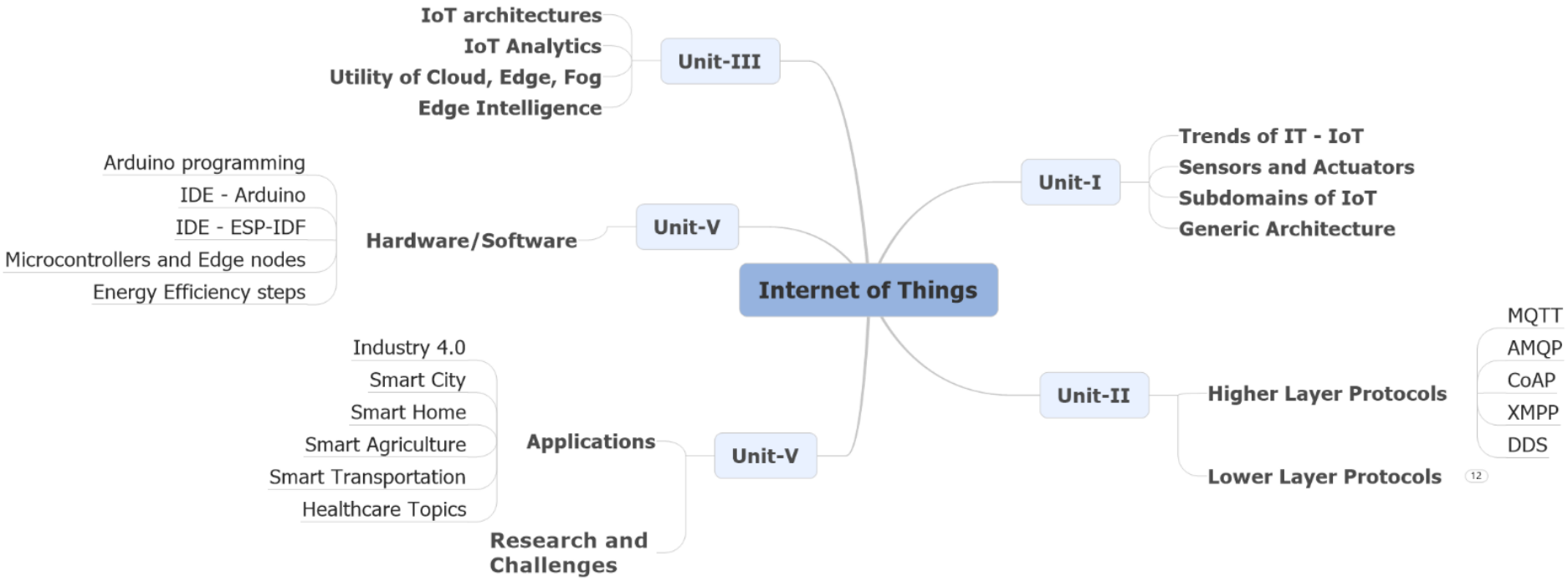
Selected Topics in Computer Architecture, Computer Networks, and Distributed Systems
(Internet of Things)
(IN3450)

–

Dr. Shajulin Benedict
shajulin@iiitkottayam.ac.in
shajulinbenedict@mytum.de

Prof. Dr. Michael Gerndt
gerndt@in.tum.de

Syllabus


Internet of Things
Unit-I
Trends of IT - IoT
Sensors and Actuators
Subdomains of IoT
Generic Architecture
Unit-II
Higher Layer Protocols
MQTT
AMQP
CoAP
XMPP
DDS
Lower Layer Protocols
12
Unit-III
IoT architectures
IoT Analytics
Utility of Cloud, Edge, Fog
Edge Intelligence
Unit-V
Hardware/Software
Arduino programming
IDE - Arduino
IDE - ESP-IDF
Microcontrollers and Edge nodes
Energy Efficiency steps
Unit-V
Applications
Industry 4.0
Smart City
Smart Home
Smart Agriculture
Smart Transportation
Healthcare Topics
Research and Challenges

LOWER LAYER PROTOCOLS

COMMUNICATIONS…

Communication Protocols

- Earlier, we have discussed the networking based protocols – mostly, at the service level.
- Now, we shall discuss the physical level or MAC level protocols for IoT systems
- (Consumer IoTs or Industrial IoTs) – ie., for connectivity of sensors to gateways or so forth.
- Several protocols that are more commonly used are listed as follows:
  - IEEE 802.15.4
  - Zigbee
  - 6LoWPAN
  - Wireless HART
  - Bluetooth
  - RFID
  - NFC
  - WiFi 5/6
  - Zwave
  - LoRaWAN
  - 5G
  - Bluetooth

Protocols and Standards

- IEEE 802.15.4
- Zigbee
- 6LoWPAN
- Wireless HART
- Bluetooth
- RFID
- NFC
- WiFi 5/6
- Zwave
- LoRaWAN
- 5G
- Bluetooth

IEEE 802.15.4

- This standard is mainly utilized for connecting PANs.
- IEEE 802.15.4 focusses on low cost, low speed, communication between PAN devices.
- The standard recommends a 10-meter communication range with a transfer rate of 250 kbit/s – i.e., it is meant for a short range communication.
- It was defined by IEEE 802.15 task group 4/4b.
- The standard was first published in 2003 and revised in 2006.
- The design of 802.15.4 takes into account the spectrum allocation rules of the US, Canada, Europe, and Japan.

