Tishk International University
Science Faculty
IT Department

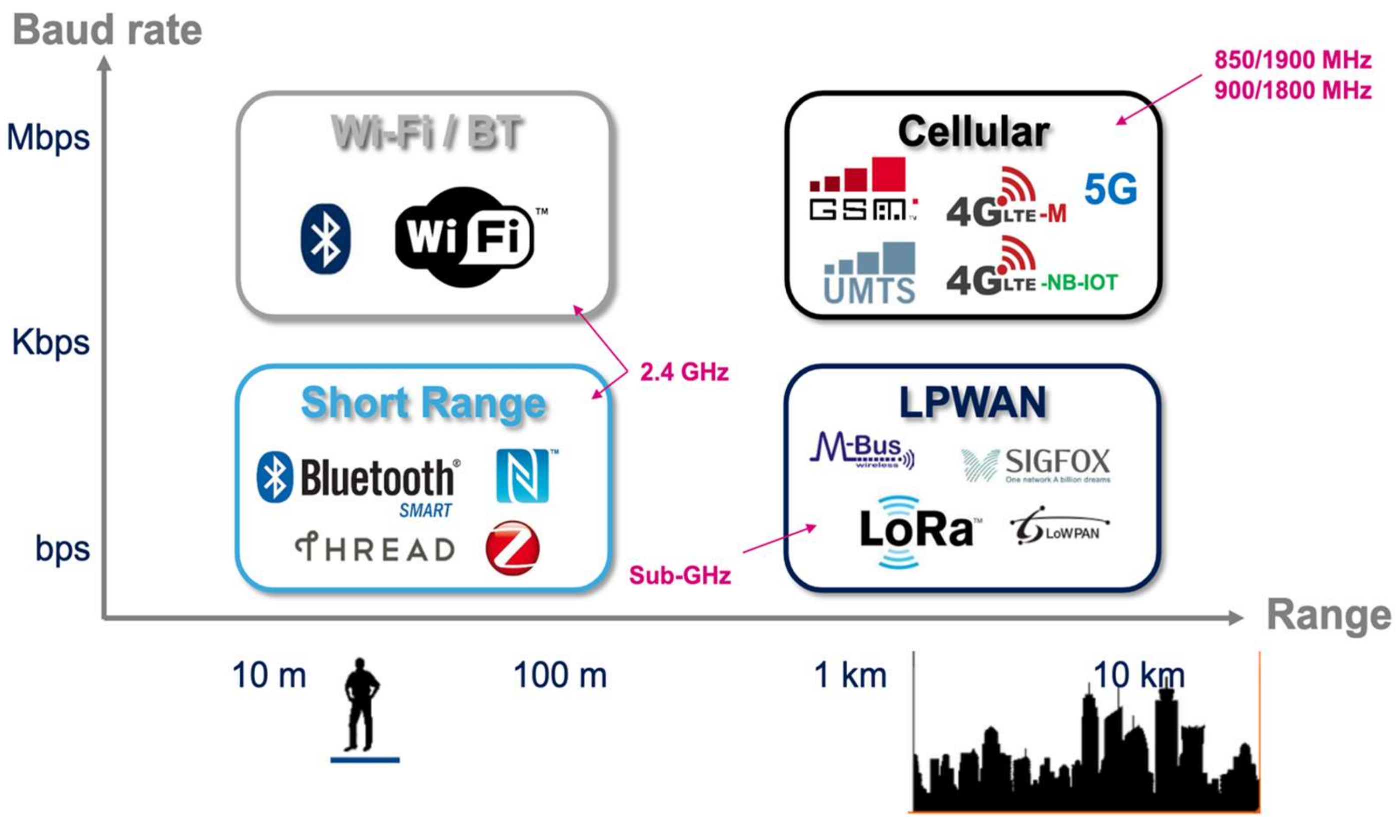
Introduction to IoT

Lecture 03: IoT Communication Protocoles

4th Grade - Spring Semester

Instructor: Alaa Ghazi

Lecture 3
IoT Communication Protocols



Lecture Topics

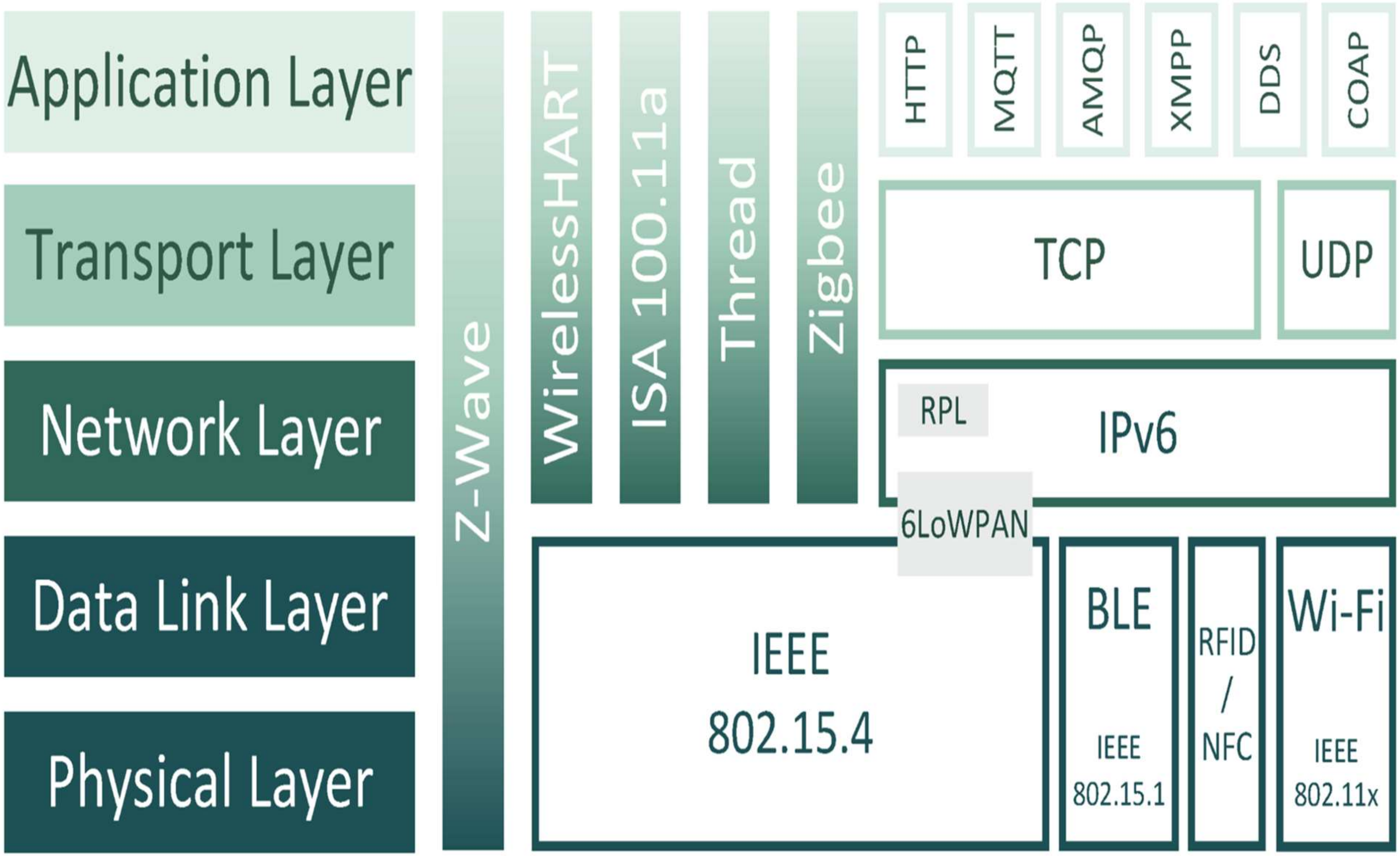
- IoT Network Stack
- Physical / Data Link Layer Protocols
  - Short Range Protocols:
  - Medium Range Protocols
  - Long Range Protocols
- Network Layer Protocols
  - Why IPv6?
  - 6LoWPAN
- Transport Layer Protocols
  - UDP vs. TCP
- Application Layer Protocol
  - HTTP - Hypertext Transport Protocol
  - CoAP - Constrained Application Protocol
  - MQTT - Message Queue Telemetry Transport
  - XMPP – eXtensible Messaging and Presence Protocol

