Introduction to MQTT

IOT AND SCADA HACKERS AUSTRALIA

Housekeeping

Group Info

- Open Community
- IoT, SCADA, ICS, Automation, PLC, security
- sharing challenges, ideas, and interests
- supportive and collaborative environment
- volunteer-driven group
- experts and beginners

Presentation

Have an idea?
Present it!

Where does MQTT Fit?

Where does MQTT Fit?

- Message Queuing Telemetry Transport (without much queuing)
- Simple and Lightweight (only 5 methods)
- Publish + Subscribe Model
- Runs over TCP/IP Stack
- Multiple Transport Options (websockets, TCP,

MQTT Methods

- **Connect** - Waits for connection to be established with the server.
- **Disconnect** – Waits for the MQTT client to finish any work, which needs to be done and for the TCP/IP session to disconnect.
- **Subscribe** – Requests the server to let the client subscribe to one or more topics.
- **Unsubscribe** – Requests the server to let the client unsubscribe from one or more topics.
- **Publish** – Returns immediately to application thread after passing request to the MQTT client.

Pub/Sub Overview

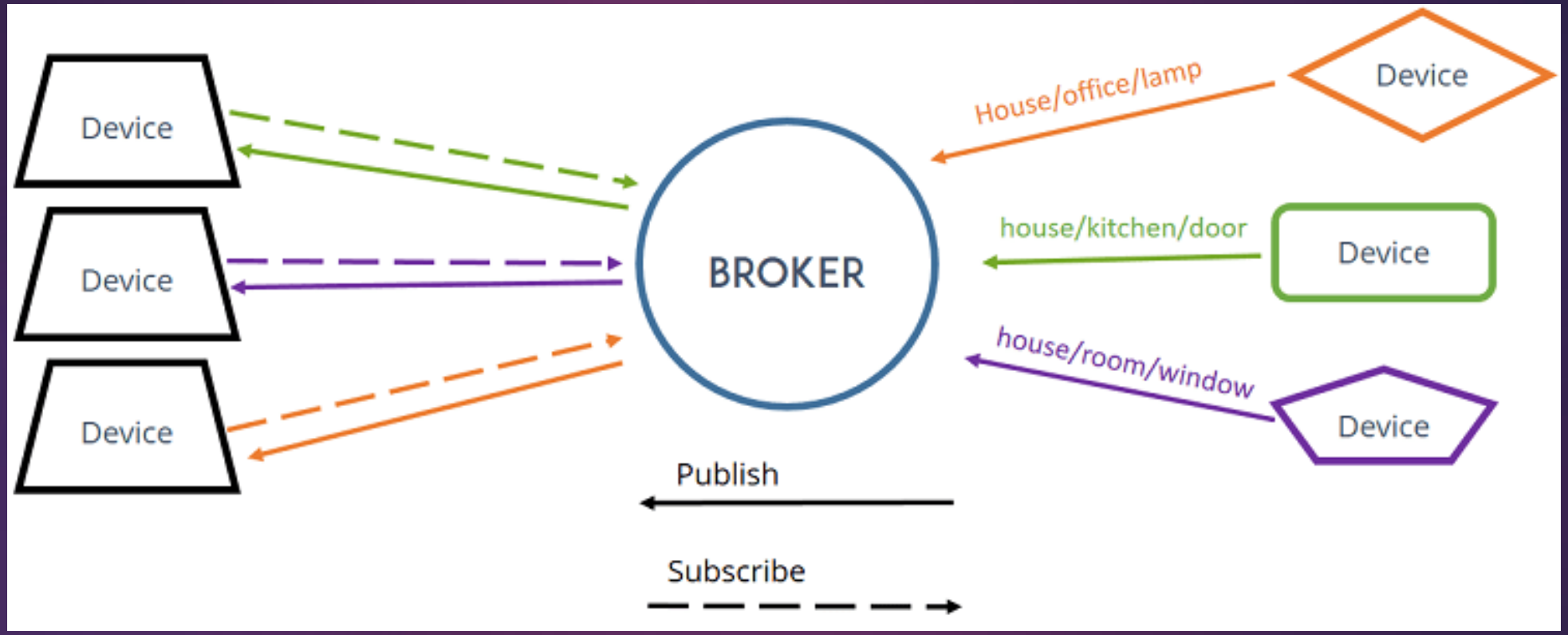


Image: https://randomnerdtutorials.com

Basic Concepts

- Publish/Subscribe
- Messages
- Topics
- Broker

Publish / Subscribe

The first concept is the publish and subscribe system.

In a publish and subscribe system, a device can publish a message on a topic, or it can be subscribed to a particular topic to receive messages

For example Device 1 publishes on a topic.

Device 2 is subscribed to the same topic as device 1 is publishing in. So, device 2 receives the message.

Courtesy: https://randomnerdtutorials.com

Messages

Messages are the information that you want to exchange between your devices. Whether it's a command or data.

For example Device 1 publishes "Door opened" on a topic "doorstatus".

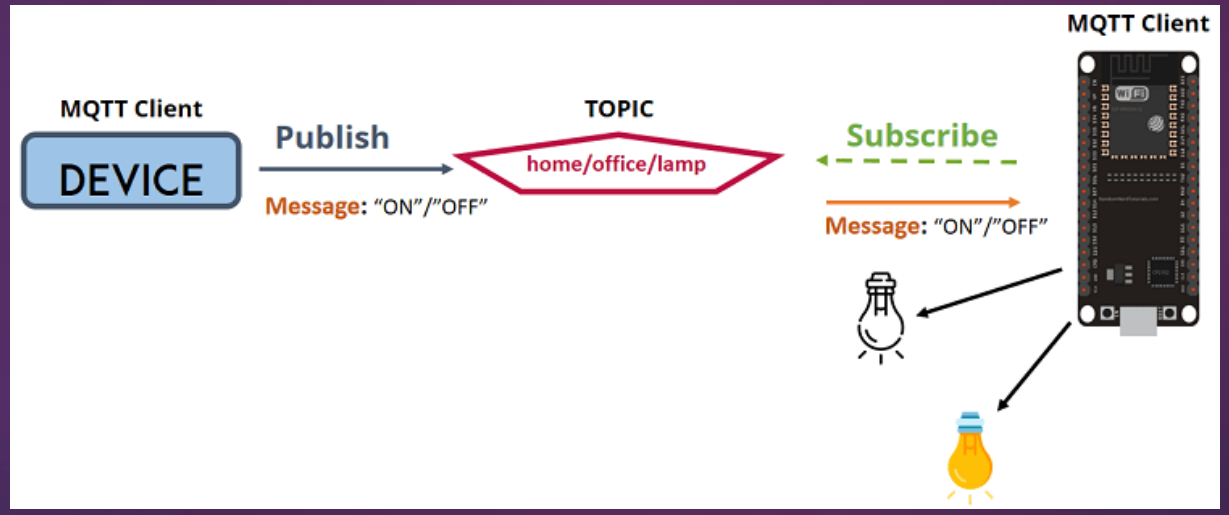
Device 2 is subscribed to the same topic as device 1 is publishing in. So, device 2 receives the message.

Courtesy: https://randomnerdtutorials.com

Topics

Topics are the way you register interest for incoming messages or how you specify where you want to publish the message.

