Modbus TCP : adresse IP, port 502 et Unit ID — lire une valeur à travers le réseau

Série A — Communications · Public : Techniciens supervision, intégrateurs, techniciens terrain

Objectif. Donner les trois informations d'une lecture Modbus TCP (IP, port, Unit ID), comprendre le rôle d'une passerelle TCP ↔ RTU et vérifier une lecture en lecture seule.

Sigles

Modbus TCP	Modbus transporté sur un réseau Ethernet/IP (port TCP 502 par défaut).
Modbus RTU	Modbus sur liaison série (souvent RS485), avec adresse esclave 1 à 247.
IP	Adresse de l'appareil sur le réseau (ex. 192.168.1.50).
Port 502	Port TCP réservé par défaut au service Modbus.
Unit ID	Identifiant d'unité dans l'en-tête Modbus TCP : désigne l'appareil visé derrière une passerelle (souvent = adresse RTU).
MBAP	En-tête Modbus TCP : identifiant de transaction, protocole (0), longueur, Unit ID.
Exception 0x0B	Code d'exception Modbus : la passerelle n'a pas obtenu de réponse de l'appareil cible.

Procédure

1. **Réseau.** Vérifier que l'adresse IP de la passerelle répond (ping) depuis le poste de supervision.
2. **Port.** Port 502 (ou celui indiqué par la notice) ouvert, aucun pare-feu entre les deux.
3. **Unit ID.** Unit ID = adresse RTU de l'appareil derrière la passerelle (selon la notice de la passerelle).
4. **Registre.** Choisir un registre documenté dans la notice de l'appareil ; noter la convention (base 0 ou base 1).
5. **Lecture seule.** Lire un seul registre avec un outil de test, en lecture ; aucune écriture sur un site en exploitation.
6. **Comparer.** Comparer à l'écran de l'appareil ; si décalage, essayer le registre voisin et noter la convention.

Erreurs fréquentes

- Confondre adresse IP (la passerelle) et Unit ID (l'appareil derrière).
- Pare-feu ou routeur qui bloque le port 502.
- Registre décalé d'un cran (notice en base 1, outil en base 0) : valeur plausible mais fausse.
- Écrire dans un registre pour « tester » : interdit sur un site en exploitation.

Sécurité.

- Lecture seule par défaut ; toute écriture Modbus doit être validée et documentée.
- Ne jamais exposer le port 502 directement sur Internet : passer par un VPN ou une passerelle sécurisée.

Exercice

Correction du film : l'adresse IP (192.168.1.50) et le port (502) restent les mêmes. Seul le Unit ID change : 2 pour le compteur A, 5 pour le compteur B (Unit ID = adresse RS485 derrière la passerelle, selon la notice de la passerelle).

Quiz corrigé

1. La passerelle répond au ping, mais exception 0x0B. Cause probable ?
   Mauvaise IP · ✔ **Unit ID ne correspond à aucun appareil derrière la passerelle** · Câble Ethernet coupé
   La passerelle est joignable mais n'obtient pas de réponse de l'appareil cible.
2. Port Modbus TCP par défaut ?
   80 · ✔ **502** · 1883
   502 (80 = HTTP, 1883 = MQTT).
3. La valeur lue est plausible mais différente de l'écran du compteur. Que vérifier ?
   Le Unit ID · ✔ **La convention de numérotation des registres (base 0 / base 1)** · Le port
   Un décalage d'un cran fait lire le registre voisin.

Sources

- [MB-TCP] Modbus Organization — Modbus Messaging on TCP/IP Implementation Guide (port 502, MBAP, Unit ID) — https://modbus.org/specs.php
- [MB-AP] Modbus Organization — Modbus Application Protocol Specification (codes d'exception, 0x0B) — https://modbus.org/specs.php
- [SIM] Adresses IP, adresses RTU et valeurs du film : exemples fictifs

Restant à documenter

- Pour chaque passerelle utilisée par NRJSOLAIRE (Teltonika RUT, passerelles compteurs) : correspondance Unit ID ↔ adresse RTU d'après la notice.
- Tableaux de registres des compteurs du parc (notice constructeur, convention base 0/1).