IoT Network Stack

The IoT protocol stack can be mapped to the five layers in the OSI (Open Systems Interconnection) model, which is widely used to understand and design network architectures. Each layer in the IoT protocol stack has specific roles and protocols that ensure efficient and reliable communication between IoT devices and systems.

IoT smart devices communicate with each other's without direct human intervention, and connect through the gateway to connect to the application server in other side by using different communication protocols and technologies. The IOT stack consist of application layer protocols (HTTP, MQTT, CoAP, and XMPP), transport layer protocols (UDP or TCP), network layer protocols (RPL, IPv6 and IPv4), the Adaption layer (6LoWPAN), Data link and physical layer protocols such as (ZigBee, Bluetooth , NFC, Wi-Fi , and Z-Wave) which are used to reduce power consumption and data cost.

IoT Network Stack Diagram

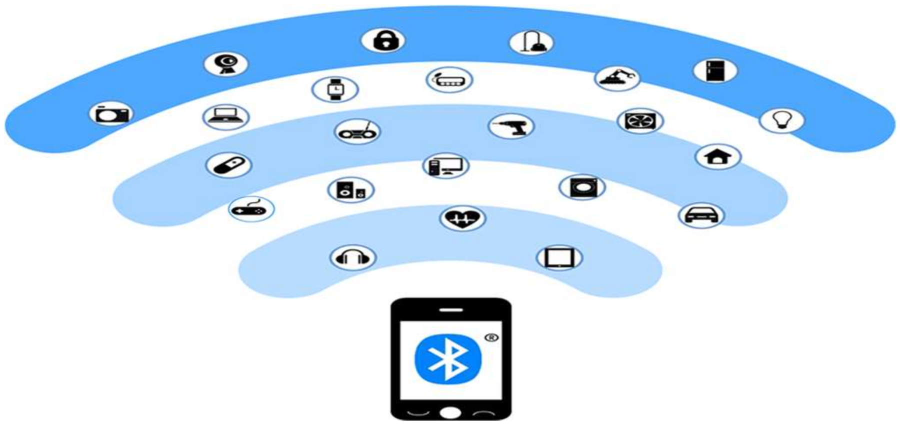


Physical / Data Link Layer Protocols

- Short Range Protocols:
- Medium Range Protocols
- Long Range Protocols

Short Range Protocols

- <u>Bluetooth -IEEE 802.15.1</u>: is used in Personal Area Network (PAN)
- Based on IEEE 802.15.1 standard
- theoretical transfer rate goes up to 3 Mbps
- Short range up to 20 m in an open field
- 2.4GHz unlicensed radio band
- Pairing mechanism Associate & authenticate
- Master initiates, slave accepts
- Multiple devices connected to the same master
- 48-bit address



Medium Range Protocols

- Wi-Fi Protocol – IEEE 802.11 a/b/g/n (covered in Wireless Networking Course)
- IEEE 802.15.4 (Zigbee):
- Z-wave

IEEE 802.15.4

- Standard for low power IoT networks - Physical & data link layers
- Base for ZigBee, Thread, WirelessHART
- compared to Wi-Fi, it boasts extremely low power consumption
- a very low bitrate up to 250 Kbit/s, enough for IoT applications with a small range, usually between 10 to 20 m.
- It uses different frequency bands: (868 MHz, 915 MHz, and 2.4 GHz).
- Multiple topologies (star, mesh)
- 64-bit or 16-bit MAC addresses
- Small frame size – 127 bytes including MAC, 102 bytes payload

Z-wave

- Z-wave – ITU-T G.9959: is based on a network that uses low-energy radio waves to establish a connection between one device and another in the home, allowing wireless control of **home appliances** such as lights, security systems, thermostats, windows, locks, and doors. It is based on FSK. And operates in sub-1GHz frequency band with data rate up to 100kbps.

