Infrastructure and Service Discovery Protocols for the IoT Ecosystem

Apply wireless protocols to develop IoT Solution

Contents

✓Layered Architecture for IoT

✓Protocol Architecture for IoT

✓IEEE 802.15.4

✓RFID, Z-Wave, Zigbee

✓6LoWPAN

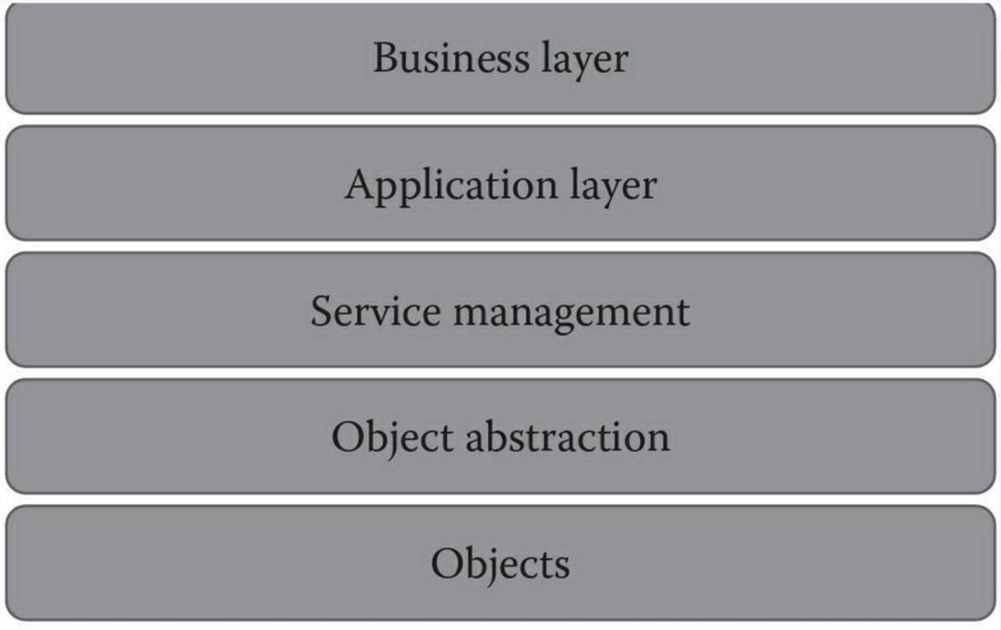
✓Bluetooth

✓Device/Service Discovery for IoT Bluetooth Beacons

✓LTE

✓WiFi Aware & Open Hybrid

LAYERED ARCHITECTURE OF IOT



Business layer

Application layer

Service management

Object abstraction

Objects

LAYERED ARCHITECTURE OF IOT

Objects Layer

Sensors/MEMS which support Plug n Play

Data collected here are transferred to the object abstraction layer using secure channels

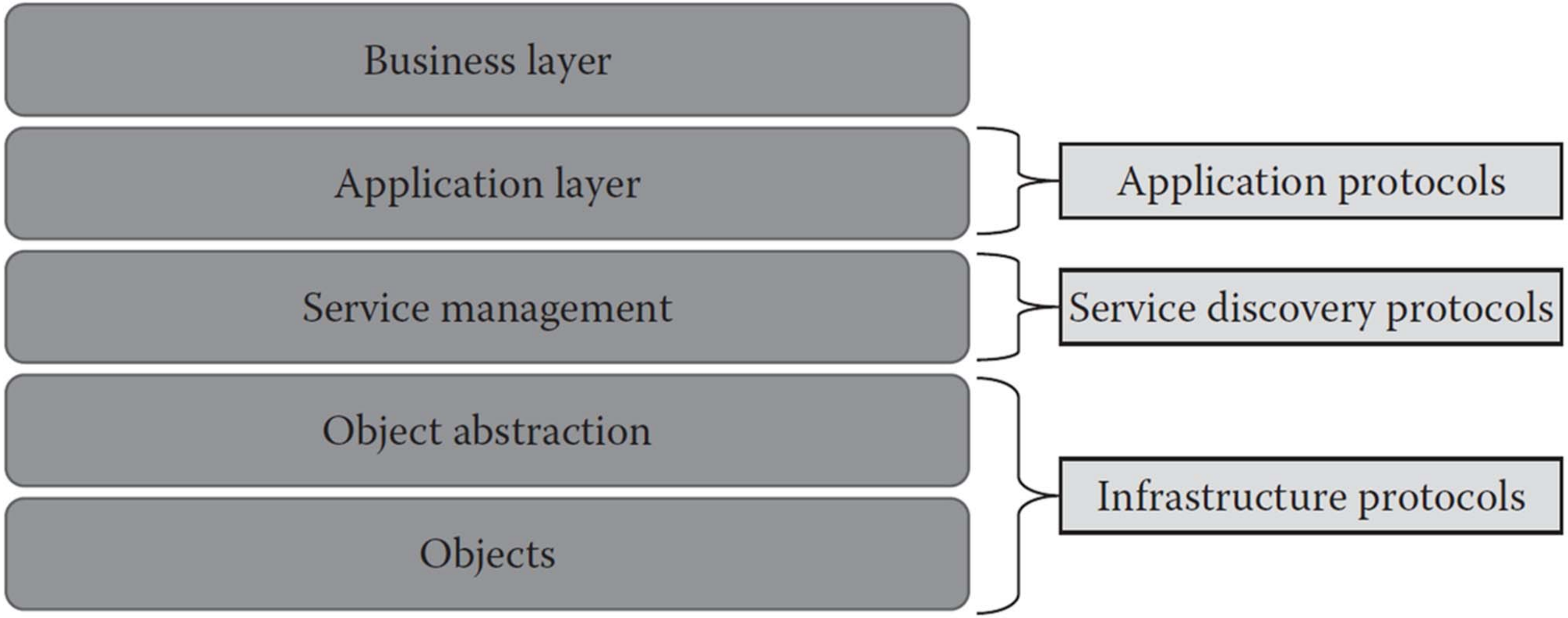
Object Abstraction Layer

transfers data that are collected from objects to service management layer using secure transmission channels

- RFID
- 3G
- GSM
- UMTS
- Wi-Fi
- Bluetooth low energy
- Infrared
- ZigBee

LAYERED ARCHITECTURE OF IOT

Service Management Layer	Middleware for IoT Systems & processes the data received from OAL
	Flexibility to the IoT programmers to work on different types of heterogeneous objects irrespective of their platforms.
	necessary decisions are taken about the delivery of required services,
Application Layer	Diverse kinds of services requested by the customer.
	■ Smart cities ■ Smart energy ■ Smart health care ■ Smart buildings or homes ■ Smart living ■ Smart transportation ■ Smart industry
Business Layer	Overall management of all IoT activities and services.
	Responsibility to design, analyze, implement, evaluate, and monitor the requirements of the IoT system.



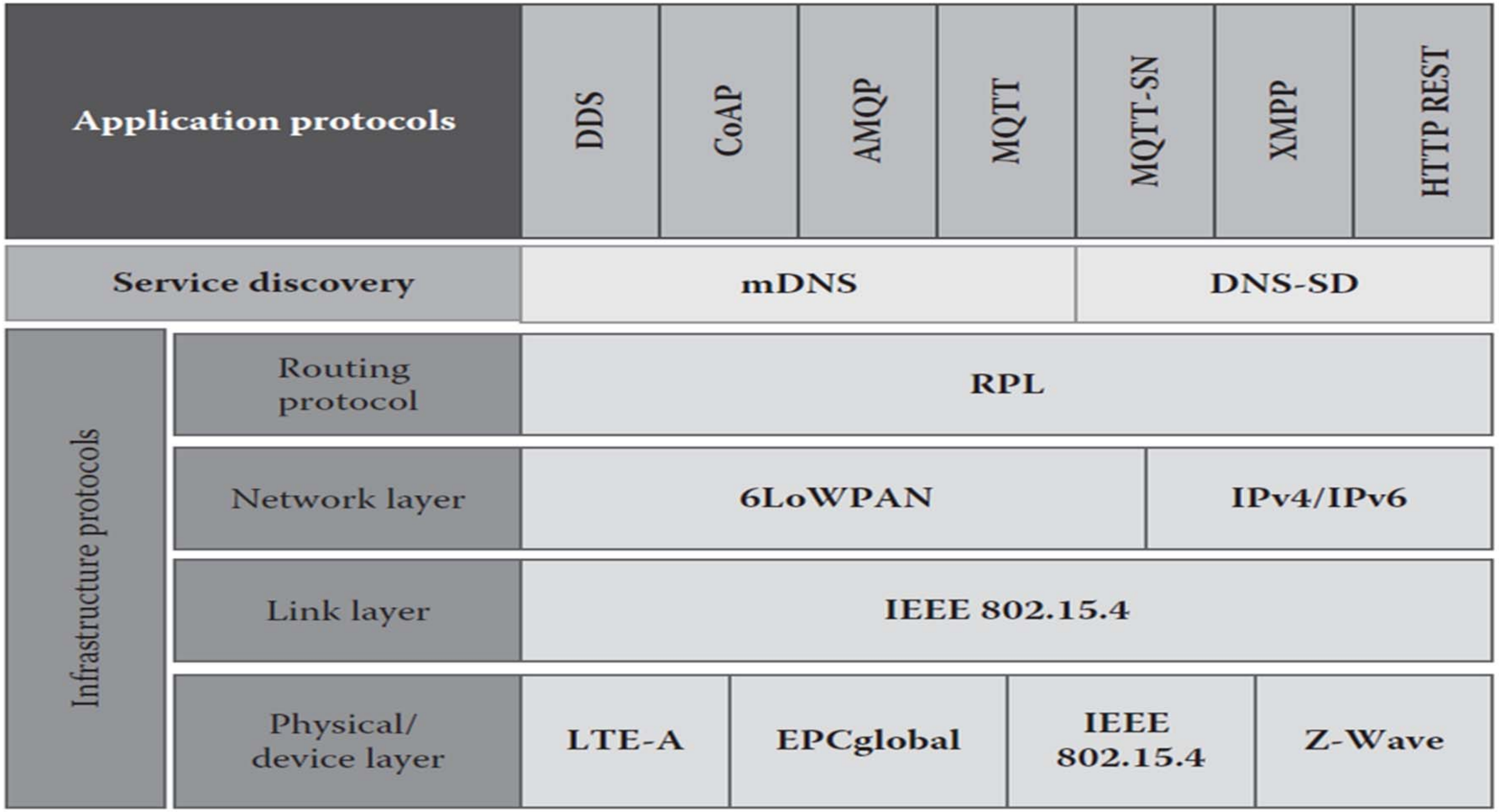
PROTOCOL ARCHITECTURE OF IOT

INFRASTRUCTURE PROTOCOLS

Routing Protocols

Lowpower lossy networks include wireless personal area networks (WPANs), low-power line communication (PLC) networks, and wireless sensor networks (WSNs)