IEEE 802.15.4

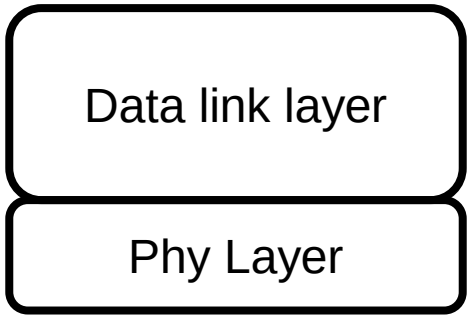
- It operates in the bottom two layers – Phy and MAC
- It has support to the ISM band (2.4 GHz)
  - The **industrial, scientific, and medical radio band** (**ISM band**) refers to a group of radio **bands** or parts of the radio spectrum that are internationally reserved for the use of radio frequency (RF) energy intended for scientific, medical and industrial requirements rather than for communications.
  - Unlicensed spectrum (for developing products)
  - Operates at 2.4GHz. https://en.wikipedia.org/wiki/ISM_radio_band

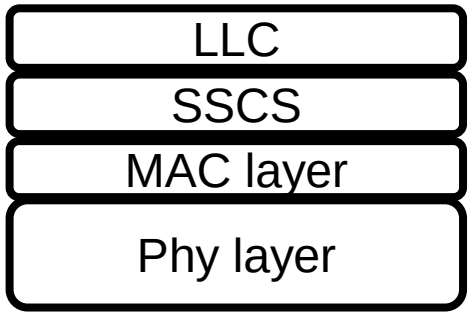
IEEE 802.15.4 -- Physical Layer

- The physical layer provides an interface between the MAC layer and the physical radio channel.
- It turns ON or OFF the transceivers.
- It is responsible to evaluate the required energy levels of communicating channels.
- It is responsible to evaluate the link quality measurement for each received packets.
- It is responsible to select wireless channels among available channels. (i.e., IEEE802.15.4 can be operated in 24 channels)
- It is responsible to initiate the modulation and spreading techniques.

IEEE 802.15.4 – DL Layer

- The datalink layer includes MAC Layer.
  - MAC Sublayer – it services the upper Service-Specific Convergence sublayer and physical layer.
  - Main duties:
    - Generating beacons if the device is a coordinator.
    - Synchronizing to the beacons if the device is a non-coordinator.





IEEE 802.15.4 – DL Layer

- Sublayers
  - SSCS – Service Specific Convergence Sublayer
    - it offers assured data transmission
    - Reliability
  - LLC – Logical Link Control
    - (mainly it provides a multiplexing mechanism for accessing links)
    - 1. slotted CSMA-CA for beacon-enabled communications.
    - 2. unslotted CSMA-CA for non-beacon-enabled communications.

Access-control methods of IEEE 802.15.4

- Access-control methods are good to avoid interferences between nodes.
- Two access methods
  - Beacon –enabled access method
  - Non-Beacon-enabled access method
- Beacon-enabled access method
  - Also, named as slotted CSMA/CA
  - Here, special nodes or routers periodically transmit beacons to confirm their presence to other network node.
  - Nodes may sleep, thus lowering their duty cycle and extending their battery lifetime.

Frequency-division multiple access (FDMA
Time-division multiple access (TDMA)
Code division multiple access (CDMA)
Spread spectrum multiple access (SSMA)
Space division multiple access (SDMA)
Power division multiple access (PDMA)

Access-control methods of IEEE 802.15.4

- Nonbeacon-enabled access method
  - Also, named as unslotted CSMA/CA
  - Here, routers typically have their receivers (nodes) continuously active. Thus, it requires continuous power supply.
  - However, it supports heterogeneous networks in which some devices continuously receive, while others only transmit when an external stimulus is detected.

IEEE 802.15.4

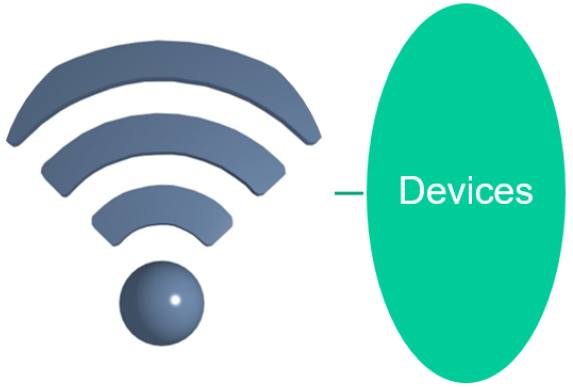
- It uses two versions of communications:
  - Low speed version – uses BPSK (Binary PSK)
  - High Speed version – uses Offset-QPSK (Quadrature-PSK)
- O-QPSK
  - Ie. The data to be transmitted is grouped in blocks of 4 bits.
  - Each block is mapped to one of 16 different symbols.
- IEEE 802.15.4 applies spread spectrum techniques to avoid noise,
  - SS approach is highly tolerant of noise and interferences.
- The power level defined on these systems ranges from 0.5mW to 1 mW.
- Transmission is mostly in the Line of Sight (LOS).
- Transmission is from 10 m to 30 m or 40 m.
- In some cases, outdoor communications range till 40 m.

IEEE 802.15.4 – number of releases and variants

- IEEE 802.15.4 Release 1 – 2003
  - It has two different PHYs - one for the lower frequency bands of 868 and 915 MHz, and the other for 2.4 GHz.
- IEEE 802.15.4 Release 2 – 2006
  - It has four new modulation schemes that could be used - three for the lower frequency bands, and one for 2.4 GHz.
- IEEE802.15.4 variants
  - A/B – normal standard
  - C for China (779-787 MHz band)
  - D for Japan (950 - 956 MHz band)
  - E for industrial applications - This release defines MAC enhancements to IEEE 802.15.4 (for industrial applications)
  - F for active RFID
  - G for smart grids - It may include the 902 - 928 MHz band

IEEE 802.15.4 – Types

- IEEE 802.15.4 networks are composed of several device types
  - Full functional devices
    - It includes PAN coordinator, router, and the device
    - Ie. Can talk to all types of devices
    - Supports full protocols.
  - Reduced functional devices
    - It could not route and do additional functions (only device)
    - The devices can only talk to FFD.



IEEE 802.15.4 topology models

- STAR topology
  - Data transfers are possible only between the PAN coordinator and the devices (in a STAR fashion).
- Peer to Peer topology
  - Data transfers can occur between any two devices.
  - However, this is simple only in networks comprising of permanently listening devices.
  - i.e., P2P communication devices that can enter sleep mode requires synchronization (which is currently not addressed by the standard).

