Communication Technologies for IoT – Part 1
Infrastructure and Service Discovery Protocols

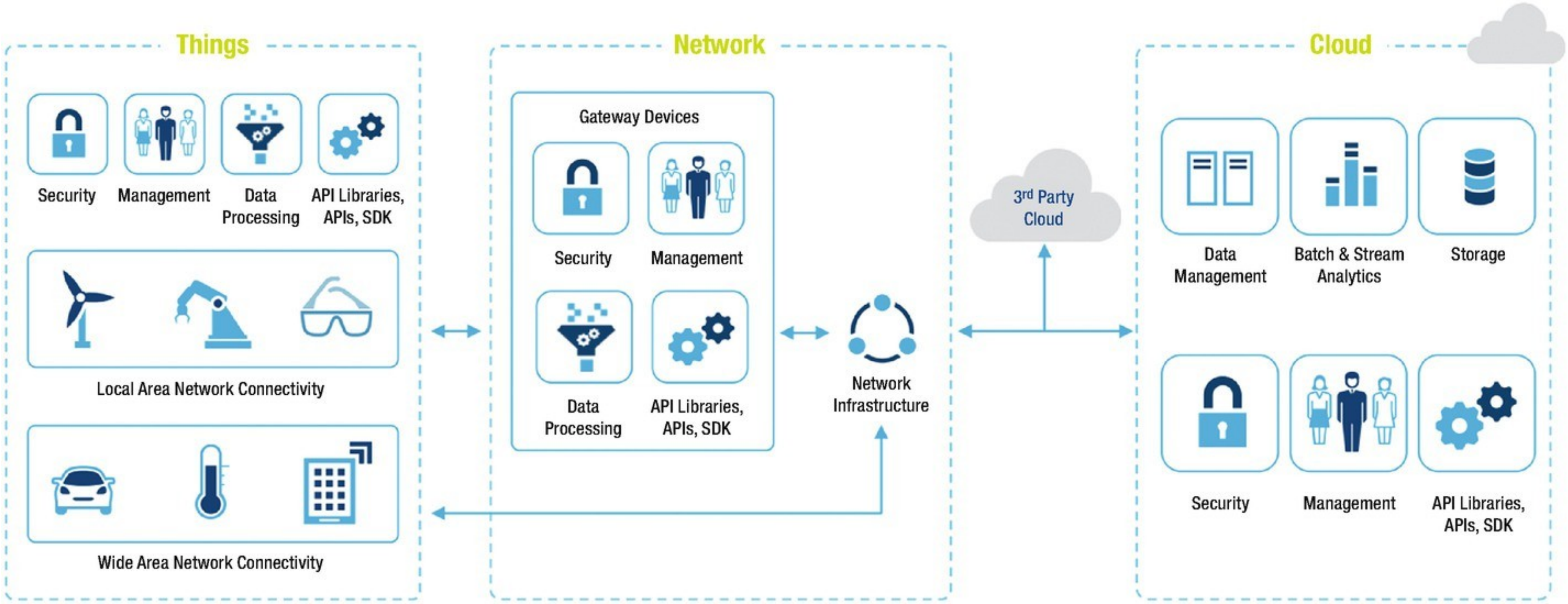
Dr. Bibhas Ghoshal

IIIT Allahabad

Connectivity Considerations

- Connectivity between IoT devices and outside world dictates network architecture
- Choice of communication technology dictates IoT device hardware requirement and costs
- Due to presence of numerous applications of IoT enabled devices, a single networking paradigm not sufficient to all needs of the consumer or IoT device
- Complexity of networks - interference among devices, network management, heterogeneity in networks, protocol standardization within networks

Network Configuration in IoT



Cheruvu S., Kumar A., Smith N., Wheeler D.M. (2020) Connectivity Technologies for IoT. In: Demystifying Internet of Things Security. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-2896-8_5

Some Network Terminologies

LAN : Local short range communication, may or may not connect to Internet

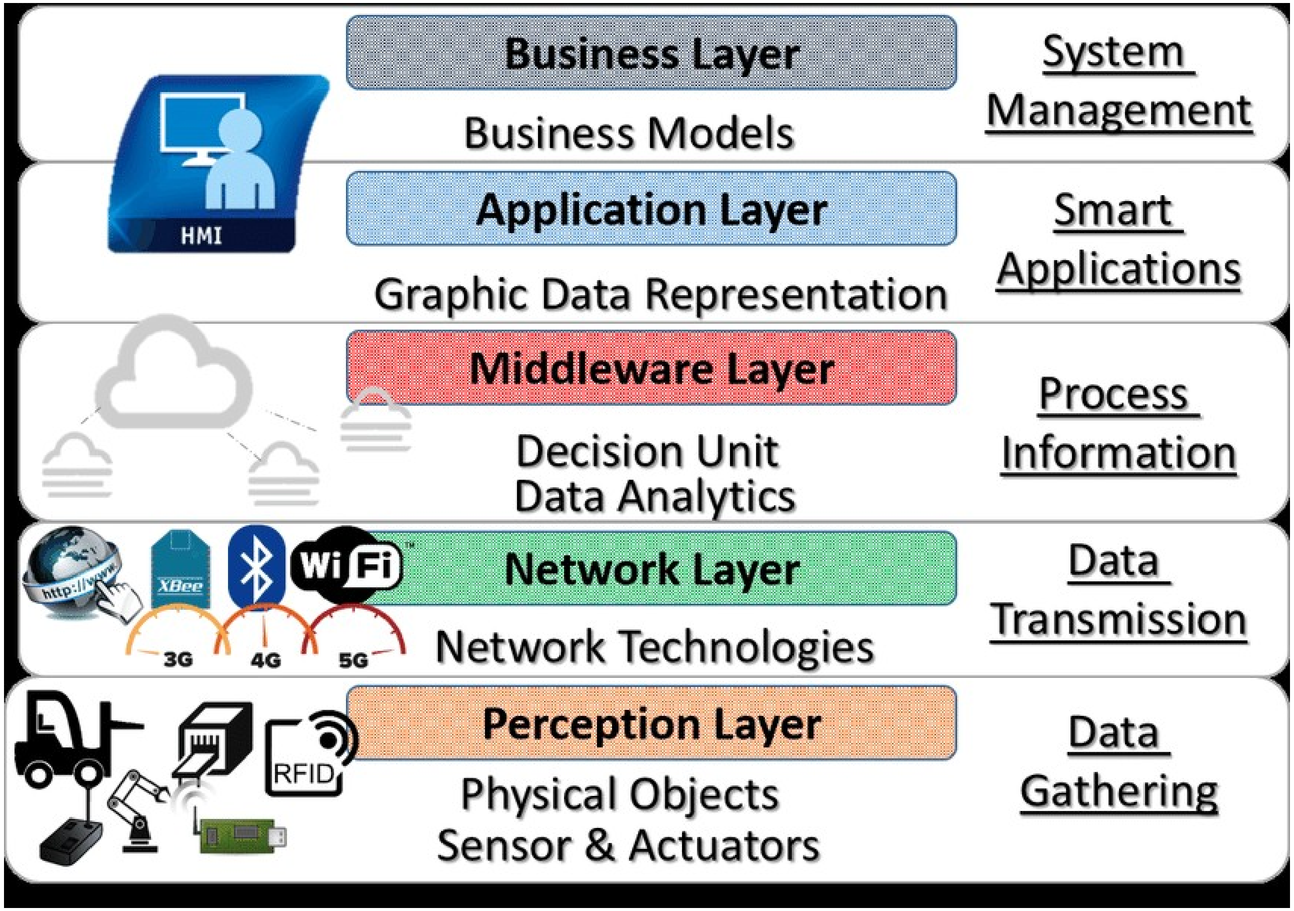
WAN : Connection of various network segments, connects to internet

Node : connects to other nodes via LAN, maybe connected to other nodes via WAN directly

Gateway : A router connecting LAN to WAN and Internet, can implement several LAN and WAN, forwards packets between LAN and WAN

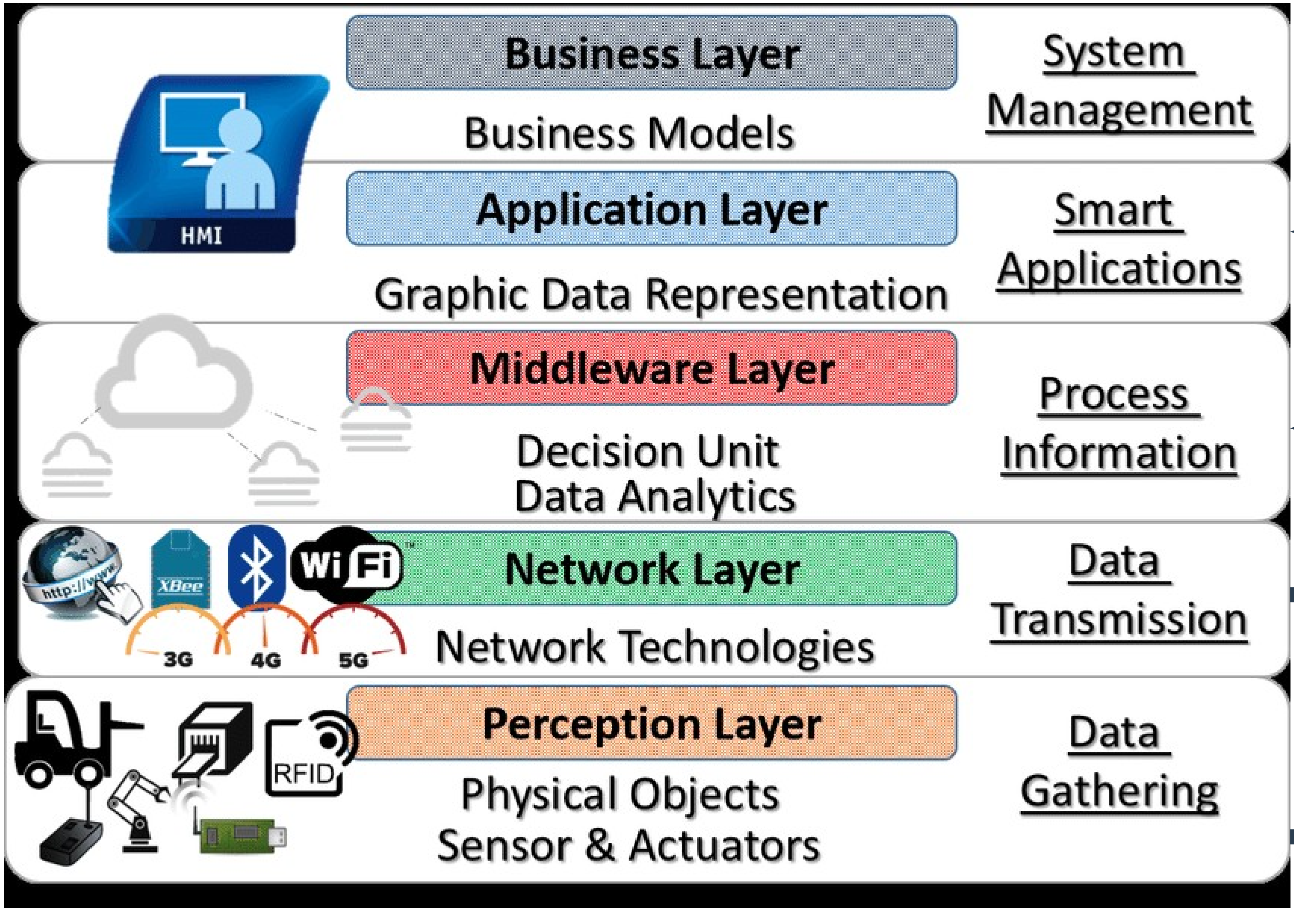
Proxy : Performs active application layer functions between nodes and other entities

