Unit - IV

IoT Protocols

4.1> Protocol Standardizatn for IoT
4.2> M2M and WSN protocols
4.3> RFID Protocol
4.4> Modbus Protocol
4.5> Zigbee Architecture
4.6> Ip based Protocols :..
  4.6.1> MQTT (Secure)
  4.6.2> 6LoWPAN
  4.6.3> LoRa

4.7) Protocol standardization of IoT: -

- In order to develop any product you have to follow standards. In IoT also you have to follow the standards for developing any product.
- What are standards, standards consist of specification and universally accepted protocols, so if any prody is developed according to standards the performance is guranteed.
- In IoT if you develop a product using those standards two things are guranted, that is interoperability & interconnectivity. These are essential things, when you follow the standards.
- Interoperability is the ability of one system to communicate with other system regardless of manufacturer or any technical specification.
- eg. In IoT if we consist of 2 diff. system, 1st is eleraly patient monitoring system & second is intrusion detection system Both uses the same infrastructure like camera & motion detector so if both the system are developed using the standards

then they will be able to share the sensor data to each other that is called as interoperability.
- Sharing the same sensor data betn two systems without any difficulty.
- All the system which are develop has to follow the standards. So what are all the organizatn which are involved in developing standards in IoT.

4.2> M2M & WSN Protocols:-
- M2M applⁿ - highly customized. From the auto sector to the smart grid, vertical industries are adopting standrds.
- Horizontal standards are a must for M2M to progress from its current condⁿ to truly linked IoT.
- In the future, a horizontal standard is likely to be the primary driver of growth.
- The International Telecommⁿ Unions and ETSI, Global standards collaboratn, which has established the M2M standardizatn Task

force.
- It defines a vertical industry and comm^n technology agnostic conceptual framework for m2m appln, as well as a service layer that allows appln developer to create applns that operate transparently across different vertical domains & comm^n technologies without having to write their own complex custom service player.

- m2m standards Activities: -
- m2mXML, JavaScript Object Notation, BiTXML, WMMP, MDMP, open binding inform^n exchange, EEML, open m2m inf$_o^m$ exchange are data transmission protocol standards.
- Extend OMA DM to include protocol mgmt. objects for m2m devices.
- m2m device mgmt., m2m gateway standardizat^n.
- m2m fraud detect^n and security
- m2m service features of N/w API.
- standards for charging.

- standardizat^n Bodies in the field of WSNs :-
- The IEEE is concerned with

the physical & MAC levels, while the IETF is concerned with layers 3 & up.
- The IEEE Instrumentation & measurement Society's Sensor Technology.
- Technical committee developed IEEE 1451, a set of smart transducer interfaces ~~for~~ connecting standards that describe a set of open, common, HW-independent comm^n interfaces for connecting transducers to microprocessors.
- The defining of transducer electronic data sheets for each transducer is one of the essential parts of these standards.

- Issues with IoT standardizat^n.
- There are also standardizat^n efforts from important vertical IoT appln^s such as smart grid and telematics, which can be characterized as one of four pillars.
- GTP is an example of a telematics standard.
- Its growth nothing that

standardization isn't always a good thing. When standards are adopted by the market, they can be a double-edged sword: they are necessary for market development, but they can also be a threat to innovation & change
- 3GPP, for example, is limited to cellular wireless ~~networks~~ nlws, while EPC global's middleware is limited to RFID events.

4.3) RFID Protocol:-
- An RFID tag is a contactless smartcard that is streamlined, low-cost, and disposable. RFID tag have a chip that stores a static number and the tagged object's properties, as well as an antenna that allows the chip to send the store number to a reader.
- The tag is powered by the reader's RF field and broadcasts its ID & characteristics to the reader when it gets within range of the suitable RF reader.
- RFID readers & tags, as well as RFID S/W or RFID middleware.

are all part of an RFID system.

- Active, Passive, and semi-passive RFID tags are available. Active RFID contains an on-board battery that constantly broadcasts its signal, whereas passive RFID does not.
- RFID differs from the other three IoT technologies in that it tags a "unintelligent" object, like a pallet or an animal to turn it into an instrumented intelligent obj. for monitoring & tracking, whereas the other three simply connect intelligent electronic devices.
- The International Organizⁿ for standardizⁿ claims jurisdictⁿ over the air interface for RFID through ISO 18000-1 through 18000-7, which are still in development.
- The Auto-ID principle is that data is kept on the Internet or the EPC global nlw, with the EPC recorded in the tag serving as an index to locate the data.

