEE 802.15.4 PHY Layer

Property	Range
Raw data rate	868 MHz: 20 kb/s; 915 MHz: 40 kb/s; 2.4 GHz: 250 kb/s
Range	10–20 m
Latency	Down to 15 ms
Channels	868/915 MHz: 11 channels 2.4 GHz: 16 channels
Frequency band	Two PHYs: 868 MHz/915 MHz and 2.4 GHz
Addressing	Short 8-bit or 64-bit IEEE
Channel access	CSMA-CA and slotted CSMA-CA
Temperature	Industrial temperature range –40 to +85 C

- Other functionalities include channel switching, link quality estimation, energy detection measurement and clear channel assessment to assist the channel selection

IEEE 802.15.4 PHY Layer Tradeoffs

- Low rate of the 816/915 MHz PHY can be translated into better sensitivity and larger coverage area, thus reduce the number of nodes in a given area
- 2.4 GHz PHY can be used to attain higher throughput and lower latency / lower duty cycle

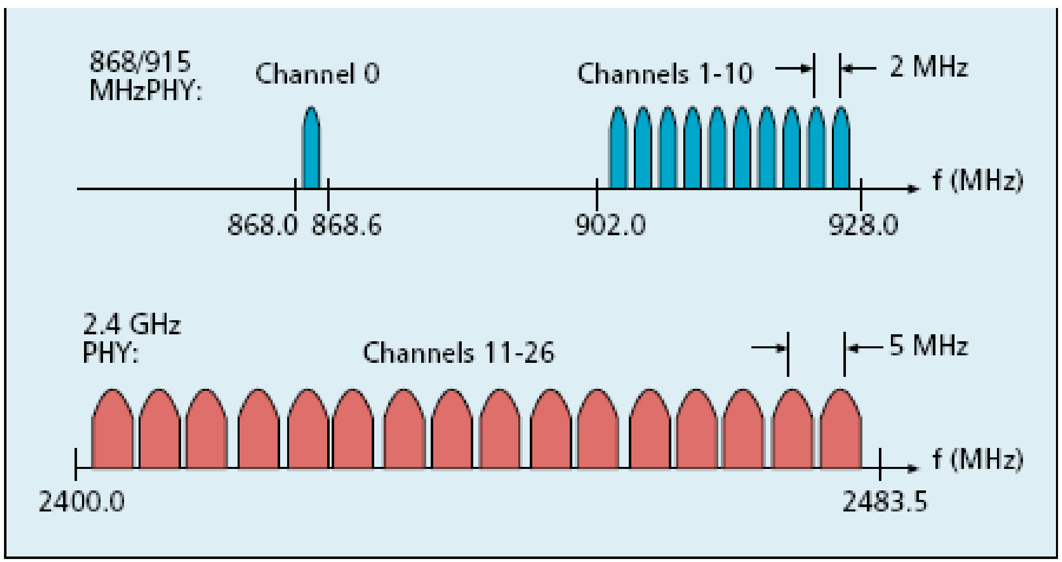
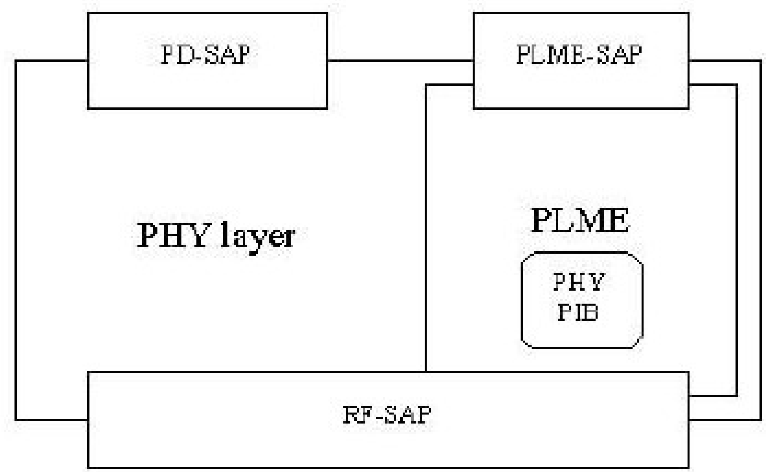
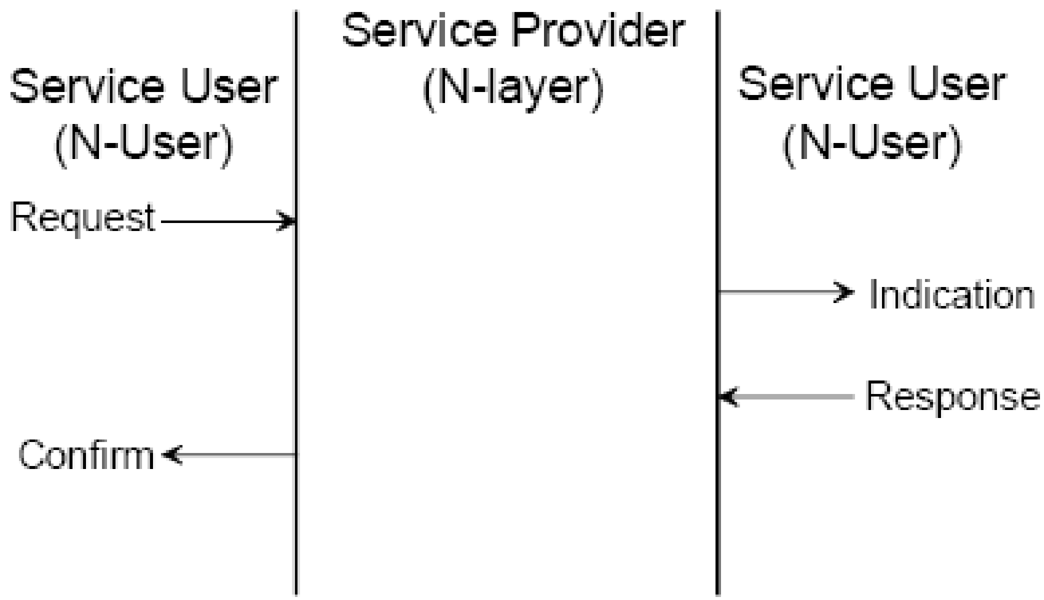


Figure 5. *The IEEE 802.15.4 channel structure.*



The PHY reference model

IEEE 802.15.4 PHY Layer Primitives

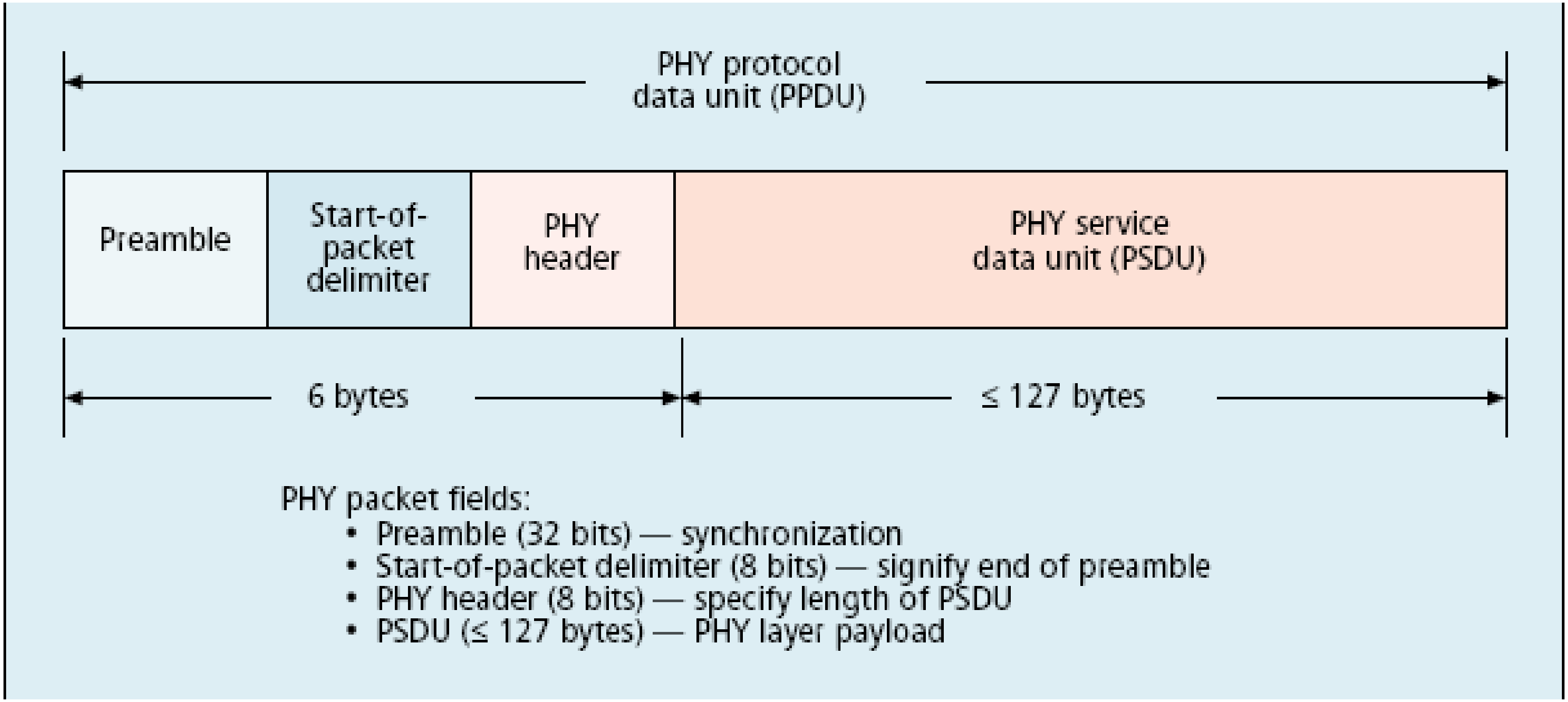


PD-SAP primitive
PD-DATA

PLME-SAP primitive
PLME-CCA
PLME-ED
PLME-GET
PLME-SET

PIB attributes
phyCurrentChannel
phyChannelsSupported
phyTransmitPower
phyCCAMode

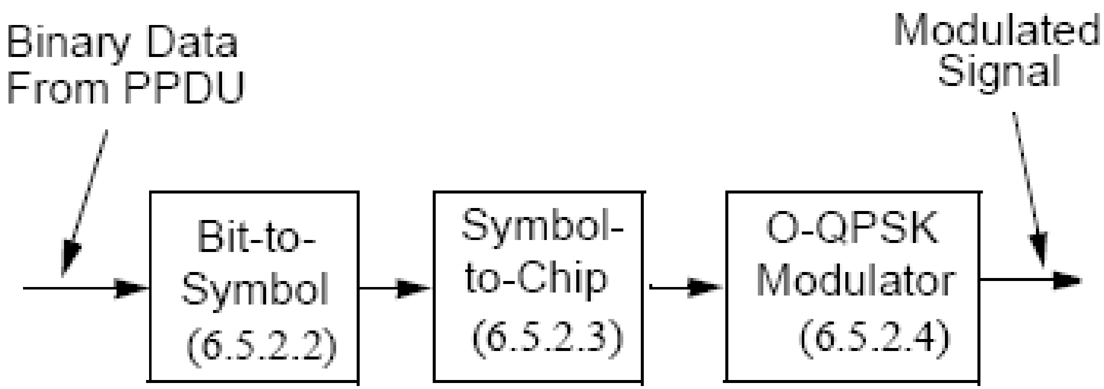
IEEE 802.15.4 PHY Layer Packet Structure



