Technology and component Analysis

IoT Development

Internet Of Things tools analysis and comparison

Intern Sebastian Arrazate Martinez

IoT Development
Points to consider

Building a general architecture for the Internet of Things (IoT) is a very complex task, exacerbated by the extremely large variety of devices, link layer technologies, and services that may be involved in such a system.

IoT Protocols

IoT protocols are an integral part of the IoT technology stack. This is because IoT protocols enable hardware to exchange data.

IoT Platforms

An IoT platform manages connectivity of the devices and allows developers to build new mobile software applications.

Libraries

Librarians are also leading the way on educating patrons about what IoT entails—its inner workings, uses, limits, and implications for our communities and society

Intern Sebastian Arrazate Martinez

Intern Sebastian Arrazate Martinez

IoT Protocols

Category: IoT Data Protocols

IoT Data Protocols

IoT data protocols are used to connect low-power IoT devices. They provide communication with hardware on the user side – without the need for any internet connection.

The connectivity in IoT data protocols and standards is through a wired or cellular network. Some examples of IoT data protocols are:

MQTT (Message Queuing Telemetry Transport)

It features a publisher-subscriber messaging model and allows for simple data flow between different devices.

CoAP (Constrained Application Protocol)

It's designed to address the needs of HTTP-based IoT systems.

AMQP (Advanced Message Queuing Protocol)

With its level of security and reliability, it's most employed in settings that require server-based analytical environments, such as the banking industry..

WebSocket

It can be applied to an IoT network where data is communicated continuously across multiple devices.

DDS (Data Distribution Service)

standard that aims to enable dependable, high-performance, interoperable, real-time, scalable data exchanges using a publish–subscribe pattern.

Comparative between MQTT and CoAP

Most used Protocols

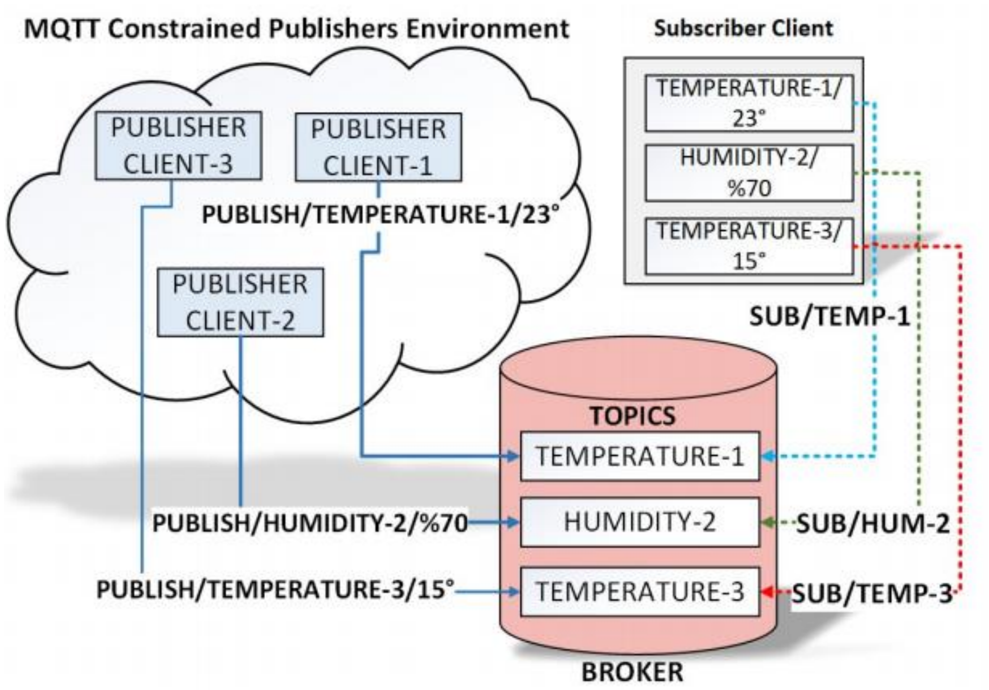
One way for wireless sensor networks to transfer data from a gateway to clients is the “publish-subscribe” architecture.

One of the major advantages of this architecture is the decoupling of the clients needing data and the clients sending data, i.e., sensor nodes need not know the identities of clients that are interested in their data and conversely, clients need not know the identities of sensor nodes generating the sensor data.

