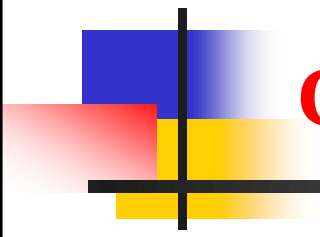


Chapter 3

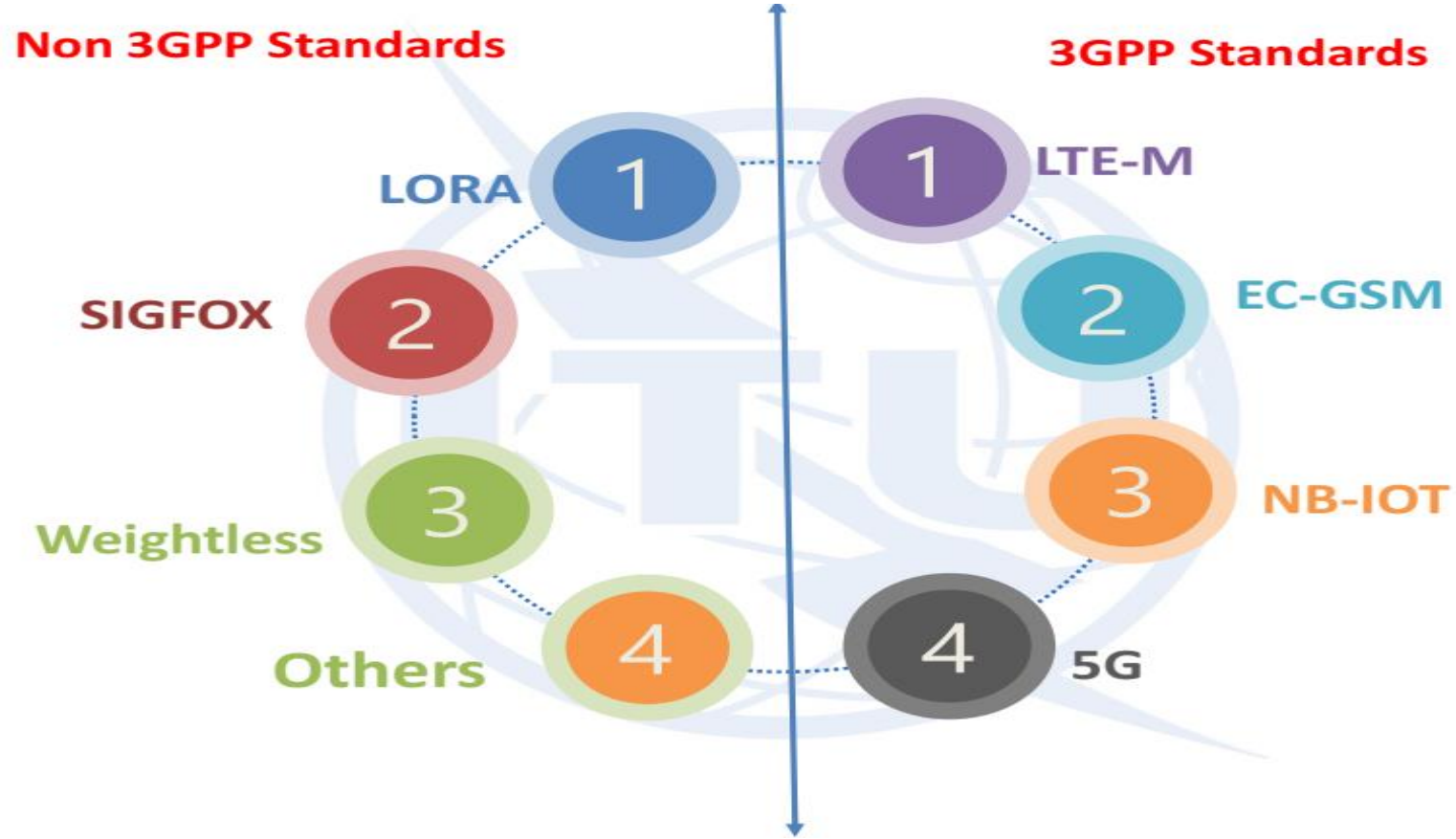
IoT NETWORKING – P2 (Connectivity Technologies)

