UNIT 3

several efforts have been taken for IoT (Internet of Things) protocol standardization to ensure interoperability, security, and efficient communication between devices and systems.

Here are some of the prominent ones:

ETSI (European Telecommunications Standards Institute): Creates various IoT-related standards and specifications.

Internet Engineering Task Force (IETF): A group of experts working together to create common internet standards, including IoT protocols.

IEEE Standards Association: The Institute of Electrical and Electronics Engineers (IEEE) develops technical standards for IoT devices, like wireless networks used in smart homes.

Consortiums and Alliances: Organizations formed to develop standards and ensure IoT devices can work together smoothly.

OneM2M: Creates technical rules for IoT devices, making them work well across different industries.

MQTT (Message Queuing Telemetry Transport): A lightweight messaging standard for IoT devices with limited power.

Thread: Thread is a low-power, wireless IoT protocol designed for home automation and smart home applications.

Bluetooth and Bluetooth Low Energy (BLE): Used for short-range wireless communication in IoT devices.

LoRaWAN (Long Range Wide Area Network): LoRaWAN is a low-power, wide-area networking protocol designed for long-range communication with IoT devices. It is managed by the LoRa Alliance.

Zigbee: Zigbee is a popular wireless communication standard for IoT devices, especially in home automation and sensor applications.

SCADA:

The SCADA protocol is a set of rules and conventions that govern communication between the SCADA system's central controller (master) and the remote Terminal Units (slaves).

Here's a simple explanation of the SCADA protocol:

SCADA Components: A typical SCADA system consists of three main components:

Master Station: The central control unit of the SCADA system, responsible for collecting and analyzing data from the field devices, as well as sending commands to control those devices.

Remote Terminal Units (RTUs) or Programmable Logic Controllers (PLCs): These are field devices deployed at remote locations and are responsible for acquiring data from sensors and actuators, as well as executing control commands sent by the master station.

Communication Network: The communication infrastructure that connects the master station with the RTUs or PLCs, enabling data exchange and command transmission.

Communication Protocols: SCADA protocols define the rules for data exchange and command transmission between the master station and field devices. Some commonly used SCADA protocols include Modbus, DNP3 (Distributed Network Protocol), and IEC 60870-5.

Standards:

International Society of Automation (ISA):

- The International Society of Automation is a non-profit professional association that focuses on standards and best practices related to automation and control systems.
- ISA-95 is a widely used standard that addresses the integration of enterprise and control systems. It provides a framework for the exchange of information between SCADA systems and business systems, promoting seamless communication and data sharing.

IEEE:

IEEE 802.15.4 is a standard for low-rate wireless personal area networks (WPANs) that was first published in 2003 by the Institute of Electrical and Electronics Engineers (IEEE).

It defines the physical Layer [PHY] and media access control (MAC) layers for short-range wireless communication in, low-data-rate applications.

This standard is specifically designed to enable the development of low-cost and low-power wireless devices for various applications, including home automation, industrial automation, healthcare monitoring, smart metering, and more.

Key features and characteristics of IEEE 802.15.4 include:

1. Low Power Consumption: The standard is optimized for energy-efficient operation, making it suitable for battery-powered devices with long battery life. This is achieved through mechanisms like duty cycling and sleep modes.

2. Low Data Rate: IEEE 802.15.4 is designed for applications that do not require high data throughput. It supports data rates ranging from 20 to 250 kilobits per second (kbps).

3. Short Range: The typical operating range is relatively short, usually within 10 to 100 meters, depending on the environmental conditions and power levels used.

4. Frequency Bands: It operates in several frequency bands, including 2.4 GHz, 868 MHz (Europe), and 915 MHz (North America), among others. The 2.4 GHz band is the most commonly used and provides worldwide license-free operation.

5. Peer-to-Peer and Star Topologies: IEEE 802.15.4 supports both peer-to-peer and star network topologies. In the peer-to-peer mode, devices can communicate directly with each other, while in the star mode, devices communicate with a central coordinator.

6. CSMA/CA-based MAC Protocol: The standard uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as its MAC protocol. This helps avoid collisions between packets transmitted by different devices.

7. Frame Format: The data frames used in IEEE 802.15.4 are relatively small, with a maximum payload size of 127 bytes. This further reduces overhead and power consumption.

8. Security: The standard includes security features to protect the communication between devices, including encryption and authentication mechanisms.

Due to its low-power and low-cost characteristics, IEEE 802.15.4 has become the foundation for other higher-layer protocols and application profiles. Notably, it serves as the basis for Zigbee, a popular communication protocol for various home and building automation applications. Additionally, it is also used in certain industrial and sensor network applications.

BACnet Protocol:

BACnet, which stands for Building Automation and Control Networks, is a widely used communication protocol specifically designed for building automation and control systems.

It is an open standard developed by the American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE) and is defined by the ANSI/ASHRAE Standard 135.

The BACnet protocol allows different building automation and control devices, such as heating, ventilation, air conditioning (HVAC) systems, lighting systems, access control systems, and more, to communicate and exchange data with each other in a standardized and interoperable manner.

The Bacnet protocol defines a set of services that facilitate communication between building devices. These services include:

i. Who-Is and I-Am used for device discovery, allowing devices to identify themselves on the network.
ii. Who-Has and I-Have: Used for object discovery, enabling devices to query and announce the presence of specific objects or properties.
iii. Read-Property and Write-Property: Services for sharing data between devices, where properties of objects can be read or modified.