IEEE 802.15.4 PHY Layer

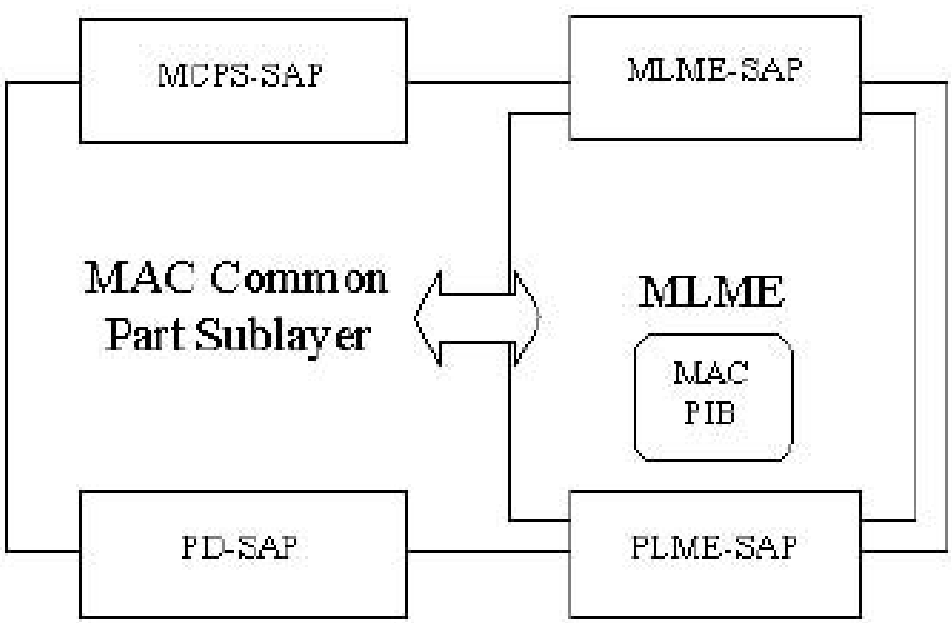
- Standard specifies that each device shall be capable of transmitting at least 1 mW
- Typical devices (1mW) are expected to cover a 10-20 m range
- Standard requires a receiver sensitivity of -85 dBm, and the defined transmit power steps are -25 dBm, -15 dBm, -10 dBm, -7 dBm, -5 dBm, -3 dBm, -1 dBm and 0

PHY	Frequency band	Data parameters			Spreading parameters	
		Bit rate (kb/s)	Symbol rate (kbaud)	Modulation	Chip rate (Mchips/s)	Modulation
868/915	868.0–868.6 MHz	20	20	BPSK	0.3	BPSK
MHz PHY	902.0–928.0 MHz	40	40	BPSK	0.6	BPSK
2.4 GHz PHY	2.4–2.4835 GHz	250	62.5	16-ary orthogonal	2.0	O-QPSK



IEEE 802.15.4 MAC Layer
Data Link Layer

- MAC layer provides two services, accessed through two SAPs:
  - The MAC data service, accessed through the MAC common part sublayer (MCPS) data SAP (MCPS-SAP)
  - The MAC management service, accessed through the MLME-SAP



IEEE 802.15.4 MAC Layer

- Features of IEEE 802.15.4 MAC are
  - association and disassociation
  - acknowledged frame delivery
  - channel access mechanism
  - frame validation
  - guaranteed time slot management
  - beacon management

IEEE 802.15.4 MAC Layer

- The IEEE 802.15.4 MAC defines four frame structures:
  - **Beacon** frame, used by a coordinator to transmit beacons.
  - **Data** frame, used for all transfers of data.
  - **Acknowledgment** frame, used for confirming successful frame reception.
  - **MAC command** frame, used for handling all MAC peer entity control transfers.

Beacon frame

Octets: 2	1	4/10	2	variable	variable	variable	2
Frame control	Sequence number	Addressing fields	Superframe specification	GTS fields (Figure 38)	Pending address fields (Figure 39)	Beacon payload	FCS
MHR			MAC payload				MFR

Data frame

Octets: 2	1	(see 7.2.2.2.1)	variable	2
Frame control	Sequence number	Addressing fields	Data payload	FCS
MHR			MAC payload	MFR

Acknowledgement frame

Octets: 2	1	2
Frame control	Sequence number	FCS
MHR		MFR

Command frame

Octets: 2	1	(see 7.2.2.4.1)	1	variable	2
Frame control	Sequence number	Addressing fields	Command frame identifier	Command payload	FCS
MHR			MAC payload		MFR

IEEE 802.15.4 MAC Layer
Reduced Function Devices (RFDs)
vs.
Full Function Devices (FFDs)

- FFDs are equipped with a full set of MAC layer functions, which enables them to act as a network coordinator or a network end-device.
- FFDs acting as network coordinators will have the ability to
  - send beacons
  - offer synchronization, communication and network join services
- RFDs can only act as end devices and are equipped with
  - sensors/actuators like transducerslight switches, lamps, etc.
  - may only interact with a single FFD

IEEE 802.15.4 MAC Layer
Star vs. Peer-to-Pear Topology

- Star topology defines master-slave network model
  - Master is a FFD and end-devices can be FFDs or RFDs
- In a mesh and tree topologies, a FFD can talk to other FFDs within its radio range and can relay messages to other FFDs outside of its radio coverage through an intermediate FFD, forming a multi-hop network
- Mesh network is a true peer-to-pear topology, where beacons will not be applied

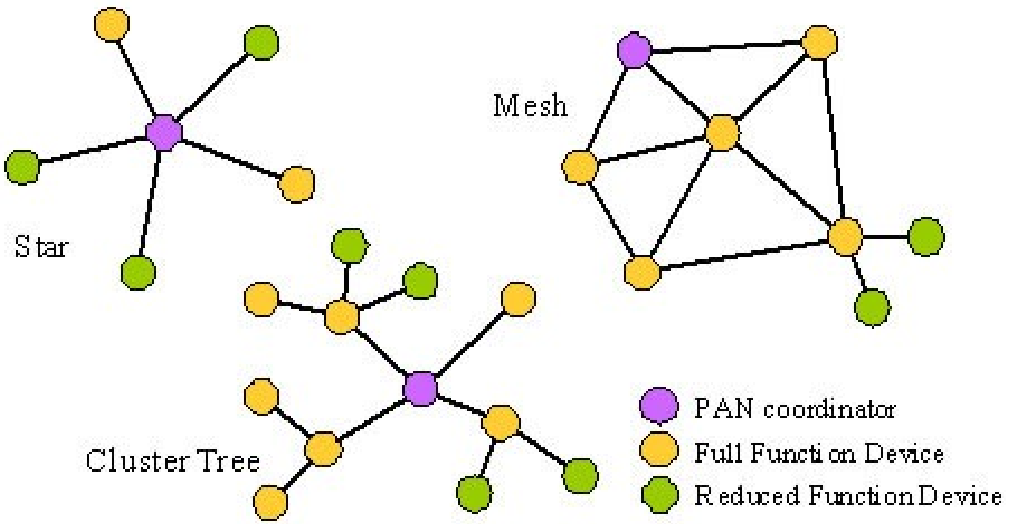
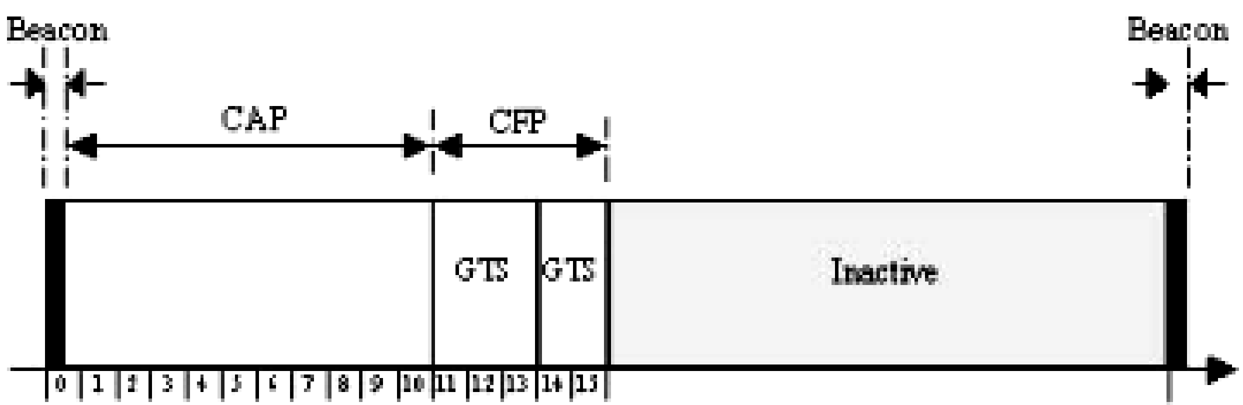


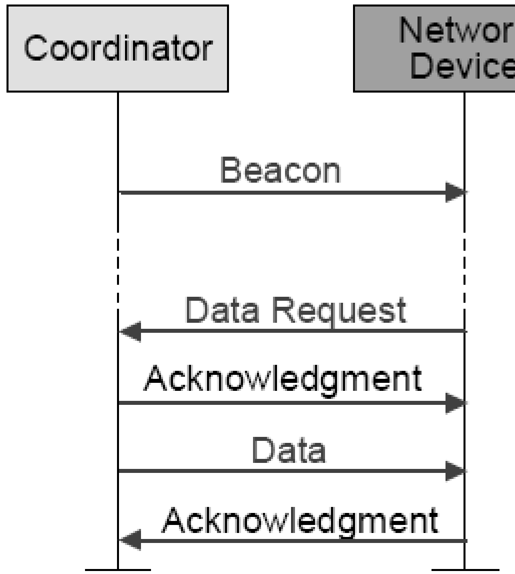
Figure 2 Different Network Topologies Specified by ZigBee

IEEE 802.15.4 MAC Layer Superframe

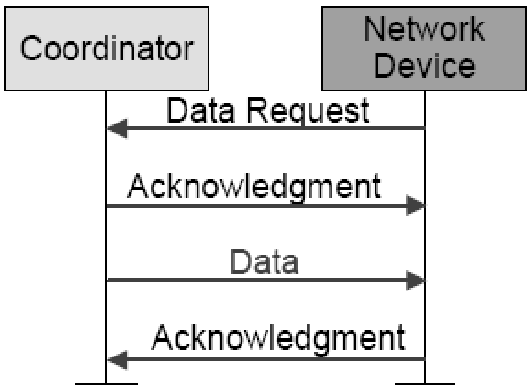
- In a **superframe**, a dedicated network coordinator, called the PAN (Zigbee) coordinator, transmits superframe beacons in predetermined intervals
  - Intervals as short as 15 ms or as long as 245 s
  - Slotted CSMA-CA is employed
  - Time between two beacons is divided into 16 equal time slots independent of the duration of the superframe
  - Time slots are split into contention-access period (**CAP**) and contention-free period (**CFP**)
- Guaranteed time slots (**GTS**) are concatenated contention-free slots
  - Allow for low latency and dedicated bandwidth applications