IoT Short Range and Long Range Systems

- A. Fixed & Short Range
  - 1. RFID
  - 2. Bluetooth
  - 3. Zigbee
  - 4. WiFi
- B. Long Range technologies
  - 1. Non 3GPP Standards (LPWAN)
  - 2. 3GPP Standards
-

Long Range technologies

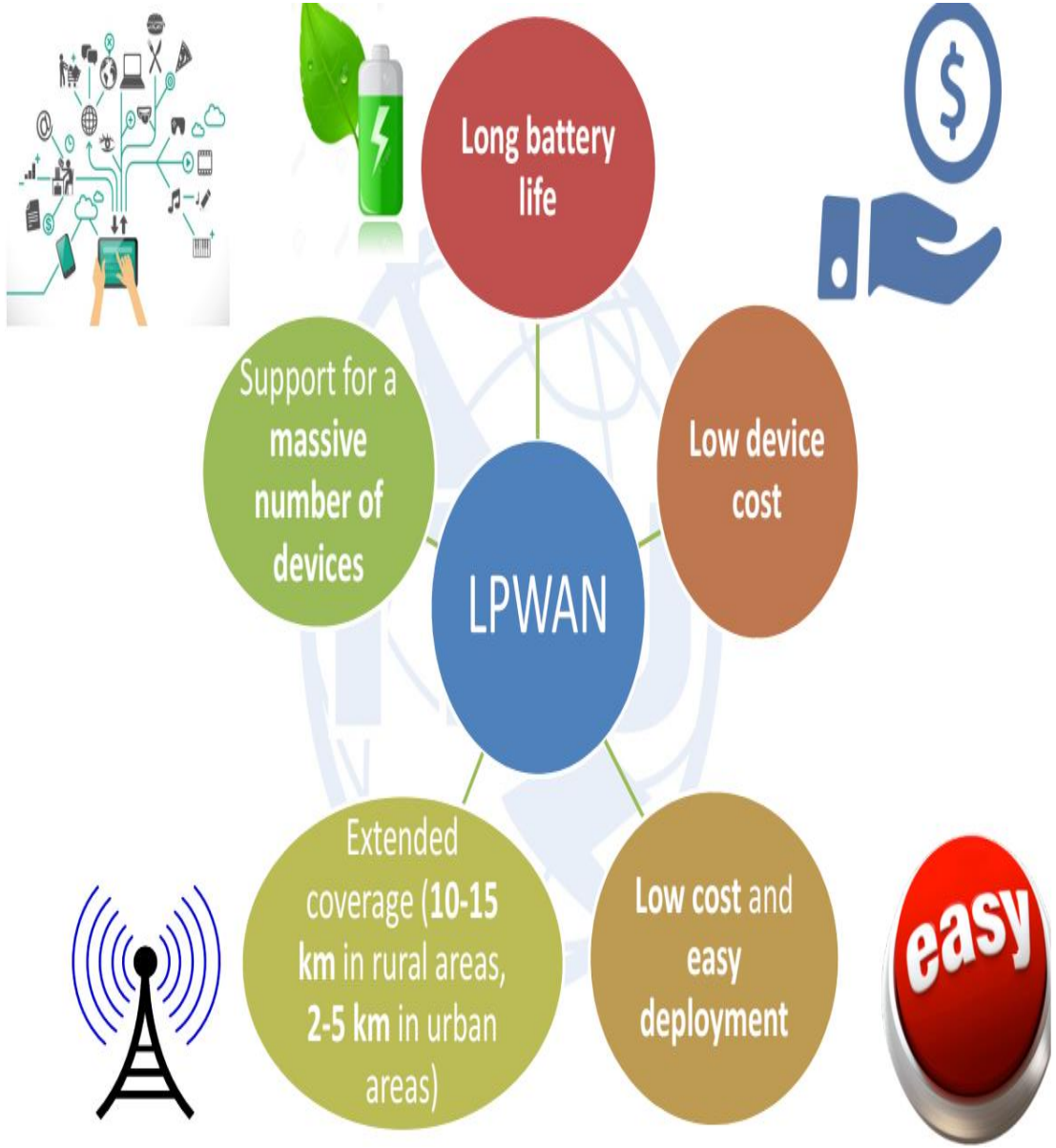
- Non 3GPP Standards (LPWAN)
- 3GPP Standards

