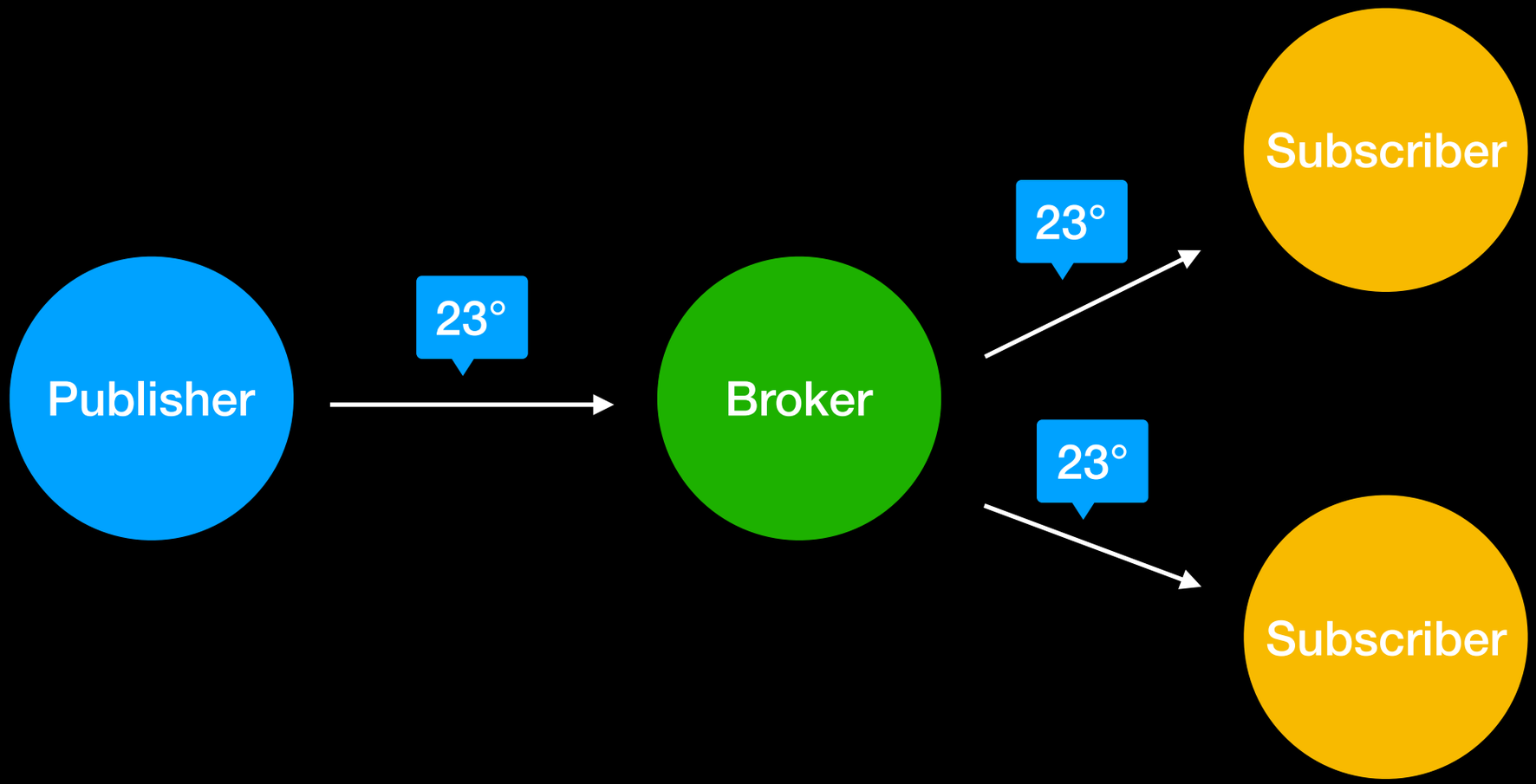
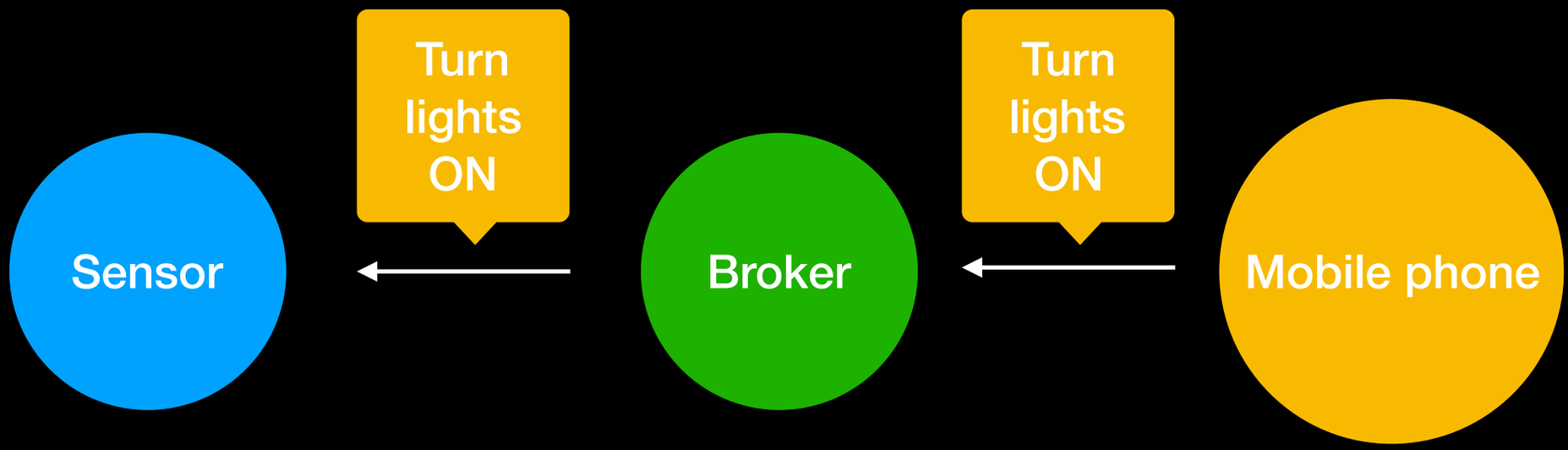
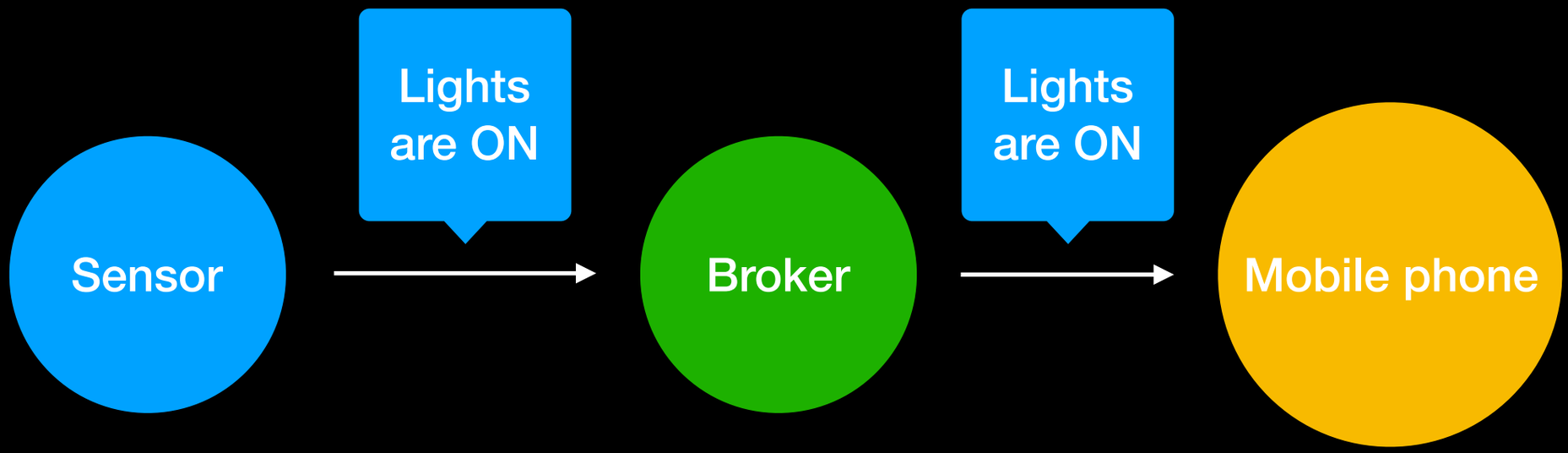
MQTT