5-Layered Architecture for IoT



Liliana Antao, Rui Pinto, Jao Pedro Reis, Gil Manuel Goncalves. (2018) : Requirements for Testing and Validating the Industrial Internet of Things 11th IEEE Conference on Software Testing, Validation and VerificationAt: Västerås - Sweden
doi : 10.1109/ICSTW.2018.00036

Protocol Architecture for IoT

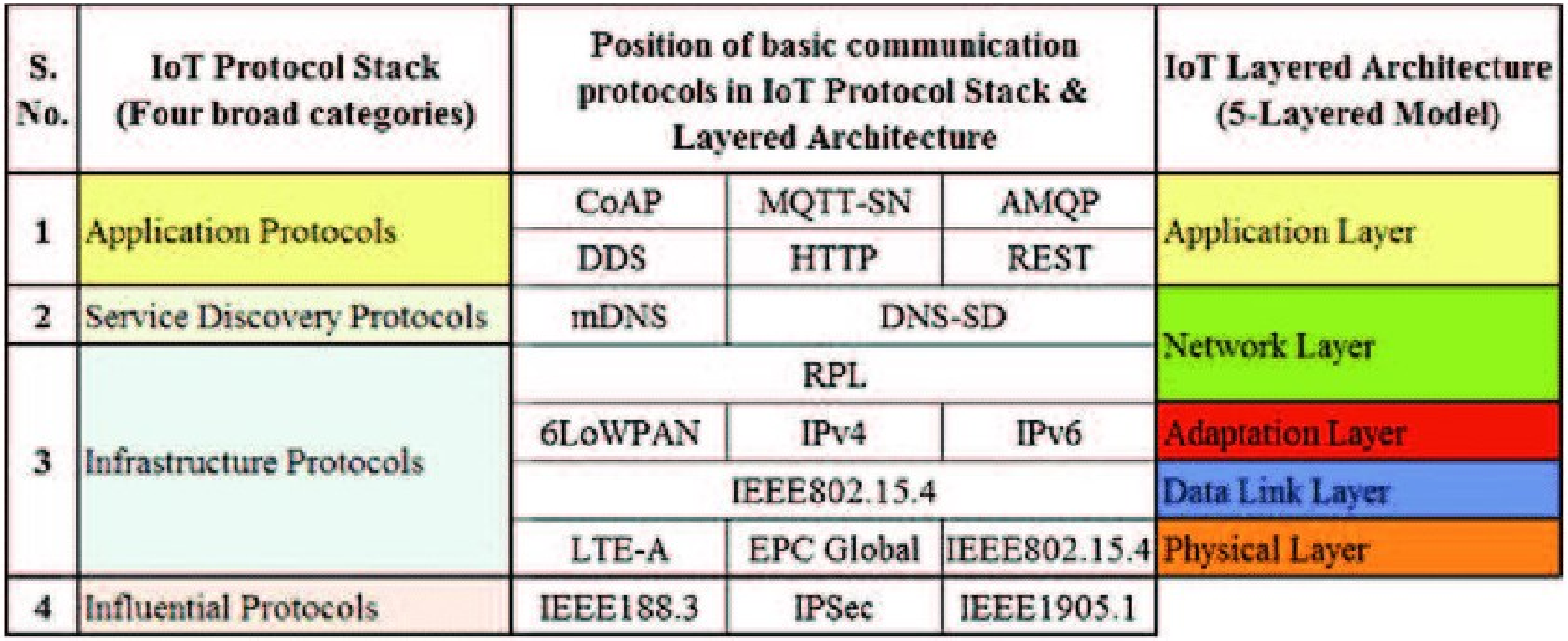


Application Protocols

Service Discovery Protocols

Infrastructure Protocols

Categorization of IoT Protocols



S. No.	IoT Protocol Stack (Four broad categories)	Position of basic communication protocols in IoT Protocol Stack & Layered Architecture			IoT Layered Architecture (5-Layered Model)
1	Application Protocols	CoAP	MQTT-SN	AMQP	Application Layer
		DDS	HTTP	REST	
2	Service Discovery Protocols	mDNS	DNS-SD		Network Layer
3	Infrastructure Protocols	RPL			
		6LoWPAN	IPv4	IPv6	Adaptation Layer
		IEEE802.15.4			Data Link Layer
		LTE-A	EPC Global	IEEE802.15.4	Physical Layer
4	Influential Protocols	IEEE188.3	IPSec	IEEE1905.1	

Source : Internet

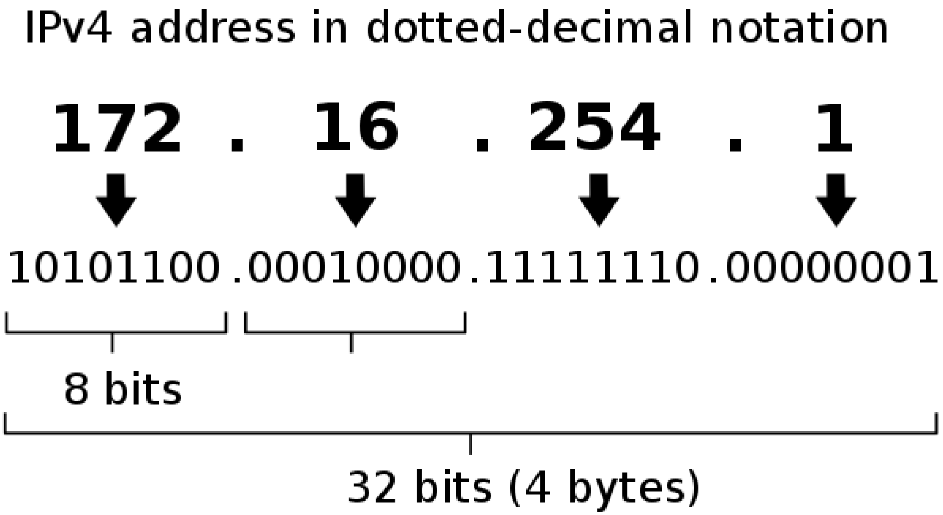
Infrastructure Layer Protocols

- Infrastructure layer receives and forwards data to the next layer using :

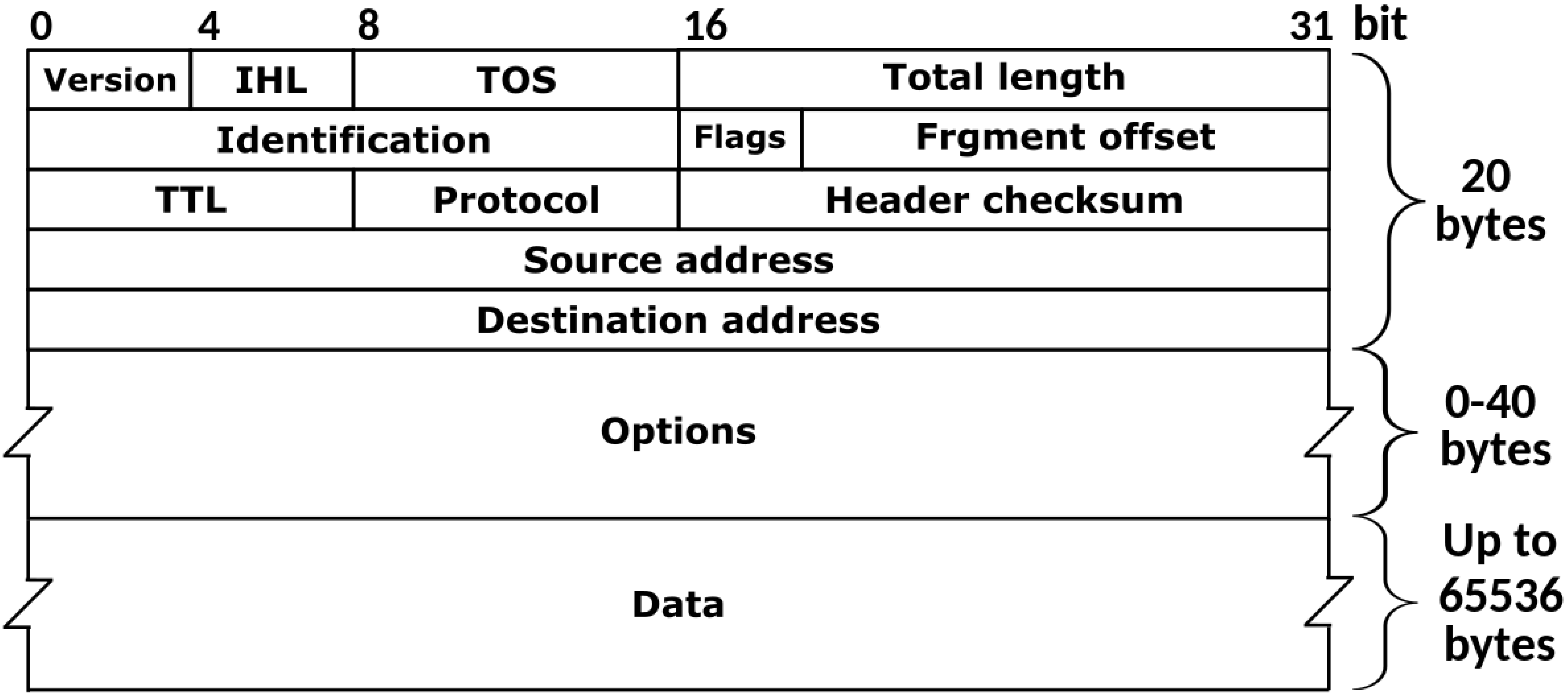
  IPv4 or IPv6 protocols

- Internet Layer Protocol (IP) – process when a packet transmits data identifier for host, router interface; unacknowledged data flow

- IPv4 address :