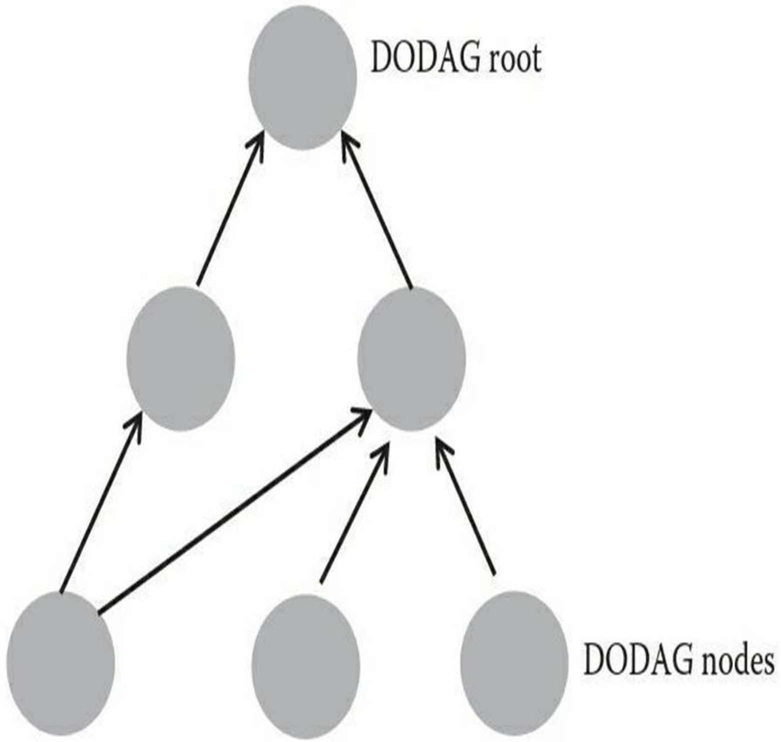
- Capability to optimize and save energy
- Capability to support traffic patterns other than unicast communication
- Capability to run routing protocols over link layers with restricted frame sizes



<table>
<tr><td colspan="2">Application protocols</td><td>DDS</td><td>CoAP</td><td>AMQP</td><td>MQTT</td><td>MQTT-SN</td><td>XMPP</td><td>HTTP REST</td></tr>
<tr><td colspan="2">Service discovery</td><td colspan="4">mDNS</td><td colspan="3">DNS-SD</td></tr>
<tr><td rowspan="4">Infrastructure protocols</td><td>Routing protocol</td><td colspan="7">RPL</td></tr>
<tr><td>Network layer</td><td colspan="5">6LoWPAN</td><td colspan="2">IPv4/IPv6</td></tr>
<tr><td>Link layer</td><td colspan="7">IEEE 802.15.4</td></tr>
<tr><td>Physical/ device layer</td><td>LTE-A</td><td colspan="2">EPCglobal</td><td colspan="2">IEEE 802.15.4</td><td colspan="2">Z-Wave</td></tr>
</table>

CATEGORIZATION OF IOT PROTOCOLS

Routing Protocol



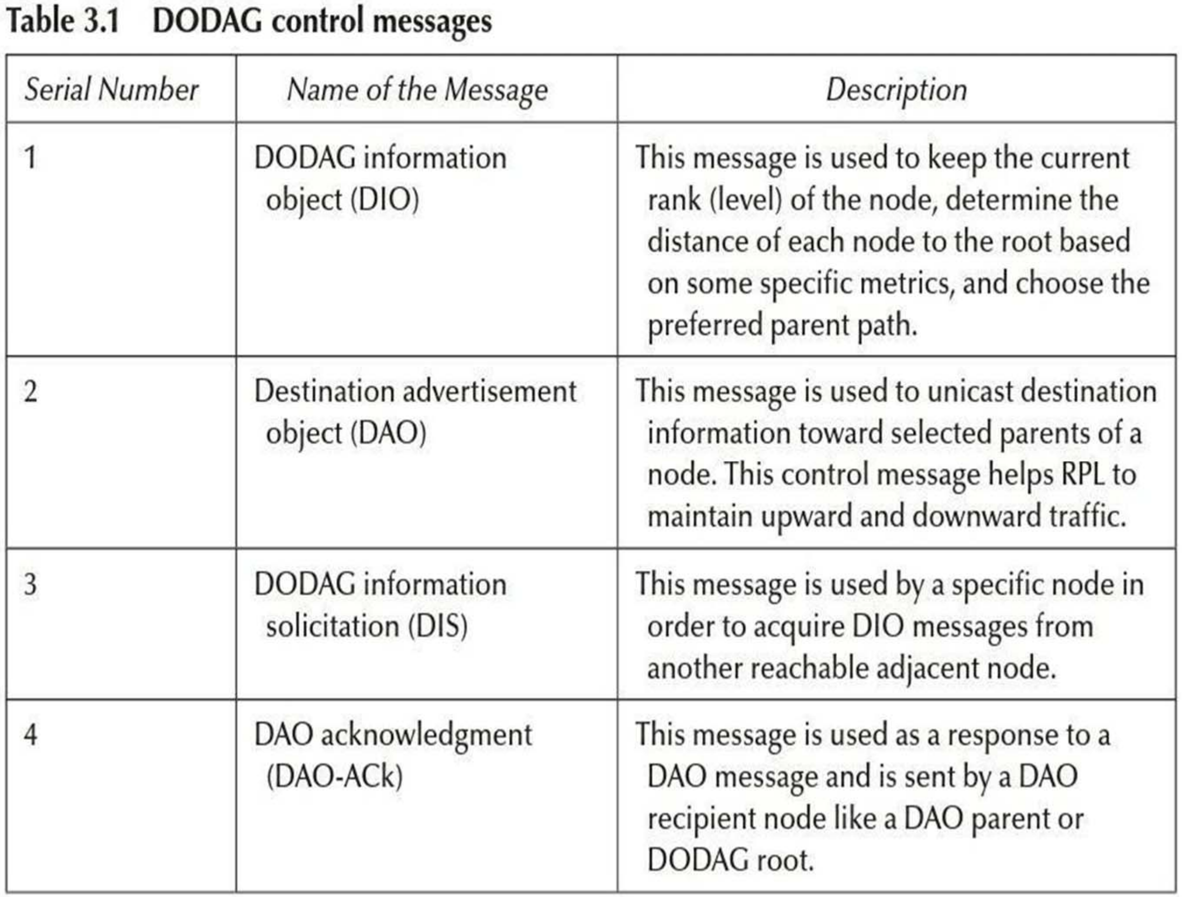


Table 3.1 DODAG control messages

Serial Number	*Name of the Message*	*Description*
1	DODAG information object (DIO)	This message is used to keep the current rank (level) of the node, determine the distance of each node to the root based on some specific metrics, and choose the preferred parent path.
2	Destination advertisement object (DAO)	This message is used to unicast destination information toward selected parents of a node. This control message helps RPL to maintain upward and downward traffic.
3	DODAG information solicitation (DIS)	This message is used by a specific node in order to acquire DIO messages from another reachable adjacent node.
4	DAO acknowledgment (DAO-ACk)	This message is used as a response to a DAO message and is sent by a DAO recipient node like a DAO parent or DODAG root.

IEEE 802.15.4

- Well-known standard for low data-rate WPAN.
- Developed for low-data-rate monitoring and control applications and extended-life low-power-consumption uses.
- This standard uses only the first two layers (PHY, MAC) plus the logical link control (LLC) and service specific convergence sub-layer (SSCS) additions to communicate with all upper layers
- Operates in the ISM band

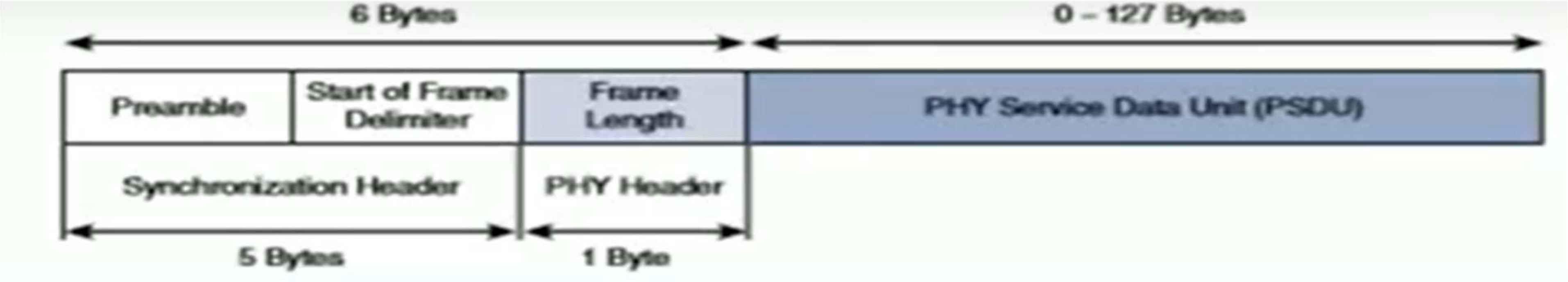
IEEE 802.15.4 Overview

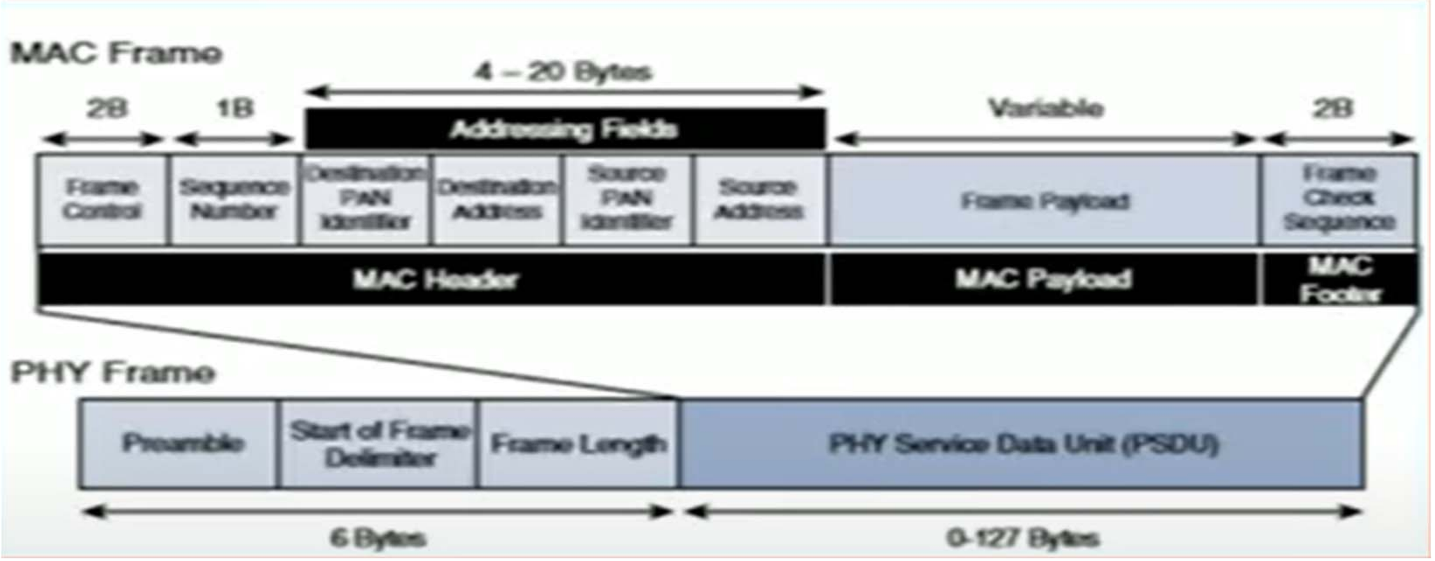
- Low Rate Wireless Personal Area Network (LR-WPAN)
- 2.4 GHz (most common). 16 5-MHz channels
- 250 kbps PHY ⇒ 50 kbps application data rate
- Peak current depends upon symbol rate ⇒ multilevel 4b/symbol)
- Similar to 802.11: Direct Sequence Spread Spectrum, CSMA/CA, Backoff, Beacon, Coordinator (similar to Access point)
- Lower rate, short distance ⇒ Lower power ⇒ Low energy
- Each node has a 64-bit Extended Unique ID (EUI-64):

U/M	G/L	OUI	40 bits assigned by the manufacturer
1b	1b	22b	40b

- No segmentation/reassembly. Max MAC frame size is 127 bytes with a payload of 77+ bytes.