Z-wave-Layers

- <u>Radio Layer</u>: Defines the way a signal is exchanged between network and the physical radio hardware. This includes frequency, encoding, hardware access, etc.
- <u>Network Layer</u>: Defines how control data is exchanged between two devices or nodes. This includes addressing, network organization, routing, etc.
- <u>Application Layer</u>: Defines which messages need to be handled by specific applications in order to accomplish particular tasks such as switching a light or changing the temperature of a heating device.
- Z-Wave has two basic types of device:
  - **Controllers** - devices that control other Z-Wave devices
  - **Slaves** - devices that are controlled by other Z-Wave devices.

Long Range Protocols

- Long Range communication protocols are often used to create **Low Power Wide Area Networks** (LPWANs) There are many protocols which can be summarized as below:
- LTE/5G: (covered in Wireless Networking Course)
- LoRaWAN Protocol: is based on LoRa modulation (PHY Layer) and Medium Access Control (MAC) layer is an open network architecture regulated by the LoRa Alliance. with an operating range that goes from hundreds of meters up to 10 km.
- Sigfox Protocol: is designed to support IoT deployments over long ranges, e.g. in excess of 20 km between a client device and a base station.

Comparison between LoRaWAN and SigFox

	Comparison	SigFox	LoRaWAN
01	Modulation	It follows Binary phase-shift keying modulation.	LoRaWAN follows Chirp spread spectrum modulation.
02	Bandwidth	100Hz.	250KHz and 125KHz.
03	Maximum data rate	up to 100bps .	maximum data rate is 50Kbps.
04	Functionality	limited bidirectional/Half-duplex	fully bidirectional/ Half-Duplex
05	Maximum messages/day	Uplink=140, Downlink =4.	Unlimited.
07	Range	10 km in urban area, 40 km in rural area.	5 km in urban, 20 km in rural area

Network Layer Protocols

IPv4	IPv6	6LoWPAN
32-bit address Exhausted in 2011	128-bit address Future Internet Addressing Protocol	Adaptation layer • Header compression • Fragmentation

IPv6 over IEEE 802.15.4

IPv6 can be very **useful** for IoT due to below features:

- It can address large number of IoT nodes
- Stateless
- No NAT is necessary
- Location aware addressing
- Efficient routing capabilities,
- Built-in security features, and
- Ability to support auto-configuration

On the other side the **challenges** for using IPv6 over 802.15.4

- IPv6 packet (1280 bytes) is 10 times larger than 802.15.4 frame (127 bytes)
- IoT nodes are low power devices
- IoT networks are with limited bandwidth