(4) MODBUS PROTOCOL:-

- Modbus is a serial comm^{n} protocol developed by Modicon for use with it's programmable logic controllers in 1979.
- It has now established a de facto standard comm^{n} protocol and is now a widely available technique of linking industrial electrical devices since it is simple and sturdy.
- Since April 2004, when Schneider Electric handed rights to the Modbus Organizat^{n}, the development & modificat^{n} of Modbus protocols has been overseen by that organizat^{n}.
- Modbus is the first widely acknowledged fieldbus standard. The Modbus protocol is a master/slave protocol, which means that a device acting as a master will poll one or more slave devices.
- The master will write data to the registers of a slave device & read data from the register of a slave device.

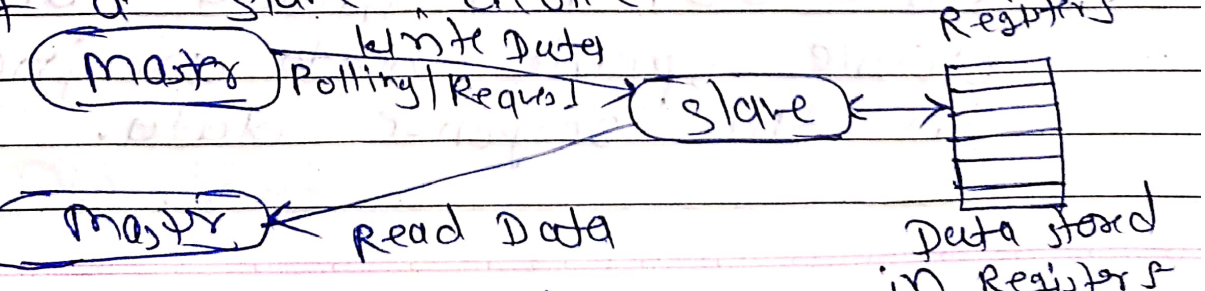

Fig. master-slave Protocol

1.) ASCII Transmission Mode:-
- Each byte is encoded on the serial line as two ASCII characters in ASCII Transmission Mode. One start bit, seven data bits, zero or one parity bit, and one or two stop bits are sent for each ASCII character.

2.) RTU Transmission Mode:-
- The msg is sent in a continous stream in RTU (Remote Terminal Unit) transmission mode.

- Modbus functions:-
- The fun code field contains 2 characters in ASCII mode and eight bits in RTU mode.
- 0X02: Status of Read Input. Starting register add' and no. of successive addresses to read are the parameters.
- 0X11: Slave ID Report. There are no parameters. Slave ID, run indicatn, and device_specific data are included in the response data.

- Modbus TCP/IP:-
Modbus TCP/IP is based on the OSI n/w Model and can be used on any ethernet n/w.

4.5) ZIGBEE Architecture:-
- The mesh comm^n protocols ZigBee & ZigBee pro are built on top of the IEEE 802.15.4 PHY.
- DigiMesh is a ZigBee alternative that modifies a few things & adds certain features to make it more user-friendly. Digi's XBee & XBee pro radio comm^n modules are known by their brand names.