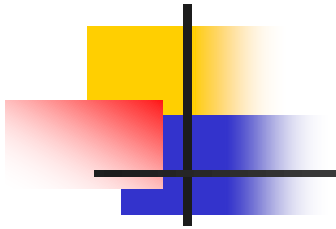


Non 3GPP Standards (LPWAN)

- Consist of :
  - LoRaWAN
  - Sigfox
  - Weightless
  - RPMA
  - Others
- LPWAN

REQUIREMENTS

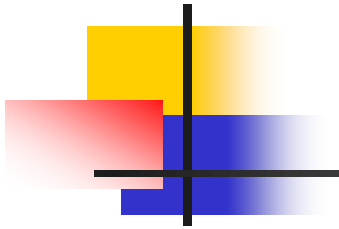




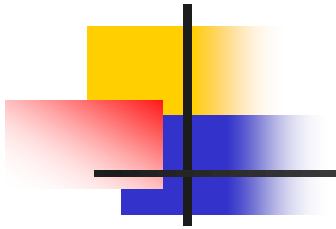
- Communication Protocols: The following communication protocols have immediate importance to consumer and industrial IoTs:
- IEEE 802.15.4
- Zigbee
- 6LoWPAN
- Wireless HART
- Z-Wave
- ISA 100
- Bluetooth
- NFC
- RFID

IEEE 802.15.4

- **Features of 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.
  - 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.
  - Networking topologies defined are -- Star, and Mesh



- **IEEE 802.15.4 supports two types of network node:**
  - **1. Full Function Device (FFD)**
    - Can talk to all types of devices.
    - Supports full protocol.
  - **2. Reduced Function Device (RFD)**
    - Can only talk to an FFD.
    - Lower power consumption.
    - Minimal CPU/RAM required.
- **IEEE 802.15.4 Types:**
  - **1. Beacon Enabled Networks**
    - Periodic transmission of beacon messages.
    - Data-frames sent via Slotted CSMA/CA with a super frame structure managed by PAN coordinator. Beacons used for synchronization & association of other nodes with the coordinator.
    - Scope of operation spans the whole network



- **2. Non-Beacon Enabled Networks**
  - Data-frames sent via un-slotted CSMA/CA (Contention Based).
  - Beacons used only for link layer discovery.
  - Requires both source and destination IDs.
  - As 802.15.4 is primarily, a mesh protocol, all protocol addressing must adhere to mesh configurations.
  - De-centralized communication amongst nodes

- **ZigBee**

  Features of ZigBee

  - Most widely deployed enhancement of IEEE 802.15.4.
  - The ZigBee protocol is defined by layer 3 and above. It works with the 802.15.4 layers 1 and 2.
  - The standard uses layers 3 and 4 to define additional communication enhancements.
  - These enhancements include

    authentication with valid nodes,

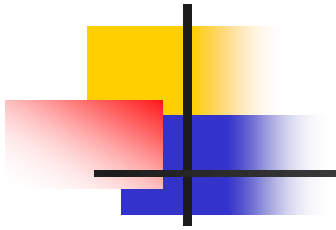
encryption for security, and a data routing and forwarding capability that enables mesh networking.

- The most popular use of ZigBee is wireless sensor networks using the mesh topology.
- ZigBee has two important components:
  - ZigBee Device Object (ZDO): ZDO responsible for Device management, Security, Policies.
  - Application Support Sub-layer (APS): APS responsible for Interfacing and control services, bridge between network and other layers

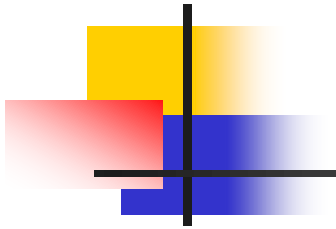
- **ZigBee Types**
  - ***1.ZigBee Coordinator (ZC)*:**
    - **T**he coordinator forms the root of the ZigBee network tree and might act as a bridge between networks.
    - There is a single ZigBee Coordinator in each network, which originally initiates the network.
    - It stores information about the network under it and outside it.
    - It acts as a Trust Centre & repository for security keys**.**
  - **2. *ZigBee Router (ZR)*:** Capable of running applications, as well as relaying information between nodes connected to it

