# OTLab 04

## *Modbus/TCP Emulation and Register Access*

Prof. Dr. Luiz Fernando Freitas-Gutierres (a.k.a. substationworm)

linkedin.com/in/lffreitas-gutierres

github.com/substationworm/OTLab

luiz.gutierres@ufsm.br

## Tasks

1. After starting OTLab 04, access the `otlab-student` workstation via VNC at `10.1.0.40:5901` using the password `123456`. *Hint: If you are running OTLab 04 on a Linux system, the use of Remmina is recommended for accessing the graphical interface of the `otlab-student` workstation. However, if you are on Windows and using WSL, the graphical interface may be accessed through `localhost:5901`, provided that WSL is running in WSL2 mode and no firewall restrictions are in place.*

2. Within the graphical interface of the `otlab-student` workstation accessed via VNC, add a Modbus slave in ModbusPal, a Java-based Modbus simulator: `Add slave: 1`, `Slave name: Slave`.

3. Edit the newly created Modbus slave by adding five holding registers with addresses `1` through `5`, assigning the corresponding values `10`, `20`, `30`, `40`, and `50`, respectively.

4. After completing these configurations, click `Run` in ModbusPal and open a terminal on the `otlab-student` workstation (`./OTLab04.sh -run`).

5. Verify the IP address of the `otlab-student` workstation.

6. Determine the subnet range of the network where the `otlab-student` workstation is deployed.

7. Discover the IP address, MAC address, and vendor information of the `otlab-student` workstation.

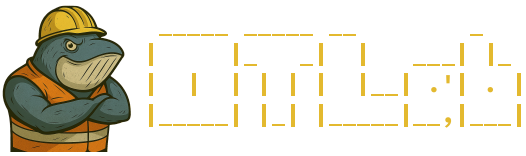
8. Use favalex/modbus-cli to read the holding registers of the slave configured in ModbusPal. *Hint: `modbus -s <Slave_ID> <IP_Address> 0 1 2 3 4` (where addresses `0` through `4` correspond to the first five registers).*

## Tools

These are the tools available on the `otlab-student` workstation for completing OTLab 04: `ifconfig`, `masscan`, `netdiscover`, `nmap`, and `modbus`.

## Nomenclature

- ID: Identifier.



- IP: Internet protocol.
- MAC: Media access control.
- TCP: Transmission control protocol.
- UDP: User datagram protocol.
- VNC: Virtual network computing.
- WSL: Windows subsystem for Linux.