6LowPAN

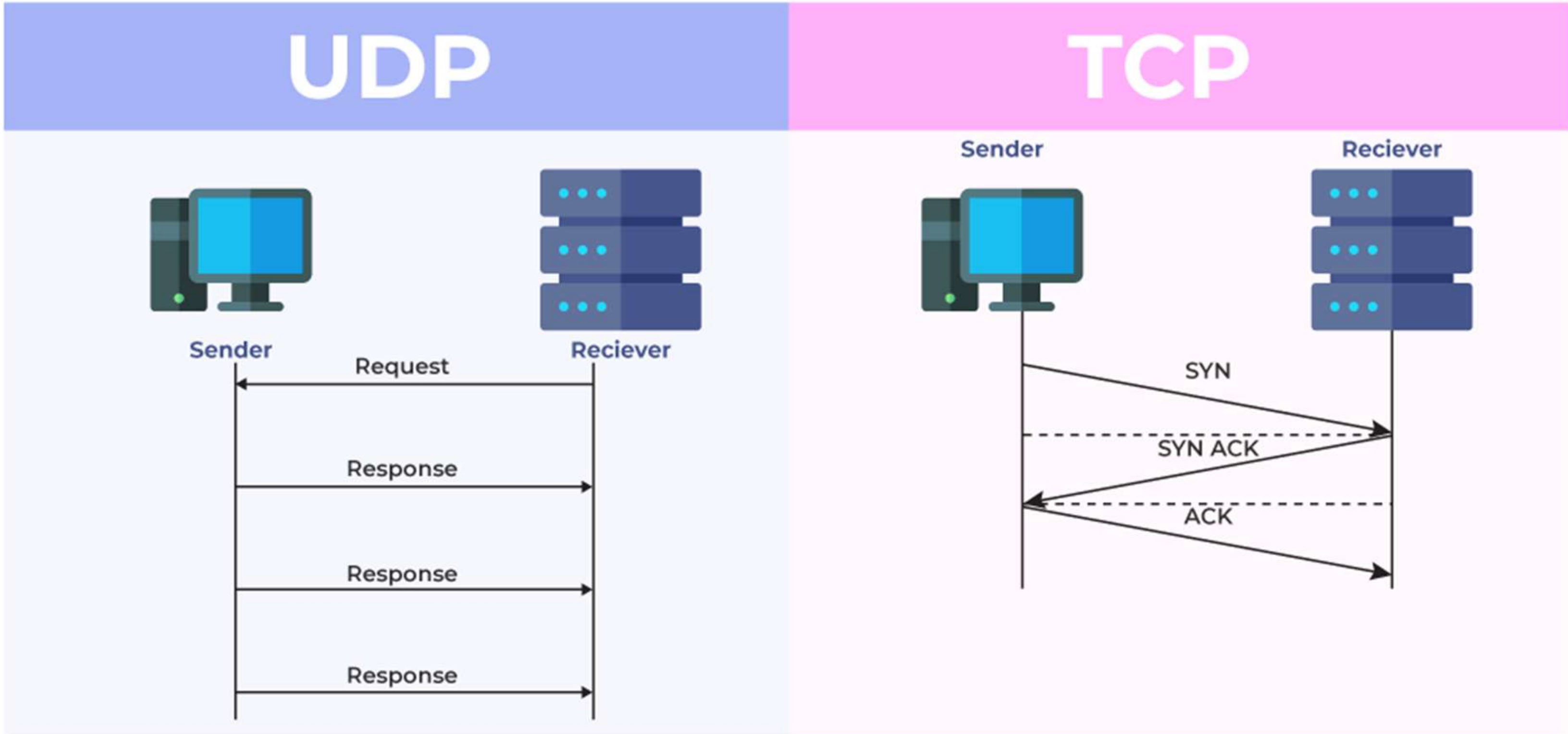
It is a n adaptation layer for IPv 6 which allows for the smallest devices with limited processing ability to transmit information wirelessly using an Internet protocol IPv6.

- Main Features:
  - 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.

Transport Layer Protocols

TCP	UDP
• Error Control, Flow Control and Congestion Control • Every packet needs an acknowledgement • Reliable Protocol	• No Acknowledgement is needed • Stateless Protocol • Simple to implement • Usually Multimedia Data is sent over UDP • IoT-friendly

UDP vs. TCP



UDP
TCP
Sender
Reciever
Request
Response
Response
Response
Sender
Reciever
SYN
SYN ACK
ACK