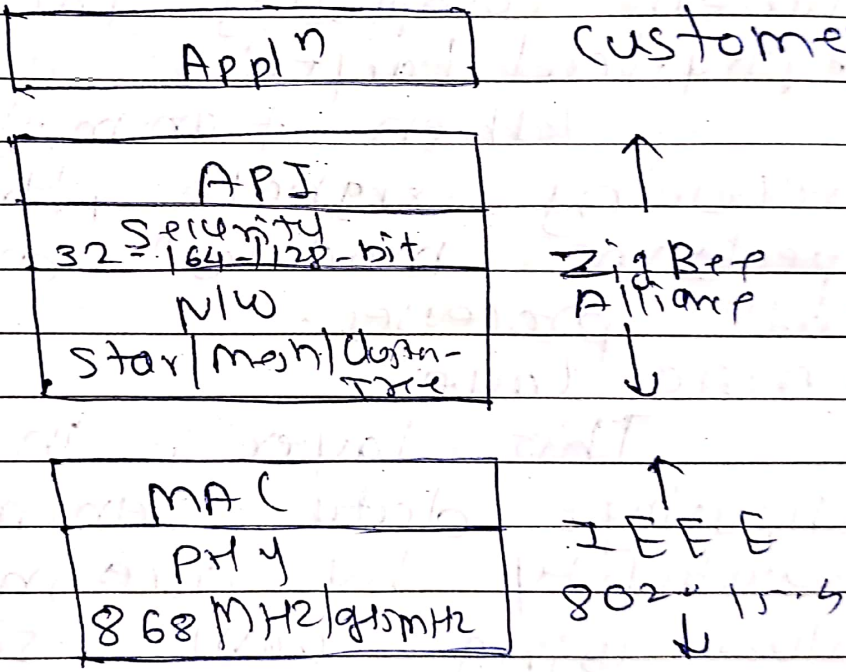

Fig. Zigbee Stacklayered Arch.

- IEEE 802.15.4 definer the low

2 layers, namely physical & media access layer, while the top layer, namely nlw layer & framework of appln layer.

- Appln support (APS) sub-layer zigbee device obj., and appln obj. for manufacturer are all supported by the appln layer.
- The zigbee protocol architecture is made up of a stack of levels, with physical & MAC layers defining IEEE 802.15.4 & zigbees own nlw & appln layers completing the protocol.

• Physical Layer:-

When transmitting & receiving signals, this layer performs modulation and demodulation processes.

• MAC layer:-

This layer is in charge of ensuring data transmission reliability by accessing several nlws using carrier sense multiple access collision avoidance.

• N/w layer:-

This layer is responsible for all nlw related oper

such as n/w setup, end device conn^n & disconnect^n, routing and configuring the device etc.

- Operating Modes in Zigbee: -
- Non-beacon mode and beacon mode are the two modes in which Zigbee 2-way data is transmitted.
- However, it uses more power and has low total power consumpt^n b'coz most of the devices in the n/w are inactive for long periods of time.
- These beacon n/ws fun on a time slot basis, which means they activate only when comm^n is required, resulting in shorter duty cycles and greater battery life.

- Topologies in zigbee: -
- zigbee supports a variety of n/w topologies, but the star, mesh & cluster tree topologies are the most frequent.
- This architecture is utilized in businesses where all endpoint devices must connect with the central controller, and it is

simple and straightforward to implement.
- These topologies automatically redirect info to other devices if any node fails.

- Why are Zigbee Data Rates so low?
- We are aware that several wireless technologies, such as Bluetooth & WiFi, are available on the market & deliver high data speeds.
- Zigbee data speeds are lower b'coz the primary goal of zegbee development is to use it for wireless control & monitoring

- Devices that Use Zigbee Technology:-
- The IEEE 802.15.4 Zigbee specification primarily comprises 2 types of devices: full fun devices & Reduced-fun Devices. An FFD Device can do any task within the n/w & performs different tasks as described in the standard.

- An RFD device has limited capabilities, therefore it can only execute certain activities, yet it can communicate with any other device on the nlw.
- The zigbee device in an IEEE 802.15.4 nlw network serve three separate roles: co-ordinator, PAN coordinator, and device.

- Advantages & Disadvantages of Zigbee.
- Advantages:-
1. This nlw has a nlw structure structure that is adaptable.
2. The battery life is adequate.
3. The amount of energy used is reduced.
4. It's quite easy to fix.
5. Less money is spent.

- Disadvantages:-
1. It is inferior when compared to Wifi.
2. The zigbee's transmission rate is lower.
3. It excludes a number of end devices.
4. Being utilized for official private info is quite dangerous.
5. This ZigBee comm system.

like other wireless n/w's, it is vulnerable to illegal interfer

4.6) IP Based Protocols:

1) MQTT (series):-

- MQTT is an acronym for m queuing Telemetry Transport.
- It is a lightwt messaging protocol designed for usage in situations where clients require a minimal code footprint and a linked to unreliable n/w or n/w with restricted capacity.
- MQTT structure:-
- MQTT uses a PUSH/SUBSCRIBE topology to run on top of TCP/I There are two sorts of syst in MQTT architecture: clients & brokers.
- MQTT is a protocol i.e. trigge by events. There is no continuou or periodic data transmission. As a result, transmission is kep to a bare minm.