The “publish-subscribe” architecture is supported by machine to machine (M2M) protocols such as MQTT and CoAP.

Comparative between MQTT and CoAP

Most used Protocols



MQTT

MQTT is a lightweight M2M communication protocol for constrained devices and unreliable networks. It has publisher/subscriber client which runs over TCP/IP. Also, TCP provides message reliability and bidirectional connections between nodes.

Advantages

- Provides reliability of messages by supporting QoS levels.
- Effectively utilizes bandwidth through packet agnostic. The data may contain binary or text.
- Publish/Subscribe mechanism has capabilities such as one-to-one, many-to-many or one-to-none. Also, this mechanism provides bi-directional communication.
- Utilizes simple methods for communication.
- The communications among nodes are asynchronous. Messages can publish/subscribe anytime.

Disadvantages

- It uses TCP/IP and TCP requires more communication capabilities unlike UDP.
- Broker has limited capacity for communication.
- All nodes are connected to Broker. Therefore, the communication collapses when the broker is a failure.

Comparative between MQTT and CoAP

Most used Protocols

CoAP

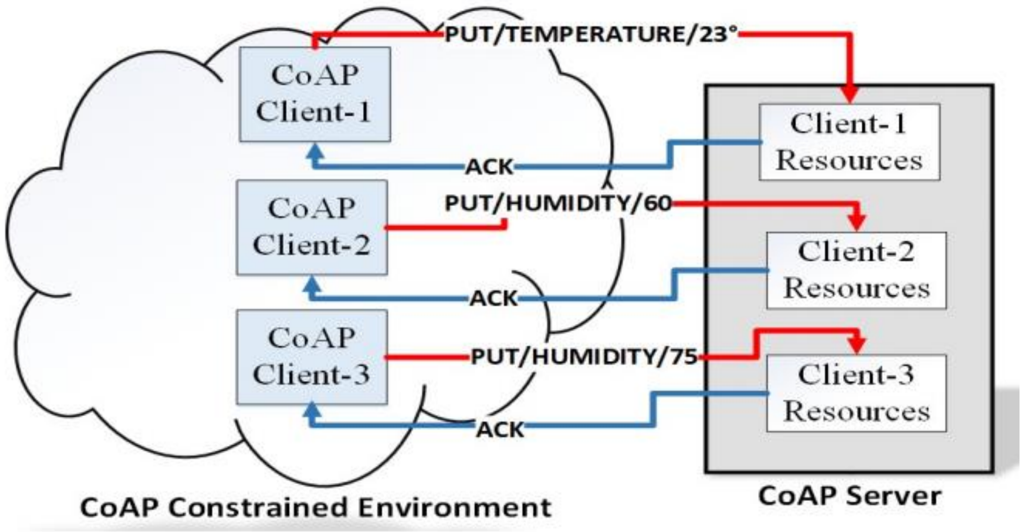
The communication between Server and Client is peer-to-peer. However, Server or Client can response unicast and multicast requests. The CoAP has four different message types to request resources from server: GET, PUT, POST and DELETE.

Advantages

- Operates fast communication by sending small packets with UDP layer.
- Asynchronous communication is provided.
- Peer-to-peer communication doesn't need to the intermediate server between clients. Also, many-to many communication is supported.
- Datagram Transport Layer Security (DTLS) provides integrity, security, and privacy by authorizing encrypting and securing.
- Good option for constrained devices.

Disadvantages

- Messages are unreliable. Therefore, ACK (acknowledgement) packets are sent to confirm the message arrives. However, it does not show clearly whether these messages are decoded correctly or completely.
- It is still standardizing. It is selected the most unstandardized protocol among other protocols.



Comparative Chart

MQTT and CoAP

Major differences between MQTT and CoAP

	CoAP	MQTT
Communication kind	Request-response model	Publish-subscribe model
Protocol type	P2P/one-to-one communication protocol	Publish-subscribe model
Messaging mode	Asynchronous and Synchronous	Only Asynchronous
Transport layer protocol	UDP	TCP/IP
RESTful-based	✓	✗
Message labeling	✓	✗

Intern Sebastian Arrazate Martinez

	MQTT	CoAP
Application Layer	Single Layered completely	Single Layered with 2 conceptual sub layers (Messages Layer and Request Response Layer)
Transport Layer	Runs on TCP	Runs on UDP
Reliability Mechanism	3 Quality of Service levels	Confirmable messages, Non-confirmable messages, Acknowledgements and retransmissions
Supported Architectures	Publish-Subscribe	Request-Response, Resource observe/Publish-Subscribe