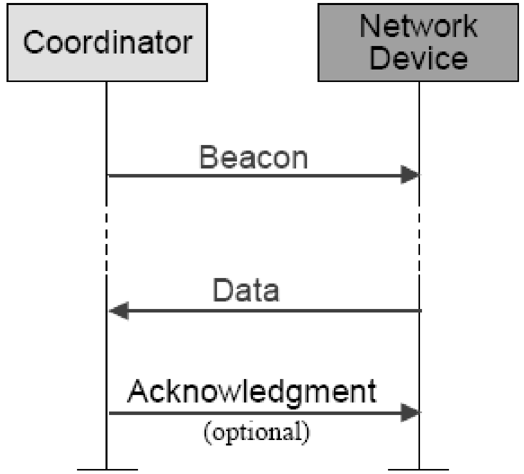
IEEE 802.15.4 MAC Layer



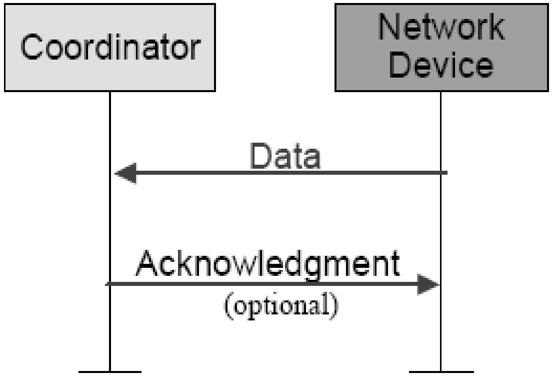
Communication from a coordinator a beacon-enabled network



Communication from a coordinator in a nonbeacon-enabled network



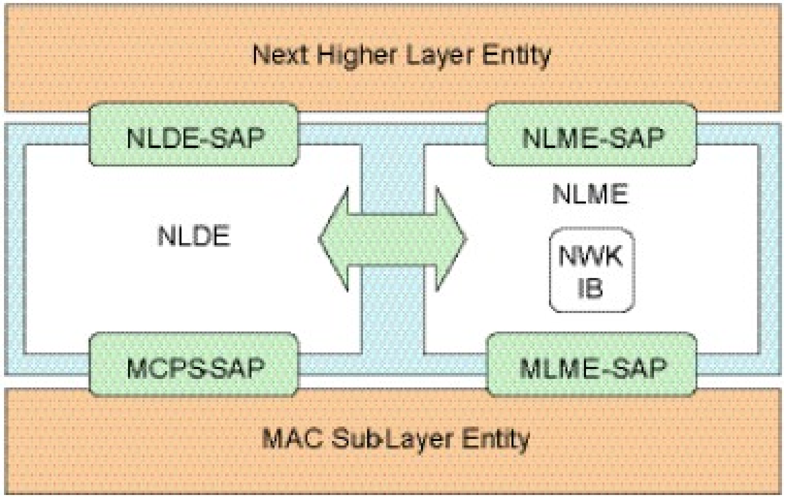
·Communication to a coordinator in a beacon-enabled network



Communication to a coordinator in a nonbeacon-enabled network

Zigbee Network Layer

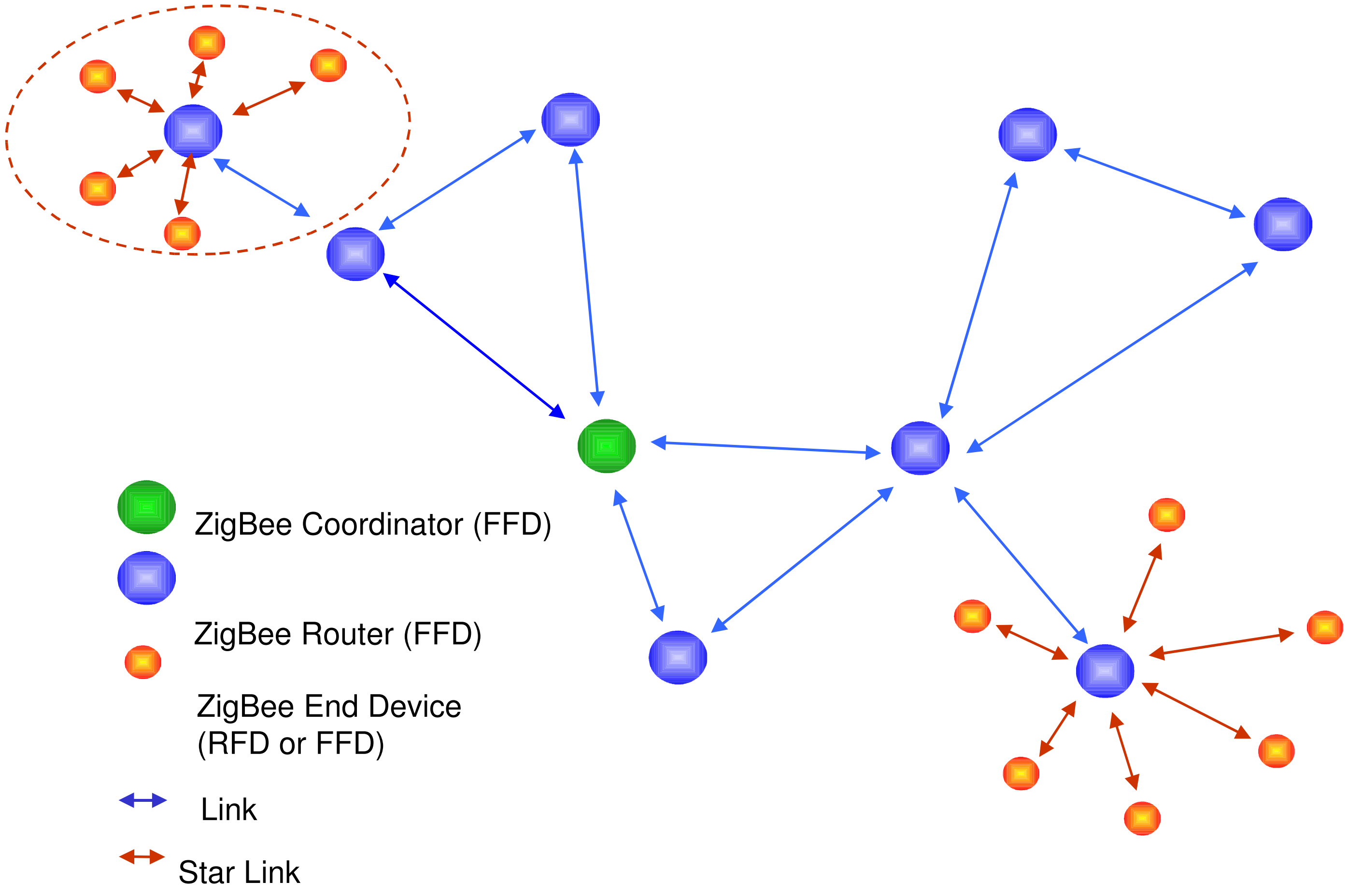
- Responsibilities of the ZigBee NWK layer are:
  - **Starting a network (NLME):** The ability to successfully establish a new network.
  - **Joining and leaving a network (NLME)**: The ability to gain membership (join) or relinquish membership (leave) a network.
  - **Configuring a new device (NLME):** The ability to sufficiently configure the stack for operation as required.
  - **Addressing (NLME):** The ability of a ZigBee coordinator to assign addresses to devices joining the network.
  - **Topology specific routing (NLDE):** The ability to transmit an NPDU to an appropriate device that is either the final destination of the communication or the next step toward the final destination in the communication chain
  - **Neighbor discovery (NLME)**: The ability to discover, record, and report information pertaining to the one-hop neighbors of a device.
  - **Routing Discovery (NLME):** routing frames to their intended destinations.



Zigbee Network Layer

- 3 device types are defined:
  - **Zigbee end-device** corresponds to an IEEE RFD or FFD acting as a simple device
  - **ZigBee router** is an FFD with routing capabilities
  - **ZigBee coordinator** (one in the network) is an FFD managing the whole network

Zigbee Network Layer Topologies



Zigbee Network Layer

Frame Formats

- Routing fields are composed of frame control fields

General Frame

Octets: 2	2	2	1	1	0/8	0/8	0/1	Variable	Variable
Frame control	Destination address	Source address	Radius	Sequence number	Destination IEEE Address	Source IEEE Address	Multicast control	Source route subframe	Frame payload
NWK Header									Payload

Frame Control

Bits: 0-1	2-5	6-7	8	9	10	11	12	13-15
Frame type	Protocol version	Discover route	Multicast flag	Security	Source Route	Destination IEEE Address	Source IEEE Address	Reserved

Command Name
Route request
Route reply
Route Error
Leave
Route Record
Rejoin request
Rejoin response
Reserved