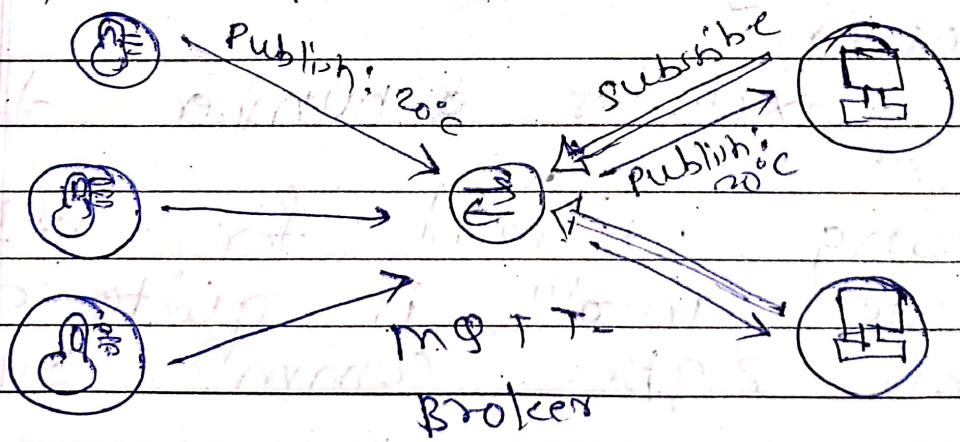

Fig. Architecture of MQTT

- Another way MQTT reduces transmission is by using a well-defined, compact msg. structure. Each msg. contains a 2 byte fixed header.

• Topics in MQTT :-

- msg.s are published on topic in MQTT. Topics are hierarchical structures delimited by the slash (/) character. This structure is similar to computer file system's directory tree.
- A structure like sensor/oil & car/pressure allows a subscriber to define whether it wants to receive data solely from clients who publish to the pressure topic, or all data from clients who publish to ~~any~~ the pressure topic, or all data from clients who publish to any sensor/oil & car topic.
- In MQTT, topics are not created directly. When a broker receives data for a subject that doesn't exist yet, the topic is simply formed, and clients can subscribe to it.

• msg. to be Retain:-

- Received msgs are not saved

on the broker unless they are indicated with the retained flag to keep the footprint short.

- MQTT messages:-
To keep the protocol short, any comm can only take one of four action: publish, subscribe, unsubscribe, or ping.

- Publish:-
This command sends a data block containing the msg. to be sent. This inform is unique to each implementation.

- subscribe:-
Turns a client into a topic subscriber. Topic can be subscribed to individually or using wildcards, which allow you to subscribe to a full subject branch or a subset of any topic branch.

- PING:-
The broker can be pinged by a client. The subscriber sends a PINGREQ packet which

is followed by a PINGRESP packet

- DISCONNECT:-
  This msg. notifies the broker that it will no longer be required to send or ques msg. for a subscriber, and that it will no longer recive data from a publisher.

- Security in MQTT:-
  The MQTT protocol's original purpose was to make data transmission as compact & efficient as feasible across expensive, unreliable comm^n links.
- Security of the n/w:-
  If the n/w can be protected, the transmission of unsafe MQTT data becomes irrelevant. In this situat^n, security vulnerabilities would have to arise from within the n/w, possibly through a bad actor or another method of n/w penetration.
- Username & p/w:-
  MQTT allows a client to establish a conn^n with a broker using usernames & passwords.

- SSL / TLS :-
  Implementing SSL / TLS on top of TCP/IP is the obvious approach for safeguarding transmissions between clients & brokers.

- MQTT v5.0 has A lot of New features :-

1. Reason codes :-
   Initially, if MQTT encountered a problem, it did nothing. The sole error code was failure itself.

2. Shared subscriptions :-
   A broker's load can be affected if there are too many subscribers to a single subject.

3. Msg. expiry :-
   If a msg. is not delivered within a certain amount of time, it can be erased.

4. Topic alias :-
   The names of topics can get so long that they obstruct the protocol's modest foot print.

1.2

2> IP Based PROTOCOLS: 6LoWPAN.

- Originally designed for 802.15.4, 6LoWPAN provides the upper layer technology for usage with low power wireless comm^n's for IoT and M2M.
- Wireless sensor n/w's are one of the many use's for the 6LoWPAN system.
- 6LoWPAN is an open standard described in RFC 6282 by the Internet Engineering Task force.
- Although 6LoWPAN group then established the encapsulat^n and compression technologies required to transport IPv6 data across a wireless n/w.