Frame Format



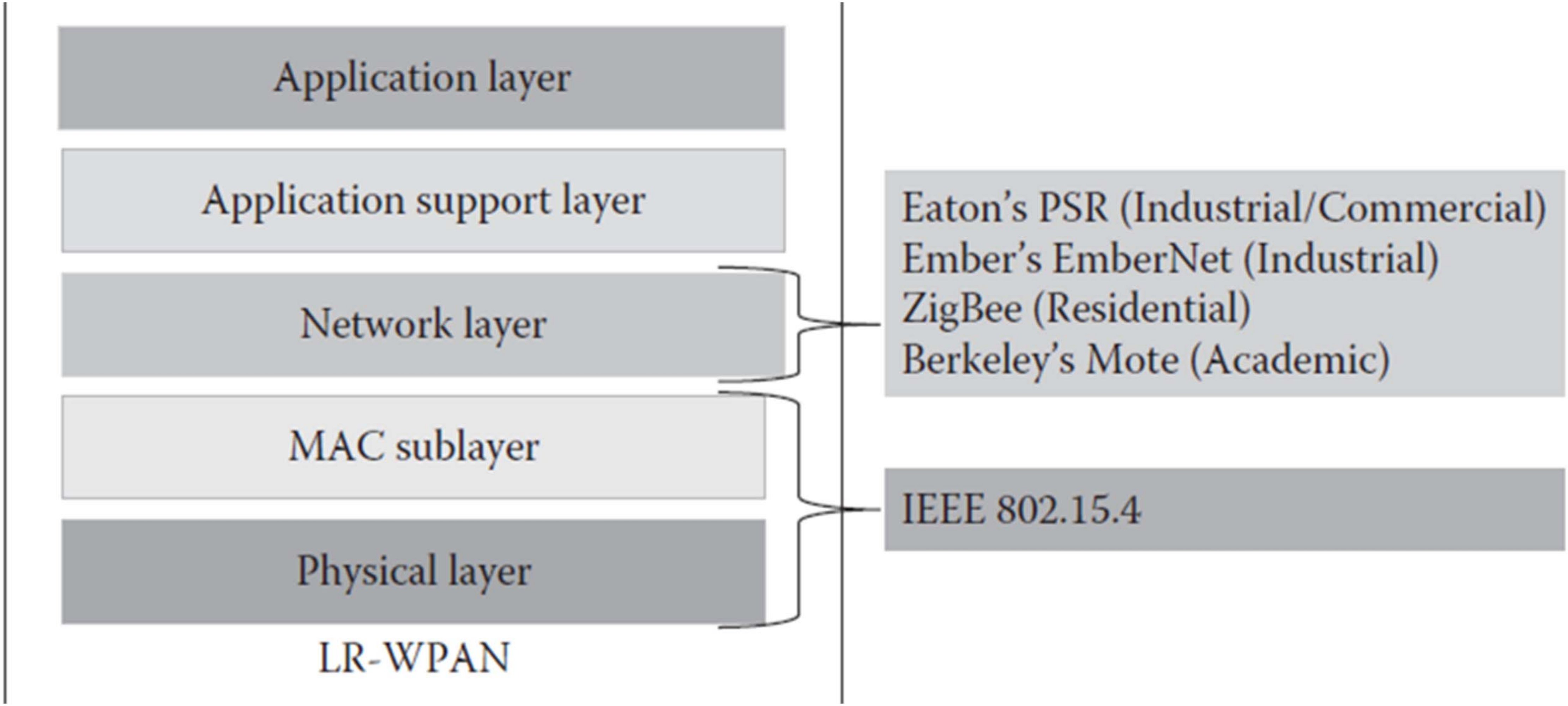


IEEE 802.15.4

- Uses direct sequence spread spectrum (DSSS) modulation.
- Highly tolerant of noise and interference and offers link reliability improvement mechanisms.
- Low-speed versions use Binary Phase Shift Keying (BPSK).
- High data-rate versions use offset-quadrature phase-shift keying (O-QPSK).
- Uses carrier sense multiple access with collision avoidance (CSMA-CA) for channel access.
- Multiplexing allows multiple users or nodes interference-free access to the same channel at different times.

IEEE 802.15.4

- Power consumption is minimized due to infrequently occurring very short packet transmissions with low duty cycle (<1%).
- The minimum power level defined is – 3 dBm or 0.5 mW.
- Transmission, for most cases, is Line of Sight (LOS).
- Standard transmission range varies between 10m to 75m.
- Best case transmission range achieved outdoors can be upto 1000m.
- Networking topologies defined are -- Star, and Mesh.


Application layer
Application support layer
Network layer
MAC sublayer
Physical layer
LR-WPAN
Eaton's PSR (Industrial/Commercial)
Ember's EmberNet (Industrial)
ZigBee (Residential)
Berkeley's Mote (Academic)
IEEE 802.15.4

IEEE 802.15.4

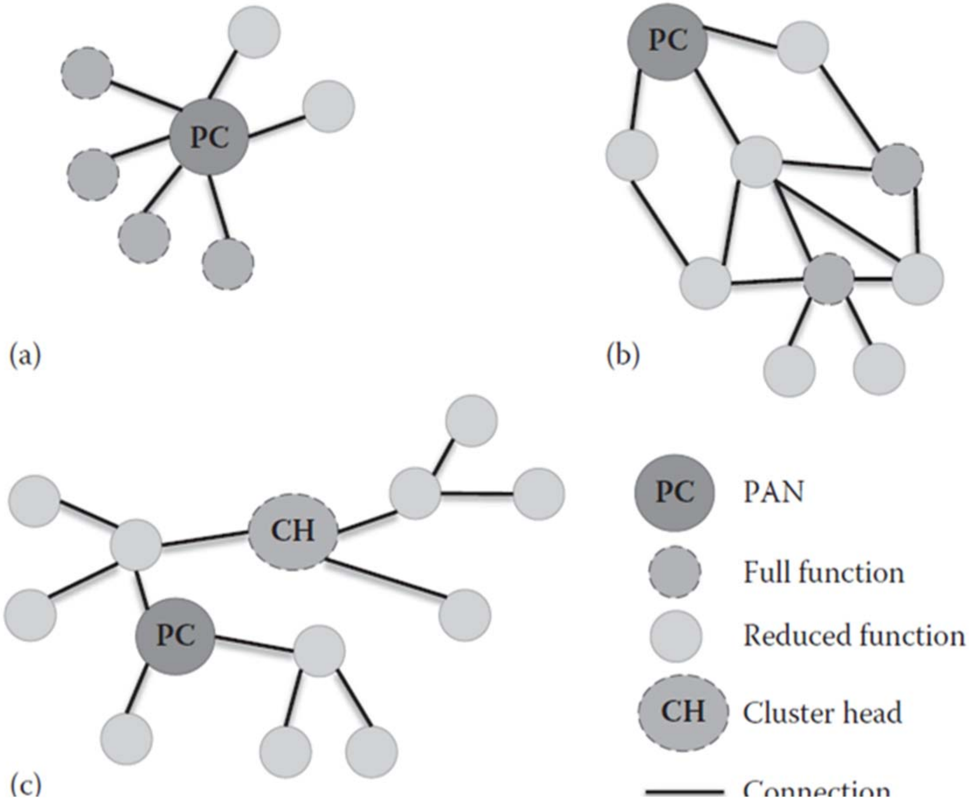
IEEE 802.15.4

Protocol supports two types of Nodes

- Full function devices (FFD): Talks to all types of devices and supports full protocol
  - PAN Coordinator, Router, Device
- Reduced function devices (RFD):Only talk to FFD, Low Power, Minimum CPU/RAM required
  - Device

Topologies

- Star
- Peer-to-peer
- Cluster-tree



IPv6 over 6LoWPWAN

Low-power Wireless Personal Area Networks over IPv6.

Allows for the smallest devices with limited processing abilit to transmit information wirelessly using an Internet protocol.

Allows low-power devices to connect to the Internet.

Created by the Internet Engineering Task Force (IETF) - **RFC 5933 and 4919.**

IPv6 over 6LoWPWAN

Allows IEEE 802.15.4 radios to carry 128-bit addresses of Internet Protocol version 6 (IPv6).

Header compression and address translation techniques allow the IEEE 802.15.4 radios to access the Internet.

IPv6 packets compressed and reformatted to fit the IEEE 802.15.4 packet format.

Uses include IoT, Smart grid, and M2M applications.