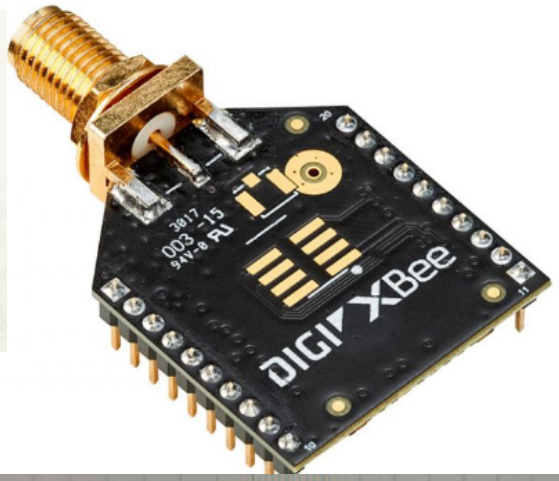
IEEE 802.15.4 – 5 different frames

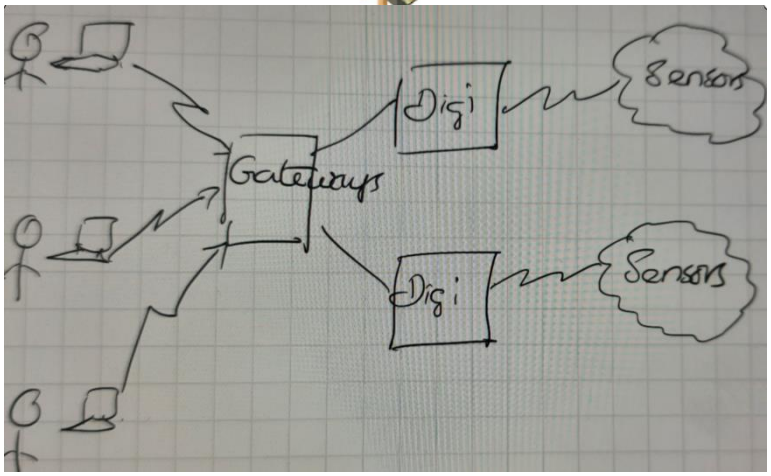
Beacon frame	• PAN coordinators at the regular interval of times may sense the availability of sensors. BEACON frames are utilized to check the availability of nodes. • Periodically frames are sent.
MAC frame	• MAC frame (link control and so forth) (ACCESs Control)
Command frame	• Used for control functions such as associating/disassociating devices from controllers or networks.
Acknowledgement frame	• For ACK of data
Data frame	• For data

Protocols

- IEEE 802.15.4
- Zigbee
- 6LoWPAN
- Wireless HART
- Bluetooth
- RFID
- NFC
- WiFi 5/6
- Zwave
- LoRaWAN
- 5G
- Bluetooth

Zigbee Devices – An example





xBee Zigbee module

Digi XBee3 PRO 2.4GHz ZB3.0 RP-SMA Female Antenna

Availability: **Out of stock - Join the waitlist to be emailed when this product becomes available**

Approx Restocking Date: NA

SKU: 130675

Add to Wishlist

1. Serial Data Interface: Uart, Spi, I2c.
2. Onboard Connector: RP-SMA Female.
3. Frequency Band: ISM 2.4 GHz.
4. Interference: Immunity Dsss (Direct Sequence Spread Spectrum).
5. Adc Inputs: (4) 10-bit Adc Inputs
6. Digital I/o: 15

₹ 3,499.00

Zigbee Protocol

- Earlier, we have discussed about IEEE 802.15.4 standard.
  - It provides a physical and link layer technology optimized for low bitrate, low duty cycle applications.
  - In practice, sensor and control applications need a mesh networking and a standard syntax for application layer messages.
- Zigbee Protocol
  - It enables the formation of clusters (via. mesh network).
  - It aims to improve encryptions (128bit AES encryption).
  - Only authenticated nodes were allowed to join the network.
  - Sophisticated routing processes via. AODV

Zigbee Protocol

- In 2002, several companies decided to form the ZigBee alliance to build additional functions to networking layers.
- Zigbee was conceived in 1998, standardized in 2003, and revised in 2006.
- The additional features were aimed at enabling a multivendor mesh network on top of IEEE 802.15.4 radio links.
- ZigBee alliance includes more than 200 members; ZigFests conferences were organized.
- Zigbee protocol became the most widely used protocol in IoT applications, especially in the smart home applications.