Application Layer Protocols

CoAP – Constrained Application Protocol

MQTT – Message Queue Telemetry Transport

XMPP – eXtensible Messaging and Presence Protocol

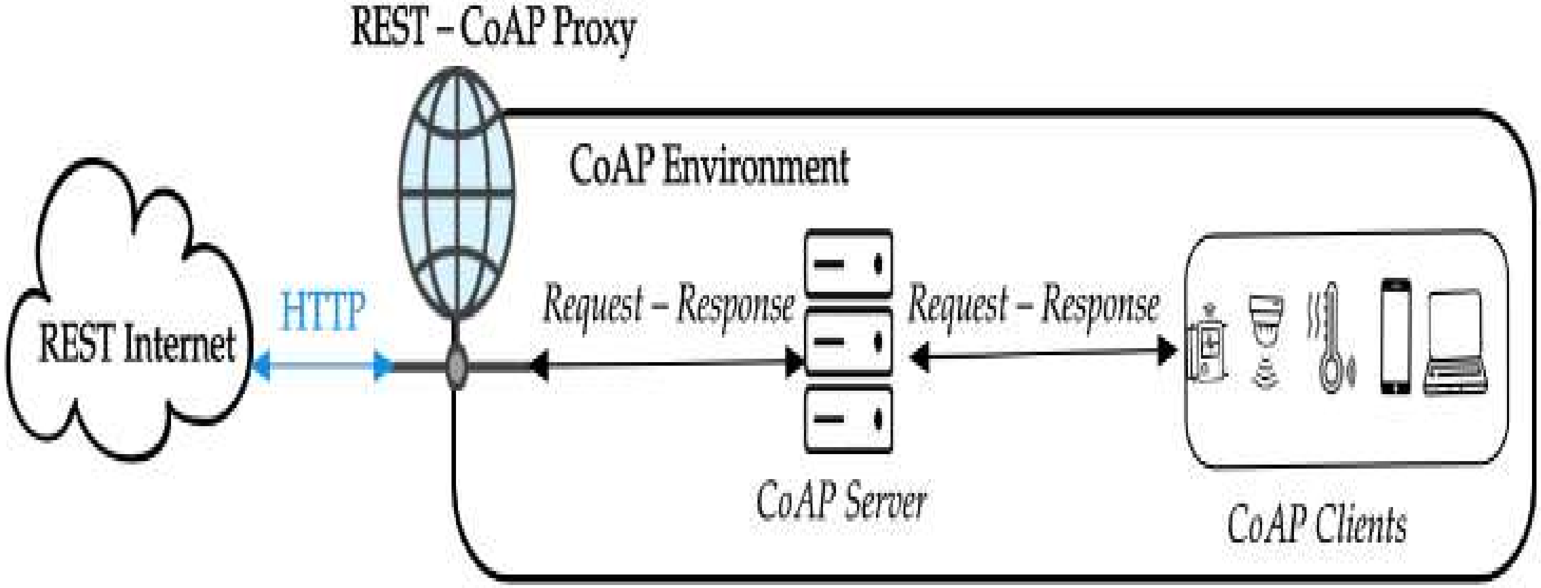
CoAP - Constrained Application Protocol

CoAP is a web transfer protocol for use with constrained nodes and networks.

- It is designed for Machine to Machine (M2M) applications
- It is based on Request-Response model between end-points
- It is a Client-Server interaction over UDP
- CoAP is designed to enable low-power sensors to use Representational State Transfer (REST) while meeting their power constraints
- CoAP architecture is divided into two main sub-layers:
  - ❖ <u>Messaging</u>: is responsible for reliability and duplication of messages
  - ❖ <u>Request/response:</u> is responsible for communication.