Data Frame

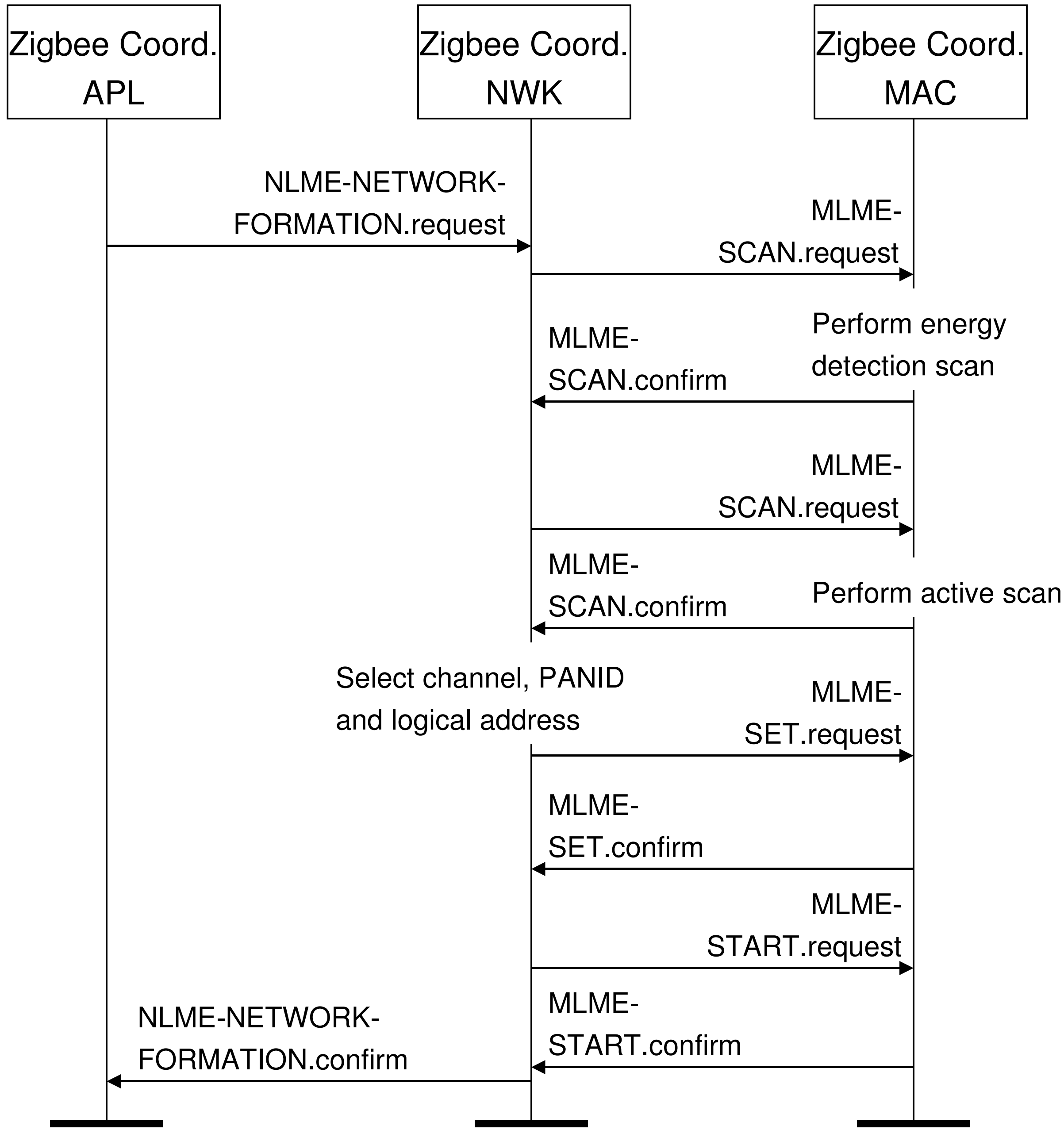
Octets: 2	Variable	Variable
Frame control	Routing fields	Data payload
NWK header		NWK payload

Command Frame

Octets: 2	Variable	1	Variable
Frame control	Routing fields	NWK command identifier	NWK command payload
NWK header		NWK payload	

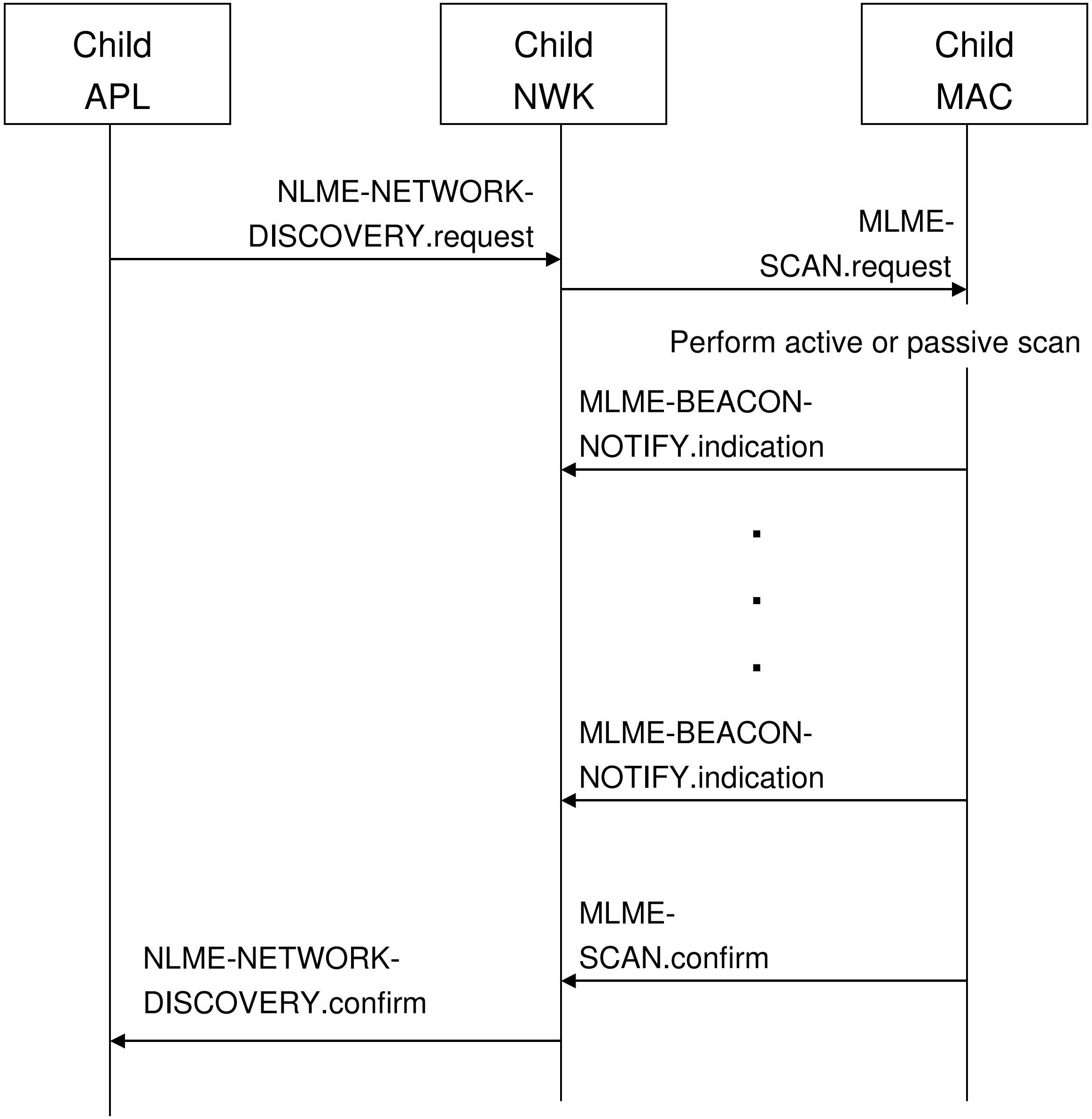
Zigbee Network Layer Network Formation

- Zigbee coordinator is the only device capable of initiating a new network formation
- All ZigBee devices shall provide the following functionality:
  - Join a network
  - Leave a network
- ZigBee coordinators and routers shall provide the following additional functionality:
  - Participate in assignment of logical network addresses.
  - Maintain a list of neighboring devices.



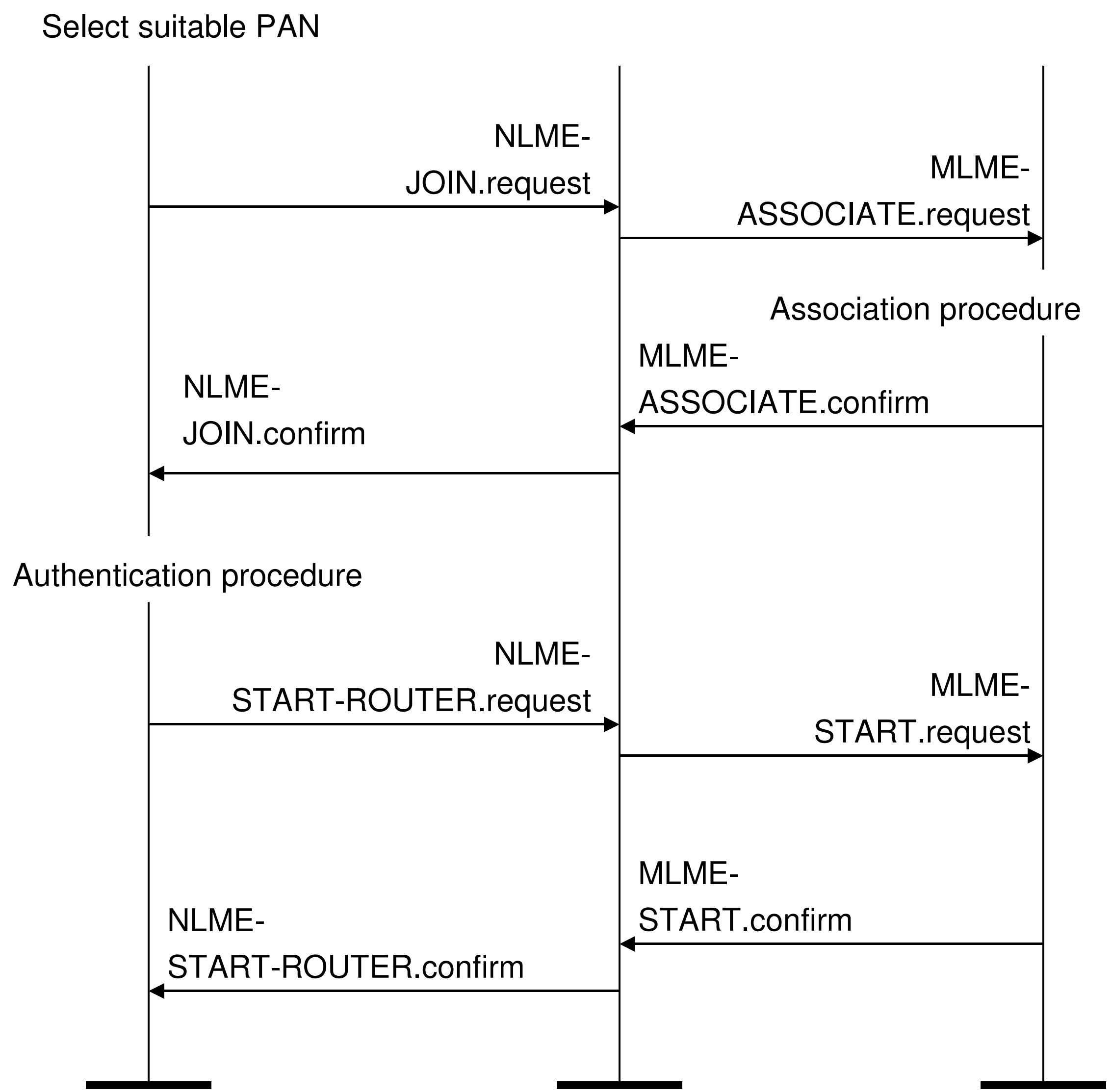
Zigbee Network Layer Joining a Network Child Procedure

- Only a ZigBee coordinator or a router is physically capable of accepting a join request, while an end device is not.



Zigbee Network Layer
Joining a Network Child Procedure (cont…)

- Only a ZigBee coordinator or a router is physically capable of accepting a join request, while an end device is not.