IPv4 Data Gram Format



0 4 8 16 31 bit

Version | IHL | TOS | Total length

Identification | Flags | Frgment offset

TTL | Protocol | Header checksum

Source address

Destination address

Options

Data

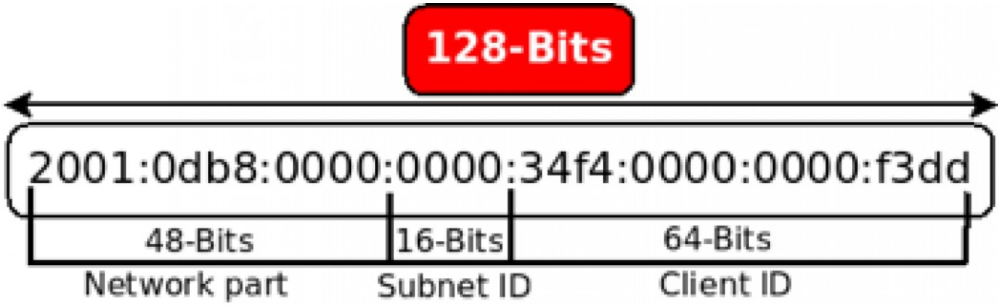
20 bytes

0-40 bytes

Up to 65536 bytes

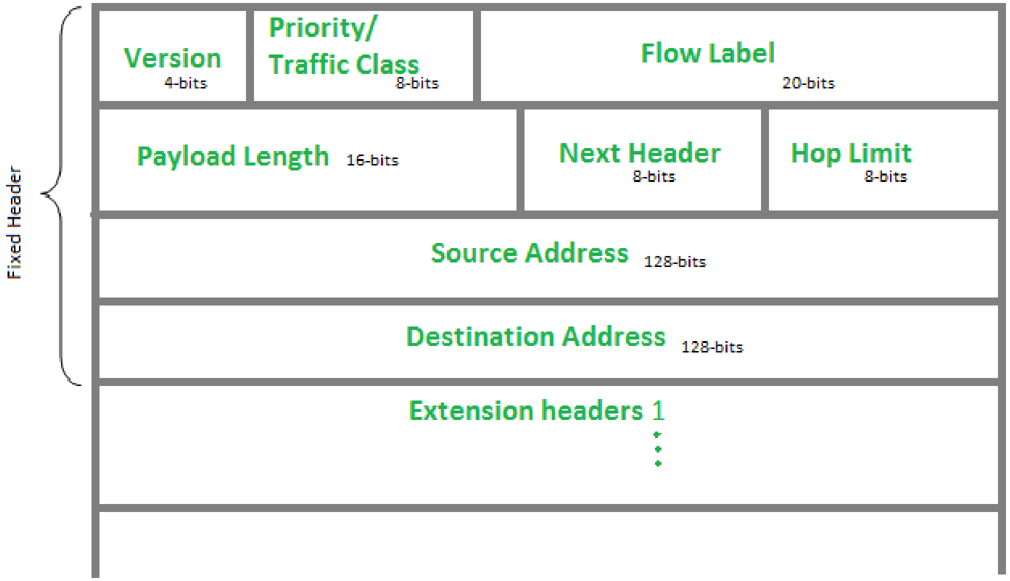
Infrastructure Layer Protocol : IPv6 protocol

- Internet protocol that provides identification and location system of devices and routes traffic across the internet
- deals with problem of IPv4 address exhaustion (protocols are not interoperable)
- uses a 128-bit address, theoretically approximately 3.4×10^{38} addresses
- address are represented as eight groups of four hex digits



IPv6 Data Gram Format

- Provides large address space
- Permits hierarchical address allocation thus route aggregation across the Internet and limit expansion of routing tables
- Provisions additional optimization for delivery of services using routers, subnets and interfaces
- Manages device mobility, security and configuration aspects
- Expanded use of multi cast routing



Version 4-bits

Priority/ Traffic Class 8-bits

Flow Label 20-bits

Payload Length 16-bits

Next Header 8-bits

Hop Limit 8-bits

Source Address 128-bits

Destination Address 128-bits

Extension headers 1

Infrastructure Layer Protocols :
Routing Protocol (RPL)

RPL : IPv6 based Routing Protocol for Low Power and Lossy Networks

(protocol for resource constrained networks)

- **Routers are limited in processing power, battery and memory**
- **Unstable links, Low data rate, Low packet delivery rate, High packet drop rate**

Such networks include :

Wireless personal area networks (**WPANs**)

Low Power line communication (**PLC**)

Wireless Sensor Networks (**WSN**)

Properties of such networks :

- 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

Infrastructure Layer Protocols :
Routing Protocol (RPL)

RPL

- Designed to support minimal routing through a robust topology over lossy networks

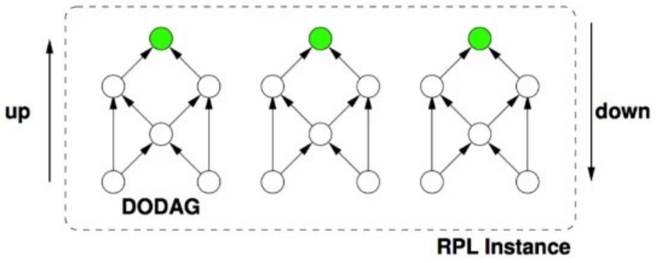
- Distance vector routing protocol

- RPL supports various type of traffic models :

Multi-point to multi-point, point-to-point

Devices are connected such that there are no cycles – builds Directed Acyclic Graphs

RPL topology



RPL Topology :
Destination Oriented Directed Acyclic Graphs (DODAG)

- **DAG rooted at single destination** ; No outgoing edges

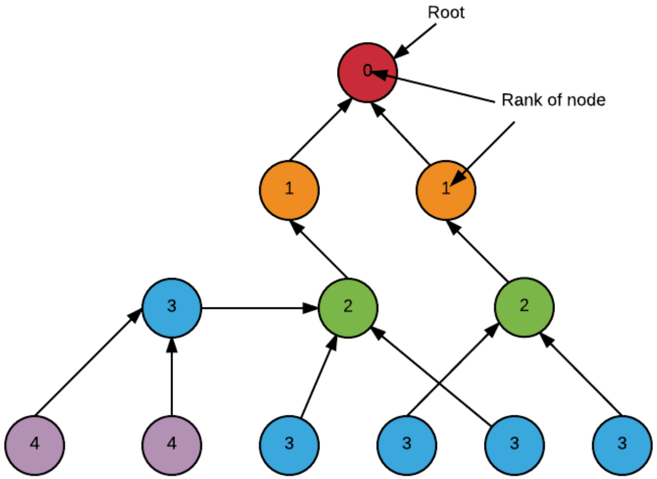
  DODAG is uniquely identified by a combination of RPL Instance and DODAG id

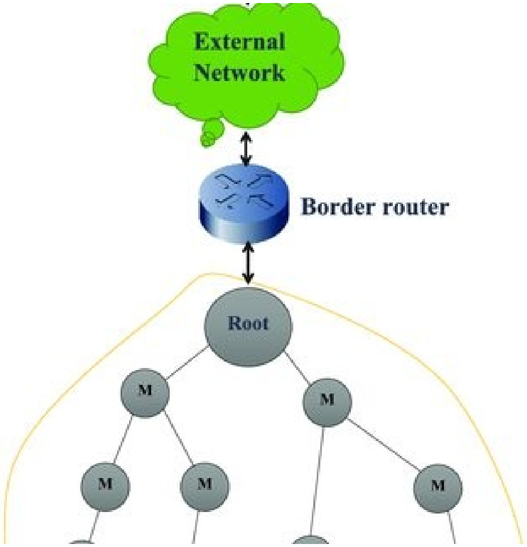
- **Rank :** Nodes rank is nodes individual position relative to other nodes with respect to DODAG root.

  Rank increases in downwards direction

- **Root :** DAG root of the DODAG; act as border router for the DODAG;

  Aggregate routes in the DODAG and may redistribute DODAG Routes into other protocols; Each node has information about the parent but no information about child





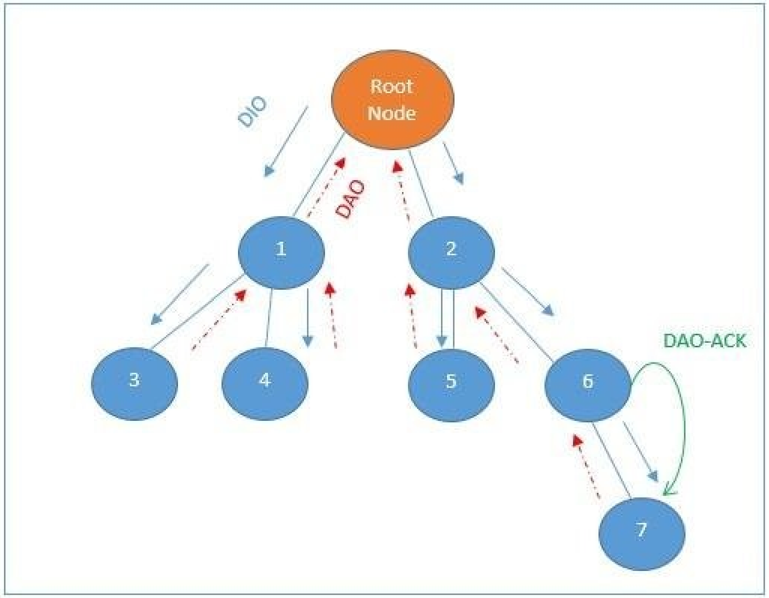
RPL Control Messages

- **DODAG Information Object (DIO) :** used to keep the current rank (level) of the node, determine distance of each node to the root based on some specific metrics and choose the preferred path

- **Destination advertisement object (DAO) :** used to unicast destination information toward selected parents of a node. Helps to maintain upward and downward traffic

- **DODAG information solicitation (DIS) :** used by a specific node in order to acquire DIO messages from another reachable adjacent node

- **DODAG Acknowledgement (DAO-ACK) :** used as response to DAO message and is sent by a DAO recipient node such as DAO parent or DODAG root



DODAG Construction

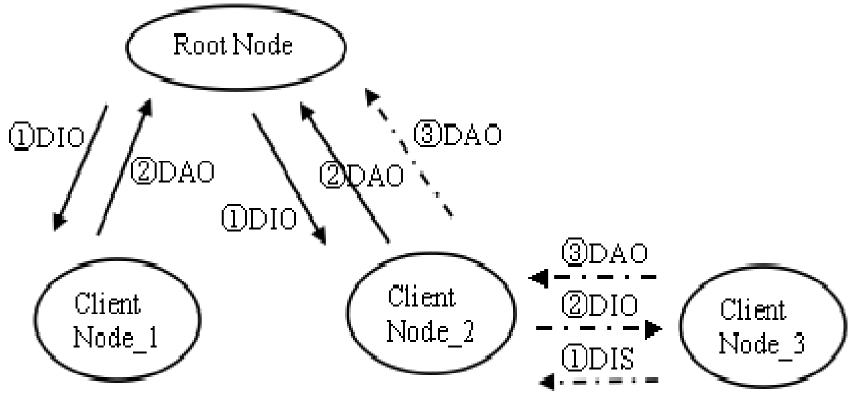
- root starts sending location information using DIO message to all levels

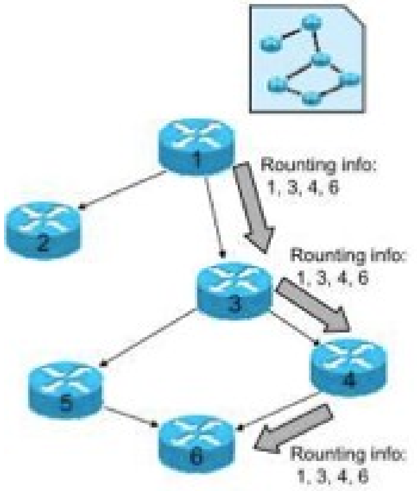
- routers that are present at each specific level register the parent paths for each node

- each node propagates its DIO message and the DODAG gets built

- for each node the preferred parent obtained by router is set as default path towards root