- CoAP server - IoT node
- CoAP client - app, browser

CoAP Architecture



MQTT - Message Queue Telemetry Transport

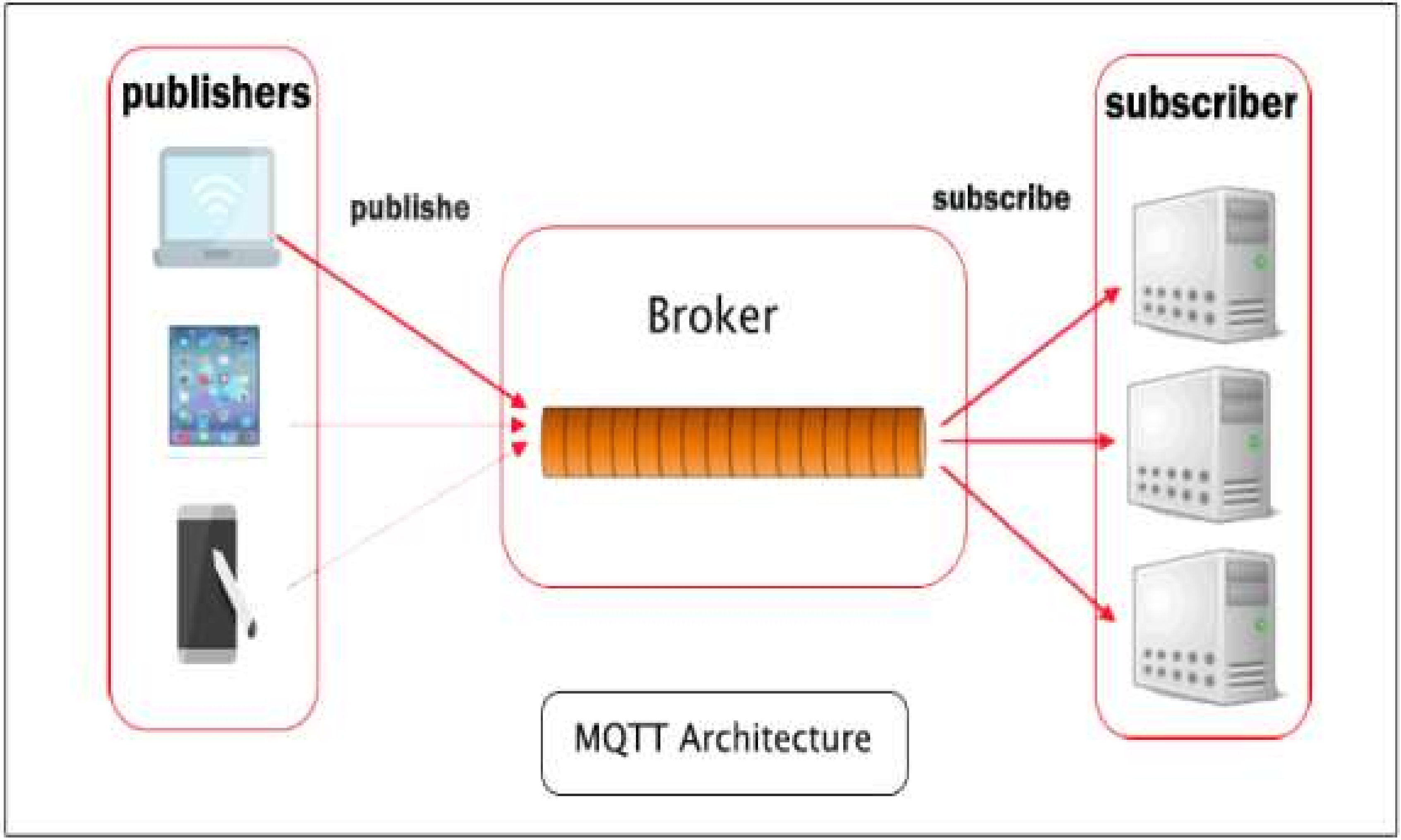
It is a publish-subscribe-based lightweight messaging protocol for use in conjunction with the TCP/IP protocol. It is designed to provide connectivity (mostly embedded) between applications and middle-ware

Publisher-subscriber model

- Nodes publish data to the MQTT broker
- Clients subscribe to the broker to receive data

- A topic to which a client is subscribed is updated in the form of messages and distributed by the message broker.
- It works mainly over TCP
- It has QoS levels
- Flexible, scalable, and designed for remote connections with limited bandwidth.

MQTT Architecture



XMPP – eXtensible Messaging and Presence Protocol

It is a Real-time communication protocol for message-oriented middleware based on XML (Extensible Markup Language).

It has the following features:

- Designed for instant messaging
- Client-server and server-server architecture
- Streaming of XML data between network elements
- Transmission of audio, video, and messaging.