ZigBee Features

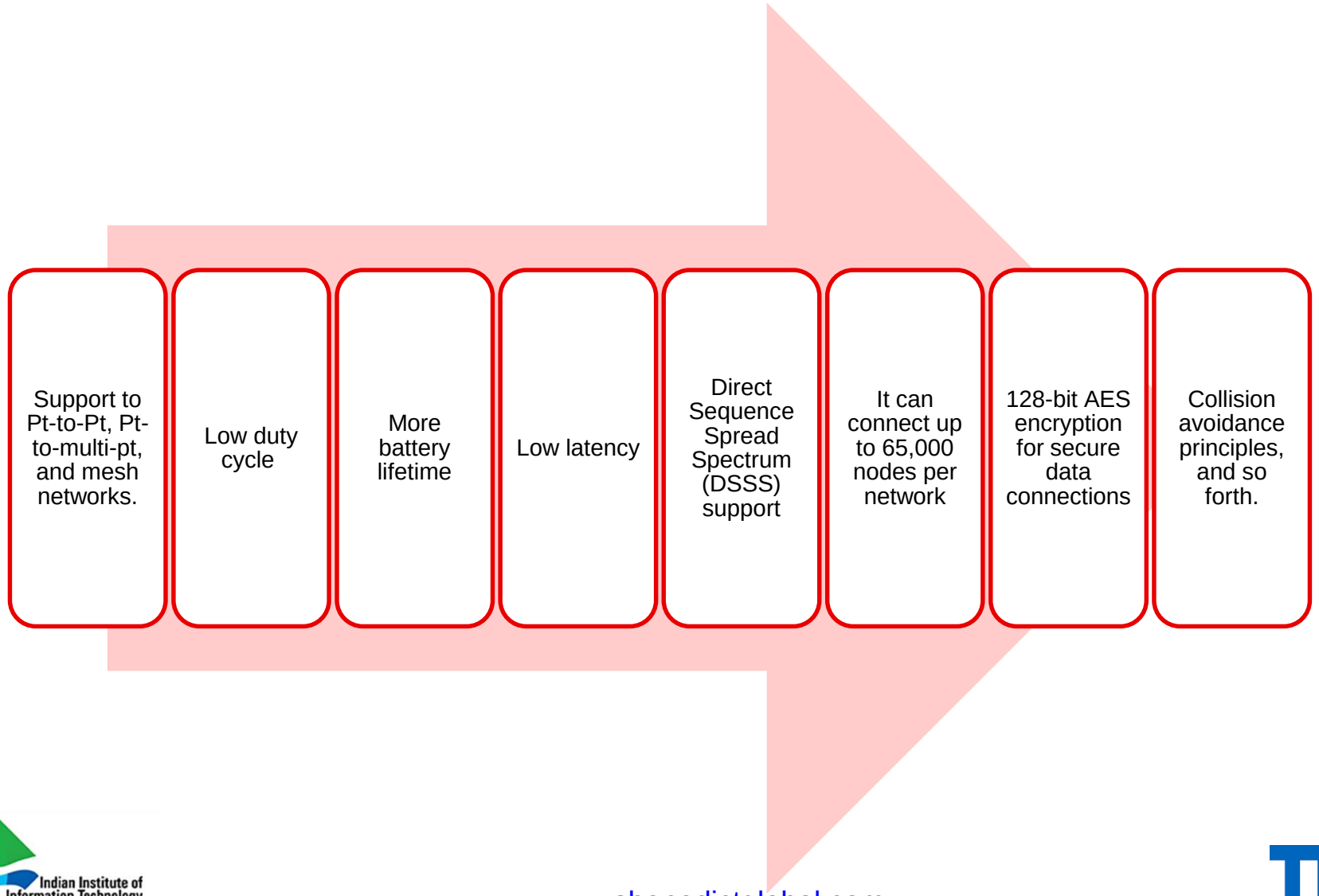
- Zigbee protocol uses IEEE 802.15.4 protocol lower layers.
- The major functions of zigbee is in top layers – i.e., layer 3 and above – for wireless mesh networks.
  - Wireless mesh networks are good for heterogeneous devices.
- The important features of Zigbee enabled devices include:
  - authentication with valid nodes.
  - encryption for security
  - Data routing and forwarding for enabling mesh networks.
- Zigbee promotes
  - Simpler connectivity
  - Less expensive modules
    - Costs of device is lesser than WiFi or Bluetooth-based devices.

Zigbee Protocol Features

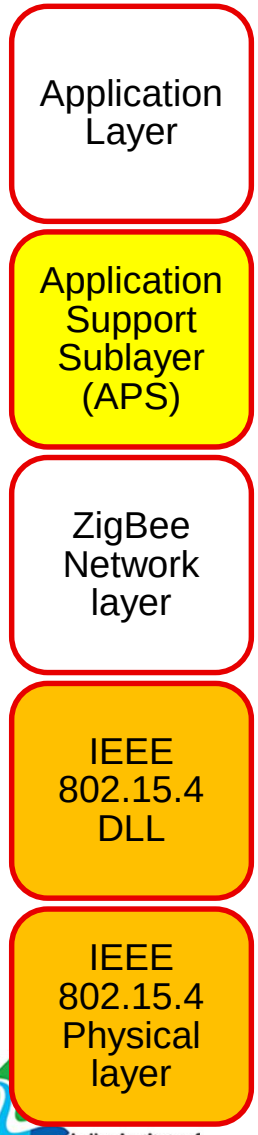
- As it utilizes IEEE 802.15.4 devices, the devices follow low range communication (ie. 10 m to 40 m)
- It also communicates within the Line of Sight.
- Zigbee has a defined data rate of 250kbit/s.

- There are several versions of ZigBee – ZigBee 2006, ZigBee 2007
- Zigbee 3.0 protocol is also released…

Zigbee 3.0 Protocol features



ZigBee Protocol Stack



- APS layer has several functions:
  1. Interface: It is responsible to serve as an interface between layers.
  2. Multiplexing / Demultiplexing – it forwards the network layer Messages to the appropriate application objects, according to their endpointID (each application is allocated an endpoint ID).
  2. Binding: the APS layer maintains the local binding table
  3. The binding table contains the information about the remote nodes and endpoints which have registered to receive messages from a local endpoint.
  4. 64-bit IEEE to 16 bit ZigBee network node address mapping is done.
  5. Management of end to end acknowledgements.
  6. Management of keys.

  7. (In succinct, APS deals with bridging between networks, interfacing and control services).

- DLL and PhyLayer belongs to IEEE802.15.4

Zigbee Protocol Stack

- Network Layer
  - Starting a network
  - Managing end devices while joining or leaving a network
  - Route discovery
  - Neighbor discovery

Zigbee Addressing Modes

- Direct Addressing
  - Two nodes talk each other directly.
  - Here, the source node will communicate with the destination by specifying the destination address and endpoint IDs.
- Group Addressing
  - This is handled by applications where a group of addresses are mentioned to send the packets.
- Broadcasting
  - In broadcasting, packets are sent to all devices in a network.
  - Typically, it is utilized to frame routes for communications.

Zigbee Node Types

- Zigbee Coordinator (ZC)
  - It forms the root of the Zigbee network tree.
  - It can act as a bridge between networks.
  - There is a single ZC in each network.
  - ZC is responsible to initiate the network.
  - It stores information about the network under it and outside it.
  - It acts as a trust centre and repository for security keys.
- Zigbee Router (ZR)
  - It is capable of running applications or relaying messages between nodes connected to it.
  - It is responsible to route packets between nodes.
- Zigbee End Device (ZED)
  - The device (mostly, with Reduced Functionality) talks to the parent node or router.