Layer **Differences**

Major differences between MQTT and CoAP

IoT Protocols

Category: IoT Network Protocols

IoT Network Protocols

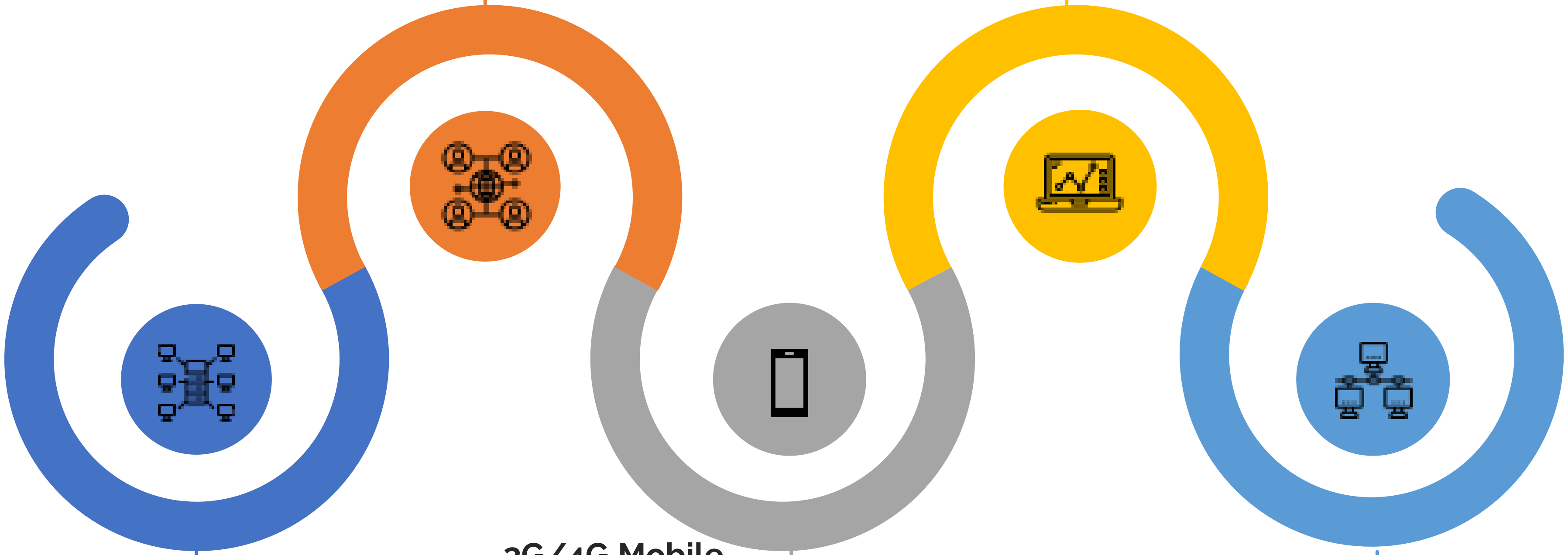
IoT network protocols are used to connect devices over a network. These sets of protocols are typically used over the internet. Here are some examples of various IoT network protocols.

Wi-Fi

Wi-Fi provides an internet connection to nearby devices within a specific range

Bluetooth

Tends to frequency hop and has a generally shorter range. It's gained a huge user base due to its integration into modern mobile devices



ZigBee

It's a relatively simple packet data exchange protocol and is often implemented in devices with small requirements, such as microcontrollers and sensors.