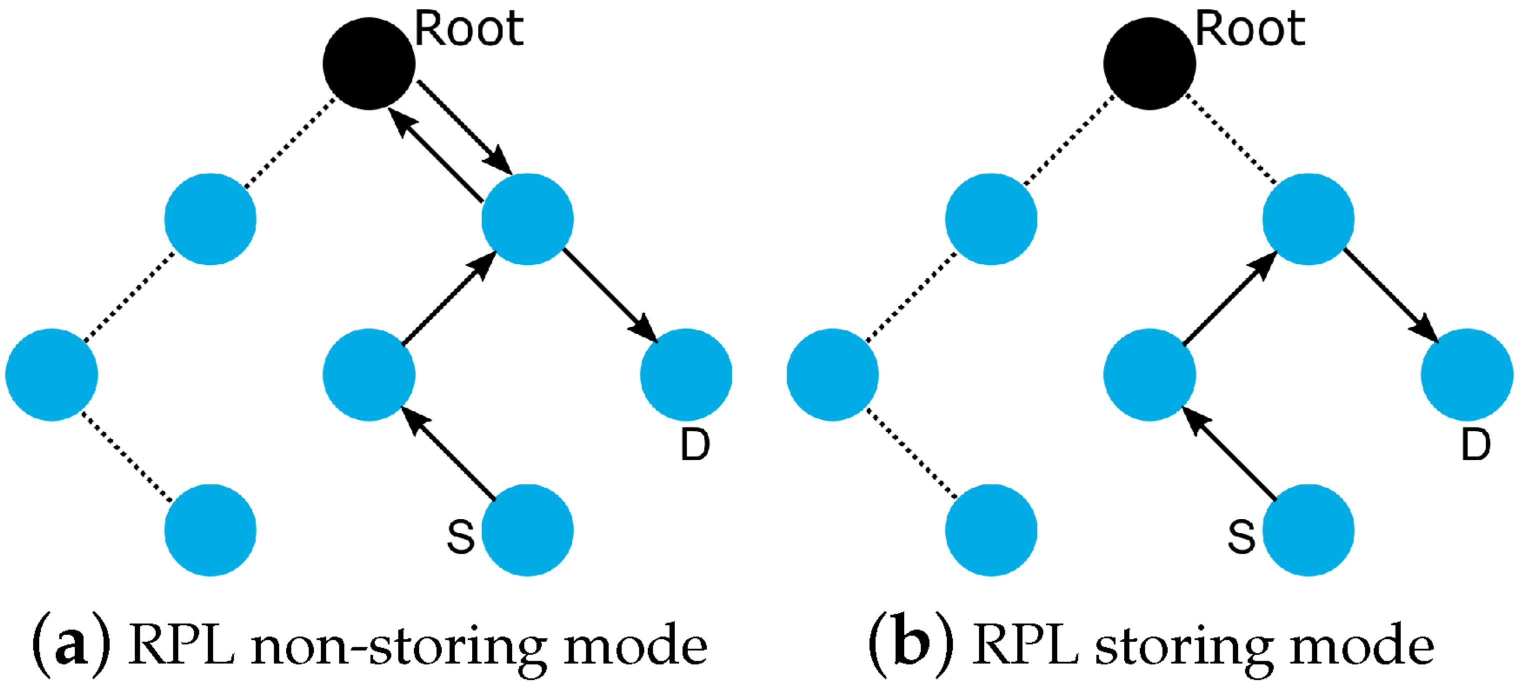
- root has capability to store destination prefixes obtained by DIOs of other routers in its DIO messages to have upward routes. To provide support for downward routes, the routers should emit and propagate DAO messages to the root by uni casting through parents




1
2
3
4
5
6
Rounting info: 1, 3, 4, 6
Rounting info: 1, 3, 4, 6
Rounting info: 1, 3, 4, 6

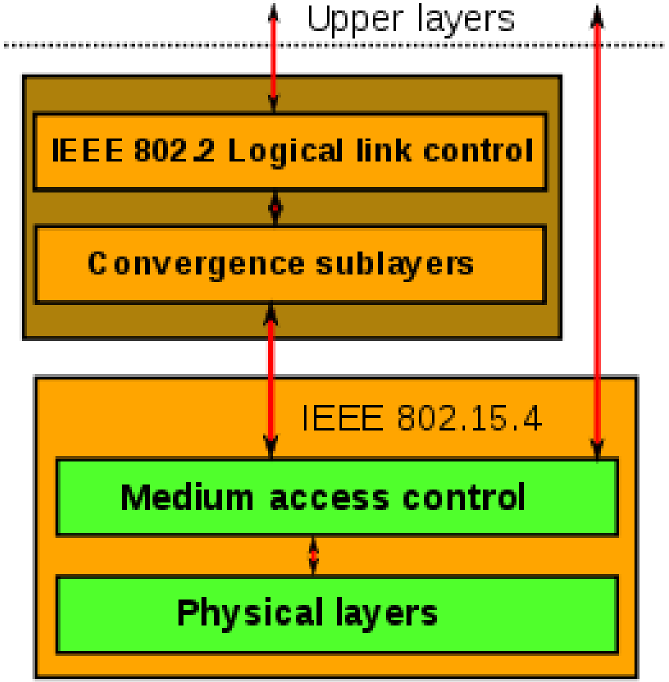
RPL Routing Modes

- non-storing mode : RPL route messages move towards lower levels based on IP source routing
- storing mode : RPL route messages move towards lower levels based on destination IPv6 address



(a) RPL non-storing mode (b) RPL storing mode

Infrastructure Layer Protocols : IEEE 802.15.4



- **IEEE 802.15.4 specifies Physical and Media Access Control for low rate wireless personal area network (LR-WPANs)**
- **It is maintained by IEEE 802.15 working group**
- **It is the basis for Zigbee, WirelessHART protocols which extend the standard by developing upper layers not defined in IEEE 802.15.4**

IEEE 802.15.4 Features

- Allows low cost, low speed ubiquitous computing
- Low data rate Wireless Personal Area Network
- Power consumption is minimized due to infrequently occurring very short packet transmission with low duty cycle
- Highly tolerant of noise and interference and offers link reliability
- Uses carrier sense multiple access with collision avoidance (CSMA-CA) for channel access
- Multiplexing allows multiple users or nodes interference free access to same channel at different times
- Transmission for most cases is Line of Sight
- Best case transmission range achieved outdoors is 1000m
- Networking topologies defined : Star and Mesh

IEEE 802.15.4 Physical and Media Access Control (MAC) Layer

- **Physical layer**
  - provides an interface to the physical layer management entity
  - maintains a database of information on related personal area networks
  - provides the data transmission service.
  - manages the physical radio transceiver, performs channel selection along with energy and signal management functions
- **MAC layer**
  - enables the transmission of MAC frames through the use of the physical channel, manages access to the physical channel and network beaconing.
  - controls frame validation, guarantees time slots and handles node associations.
  - facilitates secure services.

IEEE 802.15.4 transmission bands

- Supports three frequency bands using Direct Spread Spectrum Sequence(DSSS) method
- Data transmission rates:
- 250 Kbps at 2.4 GHz
- 40 Kbps at 915 MHz
- 20 Kbps at 868 MHz

IEEE 802.15.4 network nodes

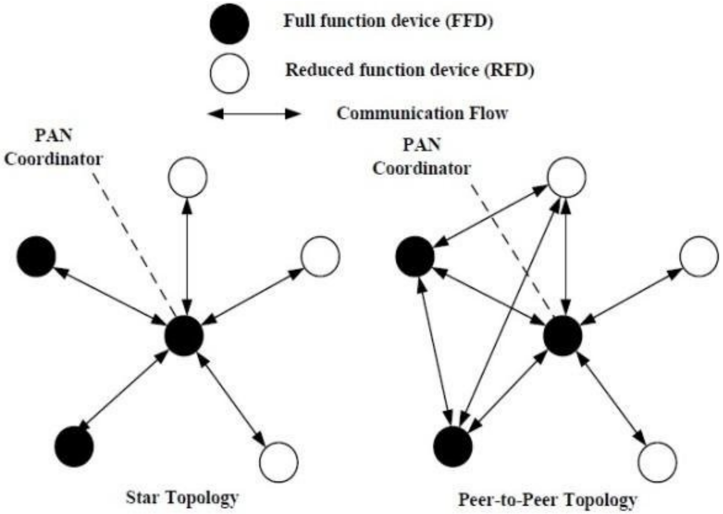
1. **Full function devices (FD) :**

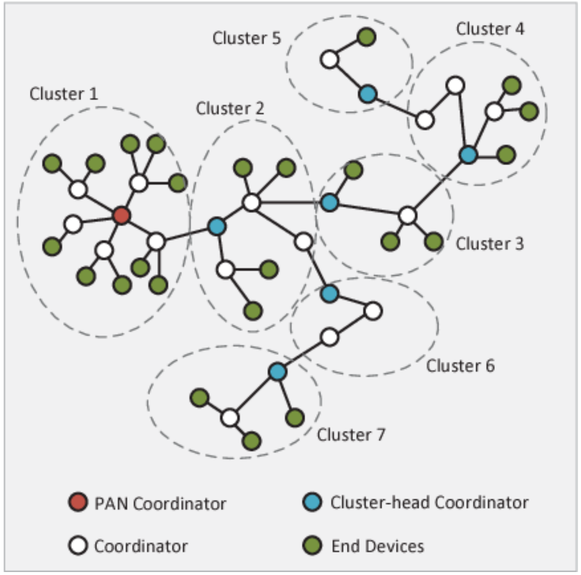
- act as PAN coordinator or normal nodes
- coordinator has capability to create, control and maintain the network
- FFDs can store routing table and can implement MAC and can communicate with other devices

2. **Reduced function devices (FD) :**

   - act as PAN coordinator or normal nodes, have constrained resources

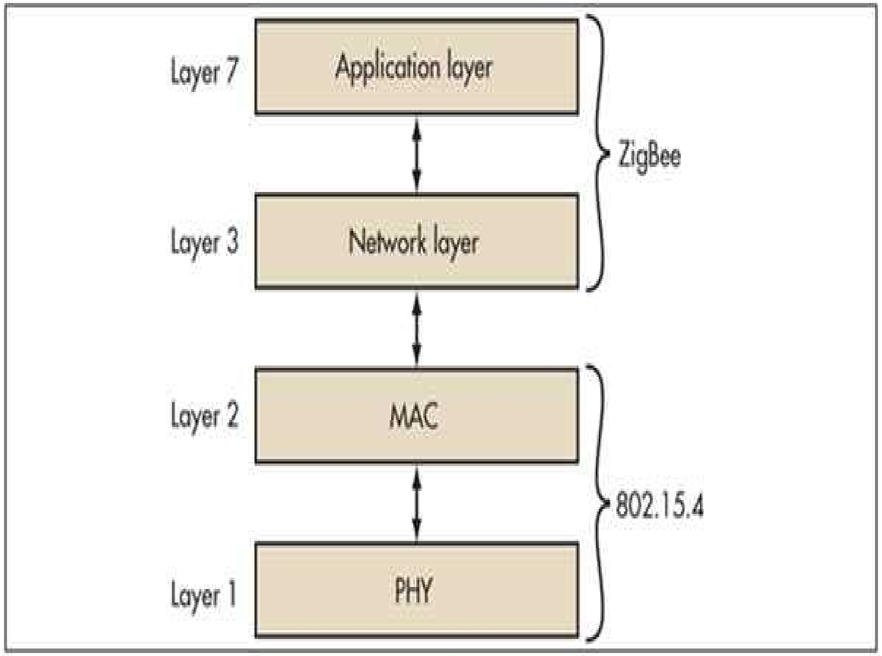
3. **Topologies : Star, Peer-to-Peer, Cluster-tree**