- Message queue telemetry transport
- Pub/Sub bus protocol
- Low bandwidth


Publisher
23°
Broker
23°
Subscriber
23°
Subscriber


Turn lights ON
Turn lights ON
Sensor
Broker
Mobile phone


Sensor
Lights are ON
Broker
Lights are ON
Mobile phone

Cloud

- Cloud providers have IoT services based on MQTT
  - AWS
  - Azure
  - IBM Cloud

IoT Areas

- Consumer applications
- Industrial applications

Consumer

- Monitoring & Control
  - Electricity
  - Lights
  - Locks
  - Activity

Industrial

- Industrial
- Telematics, Health, State
- Control
- Statistics

MQTT packet content

- Topic
- Payload
- QoS

Topics

- Tree structure
- Separates interests
- Examples:
  - sensors/<device-id>/temperature
  - $aws/things/<device-id>/update
  - iot-2/type/<type-id>/id/<device-id>/evt/<event-id>/fmt/<format-id>

Wildcards

- sensors/myRaspberryPi/temperature/kitchen
- #
  - Matches many levels
- +
  - Matches one level

Subscribing

- Wildcards
  - /some/+/things
  - /+/+/things
  - /some/#
- Examples:
  - /some/old/things
  - /many/green/things
  - /some/thing/are/blue

QoS (Quality of service)

- QoS 0
    - Fire and forget
- QoS 1
    - Its delivered, but maybe many times
    - ACK, slower
- QoS 2
    - Exactly once, i’m sure.
    - Four step handshake, slowest
- Decided when you subscribe or publish to a topic

Payload

- Can be anything!
    - Verify that you understand the payload
        - Most of the time though, it is JSON!
        - But even JSON has a format..
- MQTT is NOT a message format specification..

Security

- Anyone with MQTT access is a potential threat!
- Authentication
  - User / pass
  - Certificate verification
- Encryption
  - SSL / TLS

Filtering

- Some brokers have access rights and filtering
  - Require rights to post on specific topics
  - No chance to impersonate device

Chaining