- ***3. ZigBee End Device (ZED)*:**
  - It contains just enough functionality to talk to the parent node, and it cannot relay data from other devices.
  - This allows the node to be asleep a significant amount of the time thereby enhancing battery life.
  - Memory requirements and cost of ZEDs are quite low, as compared to ZR or ZC.
- **Applications:**
  - Building automation
  - Remote control (RF4CE or RF for consumer electronics)
  - Smart energy for home energy monitoring
  - Health care for medical and fitness monitoring
  - Home automation for control of smart homes
  - Light Link for control of LED lighting
  - Telecom services

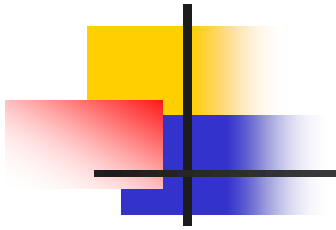
- **6LoWPAN**
  - Low-power Wireless Personal Area Networks over IPv6.
  - Allows for the smallest devices with limited processing ability to transmit information wirelessly using an Internet protocol.
  - Allows low-power devices to connect to the Internet.
  - Created by the Internet Engineering Task Force (IETF) - RFC 5933 and RFC 4919.
- **Features of 6LoWPANs**
  - 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



- **Addressing in 6LoWPAN**
  - 64-bit addresses: globally unique.
  - 16-bit addresses: PAN specific; assigned by PAN coordinator
- **6LoWPAN Routing**
  - Mesh routing within the PAN space.
  - Routing between IPv6 and the PAN domain
  - Routing protocols in use:
    - LOADng
    - RPL



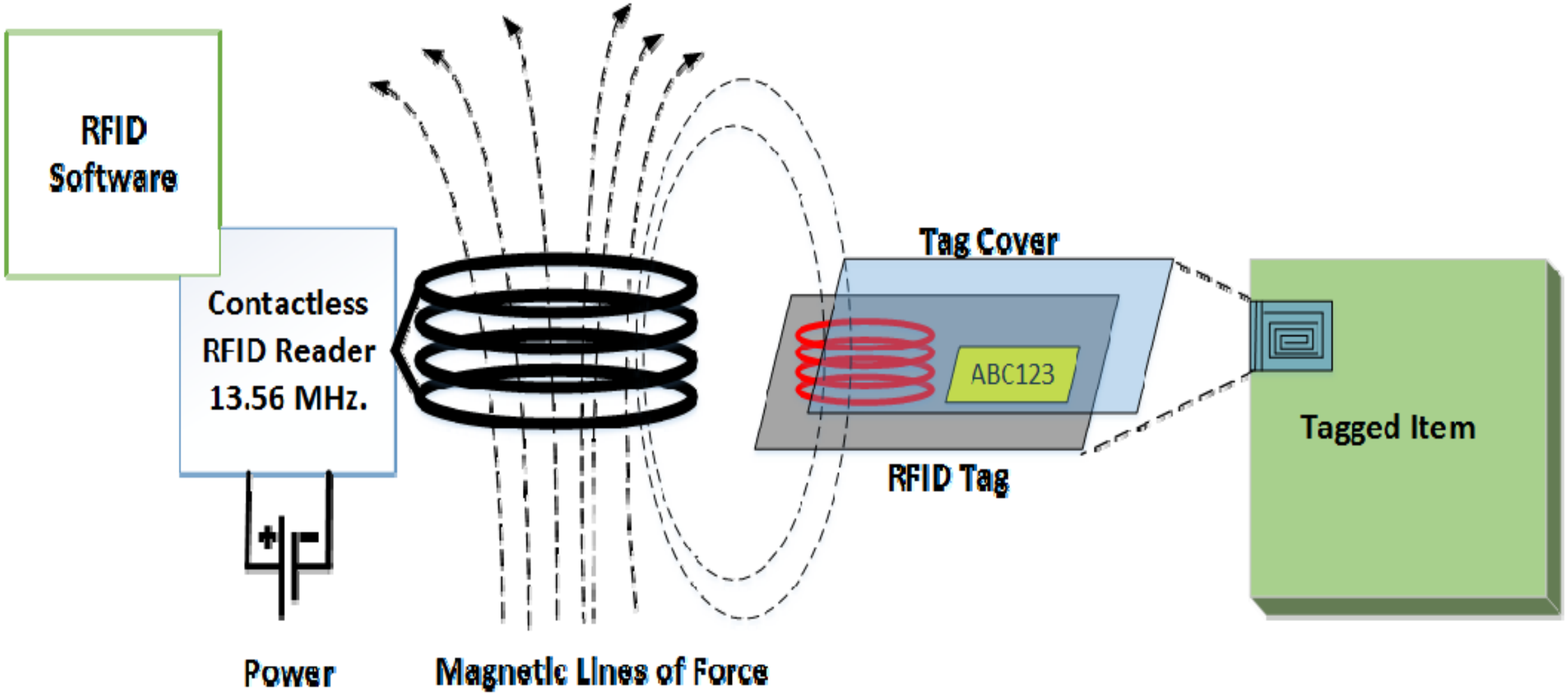
- **LOADng Routing**
  - Basic operations of LOADng include:
  - Generation of Route Requests (RREQs) by a LOADng Router (originator) for discovering a route to a destination,
  - Forwarding of such RREQs until they reach the destination LOADng Router,
  - Generation of Route Replies (RREPs) upon receipt of an RREQ by the indicated destination, and unicast hop-by-hop forwarding of these RREPs towards the originator.
  - If a route is detected to be broken, a Route Error (RERR) message is returned to the originator of that data packet to inform the originator about the route breakage.