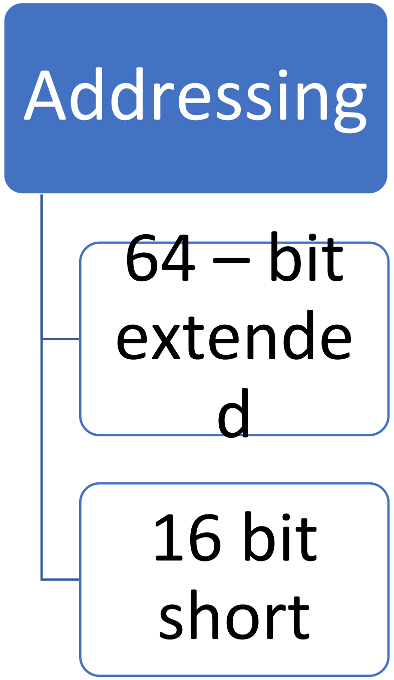
6LoWPAN

64-bit addresses: globally unique

16 bit addresses: PAN specific; assigned by PAN coordinator

IPv6 multicast not supported by 802.15.4

IPv6 are packets carried as link layer broadcast frames

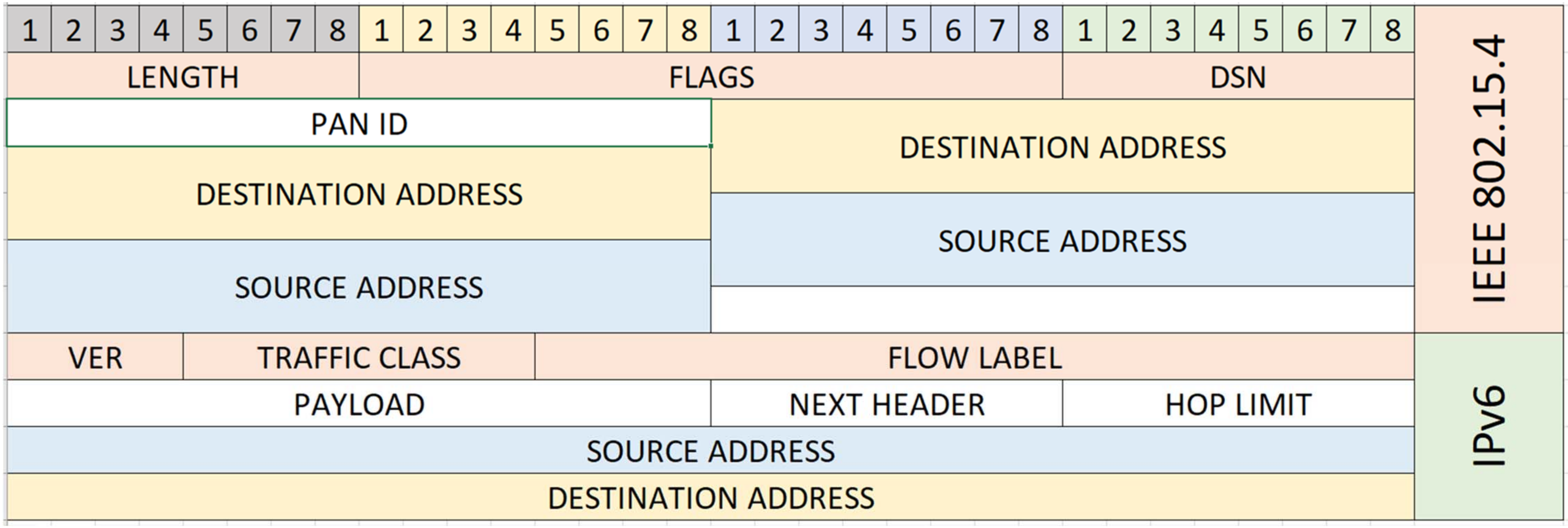


Addressing

64 – bit extende d

16 bit short

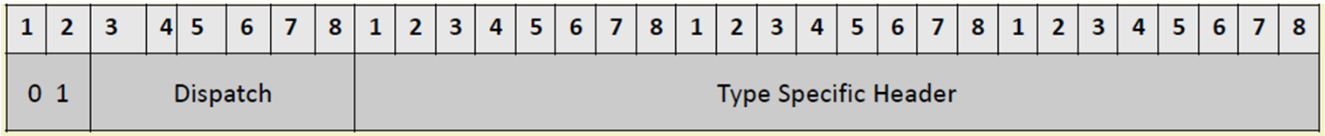
6LoWPAN Packet Format



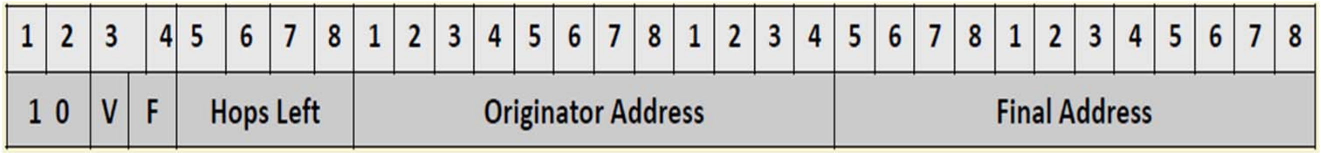
<table>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td rowspan="7">IEEE 802.15.4</td></tr>
<tr><td colspan="8">LENGTH</td><td colspan="16">FLAGS</td><td colspan="8">DSN</td></tr>
<tr><td colspan="16">PAN ID</td><td colspan="16" rowspan="2">DESTINATION ADDRESS</td></tr>
<tr><td colspan="16" rowspan="2">DESTINATION ADDRESS</td></tr>
<tr><td colspan="16" rowspan="2">SOURCE ADDRESS</td></tr>
<tr><td colspan="16" rowspan="2">SOURCE ADDRESS</td></tr>
<tr><td colspan="16"></td></tr>
<tr><td colspan="4">VER</td><td colspan="8">TRAFFIC CLASS</td><td colspan="20">FLOW LABEL</td><td rowspan="4">IPv6</td></tr>
<tr><td colspan="16">PAYLOAD</td><td colspan="8">NEXT HEADER</td><td colspan="8">HOP LIMIT</td></tr>
<tr><td colspan="32">SOURCE ADDRESS</td></tr>
<tr><td colspan="32">DESTINATION ADDRESS</td></tr>
</table>

Header Type

- Dispatch Header
- Mesh Addressing Header
- Fragmentation Header: First Fragment, Second Fragment

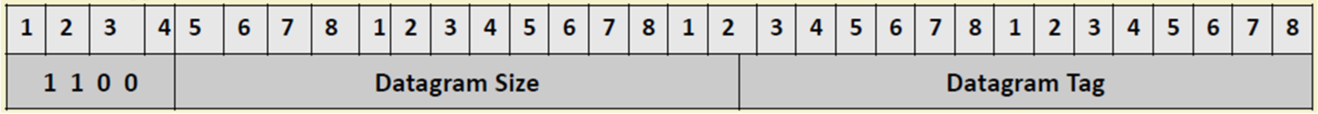


1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
0 1		Dispatch						Type Specific Header																							



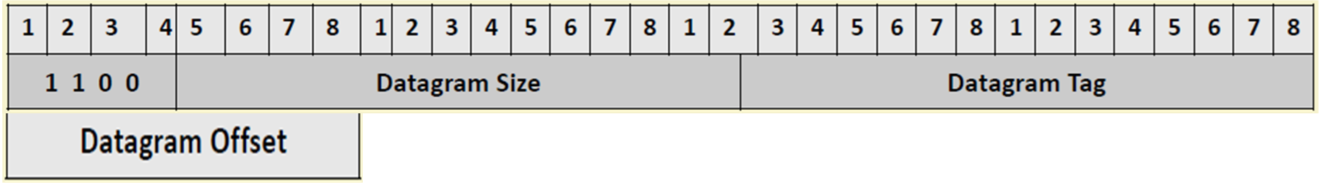
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
1 0		V	F	Hops Left				Originator Address												Final Address											

First Fragment



1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
1 1 0 0				Datagram Size														Datagram Tag													

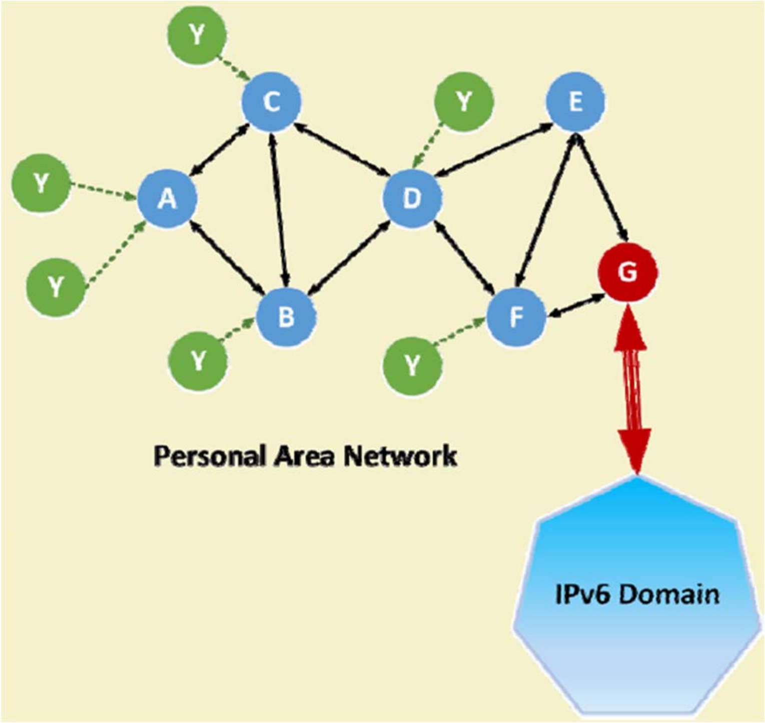
Second Fragment



1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
1 1 0 0				Datagram Size														Datagram Tag													
Datagram Offset																															

Routing in 6LoWPAN

- Mesh routing within PAN Space
- Routing between IPv6 and the PAN domain
- Types are LOADng, RPL
- LOADng
  - Built on top of AODV
  - RREQ, RREP, RERR messages
  - Uses Optimal Flooding
- RPL
  - Built over Distance vector IPv6
  - Routing information maintained within packet
  - Two modes of operation: Proactive & Reactive