Zigbee – Primany S/w Components

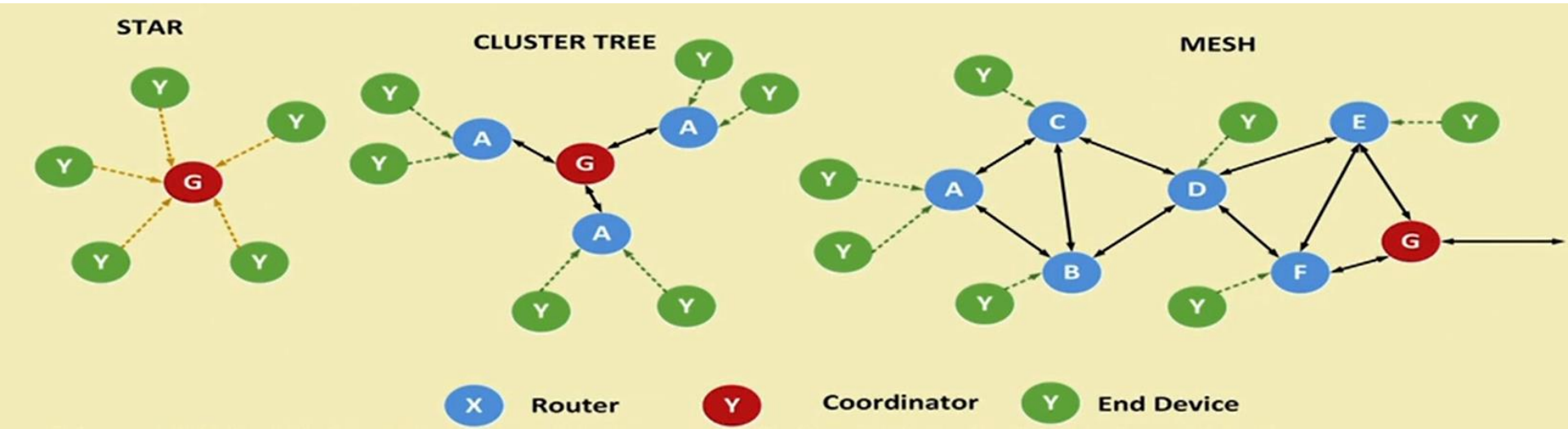
- Zigbee Device Object (ZDO)
  - ZDO works in the application layer.
  - ZDO is a specific application which runs on endpoint 0.
  - It is designed to manage the state of the ZigBee node.
  - It determines the type of device in a network (for example, end device, router, or coordinator)
  - It initializes the APS, network layer, and security service provider.
  - It performs device and service discovery.
  - It initializes the coordinator for establishing a network.
  - In succinct, this component is responsible for
    - Security management
    - Network management
    - Binding management

Zigbee – Primany S/w Components

- **Endpoints:**
  - Each end node or end device can have multiple EPs.
  - Each EP contains an application profile, such as home automation, and can be used to control multiple devices or a single device.
  - Each EP defines the communication functions within a device.

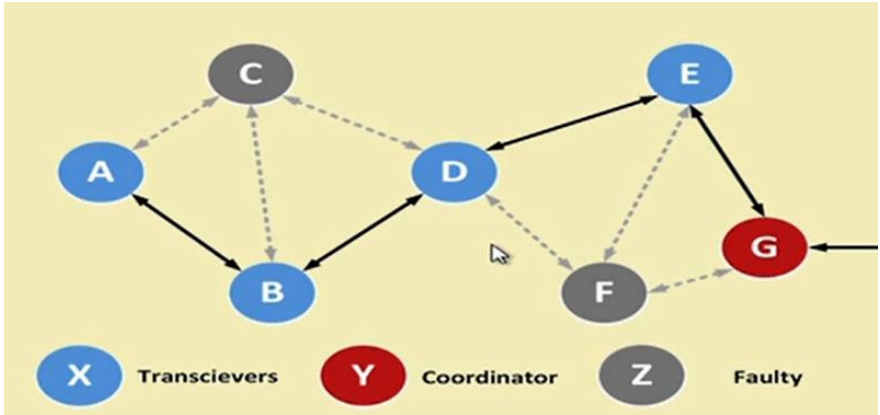
Zigbee Topologies

- Star topology
  - Coordinator and end devices communicate each other.
  - Similar to a simple LAN.
- Cluster Tree topologies
  - Here, clusters are formed;
  - Blue color represents routers (looks like a tree).
- Mesh topology
  - Here, many routers are required; However, one coordinator will acts as a gateway for internetwork.



Zigbee Mesh

- In a mesh network, any node can communicate with any other node within a range.
- If nodes are not in a range, messages are relayed through intermediate nodes.
- Thus, Zigbee mesh has the capability of framing a large network (scalable one).
- And, these networks can be highly reliable.
- For example, if node C and F are not accessible, the message packets from A can be relayed via. B, D, and E to the Gateway!
- Zigbee networks are
  - Self configurable
  - Self-healing



Zigbee Network Layer

- The network layer uses AODV (AdHoc Ondemand Distance Vector Routing) protocol
- AODV
  - An Ad Hoc On-Demand Distance Vector (AODV) is a routing protocol designed for wireless and mobile ad hoc networks.
  - It establishes routes to destinations on demand – i.e. only if they are requested by source nodes.
  - It supports both unicast and multicast routing.
  - The routes are maintained as long as they are required by the sources.
  - Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV.
  - These message types are received via UDP.

AODV -- Cases

- Case 1: Source sends packets to a destination node – Routes Found:
  - Step 1 – Source checks the routing table.
  - Step 2 – If routes are available, it sends packets via. the route to the destination.
- Case 2: Source sends packets to a destination node – Routes are not found:
  - Step 1 – Source initiates a route discovery process using broadcasting RREQ message.
  - Step 2 – Each receiving node will check the source address and the request ID on receiving a RREQ message.
  - Step 3 – To avoid any possible duplication while processing the routes, nodes that received a RREQ message earlier will not be considered.

Protocols

- IEEE 802.15.4
- Zigbee
- 6LoWPAN
- Wireless HART
- Bluetooth
- RFID
- NFC
- WiFi 5/6
- Zwave
- LoRaWAN
- 5G
- Bluetooth

Wireless HART

- It is designed by HART Communication Foundation (1986).
- WirelessHART is a subset of HART systems
  - Highway Addressable Remote Transducer
  - i.e., sensor data (mostly analog) is communicated via a low level AC digital signal.
  - i.e., configuring and reading instrumentation via 4-20mA AC signal.
- Industrialists could remotely control, calibrate, configure, and receive sensor data from a control room (laptops/PCs or hand-held instruments)
  - Especially, when the devices are located in hazardous area where humans could not reach the devices for configuring them.
- Fast installation and networking setup.