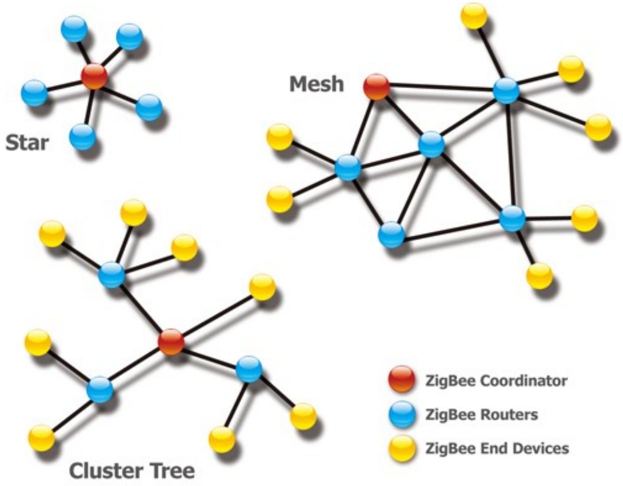


Infrastructure Layer Protocols : ZigBee

- The ZigBee protocol uses the **802.15.4** standard
- operates in two bands : **868/915MHz** and **2.4 GHz**
- Data rate of **868/915 band : 20/40 Kb/s**
- **Data rate of 2.4GHz band : 250 Kb/s.**
- The maximum number of nodes is 1024
- range up to 200 meter.
- ZigBee can use 128 bit AES encryption.
- end devices can go to sleep mode to saves battery



Zigbee Network



- A Zigbee network is made up of a **Coordinator (C)** , **Router (R)** and **End Device (E)**
- Coordinator is installed first ;

  i. it starts a new PAN (Personal Area Network)

  ii. starts other Zigbee components

  iii. selects Channel and PAN id
- Router needs to join the network then it can allow other R & E to join the PAN
- Zigbee 3. 0 : enables different application areas to communicate and form a homogenous network
- Supports connectivity with IP networks such as LAN and WAN, products from different manufacturers can communicate as a single networking devices

IPv6 over Low Power Wireless Personal Area Network : 6LoWPAN

- Supports IPv6 packets over IEEE 802.15.4 WPANs.
- Low power design - suitable for battery-operated IoT devices.
- Supports applications that need wireless internet connectivity at lower data rates for devices with very limited form factor.
- Initially designed to support IEEE 802.15.4 in 2.4 GHz band, but now supports wide range of networking media such as sub-1 GHz band, low power RF, low power WiFi
- Example usage : automation and entertainment applications in home, office and factory environments
- Challenges : management of addresses for devices that communicate across the two dissimilar domains of IPv6 and IEEE 802.15.4 is cumbersome

IPv6 over Low Power Wireless Personal Area Network : 6LoWPAN

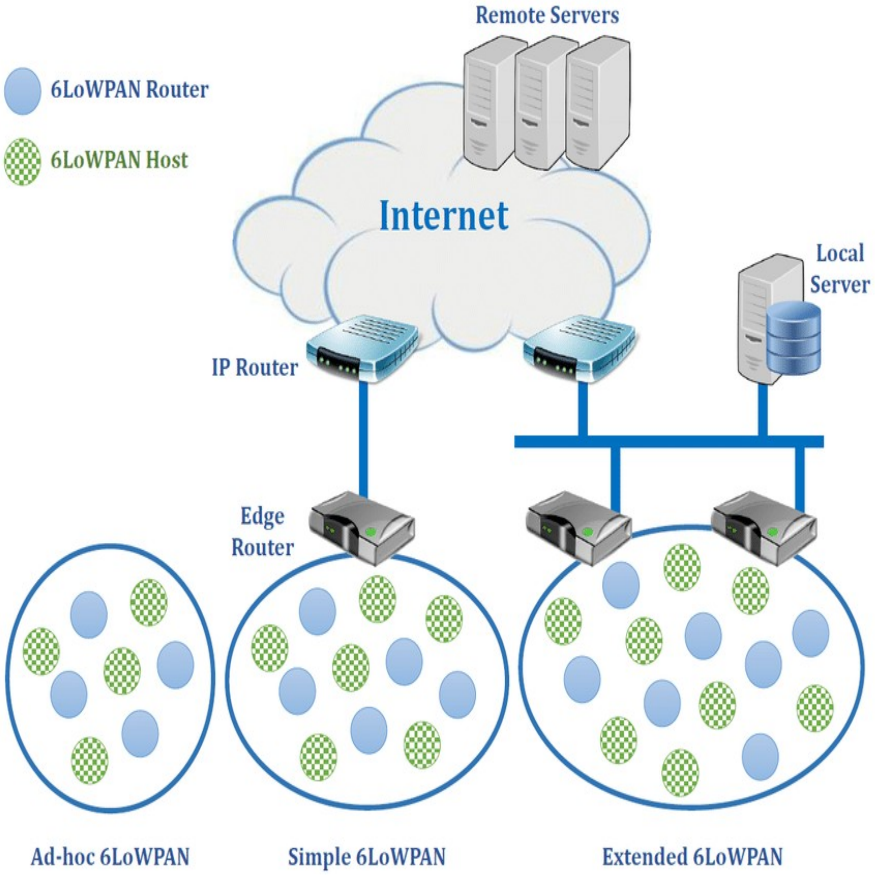
- **Uplink to Internet - IPv6 router (Access point)**
- **Connection of components – Edge router**
- **Edge router :**

  - Enables exchange of data between 6LoWPAN devices and Internet

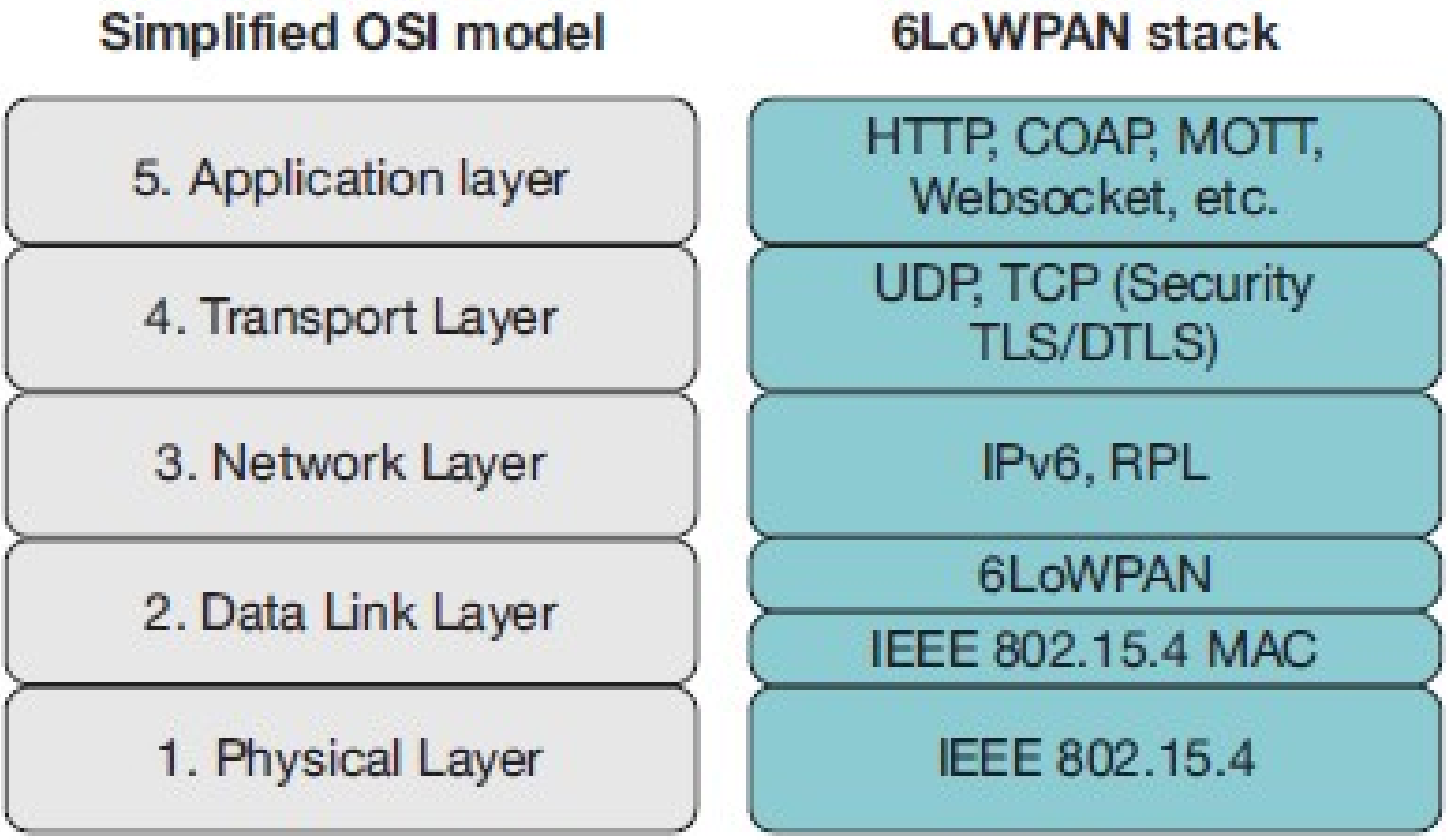
  - enables exchange of data among devices that are part of 6LoWPAN network

  - helps to generate and maintain 6LoWPAN network
- **Host : end point devices**

  checks routers at regular intervals for data
- **Routers : route data to other nodes in 6LoWPAN network**



Protocol Stack of 6LoWPAN



Simplified OSI model	6LoWPAN stack
5. Application layer	HTTP, COAP, MOTT, Websocket, etc.
4. Transport Layer	UDP, TCP (Security TLS/DTLS)
3. Network Layer	IPv6, RPL
2. Data Link Layer	6LoWPAN IEEE 802.15.4 MAC
1. Physical Layer	IEEE 802.15.4

Data formatting

Ensures multiple apps running on each device have their own communication channel