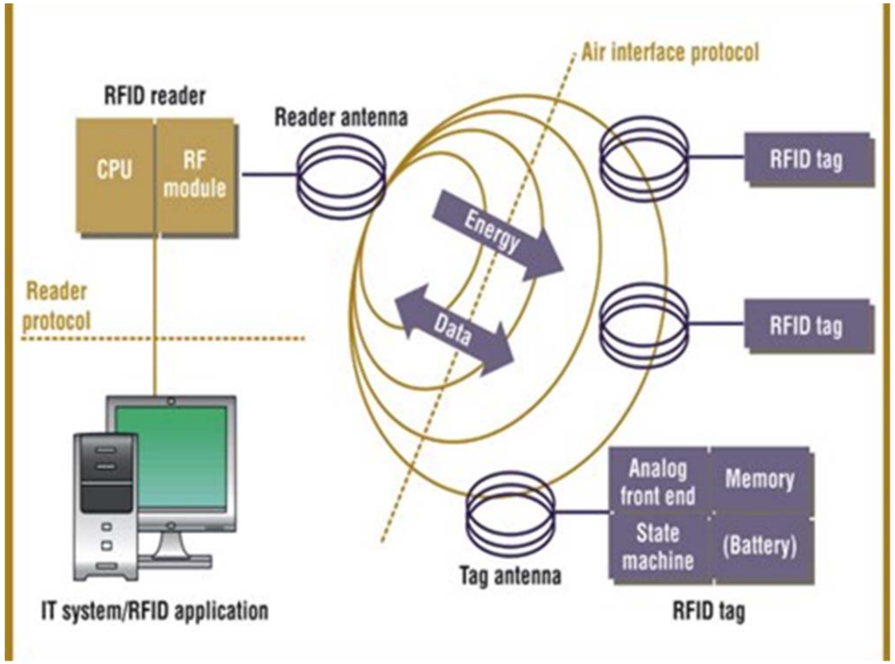


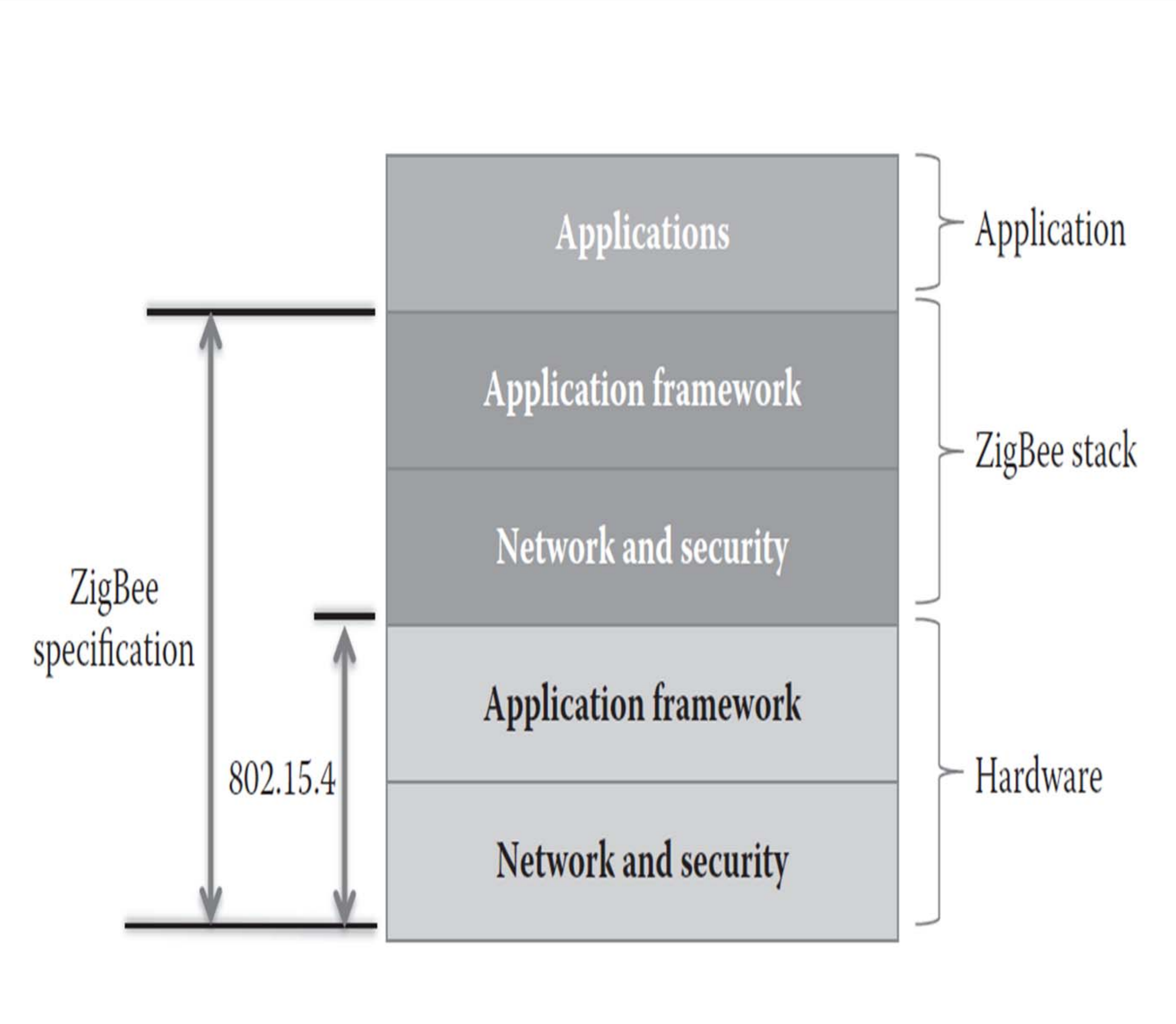
Radio Frequency Identifier (RFID)

- Data is digitally encoded in RFID tags, which can be read by a reader
- RFID tag data can be read outside the line-of-sight
- RFID tag consists of an integrated circuit and an antenna
- Tags may be passive or active
- Passive tags must be powered by a reader inductively before they can transmit information, whereas active tags have their own power supply
- Derived from Automatic Identification and Data Capture (AIDC) technology

RFID

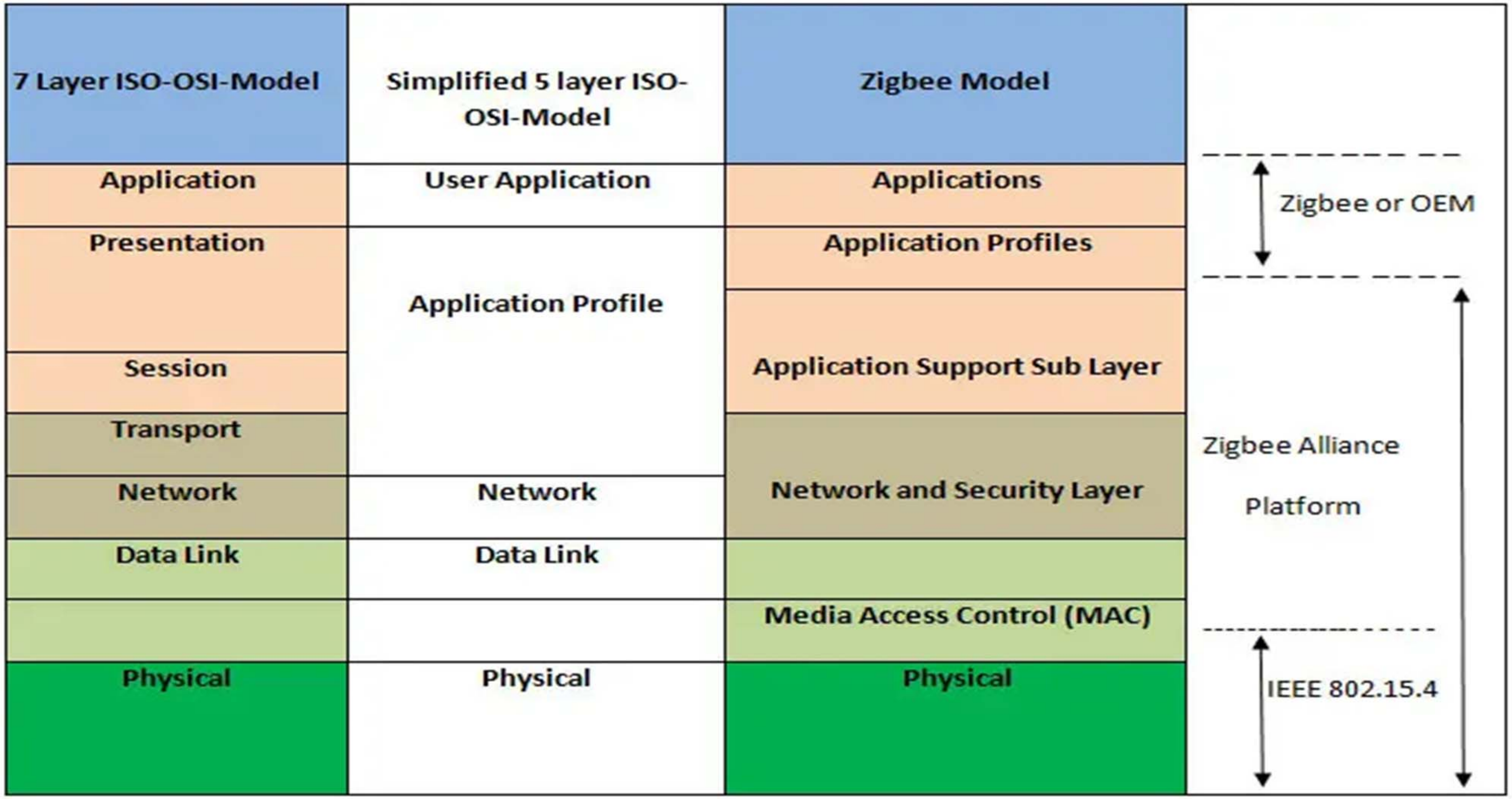
- AIDC performs object identification, object data collection and mapping of the collected data to computer systems with little or no human intervention.
- AIDC uses wired communication
- RFID uses radio waves to perform AIDC functions.
- The main components of an RFID system include an RFID tag or smart label, an RFID reader, and an antenna.





Zigbee

- Most widely deployed enhancement of IEEE 802.15.4.
- It works with the 802.15.4 layers 1 and 2
- The most popular use of ZigBee is wireless sensor networks using the mesh topology.
- Features
  - Low Power
  - Low Cost
  - Support for <=65k nodes



7 Layer ISO-OSI-Model	Simplified 5 layer ISO-OSI-Model	Zigbee Model	
Application	User Application	Applications	Zigbee or OEM
Presentation	Application Profile	Application Profiles	
		Application Support Sub Layer	Zigbee Alliance Platform
Session			
Transport		Network and Security Layer	
Network	Network		
Data Link	Data Link	Media Access Control (MAC)	
Physical	Physical	Physical	IEEE 802.15.4

Fig. 4: A Figure Illustrating Architectural Overview of Zigbee Technology

Zigbee

IMPORTANT COMPONENTS

ZigBee End Device (ZED):

ü It contains just enough functionality to talk to the parent node, and it cannot relay data from other devices.

ü This allows the node to be asleep a significant amount of the time thereby enhancing battery life.

ü Memory requirements and cost of ZEDs are quite low, as compared to ZR or ZC.

ZigBee Router (ZR):

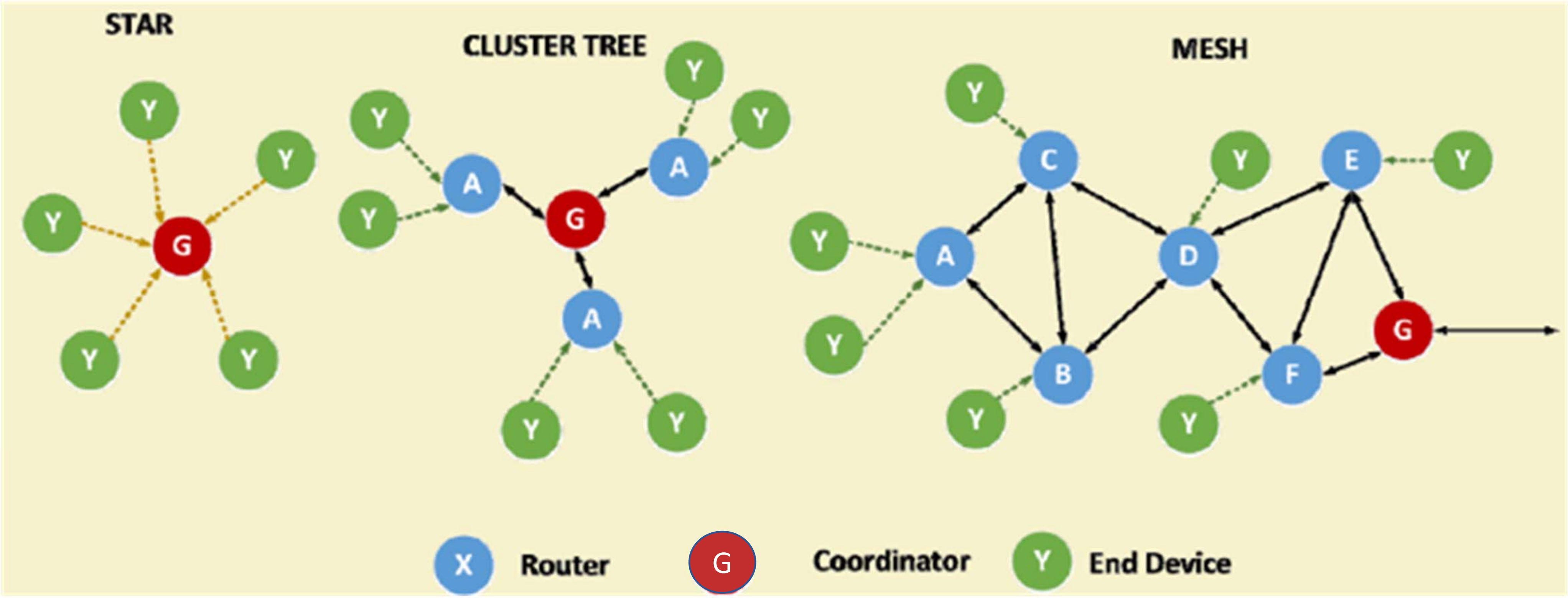
ü Capable of running applications, as well as relaying information (baecon) between nodes connected to it.