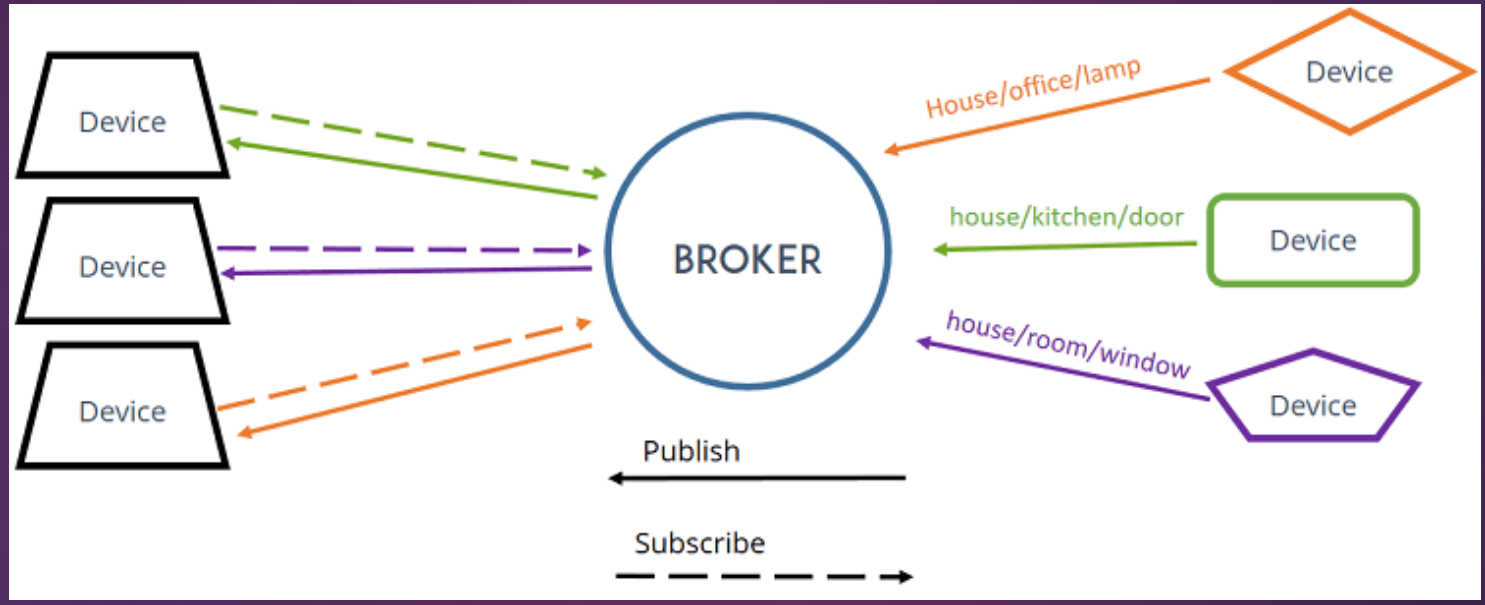
Topics are represented with strings separated by a forward slash. Each forward slash indicates a topic level. Here's an example on how you would create a topic for a lamp in your home office:



Courtesy: https://randomnerdtutorials.com

Broker

The broker is primarily responsible for receiving all messages, filtering the messages, decide who is interested in them and then publishing the message to all subscribed clients.