Device identification using IPv6 addressing

IPv6 to IEEE802.15.4 adaptation

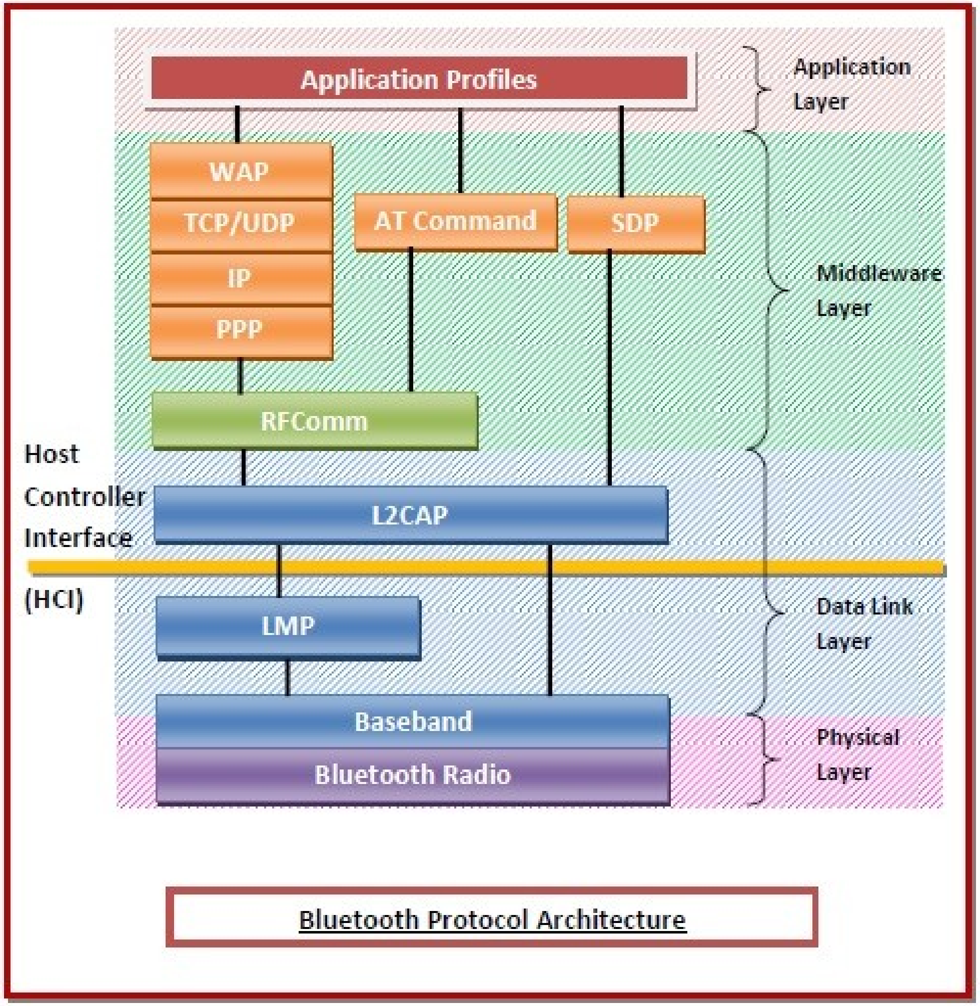
Error correction, Access to media

Data bit transmission

Bluetooth

- Network technology connects mobile devices wirelessly over a short-range to form a personal area network (PAN).
- The Bluetooth architecture has its own independent model with a stack of protocols, instead of following the standard OSI model or TCP/IP model.
- Bluetooth works in the 2.4 GHz ISM band and uses frequency hopping.
- Data rate up to 3 Mbps and maximum range of 100m.
- Each application type which can use Bluetooth has its own profile.

Bluetooth Architecture



Bluetooth Protocol Architecture

Bluetooth Architecture

Physical Layer :

Radio : defines frequency band, modulation techniques

Baseband : addressing scheme, packet format, timing, power control

Data Link Layer :

Link Manager Protocol(LMP) : establishes logical link between bluetooth devices, authentication, message encryption

Logical Link Control and Adaptation Layer : adaption between upper layer frame and baseband layer frame format

Middleware Layer :

RFComm : provides a serial interface with WAP.

Adopted : protocols adopted from standard models (PPP, UDP, TCP)

Service Discovery : takes care of service-related queries like device information so as to establish a connection between contending Bluetooth devices.

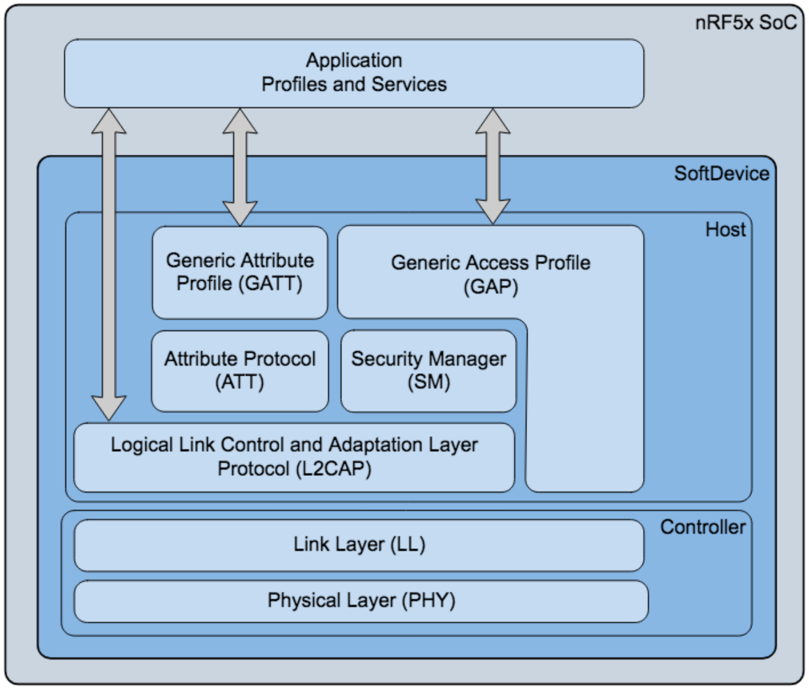
AT command set

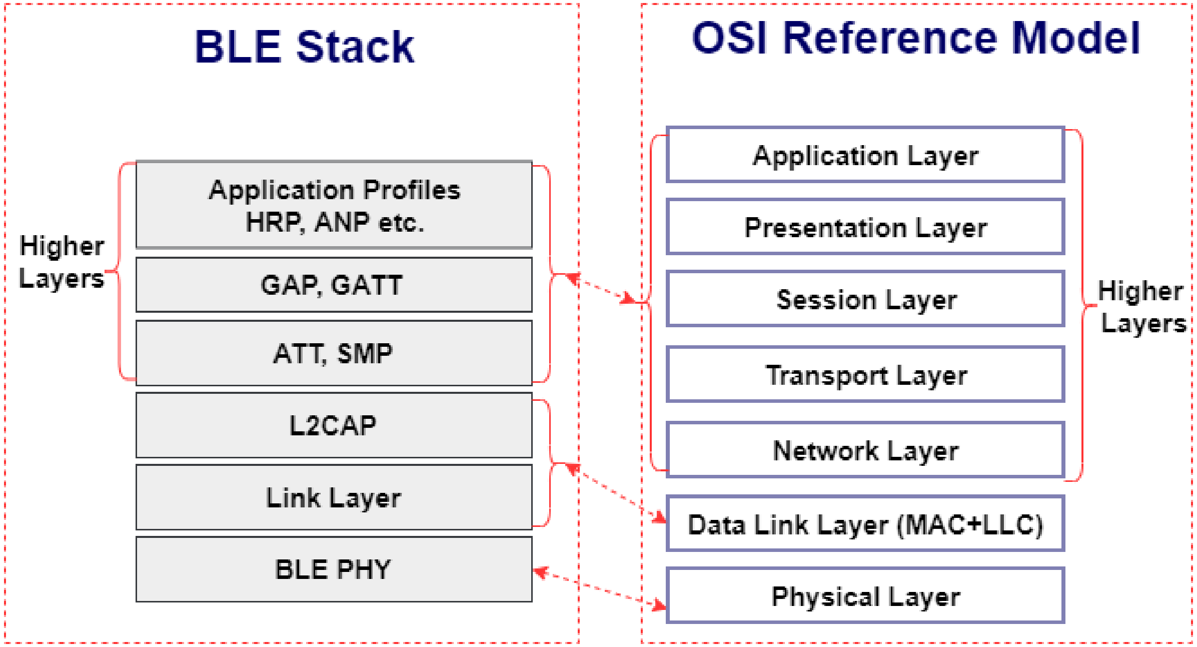
Application Layer :

includes the application profiles that allow the user to interact with the Bluetooth applications

Bluetooth Low Energy (BLE)

- Short range radio, minimum power and operates long
- Range : 100 metres (X10 times of Bluetooth)
- Latency : 15X lesser than Bluetooth
- Operating power : 0.01mW to 10mW





Bluetooth Low Energy (BLE)

- BLE Phy – receives and transmits bits
- Link – media access control, error control, flow control
- Host Control Interface – provides a command, event and data interface that allows link layer to access data from upper layers
- Logical Link Control Adaptation Protocol (L2CAP) – multiplexing of data channels; fragmentation and reassembly
- Generic Access Protocol (GAP) – defines processes related to discovery of Bluetooth devices

  Roles defined by GAP when operating over low energy physical

  channels : Broadcaster, Observer, peripheral, central,
- Generic Attribute Profile (GATT) – specifies a framework using the attribute protocol(ATT), defines services and their characteristics

Bluetooth Low Energy (BLE)

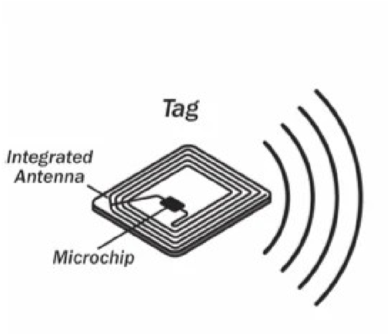
- **GATT lays down various aspects of service such as service procedures, characteristics, various aspects that pertain to the broadcast of service characteristics**
- **Two roles specified by GATT profile :**

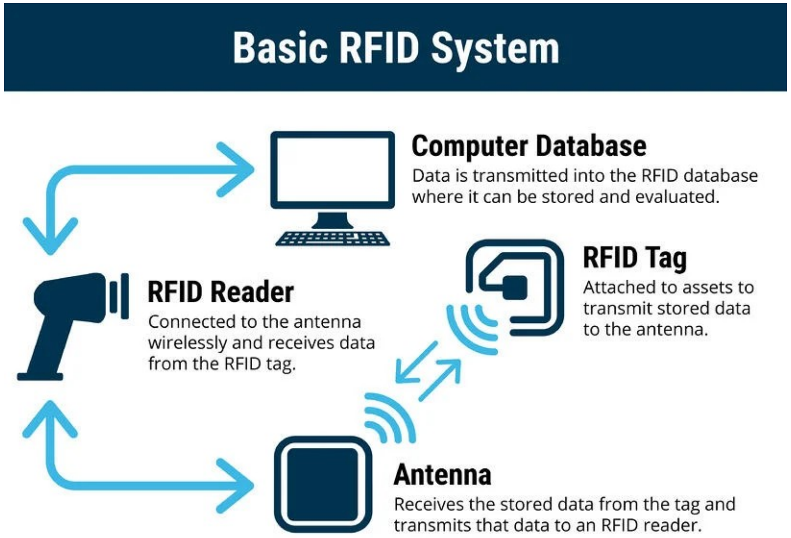
  GATT client - a device that wants data; sends request to GATT server

  GATT server- a device that has data
- **Attribute Protocol** – defines a client and server architecture above BLE logical transport channel; it allows the GATT server to communicate with the GATT client by exposing a set of attributes and interfaces
- **Security Manager Protocol (SMP) -** procedure and behaviour to ensure security by managing, pairing, authentication and encryption between devices

RFID

- RFID (Radio Frequency Identification) - wireless microchips used for tagging objects
- Electronic Product Code (EPC) is a unique identifier stored in an RFID tag that helps track objects
- EPC global developed EPC
- RFID technology – open, scalable, reliable and support for object IDs
- RFID component – radio signal transponder and Tag reader
- RFID Tag – electronic chip to store identity of objects; antenna that allow to communicate with the tag reader



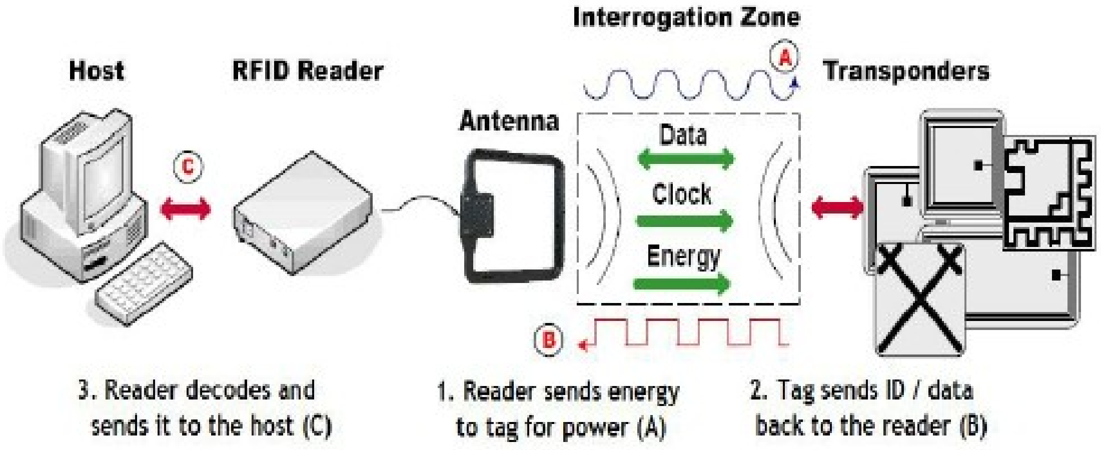

Basic RFID System

Computer Database
Data is transmitted into the RFID database where it can be stored and evaluated.