- Architecture of 6LoWPAN:-

- 6LoWPAN is a low-cost comm^n n/w that delivers IPv6 networking over IEEE 802.15.4 networks, allowing wireless access in appl^n's with low power & low throughput needs.
- When a sensor node with a lower processing capability, also known as a reduced fun device (RFD), in a 6LoWPAN

wants to send its data packet to an IP-enabled device outside the PAN, it first sends it to a higher processing capability sensor node, also known as a full fun device.

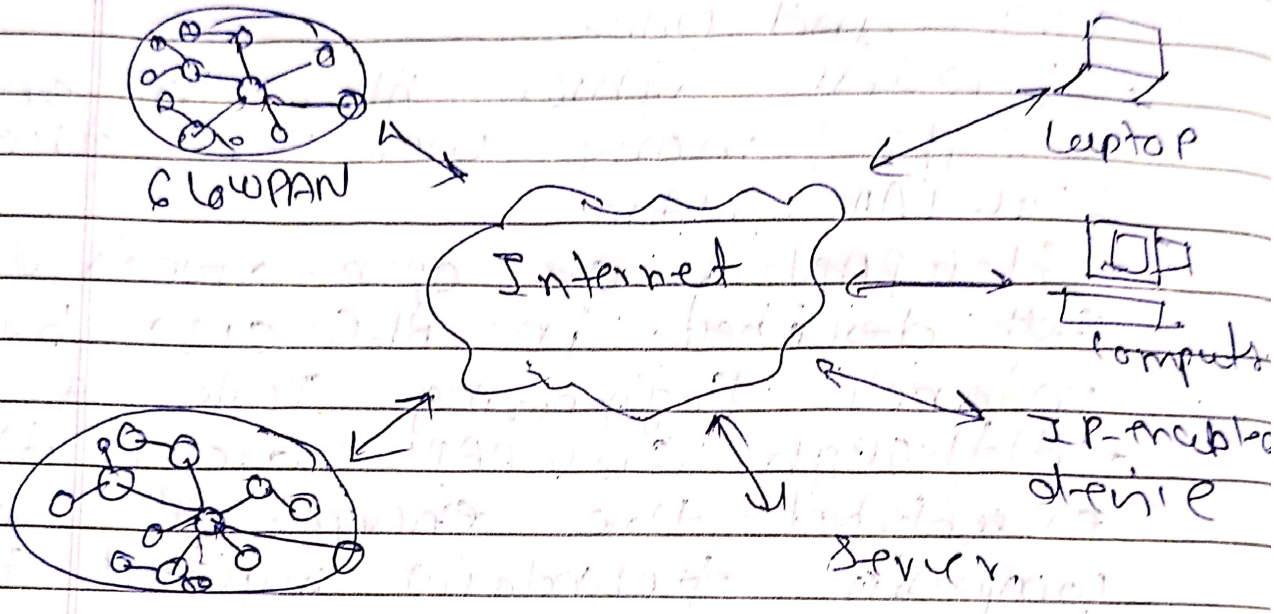

fig. Architecture of 6LoWPAN

- Appln areas for 6LoWPAN: -
  With so many low-power wireless sensor nws and other types of ad hoc wireless nws, any new wireless system or technology needs to address a specific area.

The total system is desired to provide low-data-rate, low-duty-cycle wireless internet connectivity. 6LoWPAN is utilized in a variety of appln's, including:-
General Automation, Home automation, Smart Grid, Industrial monitoring.

- Security of 6LoWPAN:-
  - The IOT, or IoT, is expected to provide hackers with a major chance to gain control of poorly secured devices & use them to help target other nlw, and devices.
  - As a result, security is a crucial concern for any standard, such as 6LoWPAN, which employs AES-128 link layer security.
  - The transport layer protocol defined in RFC 6347 can be utilized

- Characteristics of 6LoWPAN:-
  - Packet size: small
  - IEEE 64-bit extended media access control addresses or 16-bit short media access control addresses
  - The bandwidth is limited.
  - Star & mesh topologies are example of topologies.

- Low-voltage, usually battery-powered.
- Costs are relatively modest.

- Advantages of 6LoWPAN:-
  - TCP, UDP, HTTP, CoAP, MATT, and Web-sockets are among the open IP standards that it supports.
  - It provides IP addressable nodes from end to end.
  - There is no requirement for a gateway: all that is required is a router that can link the 6LoWPAN n/w to the internet.
  - Mesh routing i.e. self healing, resilient, and scalable is supported.
  - one-to-many & many-to-one routing options are available.