Bacnet supports multiple protocols, including:
i. **ARCNET:** A local area network protocol that uses token passing for communication.
ii. **Ethernet:** A widely used networking standard that allows devices to communicate over local and wide area networks.
iii. **Bacnet/IP:** Bacnet over Internet Protocol, which allows Bacnet communication over IP networks.
iv. **Bacnet/IPv6:** Similar to Bacnet/IP, but specifically designed for IPv6 networks.
v. **Point-To-Point:** Serial communication protocol that enables direct communication between two devices.
vi. **Master-Slave/Token-Passing :** A multi-drop serial communication protocol that supports communication between multiple devices on the same network.
vii. **ZigBee:** A low-power wireless communication protocol used for short-range device-to-device communication.
viii. **Lon Talk:** A protocol used in building automation systems, similar to Bacnet that allows devices to communicate over various media types, including twisted pair, power lines, and wireless.
i. These different physical and data link layers supported by Banat provide flexibility in terms of network infrastructure and enable devices to communicate seamlessly within building automation systems.

ZigBee:

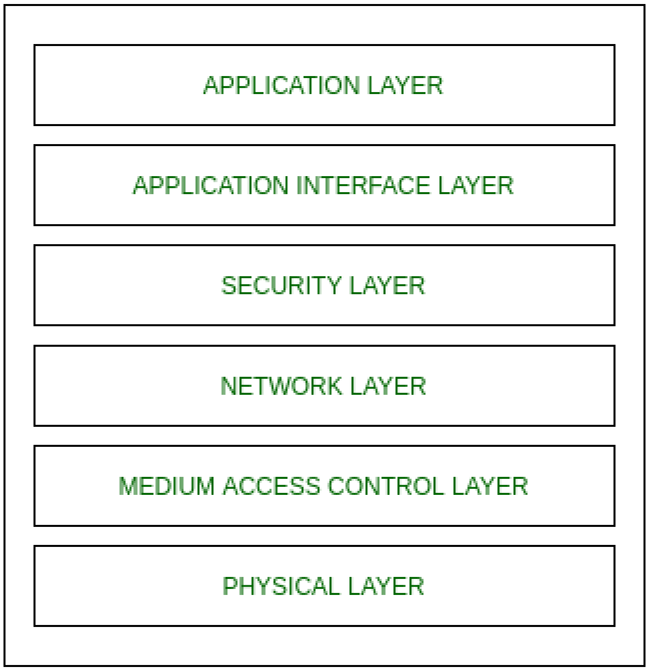
ZigBee is a low-power wireless communication protocol designed for applications that require low data rates, low power consumption, and long battery life. It operates in the 2.4 GHz frequency band and supports mesh networking, allowing devices to connect to each other and form a network.

ZigBee is commonly used in smart home automation, industrial control systems, and smart energy management. In a smart home scenario, ZigBee-enabled devices like sensors, switches, and smart appliances can communicate with a central hub or gateway. This enables remote control and monitoring of various devices and allows for automation, energy efficiency, and improved home security.

The mesh networking capability of ZigBee is particularly beneficial in scenarios where a large number of devices need to communicate over an extended range. Each device can act as a router, relaying data through the network, ensuring reliable and robust communication even if some devices fail or move out of range.

Zigbee architecture is a combination of 6 layers.

1. Application Layer
2. Application Interface Layer
3. Security Layer
4. Network Layer
5. Medium Access Control Layer
6. Physical Layer



- **Physical layer:** The lowest two layers i.e the physical and the MAC (Medium Access Control) Layer are defined by the IEEE 802.15.4 specifications. The Physical layer is closest to the hardware and directly controls and communicates with the Zigbee radio. The physical layer translates the data packets in the over-the-air bits for transmission and vice-versa during the reception.
- **Medium Access Control layer (MAC layer):** The layer is responsible for the interface between the physical and network layer. The MAC

layer is also responsible for providing PAN ID and also network discovery through beacon requests.

- **Network layer:** This layer acts as an interface between the MAC layer and the application layer. It is responsible for mesh networking.

Application layer: The application layer in the Zigbee stack is the highest protocol layer and it consists of the application support sub-layer and Zigbee device object. It contains manufacturer-defined applications.

Modbus:

Modbus is a widely used communication protocol in industrial automation and control systems. It was developed in 1979 by Modicon (now Schneider Electric)

The protocol is simple and easy to implement, making it popular in a wide range of applications, from factory automation to energy management systems.

The Modbus architecture is straightforward and consists of two main components: the Modbus Master and the Modbus Slave.

Modbus Master: The Modbus Master is the device that initiates communication on the network. It is responsible for requesting data from or sending commands to the Modbus Slaves. The Master acts as the controller or supervisor in the communication process.

Modbus Slave: The Modbus Slaves are the devices that respond to the requests from the Modbus Master. They provide the requested data or execute the commands sent by the Master. Slaves are usually sensors, actuators, or other control devices.

Request-Response Communication: In the Modbus architecture, communication between the Master and Slaves follows a request-response pattern. The Master sends a request to a specific Slave, asking for data or action, and the Slave replies with the requested information or an acknowledgment of successful execution.

Function Codes: Modbus uses function codes to specify the type of action the Master wants the Slave to perform. Each function code corresponds to a particular operation, such as reading data from a Slave or writing data to a Slave.

Addressing: Each Modbus Slave on the network has a unique address, allowing the Master to identify and communicate with specific Slaves. The address acts like a unique ID for each device.

Open Protocol: Modbus is an open and widely adopted protocol. Its openness allows different manufacturers to implement Modbus in their devices, promoting interoperability.

Industrial Applications: Modbus is commonly used in various industrial applications, such as programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, and distributed control systems (DCS).