- **RPL Routing**
  - Distance Vector IPv6 routing protocol for lossy and low power networks.
  - Maintains routing topology using low-rate beaconing.
  - Beaconing rate increases on detecting inconsistencies (e.g. node/link in a route is down).
  - Routing information included in the datagram itself.
  - **Proactive:** Maintaining routing topology.
  - **Reactive:** Resolving routing inconsistencies**.**

- **RFID**
  - RFID is an acronym for “radio-frequency identification”.
  - Data digitally encoded in RFID tags, which can be read by a reader.
  - Somewhat similar to barcodes.
  - Data read from tags are stored in a database by the reader.
  - As compared to traditional barcodes and QR codes, RFID tag data can be read outside the line-of-sight.
- **RFID Features**
  - RFID tag consists of an integrated circuit and an antenna.
  - The tag is covered by a protective material which also acts as a shield against various environmental effects.
  - Tags may be passive or active.
  - Passive RFID tags are the most widely used.
  - Passive tags have to be powered by a reader inductively before they can transmit information, whereas active tags have their own power supply.

- **Working Principle**
  - Derived from Automatic Identification and Data Capture (AIDC) technology.
  - 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.
- **Applications**
  - Inventory management 2. Asset tracking 3. Personnel tracking 4. Controlling access to restricted areas 5. ID badging 6. Supply chain management 7. Counterfeit prevention (e.g. in the pharmaceutical industry)


RFID
Software
Contactless
RFID Reader
13.56 MHz.
Power
Magnetic Lines of Force
Tag Cover
ABC123
RFID Tag
Tagged Item

