Cloud IoT Core supports two protocols for device connection and communication: MQTT and HTTP. Devices communicate with Cloud IoT Core across a "bridge" — either the MQTT bridge (https://cloud.google.com/iot/docs/how-tos/mqtt-bridge) or the HTTP bridge (https://cloud.google.com/iot/docs/how-tos/http-bridge). The MQTT/HTTP bridge is a central component of Cloud IoT Core, as shown in the components overview (/iot/docs/concepts/overview#components).

When you create a device registry, you select protocols to enable: MQTT, HTTP, or both.

- MQTT is a standard publish/subscribe protocol that is frequently used and supported by embedded devices, and is also common in machine-to-machine interactions.
- HTTP is a "connectionless" protocol: with the HTTP bridge, devices do not maintain a connection to Cloud IoT Core. Instead, they send requests and receive responses. Cloud IoT Core supports HTTP 1.1 only (not 2.0).

The following table compares how the two protocols work in Cloud IoT Core:

MQTT bridge	HTTP bridge
Device connection is maintained	Connectionless (request/response)
Full-duplex TCP connection	Half-duplex TCP connection
JWT is sent in the password field of the `CONNECT` message	JWT is sent in the `Authorization` header of the HTTP request
Telemetry events are pushed to Cloud Pub/Sub	Telemetry events are pushed to Cloud Pub/Sub
Device connection status is reported	No device connection status reported
Device configurations are propagated via subscriptions	Device configurations must be explicitly requested (via polling)
Most recent configuration (whether newer or not) is always received by devices on subscription	Devices can specify that only newer configurations should be received
Device configurations are acknowledged (ACKed) when using QoS 1	No explicit `ACK` for device configurations

MQTT bridge	HTTP bridge
Last device heartbeat time is retained	No device heartbeat data

You might also want to consider the following general features of each protocol:

MQTT	HTTP
• Lower bandwidth usage • Lower latency • Higher throughput • Supports raw binary data	• Lighter weight (easy to get started; simple curl commands) • Fewer firewall issues • Binary data must be base64-encoded, which requires more network and CPU resources

Both bridges use public key (asymmetric) device authentication and JSON Web Tokens (JWTs). For details, see the section on device security (/iot/docs/concepts/device-security).

Tip: If you're not sure which protocol is best for your use cases, start with HTTP to get familiar with Cloud IoT Core, and then switch to MQTT if needed.