

Readiness report — Zigbee2MQTT Home Automation Bridge

Checked 2026-09-03 18:30 · 8 searches, 3 pages fetched

Readiness: Zigbee2MQTT Home Automation Bridge

Verdict: Ready with caveats · 2026-09-03 · est. parts cost \$67–\$275 per station
Cybersecurity — software & network: Review before networking

Every line of this lab's bill of materials is buyable today and nothing is obsolete, discontinued or single-sourced. A host computer starts at \$35.00, a Zigbee coordinator from one of the two chip families the lab requires costs \$19.04–\$24.90 from the manufacturer's own store, a USB extension cable costs \$2.19, and a Zigbee end device costs \$10.90 — roughly \$67 to \$275 for one complete station depending on how the host is specified. Two caveats keep this off a clean "Ready". First, the coordinator product line has moved on a chip generation since this lab was written (a SONOFF "Dongle Plus MG24" now appears at retail), and although the Zigbee2MQTT supported-adapters page was fetched this run, its per-model tables render client-side and were not in the retrieved text — so which specific dongle models sit under "Recommended" today could not be confirmed from evidence, and the model must be checked against that page before an order goes in. Second, the Raspberry Pi listings are not like-for-like: the cheapest does not state its RAM size, and two of the priced entries are a desktop kit and a Compute Module rather than a plain Model B board. This is the cold check for this lab — there is no previous report, so these prices and availability establish the baseline for the next drift comparison.

Action required

Part	Problem	Recommended action
Zigbee Coordinator Radio Adapter	Model-level compatibility could not be confirmed this run — the supported-adapters page's model tables did not render in the fetched text, and SONOFF now also sells a newer MG24-based Dongle Plus	Before ordering, check the exact model against the Recommended list at zigbee2mqtt.io/guide/adapters . Both families the lab names (TI CC2652P, Silicon Labs EFR32MG21) are on sale at \$19–\$25
Host Computing Platform (Raspberry Pi 4 Model B 4GB)	Listings are not like-for-like: the \$35.00 offer does not state 4 GB, the \$165.00 offer is a desktop kit, and the \$144.00 offer is a Compute Module 4 with no USB-A host ports	Read the listing rather than sorting by price. Substitution latitude is broad — any machine running Node.js 22+ with a USB host port or Ethernet satisfies the lab

Part	Problem	Recommended action
CP2102N-A02-GQFN28 (USB-to-UART bridge)	The exact cut-tape part shows no DigiKey stock and a 31-week factory lead time	No action for this lab — the IC ships pre-soldered on the coordinator dongle. For a self-built adapter, Arrow holds 197 pcs at \$1.989 and Mouser 58 pcs at \$5.68, or use the tape-and-reel CP2102N-A02-GQFN28R (9,173 in stock, \$5.36)

Cybersecurity — software & network

Review before networking — Every one of the 302 dependencies pinned by the project's lockfile checked clean, but the bridge ships an unauthenticated web frontend bound to all interfaces plus a plaintext MQTT link, and the pinned package manager carries high-severity install-time advisories.

Component	Version	How known	Support status
zigbee2mqtt	2.14.0	read from project (version field of the fetched package.json (fetched/01-package.json, tag 2.14.0))	—
zigbee-herdsman	10.9.1	read from project (exact pin in package.json dependencies, resolved in pnpm-lock.yaml)	—
zigbee-herdsman-converters	26.103.0	read from project (exact pin in package.json dependencies, resolved in pnpm-lock.yaml)	—
zigbee2mqtt-frontend	0.9.21	read from project (exact pin in package.json dependencies, resolved in pnpm-lock.yaml)	—
zigbee2mqtt-windfront	2.15.0	read from project (exact pin in package.json dependencies, resolved in pnpm-lock.yaml)	—
Node.js runtime	22	inferred (inferred from the engines range " <code>^22.2.0 ^24 <=26.2</code> " in the fetched package.json; the project pins no single Node version, 22 is the lowest accepted line)	supported until 2027-04-30
pnpm (package manager)	10.18.3	read from project (packageManager field of the fetched package.json (pnpm@10.18.3))	—
mqtt (MQTT client library)	5.15.2	read from project (resolved version in the fetched pnpm-lock.yaml (package.json declares <code>^5.15.2</code>))	—
ws (WebSocket server library)	8.21.3	read from project (resolved version in the fetched pnpm-lock.yaml (package.json declares <code>^8.21.3</code>))	—

Component	Version	How known	Support status
ajv (config schema validation)	8.20.0	read from project (resolved version in the fetched pnpm-lock.yaml (package.json declares ^8.20.0))	—
js-yaml (configuration.yaml parser)	5.4.1	read from project (resolved version in the fetched pnpm-lock.yaml (package.json declares ^5.4.1))	—
@serialport/bindings-cpp (coordinator serial access)	13.0.1	read from project (resolved transitively and pinned in the fetched pnpm-lock.yaml; the snapshot recorded it as unpinned in the root manifest)	—
esbuild (build toolchain)	0.28.2	read from project (resolved transitively and pinned in the fetched pnpm-lock.yaml; the snapshot recorded it as unpinned in the root manifest)	—
Eclipse Mosquitto (MQTT broker)	not determined	not determined (recommended by the lab documentation; no version stated anywhere in the materials)	—
Host operating system (Linux / Windows / macOS)	not determined	not determined (the lab lets the instructor choose the host OS and states no distribution or version)	—
Coordinator firmware (TI Z-Stack or Silicon Labs EmberZNet NCP)	not determined	not determined (vendor firmware flashed to the dongle; the lab documentation states no version)	—
Koenkk/zigbee-OTA device firmware mirror	not determined	unpinned (a continuously updated Git mirror the bridge pulls device firmware from; no release is pinned)	—