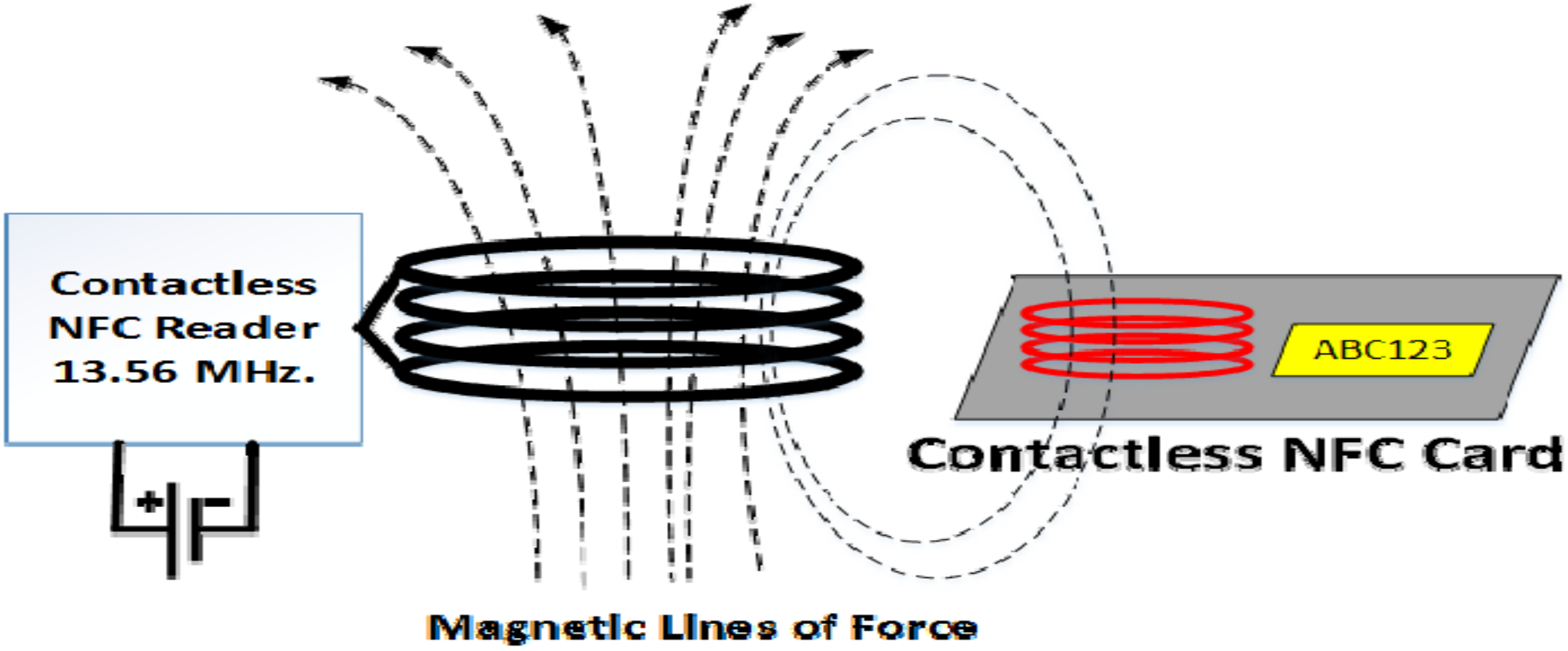
- **HART & Wireless HART**
  - WirelessHART is the latest release of Highway Addressable Remote Transducer (HART) Protocol.
  - HART standard was developed for networked smart field devices.
  - The wireless protocol makes the implementation of HART cheaper and easier.
  - HART encompasses the greatest number of field devices incorporated in any field network.
  - Wireless HART enables device placements more accessible and cheaper– such as the top of a reaction tank, inside a pipe, or at widely separated warehouses.
  - Main difference between wired and unwired versions is in the physical, data link and network layers. Wired HART lacks a network layer.

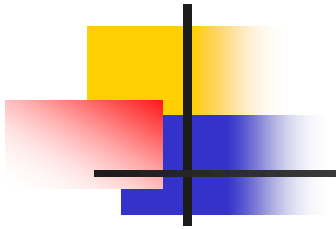
- **HART Physic al Layer**
  - Derived from IEEE 802.15.4 protocol.
  - It operates only in the 2.4 GHz ISM band.
  - Employs and exploits 15 channels of the band to increase reliability.
- **HART Data Link Layer**
  - Collision free and deterministic communication achieved by means of super-frames and TDMA. Super-frames consist of grouped 10ms wide timeslots.
  - Super-frames control the timing of transmission to ensure collision free and reliable communication.
  - This layer incorporates channel hopping and channel blacklisting to increase reliability and security. Channel blacklisting identifies channels consistently affected by interference and removes them from use

- **HART Network & Transport Layers**
  - Cooperatively handle various types of traffic, routing, session creation, and security.
  - Wireless HART relies on Mesh networking for its communication, and each device is primed to forward packets from every other device. Each device is armed with an updated network graph (i.e., updated topology) to handle routing.
  - Network layer (HART)=Network + Transport + Session layers (OSI).
- **HART Application Layer**
  - Handles communication between gateways and devices via a series of command and response messages.
  - Responsible for extracting commands from a message,
    - executing it and generating responses.
  - This layer is seamless and does not differentiate between wireless and wired versions of HART.

