- **IoT Protocols based on Functionality**
- **MQTT – Message Queue Telemetry Transport**

- Functionality based IoT Protocol Organization
- Introduction – MQTT
- MQTT components
- MQTT methods
- Fig - publish subscribe model of MQTT

- Communication
- MQTT Topics
- MQTT Applications
- SMQTT – Secure MQTT

Functionality-based IoT Protocol Organization

- ✓ **Connectivity** (6LowPAN, RPL)
- ✓ **Identification** (EPC, uCode, IPv6, URIs)
- ✓ **Communication / Transport** (WiFi, Bluetooth, LPWAN)
- ✓ **Discovery** (Physical Web, mDNS, DNS-SD)
- ✓ **Data Protocols** (MQTT, CoAP, AMQP, Websocket, Node)
- ✓ **Device Management** (TR-069, OMA-DM)
- ✓ **Semantic** (JSON-LD, Web Thing Model)
- ✓ **Multi-layer Frameworks** (Alljoyn, IoTivity, Weave, Homekit)

Source: Internet of Things Protocols (Online)

MQTT

Introduction

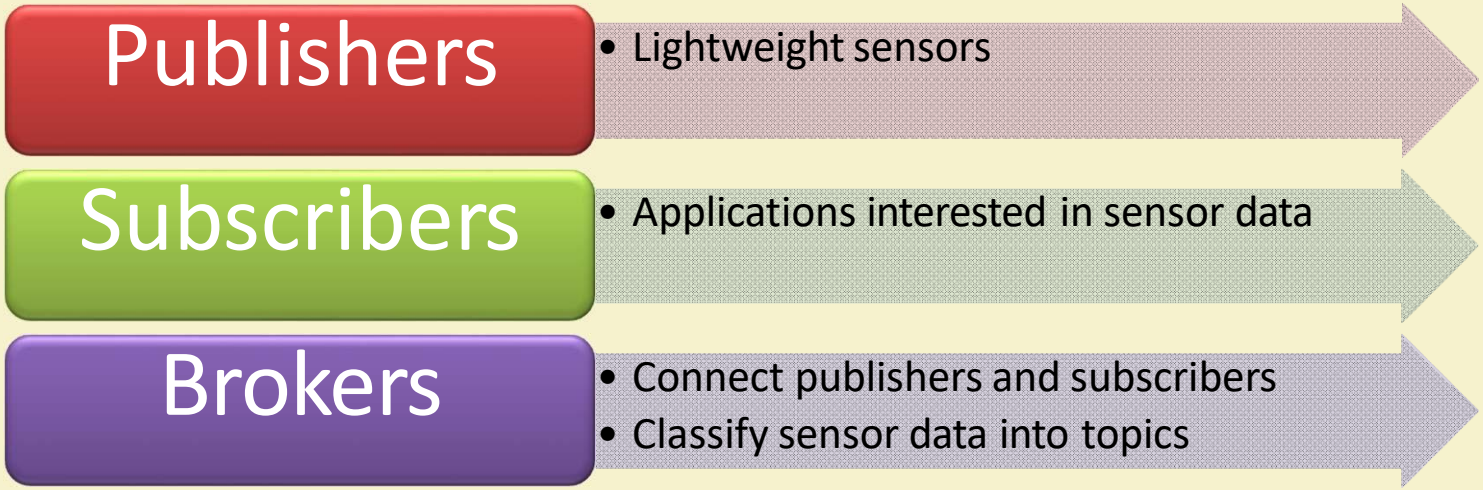
- ✓ **Message Queue Telemetry Transport.**
- ✓ ISO standard (ISO/IEC PRF 20922).
- ✓ It is a publish-subscribe-based lightweight messaging protocol for use in conjunction with the TCP/IP protocol.
- ✓ MQTT was introduced by IBM in 1999 and standardized by OASIS in 2013.
- ✓ Designed to provide connectivity (mostly embedded) between applications and middle-wares on one side and networks and communications on the other side.

Source: "MQTT", Wikipedia (Online)

- ✓ A message broker controls the publish-subscribe messaging pattern.
- ✓ A topic to which a client is subscribed is updated in the form of messages and distributed by the message broker.
- ✓ Designed for:
  - Remote connections
  - Limited bandwidth
  - Small-code footprint

Source: "MQTT", Wikipedia (Online)