3G/4G Mobile Communication

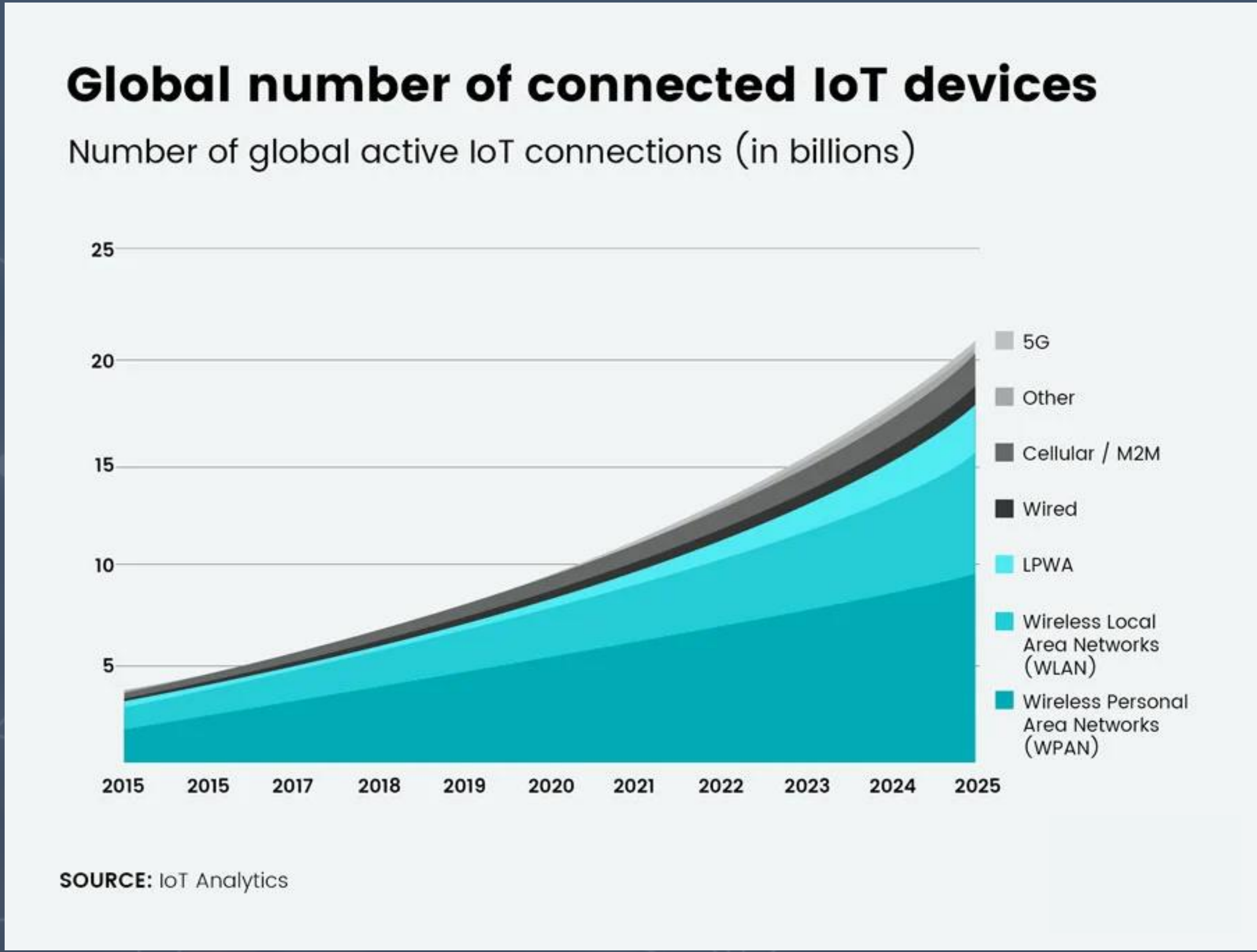
These are different generations of mobile communication standards .IoT devices on these standards can communicate over the cellular networks..

LoRaWan

Is a media access control (MAC) IoT protocol. Allows low-powered devices to communicate directly with internet-connected applications over a long-range wireless connection.

Comparative

Wi-Fi, Bluetooth and Mobile



Wi-Fi

In order to use **Wi-Fi** on an IoT device, you just need a microchip, which is easy and cheap to obtain. However, in practice you also need firmware to manage the device's Wi-Fi credentials, since Wi-Fi is a very large attack vector for malicious actors.

Generally, IoT devices that use Wi-Fi are large, stationary hubs, although they can be smaller devices as well. To use Wi-Fi, an IoT device needs to be close to a Wi-Fi access point (i.e., not located far afield).

Advantages and **Disadvantages**

The downside of Wi-Fi is that it can be difficult for the consumer to get it connected to their router and it has a very high-power draw. Wi-Fi is a great technology choice for standalone products targeted at the home or business. It can be used for battery-powered products if power is managed appropriately.