- **NFC**
  - Near field communication, or NFC for short, is an offshoot of radio-frequency identification (RFID).
  - NFC is designed for use by devices within close proximity to each other.
  - All NFC types are similar but communicate in slightly different ways.
- **NFC Types**
  - **Passive devices** contain information which is readable by other devices, however it cannot read information itself.
  - NFC tags found in supermarket products are examples of passive NFC.
  - **Active devices** are able to collect as well as transmit information.
  - Smartphones are a good example of active devices.

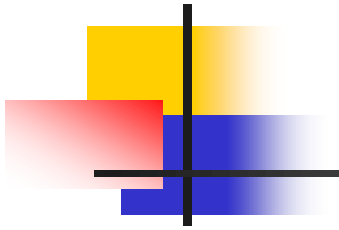
- **Working Principle**
  - Works on the principle of magnetic induction.
  - A reader emits a small electric current which creates a magnetic field that in turn bridges the physical space between the devices.
  - The generated field is received by a similar coil in the client device where it is turned back into electrical impulses to communicate data such as identification number status information or any other information.
  - ‘Passive’ NFC tags use the energy from the reader to encode their response while ‘active’ or ‘peer-to-peer’ tags have their own power source.


Contactless
NFC Reader
13.56 MHz.
+
-
ABC123
Contactless NFC Card
Magnetic Lines of Force



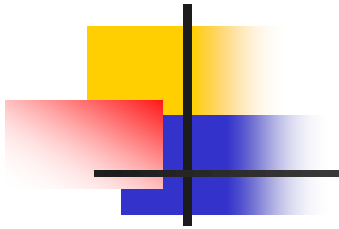
- **NFC Applications**
  - Smartphone based payments.
  - Parcel tracking.
  - Information tags in posters and advertisements.
  - Computer game synchronized toys.
  - Low-power home automation systems

- **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
- **Features**
  - 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.

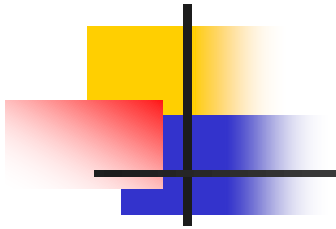


- Bluetooth operating range depends on the device:
  - Class 3 radios have a range of up to 1 meter or 3 feet
  - Class 2 radios are most commonly found in mobile devices have a range of 10 meters or 30 feet
  - Class 1 radios are used primarily in industrial use cases have a range of 100 meters or 300 feet.

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



- **Piconets:**
  - Bluetooth enabled electronic devices connect and communicate wirelessly through short range networks known as Piconets.
  - Bluetooth devices exist in small ad-hoc configurations with the ability to act either as master or slave. Provisions are in place, which allow for a **master** and a **slave** to switch their roles.
  - The simplest configuration is a point-to-point configuration with one master and one slave.
  - Devices in adjacent Piconets provide a bridge to support inner-Piconet connections, allowing assemblies of linked Piconets to form a physically extensible communication infrastructure known as Scatternet.



- **Applications**
  - Audio players
  - Home automation
  - Smartphones
  - Toys
  - Hands free headphones
  - Sensor networks

- **Z Wave**
  - Zwave is a protocol for communication among devices used for home automation.
  - It uses RF for signalling and control.
  - Operating frequency is 908.42 MHz in the US & 868.42 MHz in Europe.
  - Mesh network topology is the main mode of operation, and can support 232 nodes in a network.
  - Zwave utilizes GFSK modulation and Manchester channel encoding.
  - A central network controller device sets-up and manages a Zwave network.
  - Each logical Zwave network has 1 Home (Network) ID and multiple node IDs for the devices in it.
  - Nodes with different Home IDs cannot communicate with each other.
  - Network ID length=4 Bytes, Node ID length=1 Byte