RFID Reader
Connected to the antenna wirelessly and receives data from the RFID tag.

RFID Tag
Attached to assets to transmit stored data to the antenna.

Antenna
Receives the stored data from the tag and transmits that data to an RFID reader.



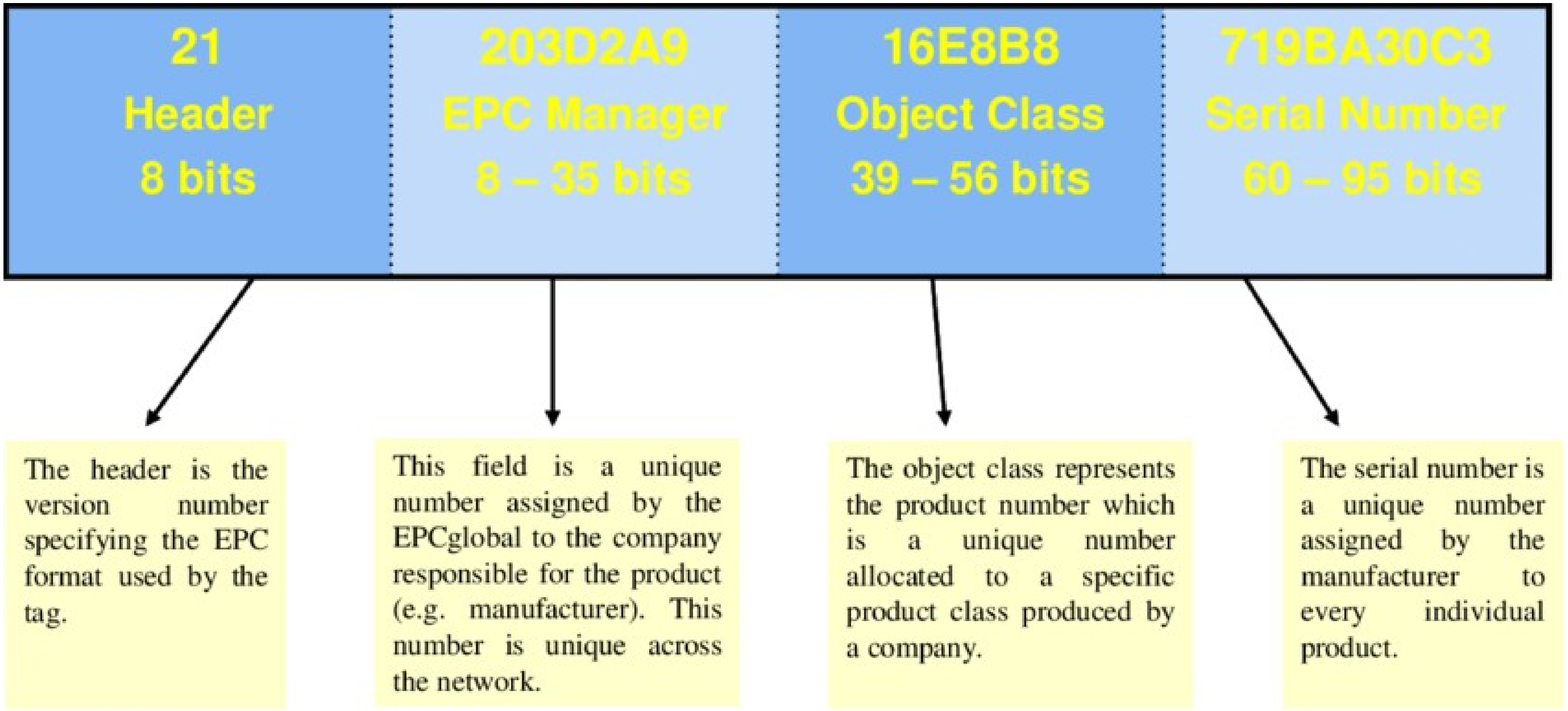
3. Reader decodes and sends it to the host (C)

1. Reader sends energy to tag for power (A)

2. Tag sends ID / data back to the reader (B)

EPC Code

EPC Code Type I – 96 bit code field



21	203D2A9	16E8B8	719BA30C3
Header	EPC Manager	Object Class	Serial Number
8 bits	8 – 35 bits	39 – 56 bits	60 – 95 bits

The header is the version number specifying the EPC format used by the tag.

This field is a unique number assigned by the EPCglobal to the company responsible for the product (e.g. manufacturer). This number is unique across the network.

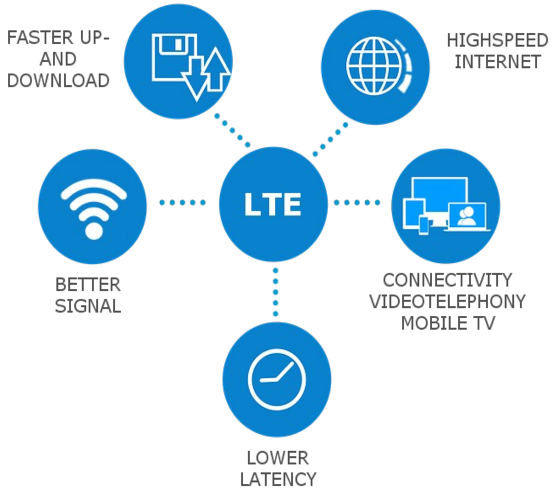
The object class represents the product number which is a unique number allocated to a specific product class produced by a company.

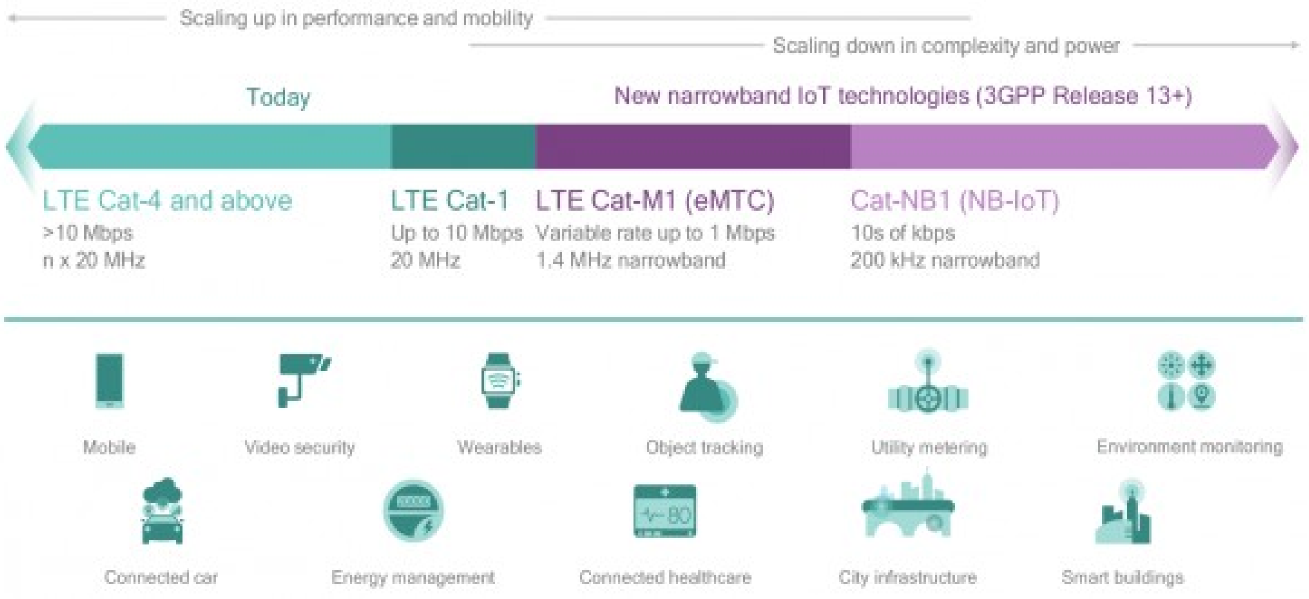
The serial number is a unique number assigned by the manufacturer to every individual product.

Ex : 01 0000A89 00116F 000169DCO

Long Term Evolution – Advanced (LTE)

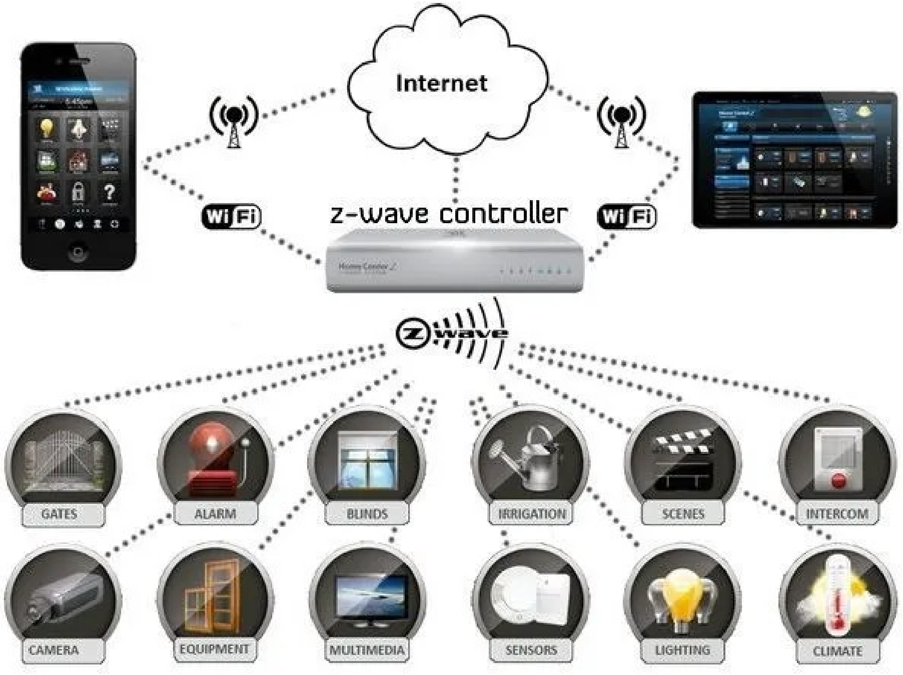
- **Standard for wireless mobile network (4G LTE)**
- **Provides high speed data transfer rates for wireless mobile networks**
- **LTE broadcast is single frequency network (SF) that operates on broadcast mode**





Z-Wave

- **Low Power Wireless Communication Protocol used for home area network**
- **Used for remote control applications for smart homes as well as small sized commercial domains**
- **Developed by Zensys, improved by Z-Alliace**
- **Operates around 900 MHz**



Source : Internet

Working of Z-Wave

WiFi

Wi-Fi is a Wireless Local Area Network (WLAN) technology based on the IEEE 802.11 standards.