115-230 ft

7Gbps

$4 - $5 Dollars

Intern Sebastian Arrazate Martinez

Bluetooth

In order to be compatible with **Bluetooth,** an IoT device must have a microprocessor that can handle Bluetooth, as well as a second device to pair with it. The Bluetooth protocol has two different versions commonly used by IoT devices that cannot directly communicate with each other: Bluetooth Classic and **Bluetooth Low Energy (BLE)**, which is designed for devices that need to consume low amounts of power.

There are several reasons why developers might choose to use Bluetooth instead of Wi-Fi for IoT devices. First, Bluetooth usually requires physical proximity to initiate a signal broadcast, so there is no possibility of remote attacks. Second, Bluetooth requires much less energy than Wi-Fi, so it works better for low-power IoT devices such as basic sensors.

Advantages and **Disadvantages**

If you're going to start building a Bluetooth product, you should include the latest standard Bluetooth chip which will be shipping in all smartphones soon. BLE es esencialmente Bluetooth, excepto que entra en modo de suspensión después de conectarse durante unos ms. El bajo consumo de energía significa que BLE es un mejor protocolo para IoT, excepto que todavía usa la topología de red PAN muy limitada.

Bluetooth 5: 800 ft
BLE: 200 ft

Bluetooth 5: 50Mbps
BLE: 10kB/s

Bluetooth 5: $8 Dollars
BLE: $7 Dollars

3G/4G Mobile Communication

Cellular technology is not designed for IoT, but it's already rolled out across most of the globe. For IoT devices that do not require battery power and need to be launched immediately, cellular is a good choice. For IoT products that can wait to launch, it's worth waiting to see who comes out on top in the cellular LPWAN war.

Advantages and **Disadvantages**

The first question to ask is: in which regions your devices will be used? Is there a full coverage of 2G / 3G / 4G or NB-IoT / LTE-M there?

There are several open-source options (along with telecom coverage maps) for finding out the coverage of mentioned network types in different regions.

Coverage Network, according the region	200kbps (3G) 10Mbps (4G)	Since $50 Dollars/Year

Intern Sebastian Arrazate Martinez

Intern Sebastian Arrazate Martinez

Long Range

- The operating range of LPWAN technology varies from a few kilometers in urban areas to over 15 km in rural settings.

Low Power

- Optimized for power consumption, LPWAN transceivers can run on small, inexpensive batteries for 10-15 years; reducing maintenance costs.

Low Cost

- reduce complexity in hardware design and lower device costs. Its long range combined with a star topology reduce expensive infrastructure requirements, and the use of license-free or already owned licensed bands, reduce network costs.

Low-Power Wide Area Network (LPWAN) technology, provides the low cost, low power and wide-area coverage needed for vast, granular wireless sensor networks. Geared for IoT telemetry applications where small amounts of data are transmitted periodically.

Another Option **LPWAN**

Intern Sebastian Arrazate Martinez

The LoRaWAN® specification is a Low Power, Wide Area (LPWA) networking protocol designed to wirelessly connect battery operated ‘things’ to the internet in regional, national or global networks, and targets key Internet of Things (IoT) requirements such as bi-directional communication, end-to-end security, mobility and localization services.

LoRaWAN baud rates range from 0.3 kbps to 50 kbps.

- A unique 128-bit Network Session Key shared between the end-device and network server
- A unique 128-bit Application Session Key (AppSKey) shared end-to-end at the application level

Class A – Lowest power, bi-directional end-devices	Class B – Bi-directional end-devices with deterministic downlink latency	Class C – Lowest latency, bi-directional end-devices
• The default class which must be supported by all LoRaWAN end-devices, class A communication is always initiated by the end-device and is fully asynchronous.	• Network ability to send downlink communications with a deterministic latency, but at the expense of some additional power consumption in the end-device.	• The network server can initiate a downlink transmission at any time on the assumption that the end-device receiver is open, so no latency. Class C is suitable for applications where continuous power is available.

Another Option
LoRaWAN

LoRa Wireless Communication Module
ST50H

IoT Platforms

With IoT platforms, developers can build applications specifically for IoT purposes. These platforms provide users with the ability to quickly build, test, deploy, and iterate on IoT-specific applications. IoT platforms often offer similar functionality to low or no-code development platforms, such as drag-and-drop elements and WYSIWYG editors for non-developers.

AWS IoT Core

You are billed separately for usage of Connectivity, Messaging, Device Shadow usage (device state storage), Registry usage (device metadata storage), and Rules Engine usage (message transformation and routing).