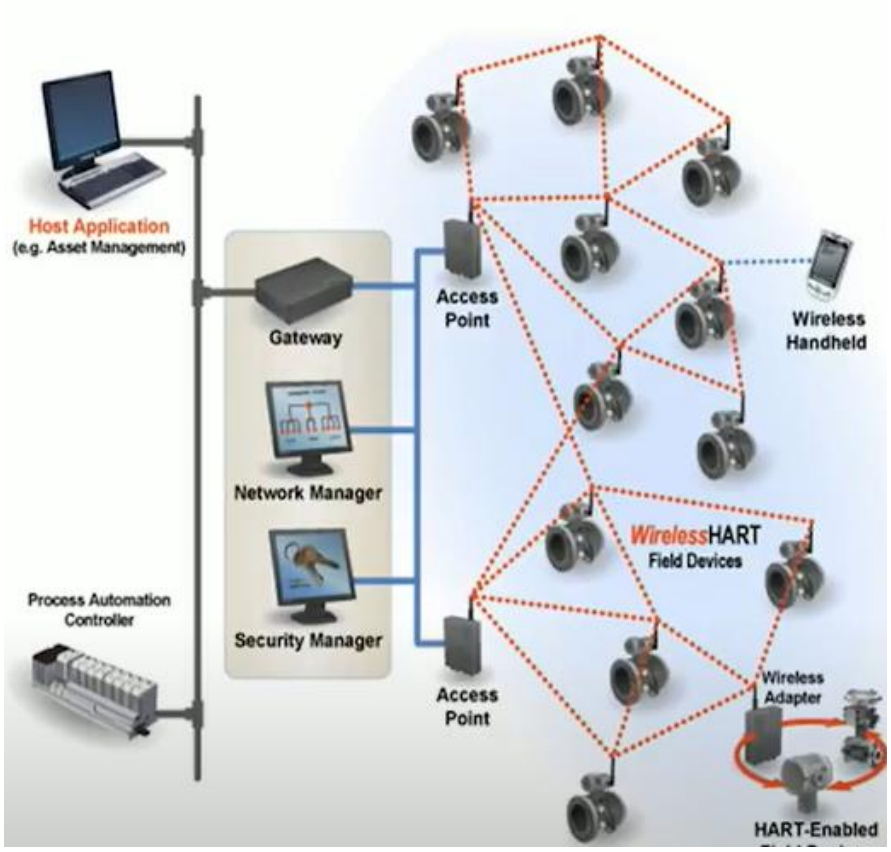
Wireless HART - features

- Self-healing – due to MESH networks
- Self-optimizing
- Secure Mesh (creating channels, blacklisting channels, 128bit AES)
- IEEE802.15.4
- 2.4GHz-ISM (with 15 channels)
- 15 channels use TDMA (compared to zigbee with CSMA/CA)
- Low cost,
- Low datarate
- Low range
- Long years (5 to 7 years)

WirelessHART -- Components

- WirelessHART Devices
  - To remotely sense data…
  - They can be powered by battery,
    cables, or renewable sources.
  - The device can be powered ON when batteries are enabled.
- WirelessHART Adapters
  - To create a connection between wired and wireless HARTs.
  - Battery-powered or line-powered.
  - Multiple wireless HARTs could be connected to one wired node.
- WirelessHART Gateways and Handhelds
  - This provides network management capabilities, security capabilities,
    \nd, forms mesh networks.

Wireless HART – Typical Connection Layout



Instrumentationtools.com

Protocols

- IEEE 802.15.4
- Zigbee
- 6LoWPAN
- Wireless HART
- Bluetooth
- RFID
- NFC
- WiFi 5/6
- Zwave
- LoRaWAN
- 5G
- Bluetooth