Zigbee Coordinator (ZC):

ü Responsible for selecting the channel, PAN ID, security policy, and stack profile for a network

ü Each Zigbee network must have one coordinator, since a ZC is responsible to start a Zigbee network

Zigbee Topologies



Z-Wave

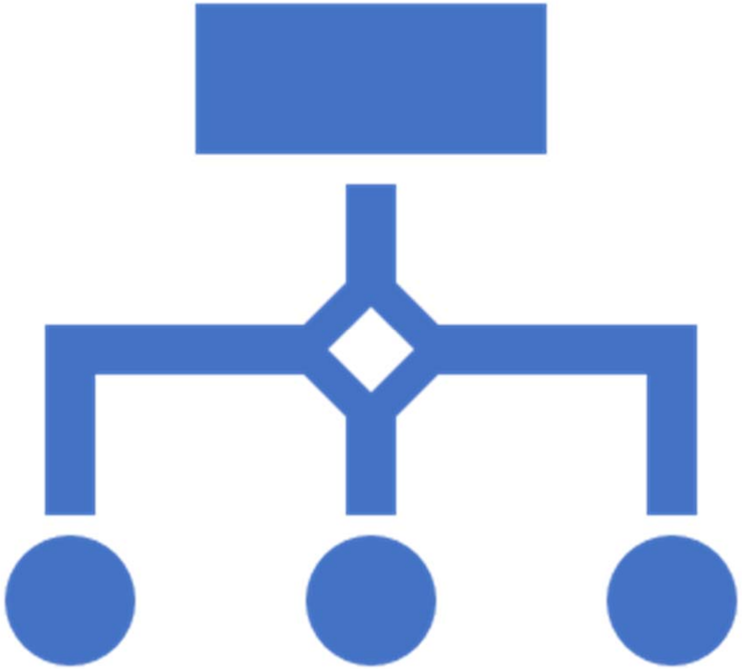
- Low-power wireless communication protocol that is mainly used for home area networks (HAN)
- Z-Wave operates mainly in the sub-GHz frequency range that is typically around 900 MHz.
- Uses low-powered mesh networking topology and works on RF.
- Important Components are *Controllers, Slave Nodes*

Z-Wave

CONTROLLERS: Devices that has the capability to build a routing table for Z-Wave network.

Types

1. Primary Controller
   - ✓ Device that contains a description of the Z-Wave network and has the capability to control the outputs.
   - ✓ There will be only one primary controller in a network at a specific point in time
2. Secondary Controller
   - ✓ Device that contains the network ID and remains stationary in order to maintain the routing table.

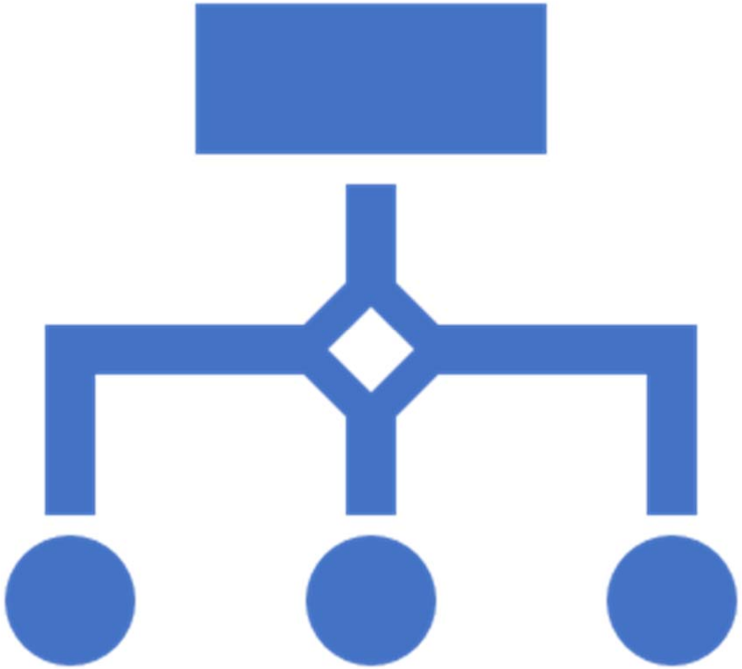


Z-Wave

SLAVE NODES: do not contain routing tables, but instead may contain a network map.

Types:

1. Slave nodes: Receives frames from other nodes and respond to them if necessary.
2. Routing slave: Provides several alternate routes for talking to other slave nodes and controllers.
3. Frequently listening routing slave: Configured to wake up at the time of every wake-up interval



Z-Wave vs Zigbee

User friendly and provides a simple system that users can set up themselves.	Requires so little power that devices can last up to seven years on one set of batteries.
Ideal for someone with a basic understanding of technology who wants to keep their home automation secure, efficient, simple to use, and easy to maintain.	Ideal for technology experts who want a system they can customize with their preferences and install themselves.

Bluetooth

- Bluetooth wireless technology is a short range communications technology.
- Intended for replacing cables connecting portable units
- Maintains high levels of security.
- Bluetooth technology is based on Ad-hoc technology also known as Ad-hoc Piconets
- Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHZ
- Uses spread spectrum hopping, full-duplex signal at a nominal rate of 1600 hops/sec
- Bluetooth supports 1Mbps data rate for version 1.2 and 3Mbps data rate for Version 2.0 combined with Error Data Rate.

Bluetooth

Bluetooth operating range depends on the device:

- **Class 3** radios have a range of up to 1 meter or 3 feet
- **Class 2** radios are most found in mobile devices have a range of 10 meters or 30 feet
- **Class 1** radios are used primarily in industrial use cases that have a range of 100 meters or 300 feet.

Connection Establishment

- **Inquiry** run by one Bluetooth device to try to discover other devices near it.
- Process of forming a **connection** between two Bluetooth devices.
- A device either actively **participates** in the network or enters a low-power sleep mode.

Bluetooth

Modes of Operation

1. Active: Actively transmitting or receiving data
2. Sniff: Sleeps and only listens for transmissions at a set interval
3. Hold: Power-saving mode where a device sleeps for a defined period and then returns back to active mode
4. Park: Slave will become inactive until the master tells it to wake back up

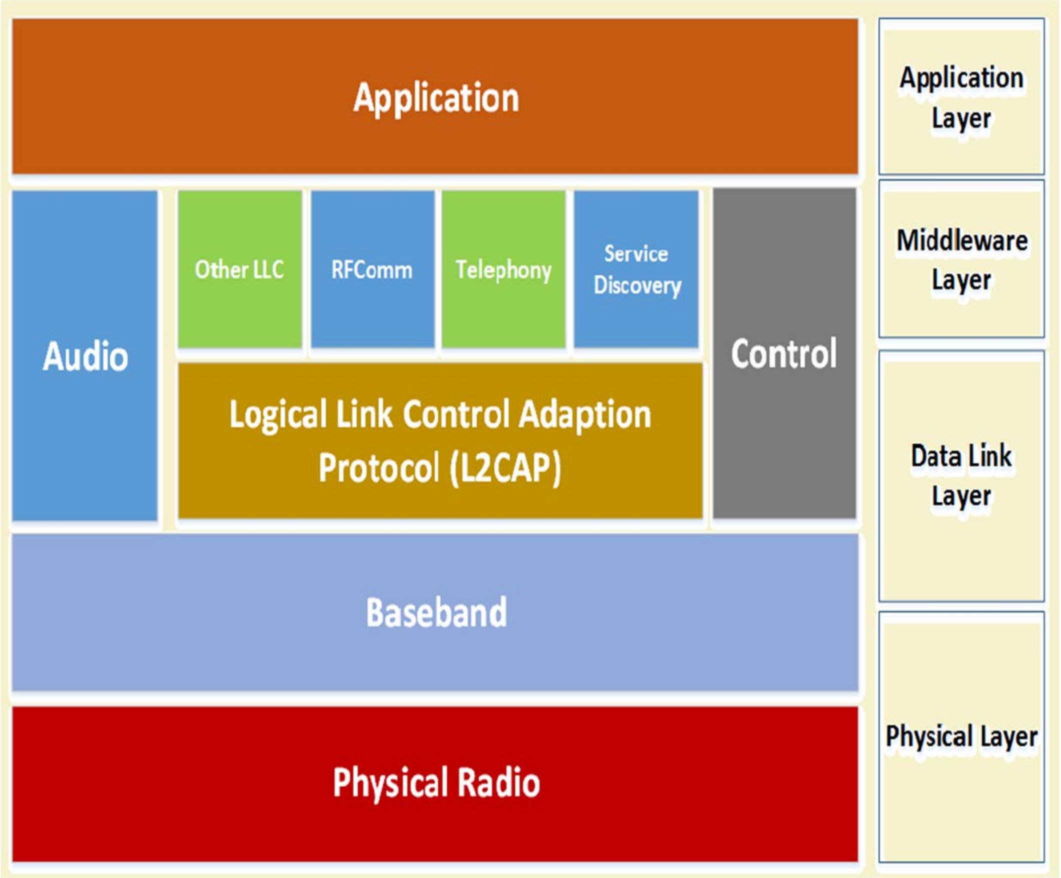
Bluetooth

Baseband:

- Physical Layer
- Manages physical channels & links
- Error correction & Security
- Paging & Enquiry

L2CAP:

- Used to multiplex multiple logical connections between two devices
- Provide con-oriented and con-less communication to upper layers

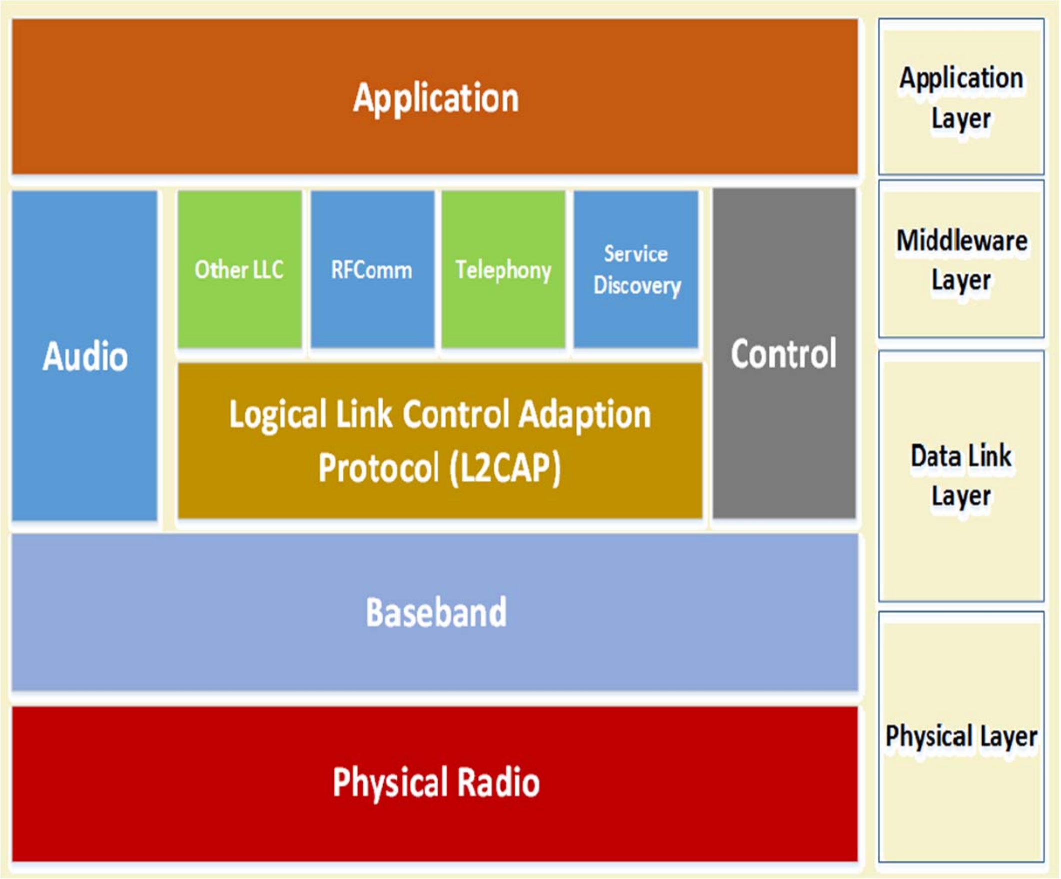


Bluetooth

RFComm:

  - provides for binary data transport
  - simple reliable data stream to the user, like TC
  - Supports up to 60 simultaneous connections between two BT devices

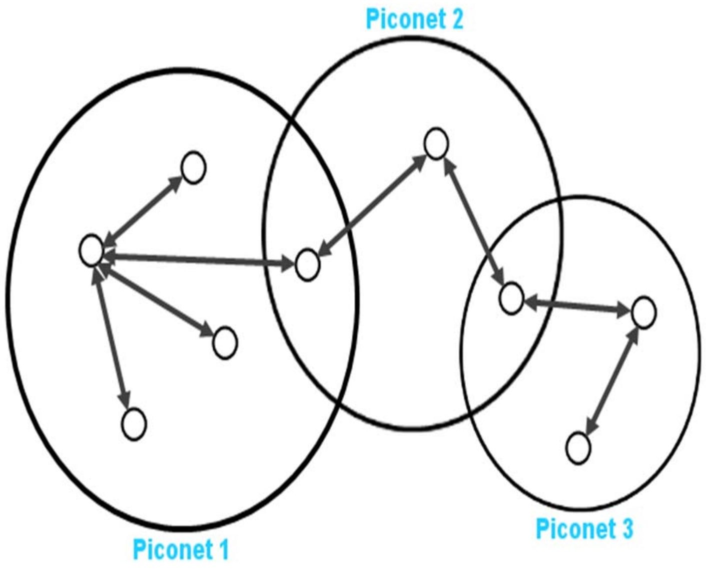
- SDP:
  - Enables applications to discover available services and their features
  - Uses a req/resp model



Bluetooth

Piconet:

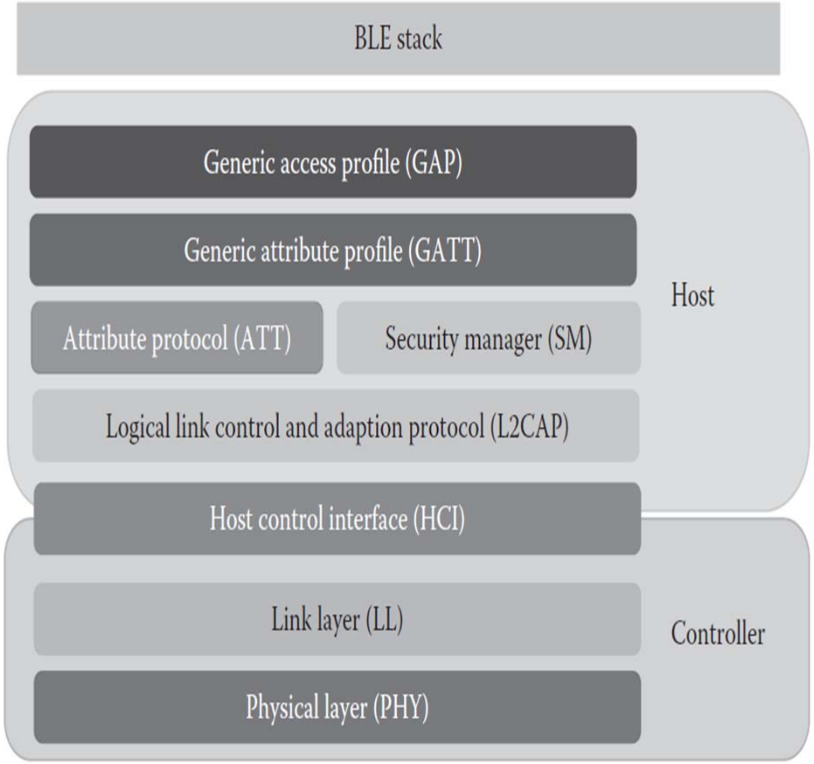
- Short range networks using which Bluetooth enabled electronic devices connect & communicate wirelessly
- Simplest configuration is a **point to point configuration** with one master and one slave
- Piconet can contain up to **seven** slaves clustered around a single master.
- Adopts **TDMA**
- The clock and **unique 48-bit address** of master determines the timing of various devices and the frequency hopping sequence of individual devices.
- All connections are either master-to-slave or slave-to-master
- Transmission starts in the **slave-to-master time slot** immediately following a polling packet from the master.



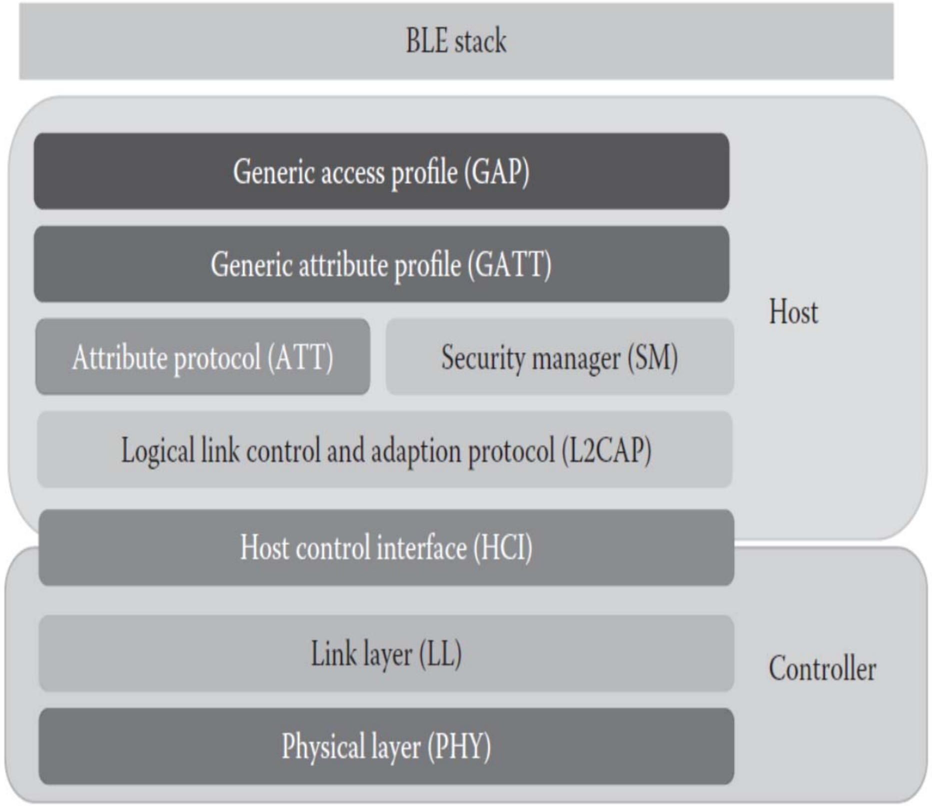
Bluetooth Low Energy

- Uses short-range radio with minimum power and operates for a long time.
- Range coverage is about 100 meters, which is roughly about 10 times more than conventional Bluetooth
- Latency of BLE is 15 times lesser than that of conventional Bluetooth.
- BLE operates using a power between 0.01mW and 10mW.

Bluetooth®
SMART READY


BLE stack
Generic access profile (GAP)
Generic attribute profile (GATT)
Attribute protocol (ATT)
Security manager (SM)
Logical link control and adaption protocol (L2CAP)
Host
Host control interface (HCI)
Link layer (LL)
Physical layer (PHY)
Controller

Bluetooth® SMART READY



BLE stack

Generic access profile (GAP)

Generic attribute profile (GATT)

Attribute protocol (ATT)

Security manager (SM)

Logical link control and adaption protocol (L2CAP)

Host

Host control interface (HCI)

Link layer (LL)

Physical layer (PHY)

Controller

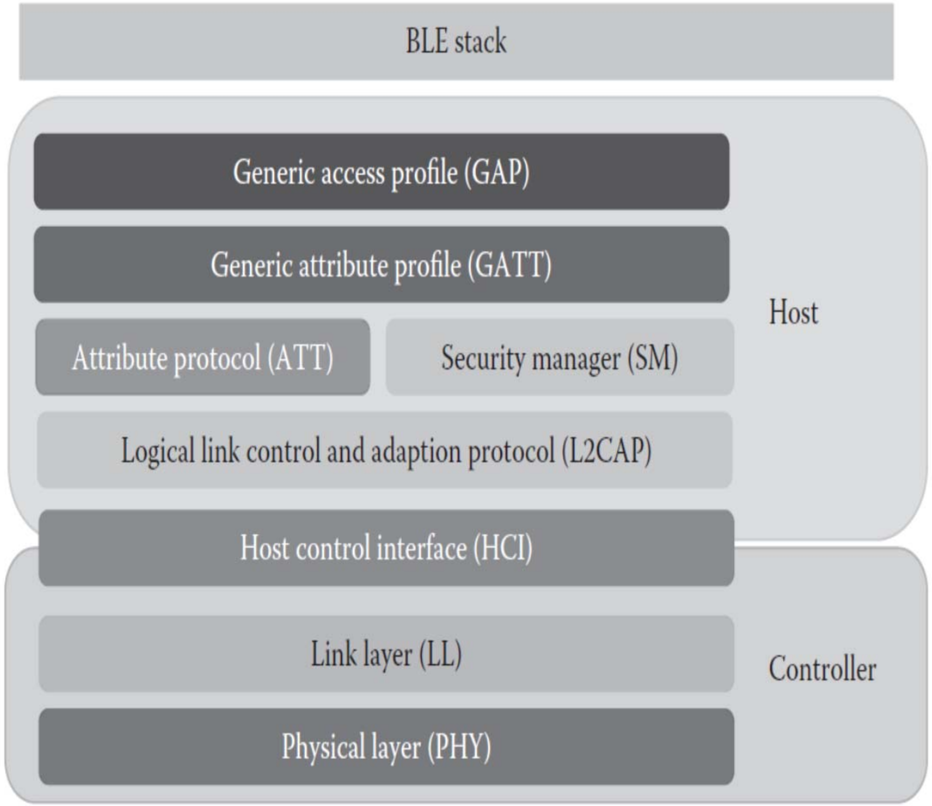
Physical layer: This layer receives and transmits data bits.