Zigbee Network Layer

Joining a Network

Beacon Payload Fields

Bits: 0 – 7	8 – 11	12 – 15	16 – 17	18	19 – 22	23	24 – 87	88 – 111
Protocol ID	Stack profile	nwkcProtocol Version	Reserved	Router capacity	Device depth	End device capacity	*nwk Extended PANID*	Tx Offset (optional)

Sample Neighbor Table Fields

Field Name
Network address
Device type
Relationship
Extended PAN ID
Permit joining
Potential parent
LQI

PAN Descriptor Fields

Field Name
Logical Channel
SuperframeSpec
GTS Permit
Link Quality
Security Use

Zigbee Network Layer
Network Address Assignment

- Network Address Assignment:
  - Zigbee coordinator fixes:
    - maximum number of routers ($\mathbf{R_m}$)
    - end-devices ($\mathbf{D_m}$) that each router may have as children
    - maximum depth of the tree ($\mathbf{L_m}$)
  - Then first integer in the range becomes the node address while the rest will be available for assignment to its children
  - Size ***A*(*d*)** of the range of addresses assigned to
  - Router node at depth $\boldsymbol{d < L_m}$ is defined by the following recurrence:

$$A(d) = 1 + D_m + R_m \qquad \text{if } d = L_m - 1$$

or

$$A(d) = 1 + D_m + R_m A(d+1) \qquad \text{if } 0 \leq d < L_m - 1$$

blue = end-device, white = router, red = coordinator

Zigbee Network Layer
Network Address Assignment

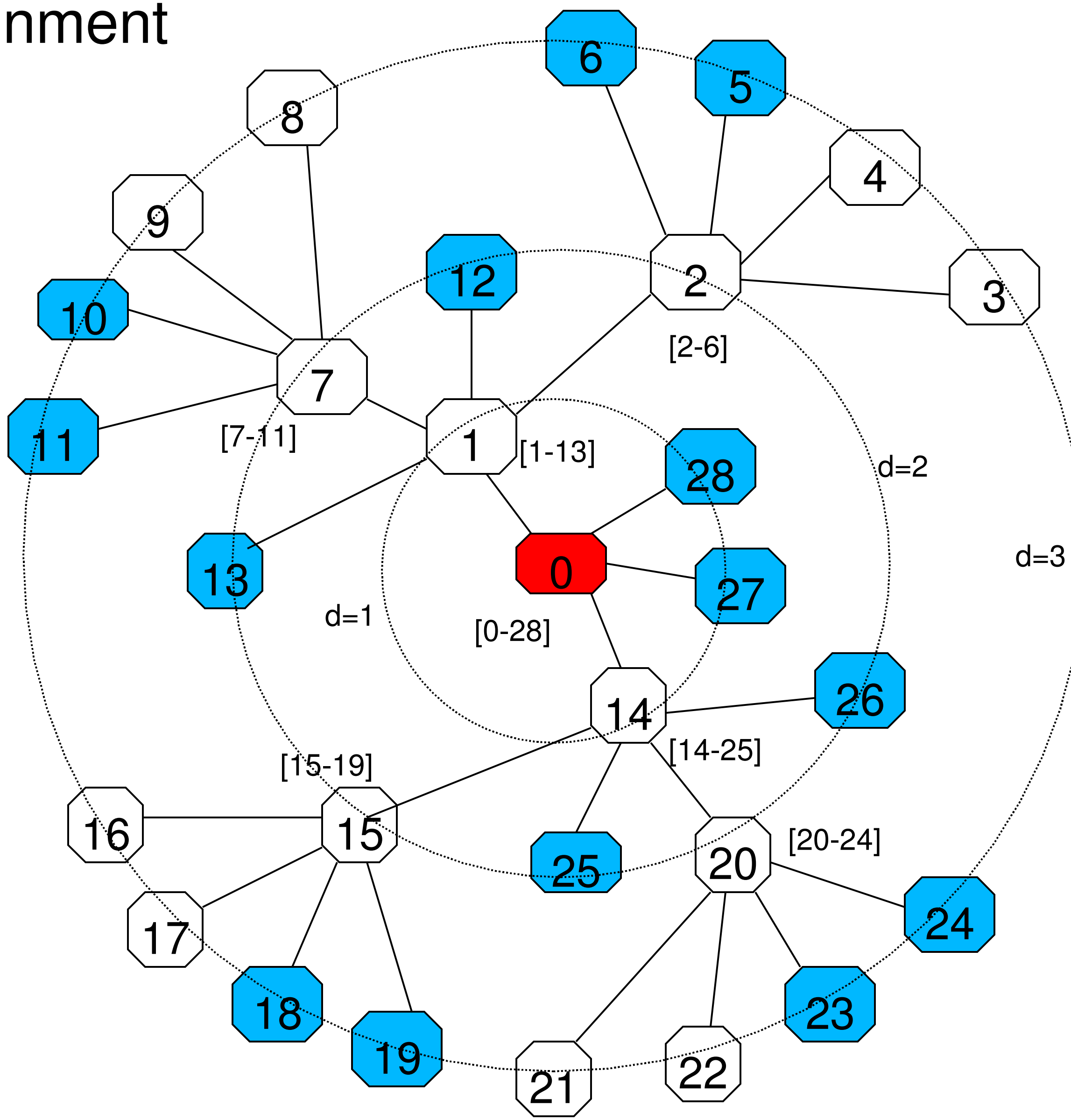
- Routers at depth L_m and end-devices are obviously assigned a single address
- Router at depth d receives the range of addresses $[x, x + A(d)]$
  - It will have address x *and* will assign range

$$[x + (i - 1)A(d + 1) + 1,\ x + i + A(d + 1)]$$

to its i-th router child where $(1 \le i \le R_m)$

and address $x + R_m A(d + 1) + j$

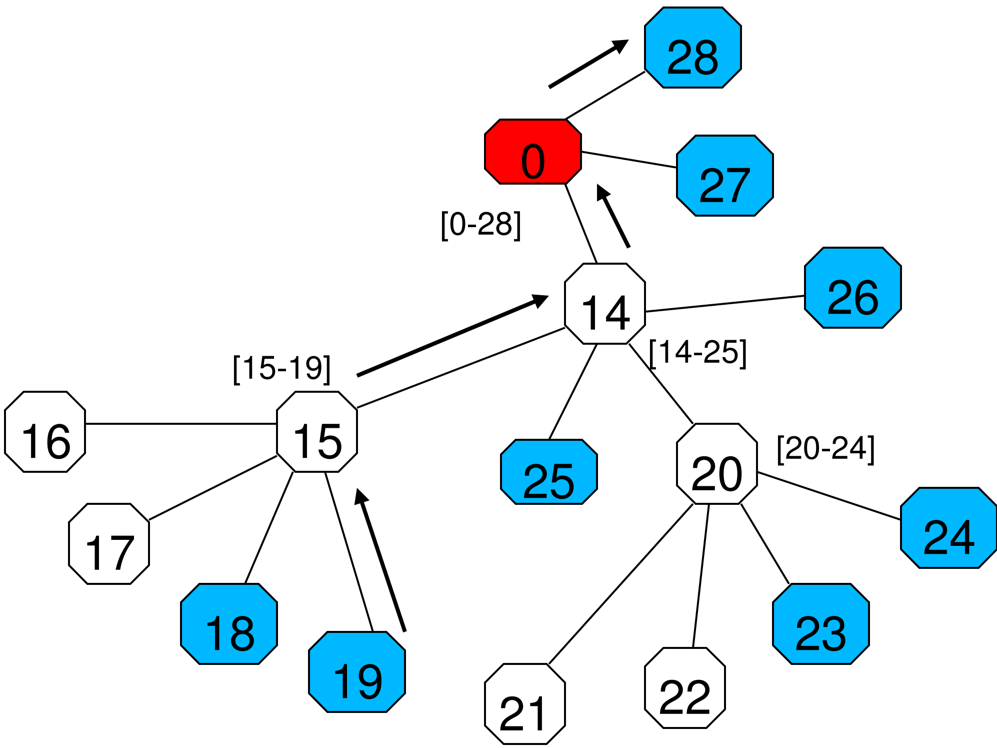
to its j-th end-device child $(1 \le j \le D_m)$



$R_m=2$, $D_m=2$ and $L_m = 3$

Zigbee Network Layer
Tree-based Routing

- Routing only along parent-child links
- Routers maintain their address and the address info associated with their children and parent
- Given an address assignment in tree-based network, router can determine if the destination belongs to a tree rooted at one of its router children or is one of its end-device children
  - If destination belongs to one of its children, it routes the packet to appropriate child
  - If destination does not belong to one of its children, it routes the packet to its parent



Node 19 is sending a packet to Node 28

Zigbee Network Layer
Tree-based Routing

- Beacon scheduling is necessary in a multi-hop topology to prevent the beacon frames of one device from colliding with either the beacon frames or data transmissions of its neighboring devices
- Only necessary in tree topology networks
- Idea is to have short active portions as compared to the beacon interval so, that neighboring routers can start their superframe suitably offset with respect to one other and avoid overlapping
- The density of devices that can be supported in the network depends on the length of inactive periods in superframe. The larger the length, the more devices that can transmit beacon frames in the same neighborhood.

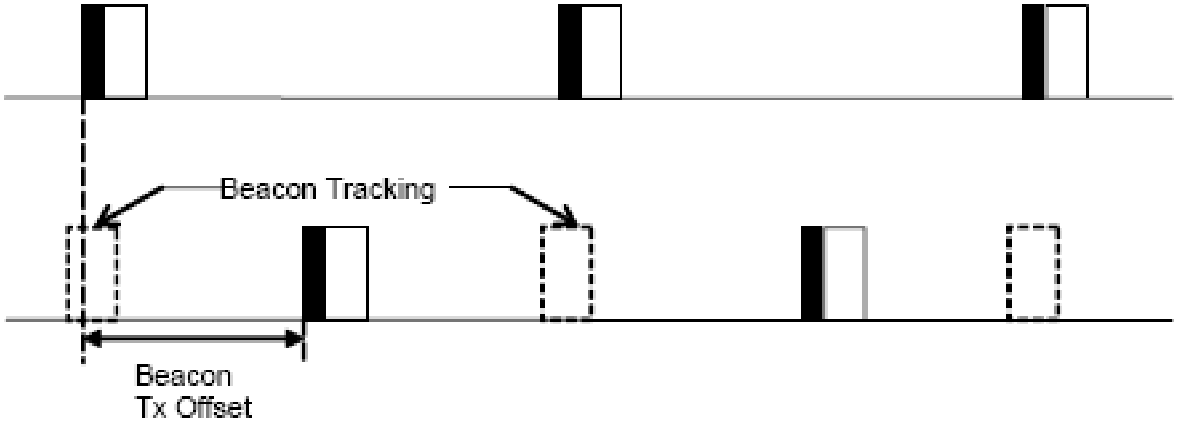


Figure 3.35 Parent-Child Superframe Positioning Relationship

Zigbee Network Layer
Mesh-based Routing

- Pros and Cons of Mesh topology as compared to Tree topology
  - Pros
    - Robust
    - Resilient to faults
  - Cons
    - More complex
    - Beaconing is not allowed
- Routers maintain a routing table (RT) and employ a route discovery algorithm to construct / update these data structures on the path nodes
- When no entry addresses the given destination, the network layer attempts to start the route discovery procedure and in case sufficient resources are not available it falls back to tree-based routing.