Component	Finding	Severity	Fix available?
pnpm (package manager)	The package manager the project pins, pnpm 10.18.3, matched 26 advisories including six rated high, in which a tampered or hostile dependency can write files outside node_modules or run its own install scripts while the bridge is being built; the risk is on the machine doing the install, not on the running Zigbee network — GHSA-hwx4-2j3j-g496 , GHSA-w466-c33r-3gjp , GHSA-379q-355j-w6rj , GHSA-qrv3-253h-g69c (+2 more)	high	Yes — update to 10.34.5 or newer in the 10.x line (change the packageManager field in package.json before installing)

Component	Finding	Severity	Fix available?
Inter-PAN (Touchlink) commissioning	Touchlink factory reset and pairing use unsecured single-hop radio messages, so someone within range can reset or re-pair the lab's end devices without any credential	posture	Mitigation only — treat Touchlink as unauthenticated: run pairing exercises away from other Zigbee networks and re-pair devices that reset unexpectedly
MQTT broker connection	The bridge's MQTT link defaults to unencrypted TCP on port 1883, so device state and commands cross the network in clear text and any host that can reach the broker can publish commands to the lab's devices	posture	Mitigation only — use TLS on port 8883 and turn on broker authentication in Mosquitto
Zigbee network key	The documentation warns that the legacy hardcoded default network key is still accepted, and a bridge left on it lets anyone within radio range decrypt the mesh and join it	posture	Mitigation only — set <code>advanced.network_key: GENERATE</code> in <code>configuration.yaml</code> before the first start
Zigbee2MQTT onboarding and frontend web server	On first start with no <code>configuration.yaml</code> the onboarding and frontend web server binds to all network interfaces on TCP 8080 with no authentication configured, so anyone who can reach the host on that port can see and control every paired Zigbee device	posture	Mitigation only — set <code>frontend.host</code> to <code>127.0.0.1</code> or a Unix socket and set <code>auth_token</code> in <code>configuration.yaml</code> (or <code>Z2M_ONBOARD_NO_SERVER=1</code>) before the host touches a shared network

What this means for your lab

The Zigbee2MQTT software itself came back clean this run: all 302 packages the project's `pnpm` lockfile pins exactly were checked against the public vulnerability database and none had a known problem, and the Node.js line the project asks for is still supported. The real risk in this lab is how the bridge is set up rather than what it is built from. Out of the box the web interface listens on every network interface on port 8080 with no password, so anyone else on the same campus or classroom network can open it and switch the lab's lights, plugs and sensors, and read everything they report; the connection to the MQTT broker is plain text on port 1883, so that traffic can be read and commands injected by anyone who can reach it. On the radio side, the lab must set `advanced.network_key` to `GENERATE` before the first start, because the old published default key would let anyone in range decrypt and join the mesh, and Touchlink pairing is unauthenticated by design, so a nearby transmitter can reset student devices. Before students connect this to anything, put the host on an isolated lab network or restrict the frontend to `127.0.0.1`, set an `auth_token`, turn on TLS and a username and password on Mosquitto, and talk to campus IT before it goes on a shared network. Two things stay unknown: nobody stated which operating system, which Mosquitto version or which

coordinator firmware version the lab uses, so none of those could be checked and none of them should be assumed clean.

Not checked

- Host operating system (Linux / Windows / macOS): the lab states no distribution or version, so no support or advisory lookup was possible
- Eclipse Mosquitto (MQTT broker): the lab recommends it but states no version; there is no version to check
- Coordinator firmware (TI Z-Stack / Silicon Labs EmberZNet NCP): vendor firmware with no pinned version and no vulnerability database covering it
- Koenkk/zigbee-OTA device firmware mirror: a continuously updated Git mirror with no pinned release, so there is no fixed version to check