- Comparison of TCP/IP & 6LoWPAN protocol stack:-
  - TCP/IP & 6LoWPAN protocol stacks are compared. The necessity of an adaptn layer in the 6LoWPAN stack, according to Zeng et al. in their survey of IIoT, is primarily to fit one IP packet into one 802.15.4 MAC frame.

- Header compression, packet fragmentation, reassembling, and edge routing are all handled by the adaptn layer.
- Due to the instability of UDP, Web applns will employ HTTP over UDP and thus be more robust.
6 LoWPAN also allows things on the Internet to be addressed by their IP address.

(3) IP Based Protocols: LORA:-
- LORA is a wireless technology that provides M2M and IoT applns with long-range, low-power, and secure data transmission.
- LORA can be used to wirelessly connect sensors, gateways, mics, devices, animals, and people to the cloud.
- LoRa tech. was developed by Cycleo, a french comany that was acquired by Semtech in 2012.
- LoRa WAN is a Low power, wide Area (LPWA) networking protocol created by the LoRa Alliance that wirelessly connects battery-powered 'things' to the internet in regional, national, or global

n/ws, addressing key Internet of Things requirements such as bi-directional comm^n, end-to-end security, mobility, and localized^n servicing.

- LoRaWAN Node System Arch:-
  - The comm^n protocol and system arch. are defined by LoRaWAN, while the physical layer is defined by LoRa.
  - A typical LoRaWAN node system arch. is shown below:-

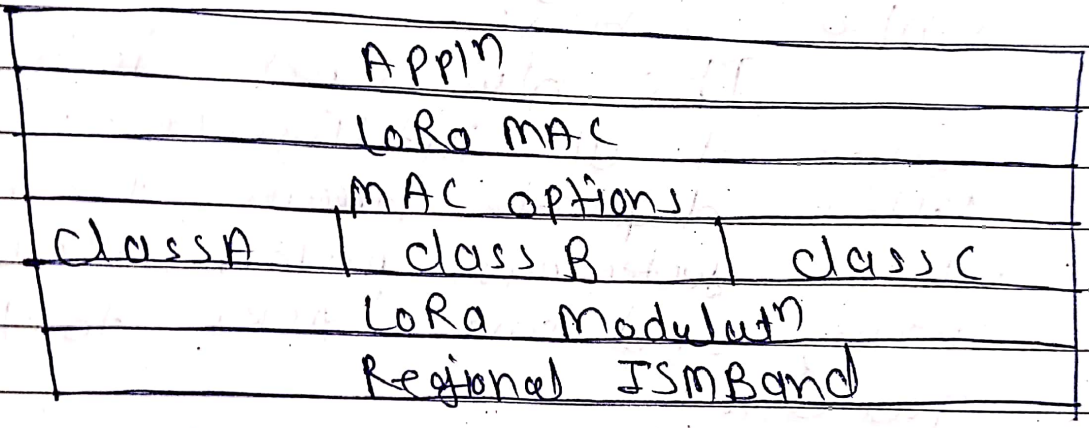

fig. LoRa N/w Arch.

- The majority of modern IoT LAN technologies employ mesh n/w architecture.
- The system can increase the comm^n range and size of the n/w by using a mesh n/w.

- LoRa N/w with several Devices
The LoRa n/w is made up of several components:
- LoRa Nodes / End Points:-
LoRa end points are sensors or applns that perform sensing and control.
- LoRa Gateways:-
Unlike cellular communication, where mobile devices are linked to serving base stations, LoRaWAN nodes are linked to a specific gateway.
- n/w Servers:-
The n/w server is the source of all intelligence. It filters duplicate packets from various gateways, performs security checks, and sends ACKs to the gateways.

- LoRa Device classification:-
- End nodes in the LoRaWAN n/w can have different device classes, similar to how end devices in other n/ws can have diff. capabilities depending on device class.
- Class A is best suited for battery power sensors:-

This device class is the most energy efficient and has the longest battery life of any device in the LoRaWAN nlw.

- End-devices in class B that have scheduled receive slots:-

At the scheduled time, open additional receive slots.

- End-device of Class C with the most receive slots:-

keep the receive window open at all times.

only when the device is transmitting is RX closed.