Connectivity Pricing (Ohio)

You pay $0.042 per device per year (1 connection * $0.08/1,000,000 minutes of connection * 525,600 minutes/year) for 24/7 connectivity

MQTT and HTTP messaging (Ohio)

Up to 1 billion messages: $1.00 (per million messages)
Next 4 billion messages: $0.80 (per million messages)
Over 5 billion messages: $0.70 (per million messages)

LoRaWAN Messaging (N. Virginia)

Up to 1 billion messages: $2.30 (per million messages)
Next 4 billion messages: $1.50 (per million messages)
Over 5 billion messages: $1.20 (per million messages)

Device Shadow and Registry (Ohio)

The Device Shadow stores the desired state or actual state of a device, and the Registry is used to name and manage devices.

1,25 USD
(per million operations)

Rules Engine (Ohio)

Rules triggered: $0.15 (per million rules triggered / per million actions executed)
Actions executed: $0.15 (per million rules triggered / per million actions executed)

Intern Sebastian Arrazate Martinez

Azure IoT Hub
Pricing

Basic Tier

Edition Type	*Price per IoT Hub unit (per month)*	*Total number of messages/day per IoT Hub unit*	*Message meter size*
B1	$10	400,000	4KB
B2	$50	6,000,000	4KB
B3	$500	300,000,000	4KB

Standard Tier

Edition Type	*Price per IoT Hub unit (per month)*	*Total number of messages/day per IoT Hub unit*	*Message meter size*
Free	Free	8,000	0.5 KB
S1	$25	400,000	4KB
S2	$250	6,000,000	4KB
S3	$2500	300,000,000	4KB

IoT Hub

Features

Azure

Feature	Basic	Standard
Device-to-cloud telemetry	✓	✓
Per-device identity	✓	✓
Message Routing, Event Grid Integration	✓	✓
HTTP, AMQP, MQTT Protocols	✓	✓
DPS Support	✓	✓
Monitoring and diagnostics	✓	✓
Device Streams	✗	✓
Cloud-to-device messaging	✗	✓
Device Management, Device Twin, Module Twin	✗	✓
IoT Edge	✗	✓

Google Cloud IoT Core

Monthly data volume	Price per MB	Registered devices	Minimum charge
Up to 250 MB	$0.00	Unlimited, within QPS maximums (Quotas and limits)	1024 bytes
250 MB to 250 GB	$0.0045	Unlimited, within QPS maximums (Quotas and limits)	1024 bytes
250 GB to 5 TB	$0.0020	Unlimited, within QPS maximums (Quotas and limits)	1024 bytes
5 TB and above	$0.00045	Unlimited, within QPS maximums (Quotas and limits)	1024 bytes

Data volume is based on data exchanged by devices that are connected to Cloud IoT Core. There is no charge for create, read, update, and delete operations through the device manager.

If you use Cloud IoT Core with Cloud Pub/Sub, then you will also be billed separately for consuming Cloud Pub/Sub resources.

Billable messages MQTT

- CONNECT
- PUBLISH (both cloud- and device-bound)
- PUBACK (ack of device configuration, cloud-bound)
- SUBSCRIBE
- PINGREQ

Billable messages HTTP

- Requests: total bytes in the body
- Responses: total bytes in the body

ThingsBoard

It enables device connectivity via industry standard IoT protocols - MQTT, CoAP and HTTP and supports both cloud and on-premises deployments. ThingsBoard combines scalability, fault-tolerance and performance so you will never lose your data.

All subscription plans including, SMS and email costs.

Maker
Become familiar with ThingsBoard features

- Up to 30 Devices
- Up to 30 Assets
- 10 million data points
- per month
- Community support

$10 / month

Prototype
For PoCs and MVPs

- Up to 100 Devices
- Up to 100 Assets
- 100 million data points
- per month
- Community support
- White-labeling

$149 / month

Startup
For upcoming IoT Unicorns

- Up to 500 Devices
- Up to 500 Assets
- 500 million data points
- per month
- Email support
- White-labeling

$399 / month

Enterprise

- Dedicated server instances
- Unlimited Devices and Assets
- Unlimited data points
- per month
- Custom SLA
- White-labeling

Custom

Blynk

Blynk is a software company that provides infrastructure for the internet of Things. In 2014 Blynk pioneered the no-code approach to IoT app building and gained global popularity for its mobile app editor. Today businesses of all sizes — from new startups to large enterprises — use the software platform to build and manage connected products.