Routing Table

Field Name	**Description**
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

Zigbee Network Layer

Mesh-based Routing

- Route discovery is a process required to establish routing table entries in the nodes along the path between two nodes wishing to communicate
- Route Discovery Table (RDT) is maintained by routers and the coordinator to implement route discovery
- Route discovery in ZigBee is based on the well-known Ad hoc On Demand Distance Vector routing algorithm

Octets: 1	1	1	2	1
Command frame identifier (see Table 3.38)	Command options	Route request identifier	Destination address	Path cost
NWK payload				

Route Discovery Table

Field Name	Description
RREQ ID	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 route request command frame corresponding to this entry's Route request identifier and Source address
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

Zigbee Network Layer
Mesh-based Routing

- Routing algorithm uses a path cost metric during route discovery
- Based on LQI (Link Quality Indicator) value provided by 802.15.4 MAC and PHY layers
- Link cost *C{l}* can be defined as:

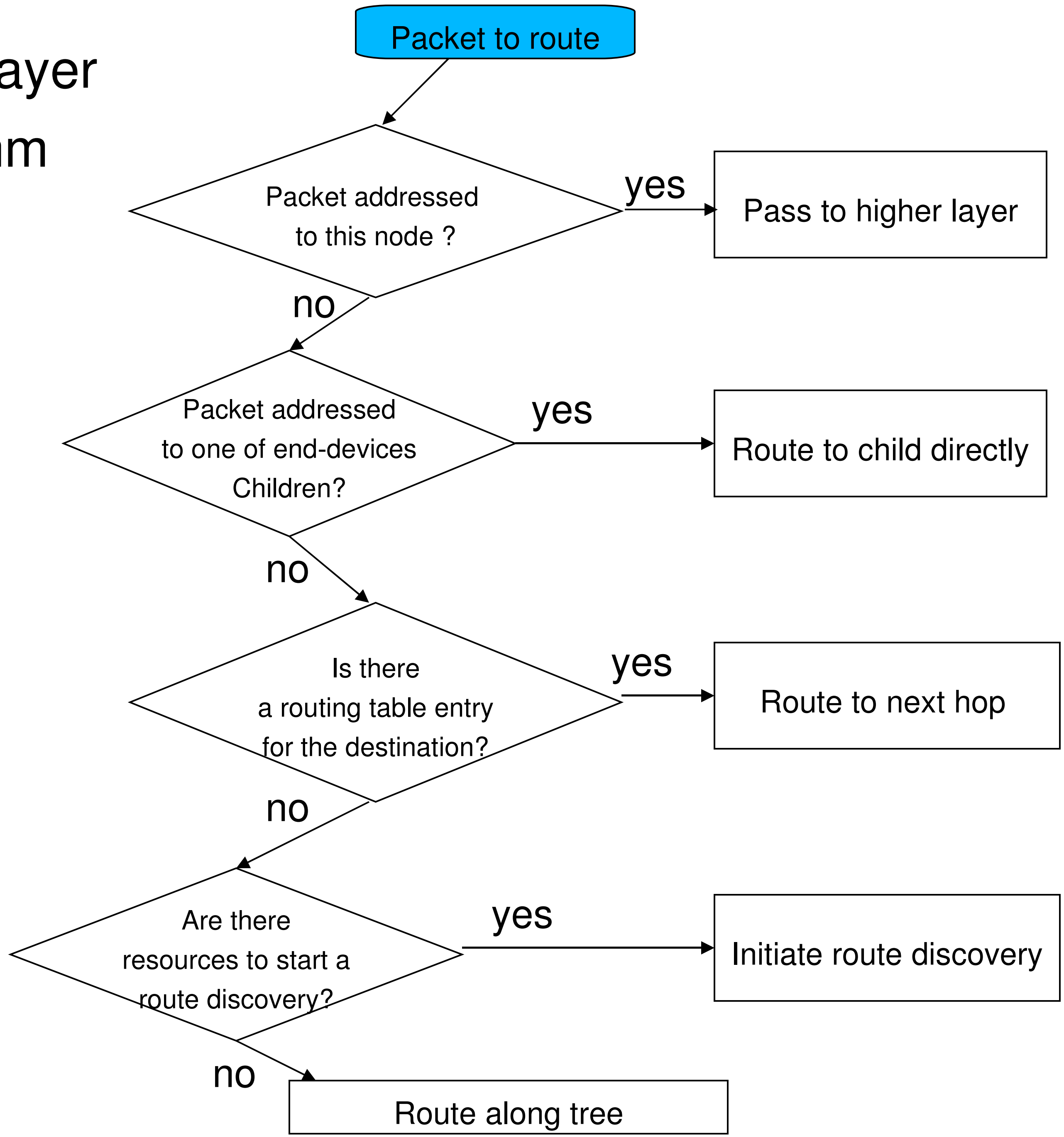
$$C\{l\} = \begin{cases} 7, \\ \min\left(7, \mathrm{round}\left(\dfrac{1}{p_l^4}\right)\right) \end{cases}$$

where p_l is defined as the probability of packet delivery on the link *l* and link cost is a function of values in the interval [0…7]

- p_l reflects the number of expected attempts required to get a packet through on that link

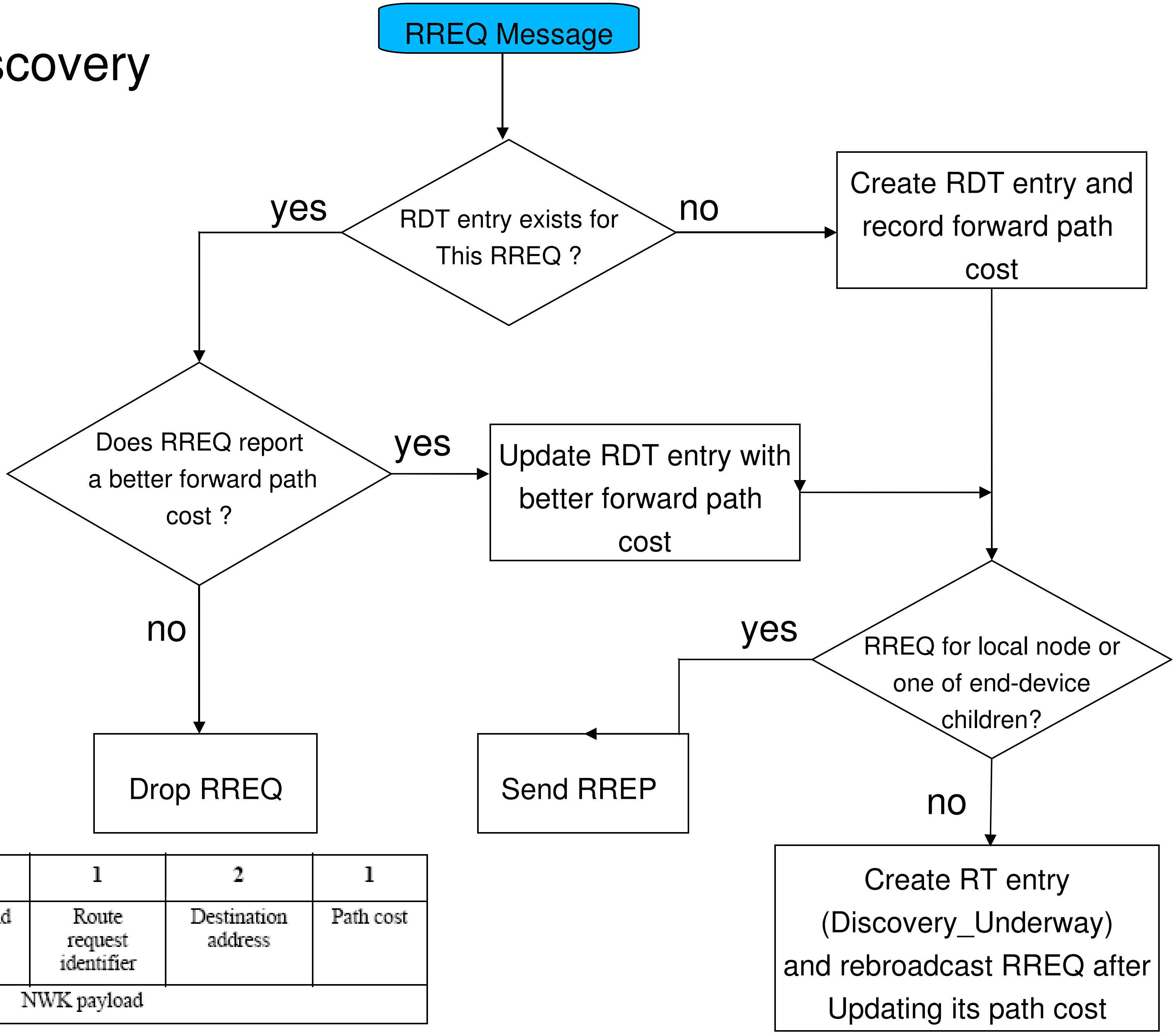
Zigbee Network Layer Routing Algorithm

- Simplified execution flow of the routing algorithm
- A device is said to have routing table capacity if:
  - It is a ZigBee coordinator or ZigBee router
  - It maintains a routing table
  - It has a free routing table entry or it already has a routing table entry corresponding to the destination