Link layer: Following are the functions performed by the link layer:

- Media access control
- Error control
- Connection establishment
- Flow control

Host control interface (HCI): The HCI layer provides a command, event, and data interface that allows link layer to access the data from upper layers such as GAP, L2CAP, and SMP.

Logical link control adaptation protocol (L2CAP): This layer mainly performs multiplexing of data channels. This layer also does fragmentation and reassembly of larger packets


BLE stack
Generic access profile (GAP)
Generic attribute profile (GATT)
Attribute protocol (ATT)
Security manager (SM)
Logical link control and adaption protocol (L2CAP)
Host
Host control interface (HCI)
Link layer (LL)
Physical layer (PHY)
Controller

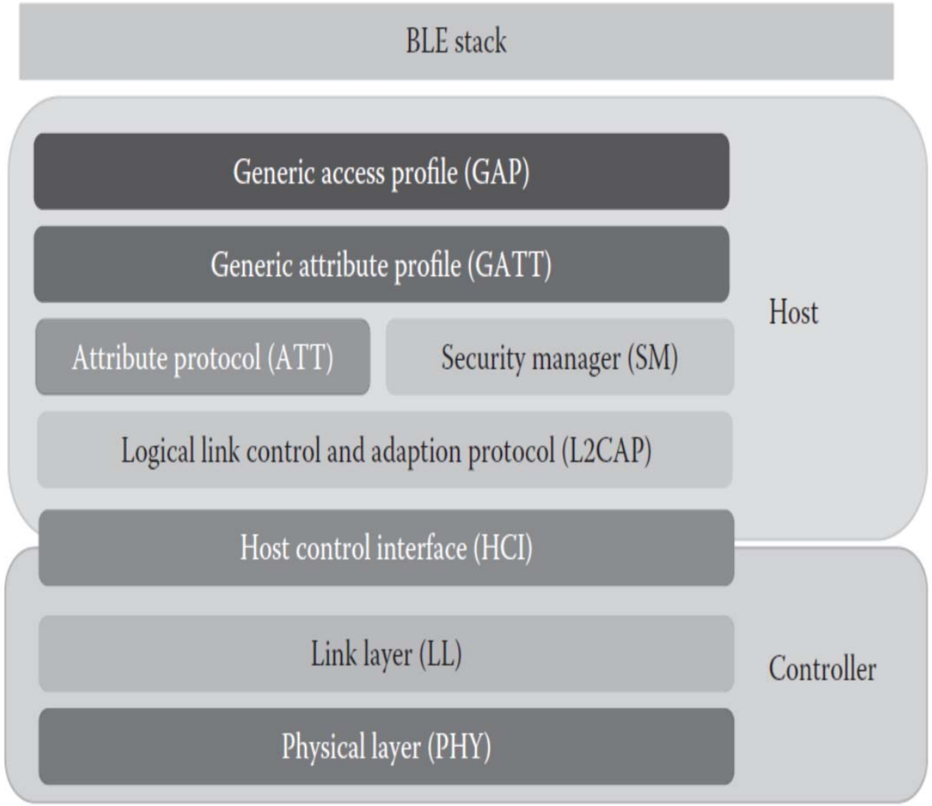
Bluetooth® SMART READY

Generic attribute profile (GATT) specifies a framework using the attribute protocol (ATT) layer.

- **GATT client**:
  - Any device that wants data is called a GATT client.
  - It sends requests and commands to the GATT server.
  - A GATT client can receive responses and other notifications sent by the GATT server.
- **GATT server**:
  - Any device that has the data and can accept incoming requests from the GATT client is called GATT server.
  - A GATT server sends responses to a GATT client.

Attribute Protocol: Thiis layer allows a GATT server to communicate with a GATT client by exposing a set of attributes and interfaces.

Security Manager Protocol (SMP): Specifies the procedures and behavior to ensure security by managing pairing, authentication, and encryption between the devices.



BLE stack

Generic access profile (GAP)

Generic attribute profile (GATT)

Attribute protocol (ATT)

Security manager (SM)

Logical link control and adaption protocol (L2CAP)

Host

Host control interface (HCI)

Link layer (LL)

Physical layer (PHY)

Controller

Bluetooth® SMART READY

Generic access profile (GAP): This layer defines processes related to the discovery of Bluetooth devices and lays down link management aspects while establishing connection between Bluetooth devices.

Following are different types of roles defined by GAP:

- **Broadcaster role**: A device that operates in this role can send advertising events.
- **Observer role**: A device that operates in this mode can receive advertising events.
- **Peripheral role**: A device that is in the peripheral role accepts the establishment of an LE physical connection.
- **Central role**: A device that is in central role initiates establishment of a physical connection.

Long Term Evolution - Advanced

LTE broadcast is a single frequency network (SFN) that operates in a broadcast mode.

There are several key use cases of LTE for IoT because of its service cost, scalability, and performance especially from a smart city or intelligent city perspective.

Applications include Live Streaming, TV Broadcast, New, Stock Weather reports etc.

is a part of the series of standards known as evolved multimedia broadcast multicast service

Device or Service Discovery for IoT

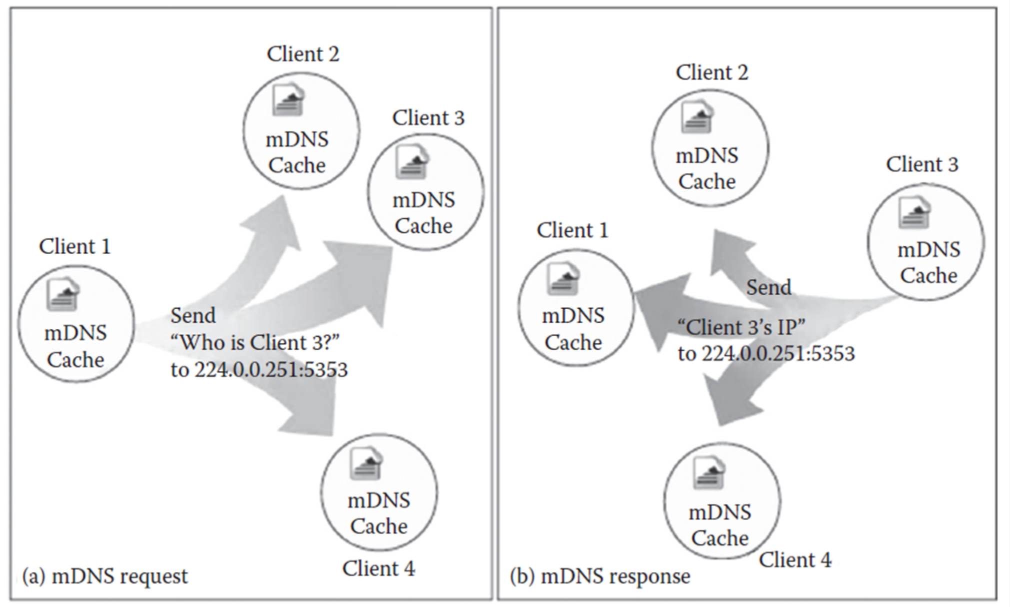
- Bluetooth Beacon's:
  - Communication based on unique Beacon ID

- Wi-Fi Aware:
  - allow a user’s smart phone to act as both a broadcaster and a receiver
  - allow other smart phone users to discover and connect
  - Share photos, play games, and for several other purposes.

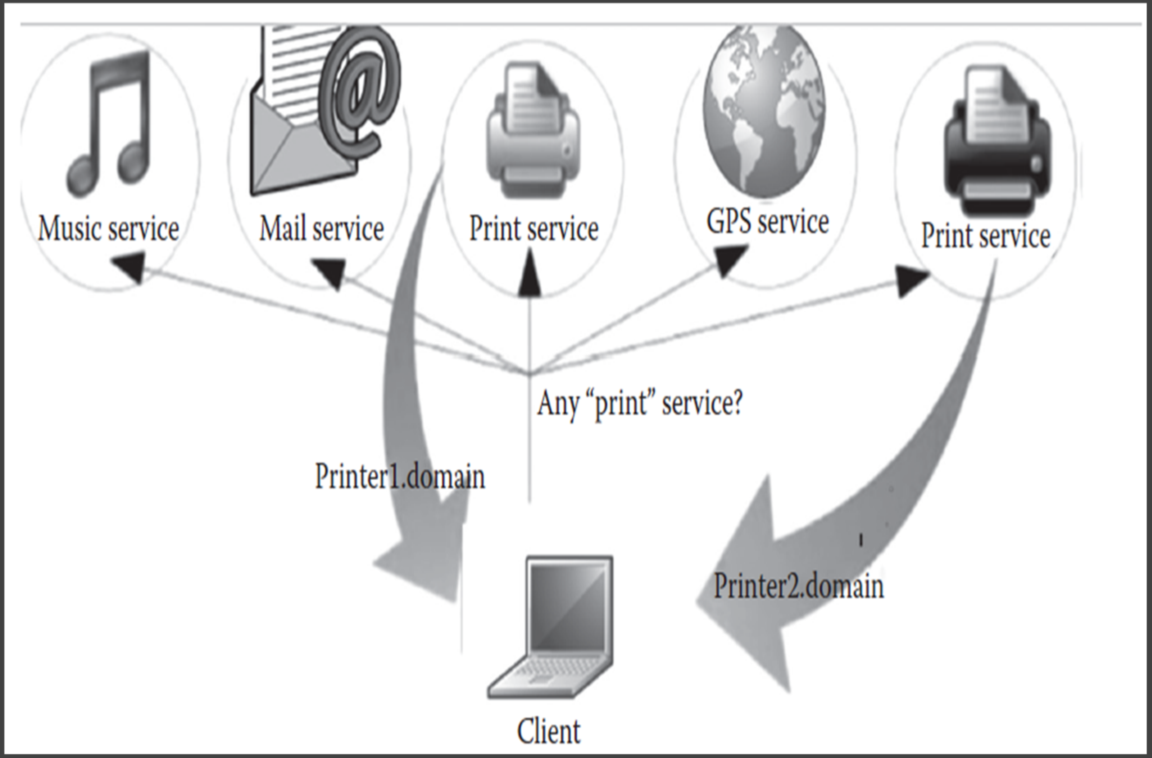
Wi Fi™
Aware

Protocols for IoT Service discovery

- **Multicast Domain Name System**:
  - Adopts a simple multicast messaging technique
  - Every node in the network receives this multicast request which contains the name of the intended receipient
  - The recepient sends a multicast response with its IP address
  - All devices within the network update their cache with the latest IP Address.



Protocols for IoT Service discovery



- **DNS Service Discovery**
  - Helps to discover the desired services present in the network
  - Uses standard DNS messages that typically uses mDNS.
  - Finding host names of required services (ex: printer service)
  - Pairing IP addresses with their host names using mDNS

Protocols for IoT Service discovery

- Universal Plug n Play:
  - Is a collection of networking protocols
  - Capability of a UPnP device is to join a network dynamically (automatically) and obtain IP addresses of other devices
  - At the same time convey its capabilities to other devices
  - Zero configuration and administration
  - Three basic components of UPnP are Device, Control Points, Services
  - The protocol that offers service discovery feature for a UPnP network is the simple service discovery protocol (SSDP).