Yearly Pricing

FREE
For exploring and early prototyping

- 1 device included
- 5 users
- Basic Widgets
- 1 week of historical data

$0

PLUS
For more advanced projects

- 10 devices included
- 10 users
- PRO Widgets
- 3 months of historical data
- Client management

$4.99 /month

PRO
For small businesses

- 40 devices included
- 20 users (add more if needed)
- PRO Widgets
- 12 months of historical data
- Client management
- Roles and permissions controls

$39 /month

White-label
Branded apps
+
private server

- Up to 10,000 devices
- Unlimited users
- Private server
- Branded iOS, Android and
- Branded Web Portal
- No limits on features

From
$699 /month

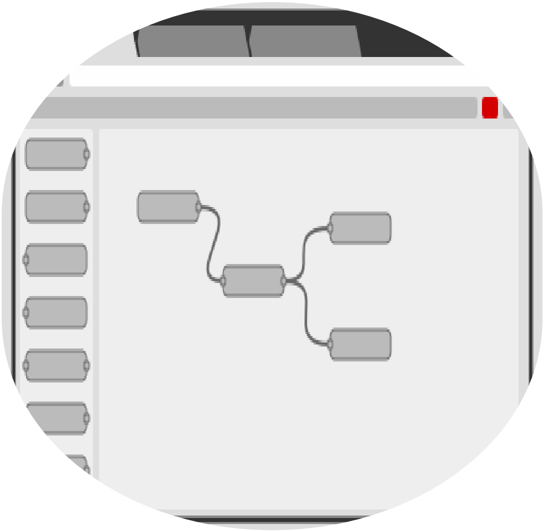
Intern Sebastian Arrazate Martinez

Node-RED

- Node-RED is a programming tool for wiring together hardware devices, APIs and online services in new and interesting ways.
- It provides a browser-based editor that makes it easy to wire together flows using the wide range of nodes in the palette that can be deployed to its runtime in a single-click.

Node-RED

Features



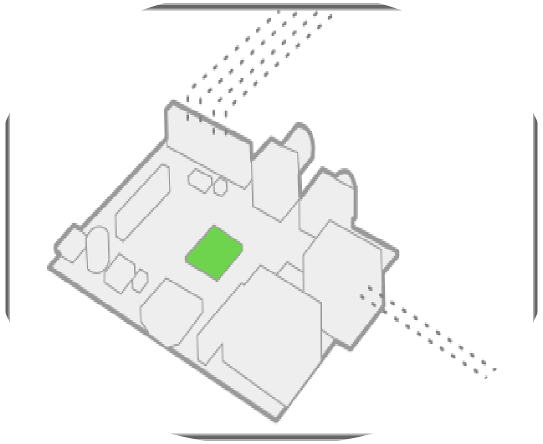
Browser-based flow editing

Node-RED provides a browser-based flow editor that makes it easy to wire together flows using the wide range of nodes in the palette.
A built-in library allows you to save useful functions, templates or flows for re-use.

Social Development

The flows created in Node-RED are stored using JSON which can be easily imported and exported for sharing with others.

An online flow library allows you to share your best flows with the world.



Built on Node.js

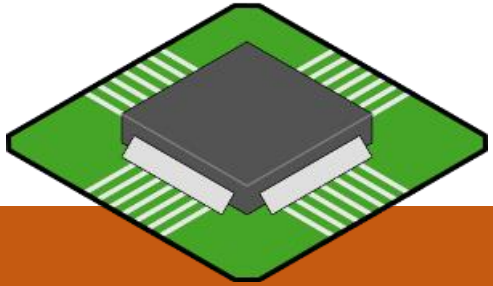
The light-weight runtime is built on Node.js, taking full advantage of its event-driven, non-blocking model. This makes it ideal to run at the edge of the network on low-cost hardware such as the Raspberry Pi, BeagleBone Black as well as in the cloud.

Get
Started Node-RED

Node-RED is built on Node.js, taking full advantage of its event-driven, non-blocking model. This makes it ideal to run at the edge of the network on low-cost hardware such as the Raspberry Pi as well as in the cloud..

Run locally

- Getting started
- Docker



Run on a device

- Raspberry Pi
- BeagleBone Black
- Interacting with Arduino
- Android

Run in the cloud

- IBM Cloud
- SenseTecnic FRED
- Amazon Web Services
- Microsoft Azure