Routing Discovery Algorithm

- Route Request message processing

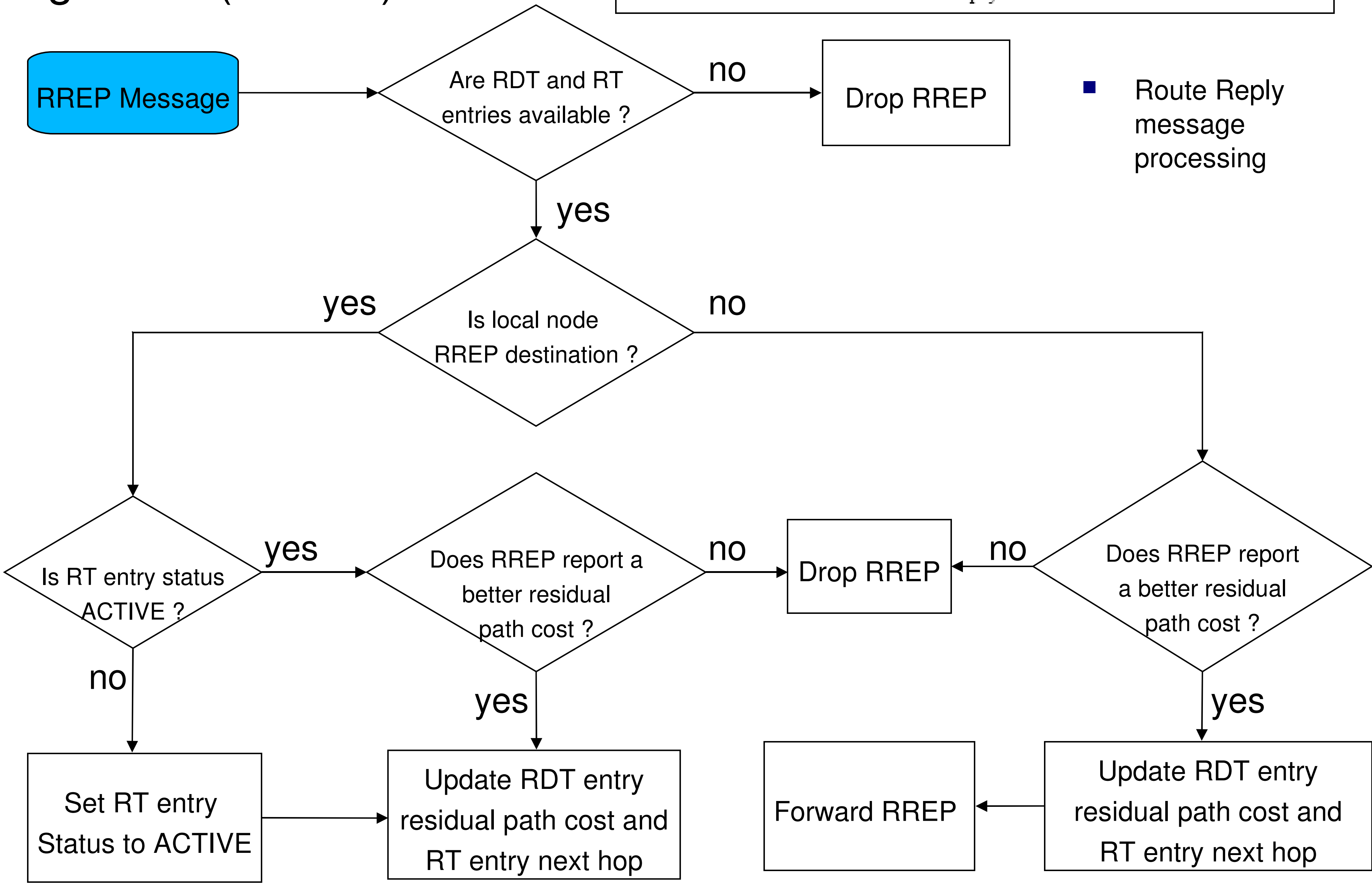


Octets: 1	1	1	2	1
Command frame identifier (see Table 3.38)	Command options	Route request identifier	Destination address	Path cost
NWK payload				

Routing Discovery Algorithm (cont …)

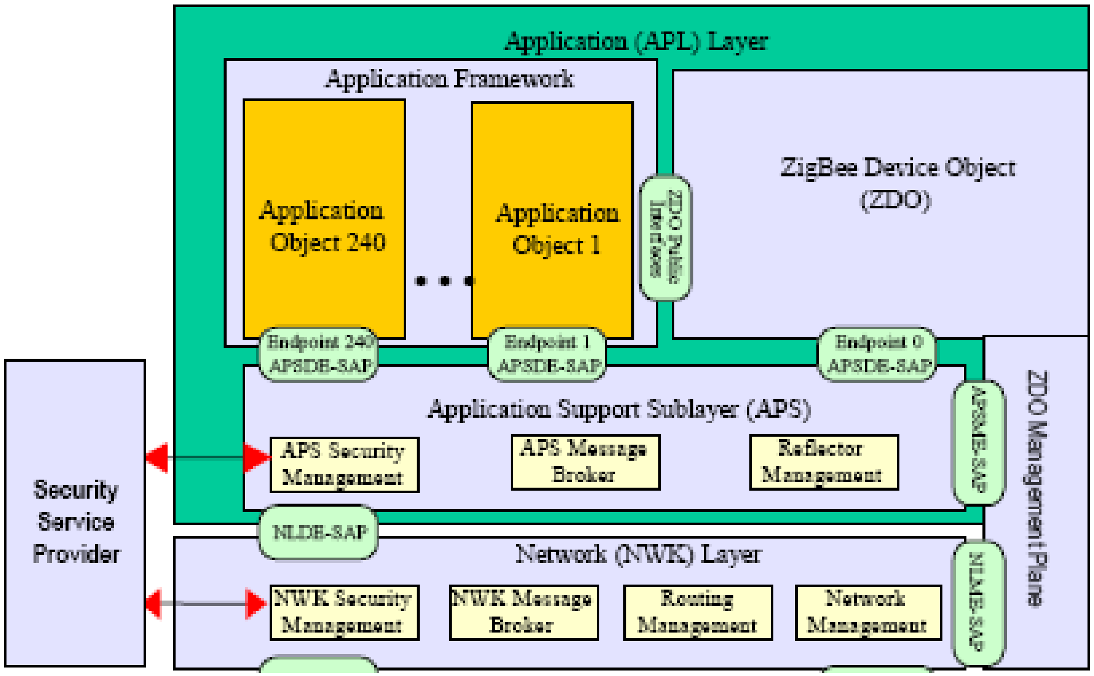
Octets: 1	1	1	2	2	1
Command frame identifier (see Table 3.38)	Command options	Route request identifier	Originator address	Responder address	Path cost
NWK payload					

- Route Reply message processing



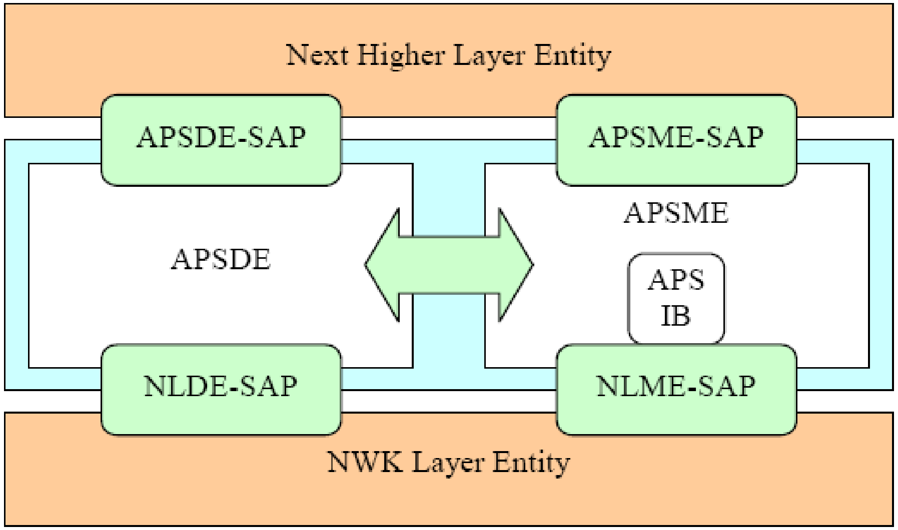
Zigbee Application Layer

- Consists of Application Support Sub-layer, Zigbee Device Object (ZDO) and Application Framework containing manufacturer-defined application objects



Zigbee Application Layer
Application Support Sub-Layer

- Application support sub-layer (APS) provides an interface between the network layer (NWK) and the application layer (APL) through a general set of services
- APSDE provides the data transmission service for the transport of application PDUs between two or more devices located on the same network
- APSDE supports fragmentation and reassembly of packets and provides reliable data transport
- APSME provides security services, binding of devices, establishment and removal of group addresses and also maintains a database of managed objects



Zigbee Application Support Sub-Layer Frame Formats

- All commands in APS are of security type

Name
APSME-BIND
APSME-GET
APSME-SET
APSME-UNBIND
APSME-ADD-GROUP
APSME-REMOVE-GROUP
APSME-REMOVE-ALL-GROUPS

General Frame

Octets: 1	0/1	0/2	0/2	0/2	0/1	1	Variable
Frame control	Destination endpoint	Group address	Cluster identifier	Profile Identifier	Source endpoint	APS counter	Frame payload
	Addressing fields						
APS header							APS payload

Frame Control

Bits: 0-1	2-3	4	5	6	7
Frame type	Delivery mode	Indirect address mode	Security	Ack. request	Reserved

Data Frame

Octets: 1	0/1	0/2	0/2	0/2	0/1	1	Variable
Frame control	Destination endpoint	Group address	Cluster identifier	Profile Identifier	Source endpoint	APS counter	Frame payload
	Addressing fields						
APS header							APS payload

Command Frame

Octets: 1	0/2	1	1	Variable
Frame control	Group Address	APS counter	APS command identifier	APS command payload
APS header			APS payload	

Zigbee Application Layer
Application Framework

- Environment for hosting manufacturer-defined application objects on Zigbee devices
- Uses APSDE-SAP interface for executing standard network functions and managing protocol layers in the Zigbee device
- Data service, provided by APSDE-SAP, includes request, confirm, response and indication primitives for data transfer
- Up to 240 distinct application objects can be defined, each interfacing on an endpoint indexed from 1 to 240.
- Application object represents different application types (or profiles) that can be defined on a single Zigbee device
- Endpoints (8-bit field) address specific application objects on a single Zigbee Device

Zigbee Application Layer
Application Profiles and Application Objects

- **Application profiles** are agreements for messages, message formats and processing actions that enable applications to create an interoperable, distributed application between applications that reside on separate devices
- Profile Designer must specify Device Descriptors
- In the context of a profile, a group of related attributes is termed a "**cluster**" and identified with a **clusterId**. Typically a cluster represents a sort of interface (or part of it) of the APO to the other APOs
- Example:
  - A thermostat on one node can communicate with a furnace on another node. Together, they cooperatively form a heating application profile. ZigBee vendors develop application profiles to provide solutions to specific technology needs
- **Application Objects (APOs)** encapsulate a set of attributes (data entities representing internal state, etc.) and provides functionalities (services) for setting/retrieving values of these attributes or being notified when an attribute value changes.

Zigbee Application Layer Application Profile

Table 2.25 ZigBee Descriptors

Descriptor Name	Status	Description
Node	M	Type and capabilities of the node
Node power	M	Node power characteristics
Simple	M	Device descriptions contained in node
Complex	O	Further information about the device descriptions
User	O	User-definable descriptor

Table 2.30 Fields of the Node Power Descriptor

Field Name	Length (Bits)
Current power mode	4
Available power sources	4
Current power source	4
Current power source level	4

Table 2.35 Fields of the Simple Descriptor

Field Name	Length (Bits)
Endpoint	8
Application profile identifier	16
Application device identifier	16
Application device version	4
Reserved	4
Application input cluster count	8
Application input cluster list	16**i* (where *i* is the value of the application input cluster count)
Application output cluster count	8
Application output cluster list	16**o* (where *o* is the value of the application output cluster count)