- **Wi-Fi Devices - Smartphones, Smart Devices, Laptop Computers, PC, etc.**

Applications Areas - Home, School, Computer Laboratory, Office Building

- **Wi-Fi devices and Access Points (APs) have a wireless communication range of about 30 meters indoors.**
- **Wi-Fi data rate is based on its protocol type :**

IEEE 802.11a can achieve up to 54 Mbps
IEEE 802.11b can achieve up to 11 Mbps
IEEE 802.11g can achieve up to 54 Mbps
IEEE 802.11n can achieve up to 150 Mbps
IEEE 802.11ac can achieve up to 866.7 Mbps
IEEE 802.11ad can achieve up to 7 Gbps

Device or Service Discovery for IoT

- **Need for resource management mechanisms –** capability to register and discover resources in a self configured, dynamic and efficient way
- **IoT service discovery technologies :**
  - Bluetooth beacons
  - Wifi Aware
  - Physical web
  - Open Hybrid
  - Chirp
  - Shazam

Device or Service Discovery Technologies for IoT

- **Bluetooth beacons :**

  Beacons are sent out consisting of unique identifier which belongs to the beacon

  A Bluetooth mobile receives beacons recognizes ID, triggers notifications
- **Wifi Aware :**

  Update to wifi with beacon like features for discovering and establishing connection with nearby devices
- **Physical Web :**

  Device broadcasts beacons containing URL

  Mobile os detects physical web signals (BLE signals)
- **Chirp :**

  Software that allows devices to communicate using brief melodic tweedles (alphabets of electronic birdsongs)
- **Shazam :**

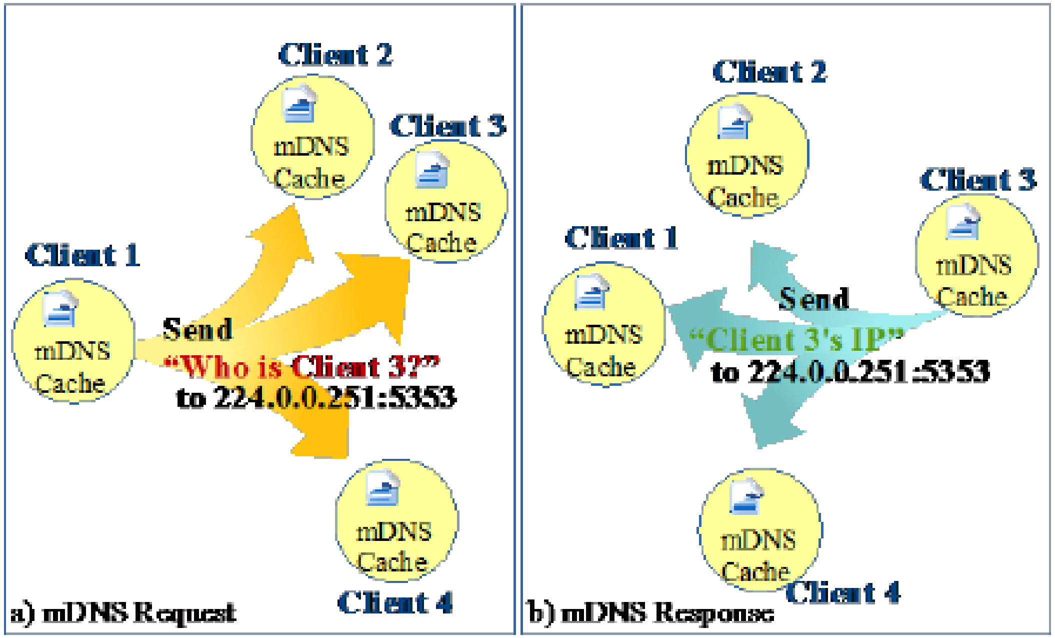
  Mobile app that is used to identify music by taking over a device's microphone for few seconds; now used for identifying digital contents associated with all types of real world objects and experiences

Protocols for IoT Service Discovery

- **DNS service discovery (DNS-SD)**
- **Multi-cast domain name system (m-DNS)**
- **Simple service discovery protocol (part of UPnP)**

Multi-cast Domain Name System (m-DNS)

- m-DNS works like a unicast DNS server
- DNS name space can be used with locally without any additional configuration
- High level of fault tolerance because of the capability to function even if the infrastructure failure happens

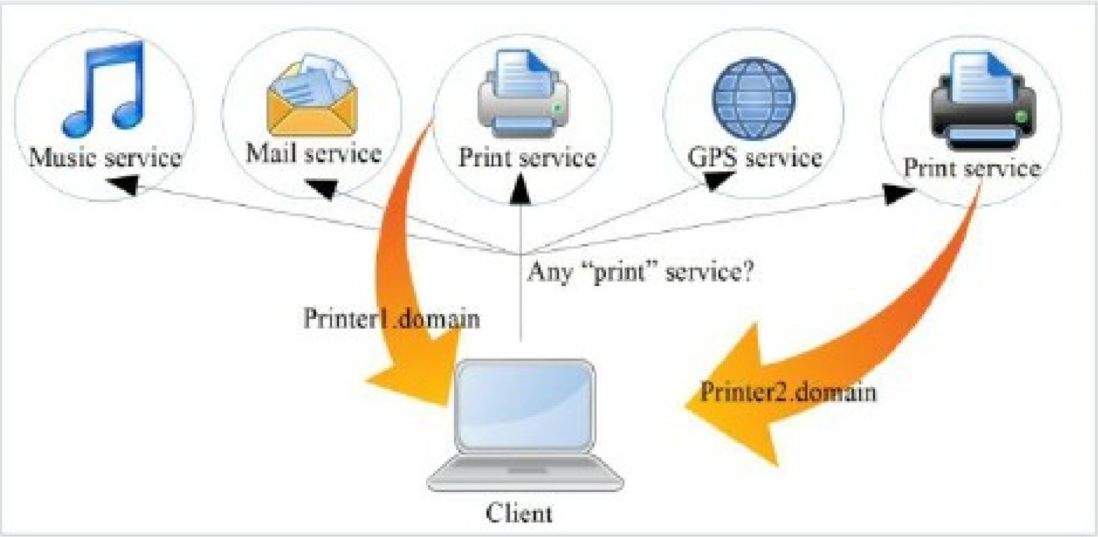


Working of the multi-cast domain name system (m-DNS)

Ref : The Internet of Things, Enabling Technologies, Platforms and Use Cases: Pethuru Raj and Anupama C. Rajan, CRC Press

DNS Service Discovery

- Helps clients to discover a set of services that are present in the network with the help of DNS messages; connects devices without any external administration or configuration
- DNS service discovery uses m-DNS to send packets to specific multicast destinations using UDP
- Two step process : i. Finding host names of required services ii. Pairing IP addresses to host names using m-DNS

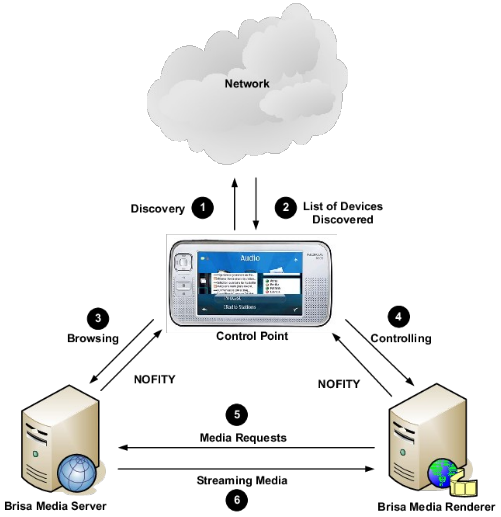


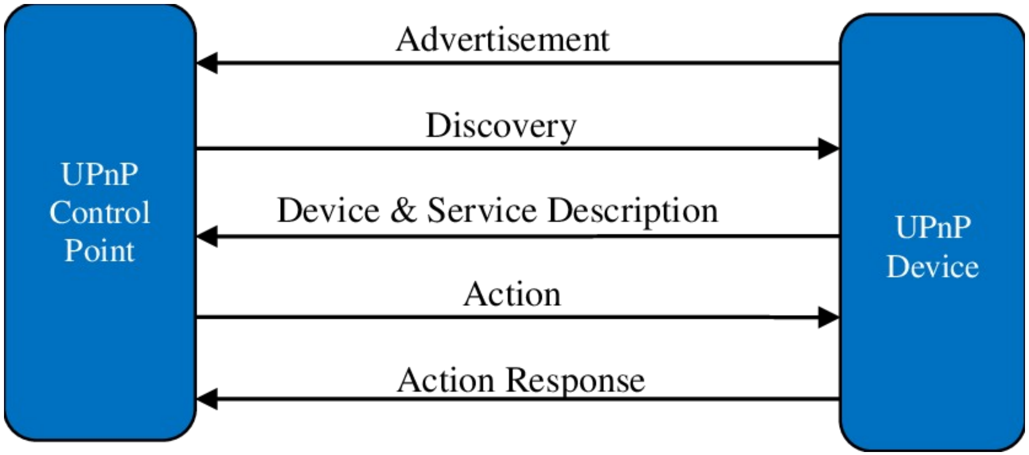
<u>Service discovery of printer service using DNS-SD protocol</u>

Ref : The Internet of Things, Enabling Technologies, Platforms and Use Cases: Pethuru Raj and Anupama C. Rajan, CRC Press

Universal Plug and Play

- UPnP device can join a network dynamically (automatically) and obtain IP addresses of other devices and at the same time convey its capabilities to other devices; no administration or configuration
- Basic components of UPnP – Devices, Services, Control points
- Devices- container for services and other nested devices
- Control points – device discovery and control by receiving device descriptions and by invoking service actions
- Services – set of services offered by the UPnP devices





Ref : Internet

Prominent IoT Service Discovery Products

- Bonjour - zero configuration and service discovery protocol from Apple

  the networking architecture provides features that help and discover TCP or

  IP based services available in LAN or WAN. It can connect a printer to network

  without assigning a IP address to it.

- Consul - health discovery of services; Product of Hashi Corp.

  key or value store for dynamic configuration of services; support for multi-data centre integration with any additional layers of abstraction

  Architecture – Consul agent in each node (for health checking),

  Consul server stores data. Components that need to discover services can either

  query consul servers or consul agent.

- AllJoyn - Open source framework from AllSeen Alliance

  Devices operating in this framework share data irrespective of their manufacturer,

  brand, operating system and other technical specifications

  Two components – AllJoyn apps and AllJoyn routers. They communicate among

  themselves