MQTT Components

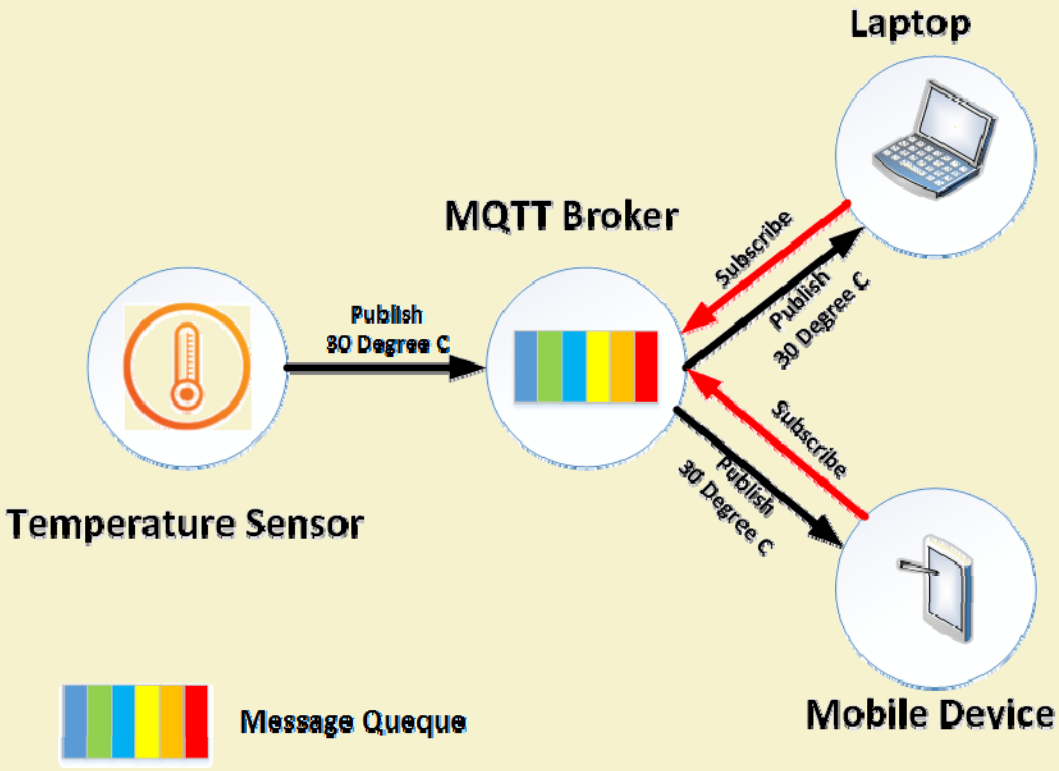


Source: "MQTT", Wikipedia (Online)

MQTT Methods

- Connect
- Disconnect
- Subscribe
- Unsubscribe
- Publish

Source: "MQTT", Wikipedia (Online)



Source: "MQTT 101 – How to Get Started with the lightweight IoT Protocol", HiveMQ (Online)

Communication

- ✓ The protocol uses a **publish/subscribe** architecture (HTTP uses a request/response paradigm).
- ✓ Publish/subscribe is **event-driven** and enables messages to be pushed to clients.
- ✓ The central **communication point is the MQTT broker**, which is in charge of dispatching all messages between the senders and the rightful receivers.
- ✓ Each client that publishes a message to the broker, includes a **topic** into the message. The **topic is the routing information for the broker.**

Source: "MQTT 101 – How to Get Started with the lightweight IoT Protocol", HiveMQ (Online)

- ✓ Each client that wants to receive messages subscribes to a certain topic and the broker delivers all messages with the matching topic to the client.
- ✓ Therefore the clients don't have to know each other. They only communicate over the topic.
- ✓ This architecture enables highly scalable solutions without dependencies between the data producers and the data consumers.

Source: "MQTT 101 – How to Get Started with the lightweight IoT Protocol", HiveMQ (Online)

MQTT Topics

- ✓ A topic is a **simple string** that can have more hierarchy levels, which are separated by a slash.
- ✓ A sample topic for sending temperature data of the living room could be *house/living-room/temperature*.
- ✓ On one hand the client (e.g. mobile device) can subscribe to the exact topic or on the other hand, it can use a **wildcard**.

Source: "MQTT 101 – How to Get Started with the lightweight IoT Protocol", HiveMQ (Online)

- ✓ The subscription to *house/+/temperature* would result in all messages sent to the previously mentioned topic *house/living-room/temperature,* as well as any topic with an arbitrary value in the place of living room, such as *house/kitchen/temperature*.
- ✓ The plus sign is a **single level wild card** and only allows arbitrary values for one hierarchy.
- ✓ If more than one level needs to be subscribed, such as, the entire sub-tree, there is also a **multilevel wildcard** (#).
- ✓ It allows to subscribe to all underlying hierarchy levels.
- ✓ For example *house/#* is subscribing to all topics beginning with *house*.

Source: "MQTT 101 – How to Get Started with the lightweight IoT Protocol", HiveMQ (Online)

Applications

- ✓ **Facebook Messenger** uses MQTT for online chat.
- ✓ **Amazon Web Services** use Amazon IoT with MQTT.
- ✓ **Microsoft Azure** IoT Hub uses MQTT as its main protocol for telemetry messages.
- ✓ The **EVRYTHNG IoT platform** uses MQTT as an M2M protocol for millions of connected products.
- ✓ **Adafruit** launched a free MQTT cloud service for IoT experimenters called Adafruit IO.

SMQTT

- ✓ **Secure MQTT** is an extension of MQTT which uses encryption based on lightweight attribute based encryption.
- ✓ The main advantage of using such encryption is the broadcast encryption feature, in which one message is encrypted and delivered to multiple other nodes, which is quite common in IoT applications.
- ✓ In general, the algorithm consists of four main stages: setup, encryption, publish and decryption.

Source: M. Singh, M. Rajan, V. Shivraj, and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)," in Fifth International Conference on Communication Systems and Network Technologies (CSNT 2015), April 2015, pp. 746-751

- ✓ In the setup phase, the subscribers and publishers register themselves to the broker and get a master secret key according to their developer's choice of key generation algorithm.
- ✓ When the data is published, it is encrypted and published by the broker which sends it to the subscribers, which is finally decrypted at the subscriber end having the same master secret key.
- ✓ The key generation and encryption algorithms are not standardized.
- ✓ SMQTT is proposed only to enhance MQTT security features.

Source: M. Singh, M. Rajan, V. Shivraj, and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)," in Fifth International Conference on Communication Systems and Network Technologies (CSNT 2015), April 2015, pp. 746-751