Table 2.37 Fields of the Complex Descriptor

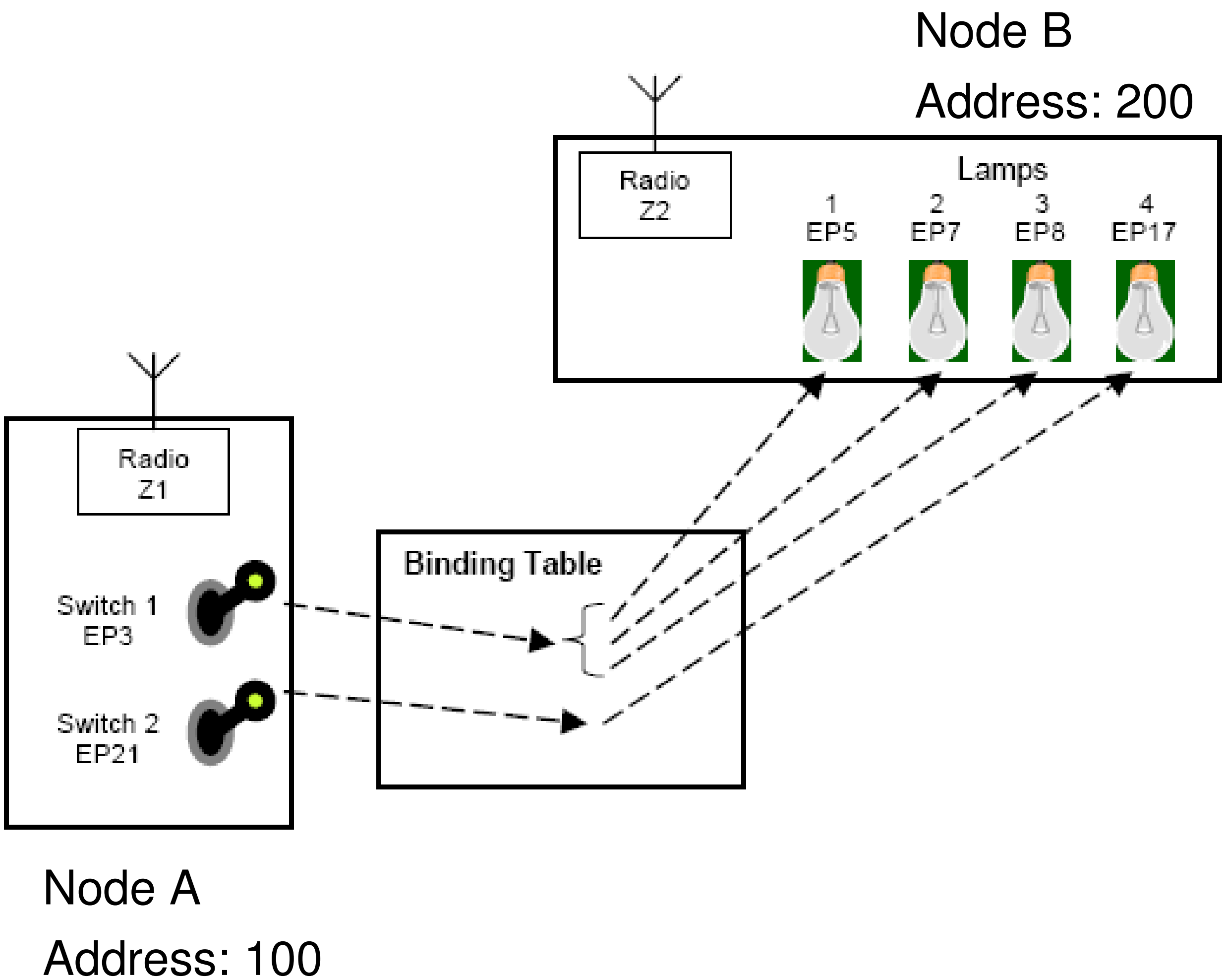
Field Name	XML Tag	Compressed XML Tag Value $b_3b_2b_1b_0$	Data Type
Reserved	-	0000	-
Language and character set	<languageChar>	0001	See sub-clause 2.3.2.7.1
Manufacturer name	<manufacturerName>	0010	Character string
Model name	<modelName>	0011	Character string
Serial number	<serialNumber>	0100	Character string
Device URL	<deviceURL>	0101	Character string
Icon	<icon>	0110	Octet string
Icon URL	<outliner>	0111	Character string
Reserved	-	1000 – 1111	-

Table 2.39 Fields of the User Descriptor

Field Name	Length (Octets)
User description	16

Zigbee Application Layer Addressing example

- Node A and B are given unique addresses when they join a Zigbee network
- Switch 1 and 2 would have unique endpoint numbers
- Lamps 1, 2, 3 and 4 would have unique endpoint numbers as well
- Setup allows Switch 1 to uniquely address and control Lamps 1, 2 and 3 using **clusterIds**



Zigbee Application Layer
Device Profile

- Must be implemented by all nodes in the Zigbee network
- Zigbee Device Objects (ZDO) implement this profile and provide a base class of functionality that provides an interface between the application objects, the device profile and the APS
- Utilizes APS Data Services to transport messages
- Four key inter-device communication functions (implemented by different Zigbee Device Objects):
  - Device and Service Discovery
  - End Device Bind and Unbind
  - Binding Table Management
  - Network Management

Zigbee Application Layer
Discovery Procedure

- **Device Discovery** is the process whereby a ZigBee device can discover other ZigBee devices by initiating queries that are broadcast (of any broadcast address type) or unicast addressed
- **Service Discovery** is the process whereby services available on endpoints at the receiving device are discovered by external devices
- Query types supported by Service Discovery
  - **Active Endpoint**
  - **Match Simple Descriptor**
  - **Simple Descriptor**
  - **Node Descriptor**
  - **Power Descriptor**
  - **Complex Descriptor**
  - **User Descriptor**
- Discovery information may also be cached within the devices in the network designated as the Primary Discovery Cache device

Zigbee Application Layer
Device and Service Discovery
Client and Server Services

Device and Service Discovery Client Services	Client Transmission	Server Processing
NWK_addr_req	O	M
IEEE_addr_req	O	M
Node_Desc_req	O	M
Power_Desc_req	O	M
Simple_Desc_req	O	M
Active_EP_req	O	M
Match_Desc_req	O	M
Complex_Desc_req	O	O
User_Desc_req	O	O
Discovery_Cache_req	O	M
End_Device_annce	O	O
User_Desc_set	O	O
System_Server_Discover _req	O	M
Discovery_store_req	O	O
Node_Desc_store_req	O	O
Power_Desc_store_req	O	O
Active_EP_store_req	O	O
Simple_Desc_store_req	O	O
Remove_node_cache_req	O	O
Find_node_cache_req	O	M

Device and Service Discovery Server Services	Server Processing
NWK_addr_rsp	M
IEEE_addr_rsp	M
Node_Desc_rsp	M
Power_Desc_rsp	M
Simple_Desc_rsp	M
Active_EP_rsp	M
Match_Desc_rsp	M
Complex_Desc_rsp	O
User_Desc_rsp	O
User_Desc_conf	O
System_Server_Discovery_rsp	M
Discovery_store_rsp	O
Node_Desc_store_rsp	O
Power_Desc_store_rsp	O
Active_EP_store_rsp	O
Simple_Desc_store_rsp	O
Remove_node_cache_rsp	O
Find_node_cache_rsp	O

Zigbee Application Layer

Discovery Procedure Command Frame Structure

Table 2.41 Fields of the NWK_addr_req Command

Name	Type	Valid Range	Description
IEEEAddr	IEEE Address	A valid 64-bit IEEE address	The IEEE address to be matched by the Remote Device
RequestType	Integer	0x00-0xff	Request type for this command: 0x00 – Single device response 0x01 – Extended response 0x02-0xFF – reserved
StartIndex	Integer	0x00-0xff	If the Request type for this command is Extended response, the StartIndex provides the starting index for the requested elements of the associated devices list

Table 2.83 Fields of the NWK_addr_rsp Command

Name	Type	Valid Range	Description
Status	Integer	SUCCESS, INV_REQUESTTYPE or DEVICE_NOT_FOUND	The status of the NWK_addr_req command
IEEEAddrRemoteDev	Device Address	An extended 64-bit, IEEE address	64-bit address for the Remote Device
NWKAddrRemoteDev	Device Address	A 16-bit, NWK address	16-bit address for the Remote Device
NumAssocDev	Integer	0x00-0xff	Count of the number of associated devices to the Remote Device and the number of 16-bit short addresses to follow; If the RequestType in the request is Extended Response and there are no associated devices on the Remote Device, this field shall be set to 0; If the RequestType in the request is for a Single Device Response, this field shall not be included in the frame

Table 2.43 Fields of the Node_Desc_req Command

Name	Type	Valid Range	Description
NWKAddrOfInterest	Device Address	16 bit NWK address	NWK address for the request

Table 2.26 Fields of the Node Descriptor

Field Name	Length (bits)
Logical type	3
Complex descriptor available	1
User descriptor available	1
Reserved	3
APS flags	3
Frequency band	5
MAC capability flags	8
Manufacturer code	16
Maximum buffer size	8
Maximum transfer size	16
Server Mask	16

Table 2.85 Fields of the Node_Desc_rsp Command

Name	Type	Valid Range	Description
Status	Integer	SUCCESS, DEVICE_NOT_FOUND ,INV_REQUESTTYPE or NO_DESCRIPTOR	The status of the Node_Desc_req command
NWKAddrOfInterest	Device Address	16 bit NWK address	NWK address for the request
NodeDescriptor	Node Descriptor		See the Node Descriptor format in sub-clause 2.3.2.4. This field shall only be included in the frame if the status field is equal to SUCCESS

Zigbee Application Layer Messaging

- Direct addressing mode
  - Message is addressed to a specific destination address (16-bit network address) and endpoint number and the sending node is responsible for discovering both via the ZDO discovery services
  - Direct addressing assumes device discovery and service discovery have identified a particular device and endpoint, which supply a complementary service to the requestor
- Indirect addressing mode (used by end-devices)
  - Only requires the sender to supply a cluster id but needs support from a neighboring (or local) ZigBee router (or coordinator) to locate the destination node(s) for the message
  - Possible since APS of the ZigBee router maintains a binding table associating (source address, source endpoint, cluster id) tuples to a list of (destination address, destination endpoint) tuples, one for each device the message must reach
  - Message sent by an end-device with indirect addressing reaches the parent node where the APS consults its binding table in order to determine the actual destinations and send them appropriate messages with direct addressing

Conclusion and Future Work

- Presented main features of IEEE 802.15.4’s MAC and PHY layers
- Covered in detail Zigbee Alliance’s specifications of NWK and APL layers
- **Next step**
  - Study potential DoS attacks in Zigbee wireless sensor networks
  - Study security features supported by the Zigbee standard

Questions ?

References:

2. ZigBee Alliance, “ZigBee Specifications”, version 1.0 r13, December 2006. http://www.zigbee.org/
3. Paolo Baronti, Prashant Pillai, Vince Chook, Stefano Chessa, Alberto Gotta, Y. Fun Hu, “Wireless Sensor Networks: a Survey on the State of the Art and the 802.15.4 and ZigBee Standards”, Computer Communication, Volume 30 , Issue 7, pages 1655-1695, 2007.
4. Ed Callaway, Paul Gorday, Lance Hester, Jose A. Gutierrez, Marco Naeve, Bob Heile, Venkat Bahl, “Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate Wireless Personal Area Networks”, IEEE Communications Magazine, August 2002.
5. Jianliang Zheng, Myung J. Lee, “Will IEEE 802.15.4 make ubiquitous networking a reality?: A discussion on a potential low power, low bit rate standard”, IEEE Communications Magazine, June 2004.
6. Institute of Electrical and Electronics Engineers, Inc., IEEE Std. 802.15.4- 2003, IEEE Standard for Information Technology — telecommunications and Information Exchange between Systems — Local and Metropolitan Area Networks — Specific Requirements — Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs). New York: IEEE Press. 2003.