Parts

Bill of Materials

Part	Spec/Package	Status	Stock	Price	Source
Host Computing Platform (Raspberry Pi 4 Model B 4GB, Intel NUC, or any Linux PC)	Single-board computer or small-form-factor PC; 5 V DC $\geq$ 3.0 A USB-C, or 12–19 V DC adapter	readily available	not published by seller	~~\$35.00~~ – ~~\$165.00~~	Seed Studio (\$35.00, RAM size not stated), Vilros 4GB kit \$61.05, PiShop USA desktop kit \$165.00
Zigbee Coordinator Radio Adapter (SONOFF ZBDongle-P / CC2652P, or ZBDongle-E / EFR32MG21)	USB Type-A dongle, external antenna; 5 V DC VBUS, 3.3 V internal rail, 2.4 GHz IEEE 802.15.4	readily available (model compatibility unverified)	not published by seller	~~\$19.04~~ – ~~\$52.53~~	Sonoff Official Store , ZBDongle-E \$19.90 ; AliExpress ZBDongle-P \$19.04; Newegg \$52.53 outlier
USB Extension Cable	USB 2.0/3.0 Type-A male to Type-A female, 0.5–1.5 m, 5 V pass-through $\geq$ 500 mA	readily available	not published by seller	~~\$2.19~~ – ~~\$10.49~~	CableWholesale ~~\$2.23~~ , Walmart C2G \$8.99, Best Buy \$9.99
Zigbee Peripheral Device (sensor, plug or bulb)	Commercial Zigbee end device; 3.0 V CR2032/CR2450 or 100–240 V AC; channels 11–26	readily available	not published by seller	~~\$10.90~~ – ~~\$46.95~~	SONOFF door/window sensor \$10.90; Aqara T1 \$11.69 ; Tuya/MOES \$13.99

Part	Spec/Package	Status	Stock	Price	Source
CP2102N-A02-GQFN28 (USB-to-UART bridge, pre-soldered on the adapter)	28-WFQFN Exposed Pad, 28-QFN (5x5); supply 3 V ~ 3.6 V, 9.5 mA, -40 °C ~ 85 °C	Active — no DigiKey stock, 31-week factory lead; stocked elsewhere	DigiKey 0; Arrow 197; Mouser 58 (22,995 on order)	\$5.36 (Arrow \$1.989 at qty 1533; Mouser \$5.68)	DigiKey — CP2102N-A02-GQFN28 ; ECIA/TrustedParts corroboration: lifecycle risk Low, supply-chain risk Low-Med

Substitutes

For part	Substitute	Differences	Verified	Judgment
CP2102N-A02-GQFN28	CP2102N-A02-GQFN28R — Silicon Labs, Active, 9,173 in stock, \$5.36	Same manufacturer and description (IC USB TO UART BRIDGE QFN28); same Package/Case 28-WFQFN Exposed Pad and Supplier Device Package 28-QFN (5x5); same supply range 3 V ~ 3.6 V (the lab runs this rail at 3.3 V, inside the range); same 9.5 mA supply current; same -40 °C ~ 85 °C range; same \$5.36 unit price. Only difference is the trailing R, assumed to denote tape-and-reel packaging	verified: package/case and supplier device package (DigiKey parametrics, both parts), supply-voltage range 3 V ~ 3.6 V against the lab's 3.3 V logic rail (DigiKey parametrics, both parts), lifecycle status and price (DigiKey, both parts). not verified: what the R suffix encodes (assumed packaging only); pin-for-pin pinout (no datasheet fetched)	Acceptable for a self-built adapter, with the packaging assumption stated. Not needed for the lab as written, which buys the assembled dongle

Verify any substitute against its datasheet before ordering.

Other dependencies

- **Zigbee2MQTT Git source repository** (<https://github.com/Koenkk/zigbee2mqtt.git>) — reachable this run: the 2.14.0 tag's `package.json` and `pnpm-lock.yaml` were both fetched successfully.
- **Official documentation and hardware compatibility guides** (<https://www.zigbee2mqtt.io/>) — live; the adapters guide returned 2,781 characters this run. Its per-model tables render client-side and did not come through as text, which is why coordinator model compatibility is flagged above.
- **USB-to-UART VCP driver pages** (Silicon Labs, FTDI, WCH) — not fetched directly, but the fetched Zigbee2MQTT adapters page still points users to the same three vendors for VCP drivers, so the dependency remains current in the project's own documentation.
- **Mosquitto download portal** (<https://www.mosquitto.org/download/>) — not checked; no lookup was dispatched for it this run.

- **Fabrication** — none. The lab has no Gerbers, CAD, drill files or board dimensions; the system is assembled entirely from commercial off-the-shelf hardware, so there is no PCB fabrication dependency.

Watch list

- **Zigbee coordinator dongle** — the most likely thing to break by the next check. SONOFF has already introduced an MG24-based Dongle Plus, and the Zigbee2MQTT project moves models between its Recommended, Not recommended and Not maintained lists over time. Re-confirm the model against the supported-adapters page each term.
- **Raspberry Pi 4 Model B 4GB** — a superseded board with a 5x price spread across sellers and several look-alike listings (Compute Module, desktop kits). Expect this line to drift toward a Pi 5 or a generic mini-PC; the lab's own substitution latitude already permits it.
- **CP2102N-A02-GQFN28** — DigiKey's 31-week factory lead on the cut-tape part is worth re-checking only if anyone builds a custom adapter; the reel variant and two other authorized distributors currently cover it.
- **Zigbee end-device models** — individual consumer models are discontinued and replaced constantly. The lab is insulated because any device supported by zigbee-herdsman-converters works, but the specific model named in a lab handout will go stale.
- **Stock levels generally** — four of the five lines are retail, and shopping listings publish no inventory. Prices here are current; quantity on hand is unknown for every retail line.