Courtesy: https://randomnerdtutorials.com

Pub/Sub Overview

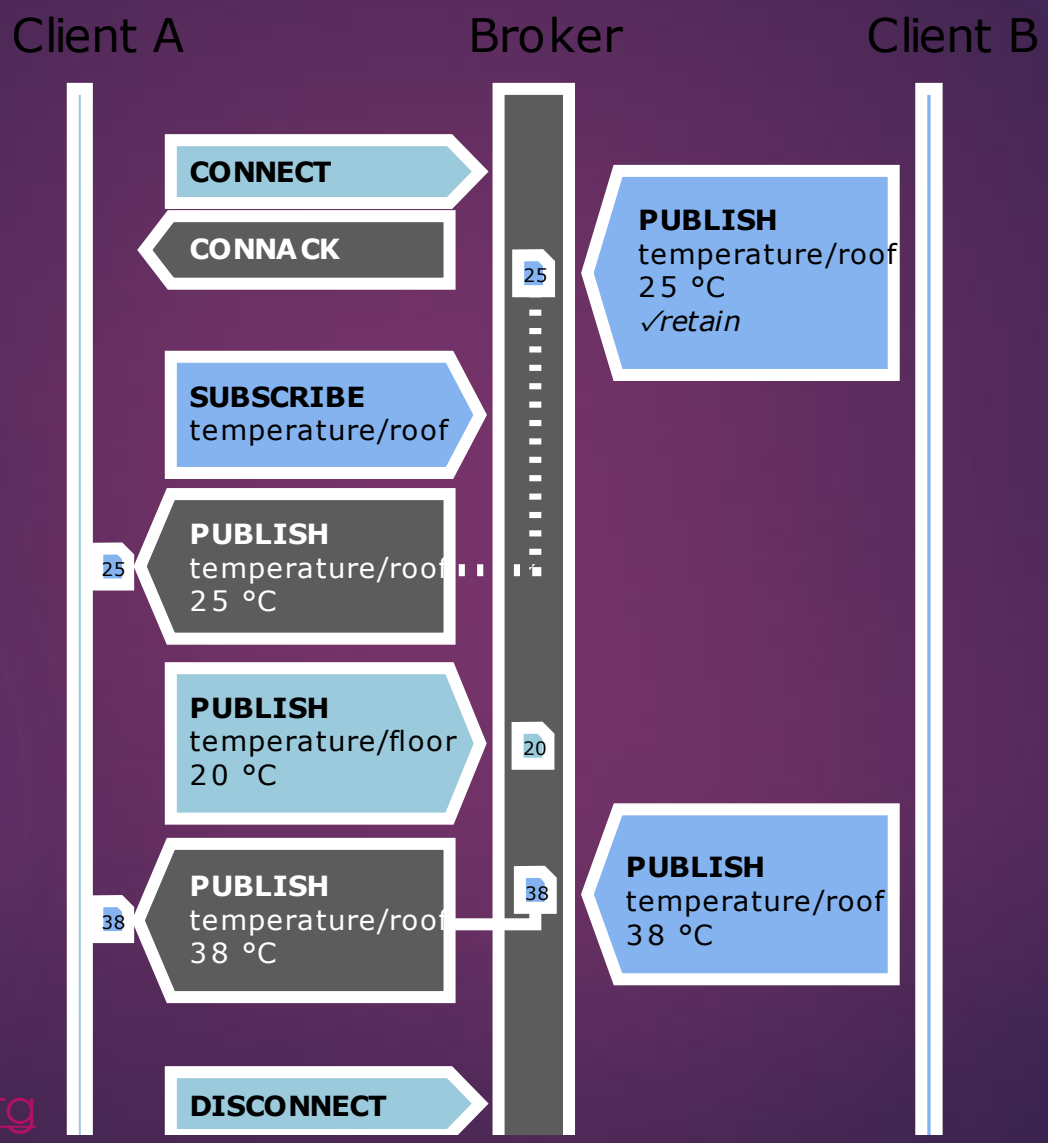


Image: https://wikipedia.org

MQTT Resources

http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html

https://randomnerdtutorials.com/what-is-mqtt-and-how-it-works/

2.2.1 MQTT Control Packet type

Position: byte 1, bits 7-4.

Represented as a 4-bit unsigned value, the values are listed in Table 2.1 - Control packet types.

Table 2.1 - Control packet types

Name	Value	Direction of flow	Description
Reserved	0	Forbidden	Reserved
CONNECT	1	Client to Server	Client request to connect to Server
CONNACK	2	Server to Client	Connect acknowledgment
PUBLISH	3	Client to Server or Server to Client	Publish message
PUBACK	4	Client to Server or Server to Client	Publish acknowledgment
PUBREC	5	Client to Server or Server to Client	Publish received (assured delivery part 1)
PUBREL	6	Client to Server or	Publish release (assured delivery part 2)

Thanks for coming!

- Twitter @IoTSCADA_AU
- Web scadahackers.com