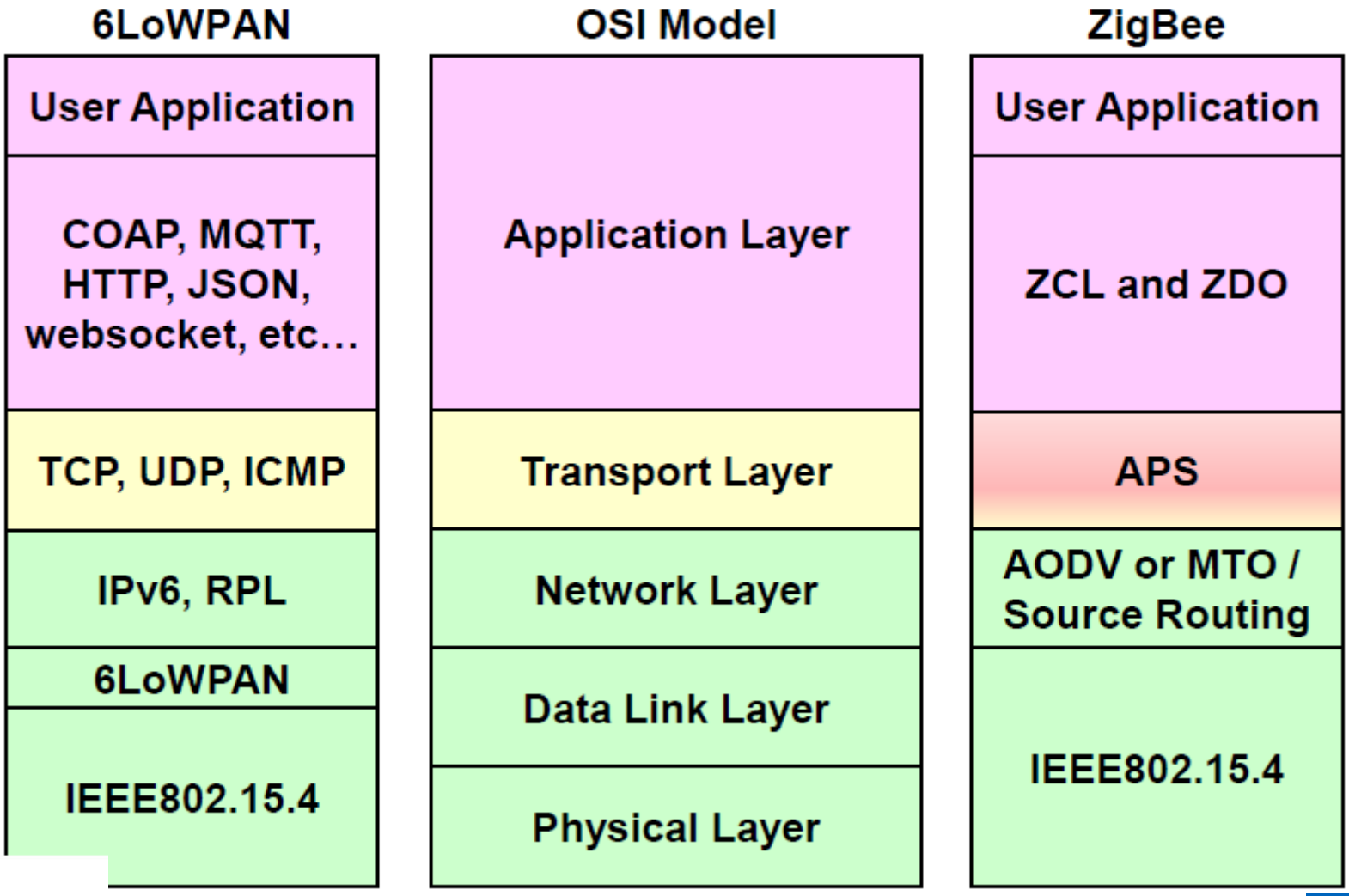
6LoWPAN

- 6LoWPAN
  - IPv6 over Low Power Wireless PAN.
- It is used for connecting IoT devices over internet.
  - Intended for IEEE802.15.4 devices.
- It runs over IPv6 – mostly, wireless devices
  - Hence, the name is 6LowPAN
- It allows the low power devices to connect to the internet.
- It allows IEEE802.15.4 radios to carry 128-bit addresses of IPv6.
- It adds header compression and address translation techniques to support internet.
  - i.e., IPv6 are compressed to support the low power IEEE802.15.4 radios.

6LoWPAN vs. ZigBee

- Essentially, 6LoWPAN products have reached the competition level of ZigBee's market.
- As 6LoWPAN can utilize 802.15.4,
  - Low power and low data rate are ensured.
- 6LoWPANs have seamless integration with other IP-based systems.

6LoWPAN vs. ZigBee



6LoWPAN - 2 types of MAC addresses

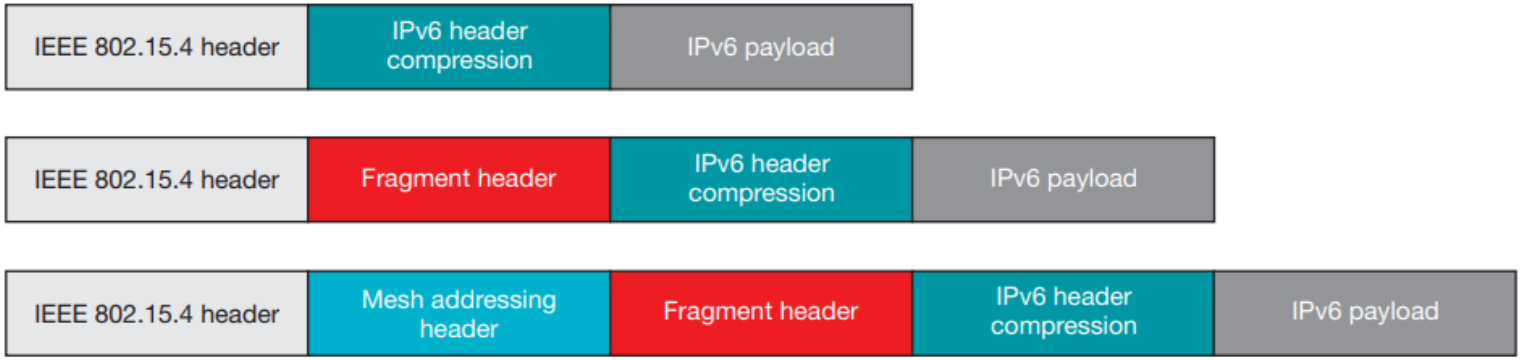
- 64-bit extended
  - It is used for global unique addressing or global unique connectivity.
- 16-bit short addresses
  - It is PAN specific.
  - The 16-bit short addresses are assigned by the PAN coordinator.

6LoWPAN packet format

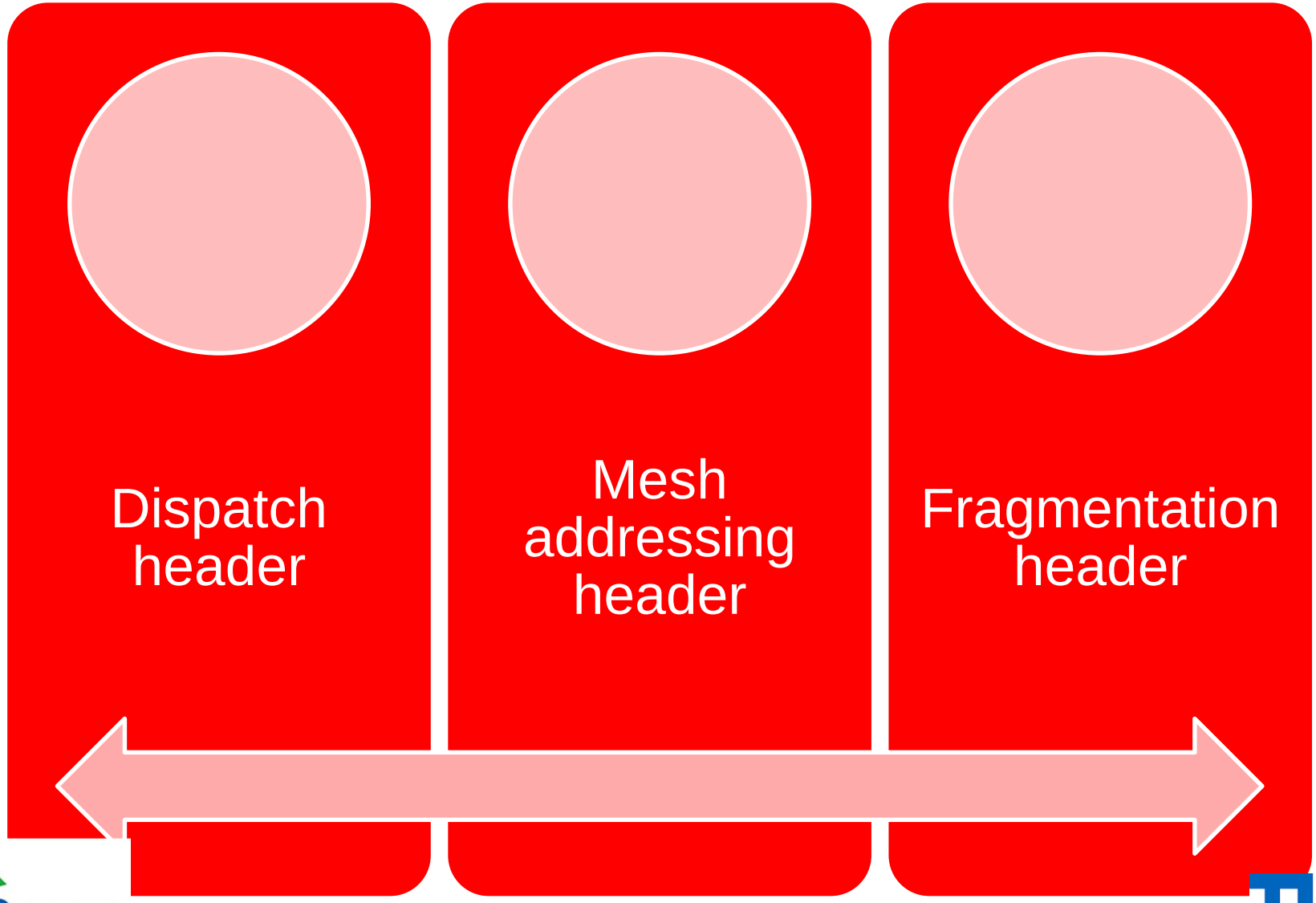
- It uses stacked headers (or, termed as extension headers)
- i.e., it has IEEE802.15.4 and IPv6 together for the internet.
- Note that IPv6 and IEEE802.15.4 are together combined with a header.
- 32 bit header.

6LoWPAN packet format

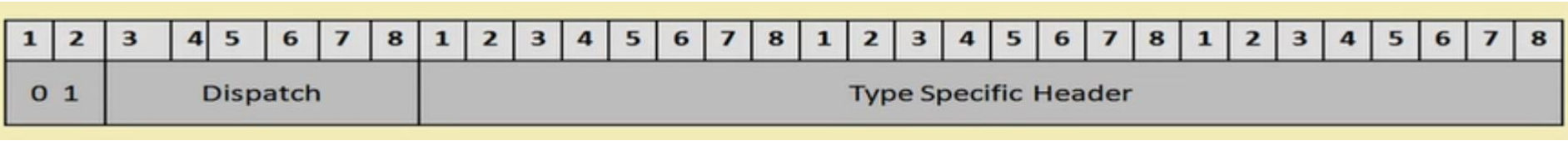
- It utilizes header compression techniques
  - Due to this feature, the header size could be reduced
  - to 2 bytes to 20 bytes when compared to 40 bytes in IPv6.



Types of headers



Dispatch Header

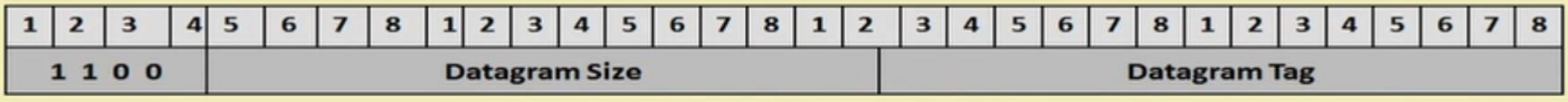


- Dispatch header is used for initiating the communication.
- First two bits indicate the dispatch packet.
- Dispatch information has 6-bits
- Dispatch bits identify the next header type.
- Type specific header (24 bits) – mentioning a specific routing process.

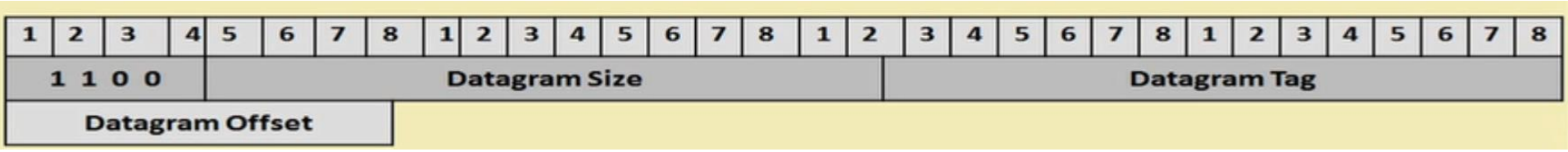
Mesh Addressing Header

- 1-0 defines the packet as Mesh Addressing Header.
- V → 0 if source is 64-bit extended address
- V → 1 if source is 16-bit address.
- F → 0 if destination is 64 bit address
- F → 1 if destination is 16 bit address
- Hops left
  - Consists of 3 bits
  - Represents the hops
  - Decremented by each node before sending it to next hop.

Fragmentation Header



- First fragment has 1100, Datagram size and the tag.



- Subsequent fragments have 1100, datagram size, tag and the datagram offset.

6LoWPAN Routing

- Mesh based routing
- It is applied in PAN domain.
- Two commonly used routing protocols are
  - LOADng – a lightweight version of AODV routing protocol.
    - Ie. RREQs, RREPs, and RERR messages.
  - RPL – Routing Protocol for Lossy and Low Power networks.
    - Based on DVR; Maintains routing topology using low rate beaconing.
- As seen, PAN networks are connected to IP domains using gateway.
- Both routing protocols aims at
  - Optimizations such as
    - Minimizing energy
    - Minimizing latency
    - Node power
    - Bandwidth and so forth