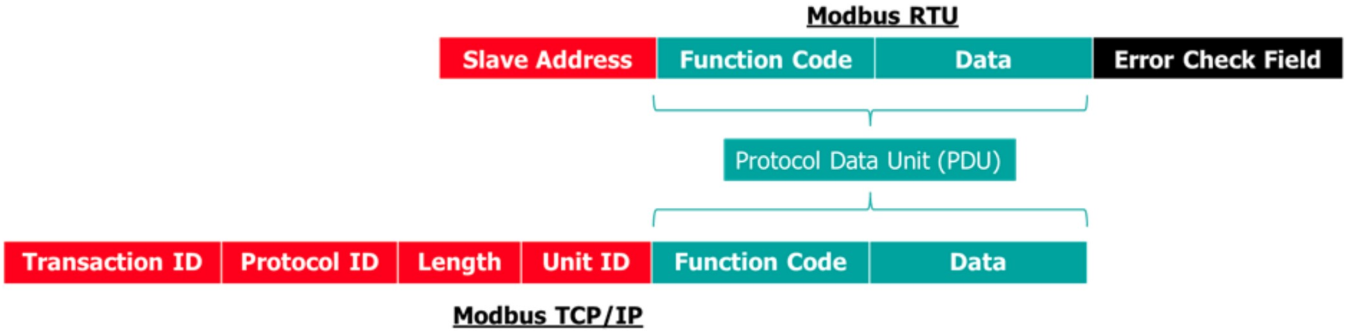
Modbus Data Structure

Data structure is the language in a device communication network. Imagine that you are an english native trying to communicate with someone speaking spanish. You both will lost in translation and the communication will be ineffective (or you can hire translator, but that is a different case). That is why we need to talk in the same language to make the communication effective.

The Data Structure

Modbus commonly comes in RTU or TCP/IP. Despite the differences in their wiring and devices, the core structure is same which called Protocol Data Unit (PDU). Check out the diagram below:



modbus RTU & TCP/IP data structure

The explanation is served on the table below:

Name	Description
Slave Address	Contains Slave Device Address that will be executed or the data origin
Function Code	Contains type of command that will be sent or received
Data	Contains information that will be sent or received
Error Check Field	Used to hold data for error checking process

Name	Description
Transaction ID	Contains the ID of the data packet itself
Protocol ID	Contains port informations of the modbus network
Length	Contains information about the length of the modbus data
Unit ID	Contains the slave device address that will be executed or the origin adress slave device of the data

We can see the differences between the RTU and TCP/IP. The RTU have header data to identified the slave ID that will be executed where the TCP/IP have their slave ID encapsulated with TCP/IP standard protocol (click here to find out more). furthermore, the TCP/IP has its own algorithm to detect error which is why it doesn't have error checking field in their structure like the RTU does.

Modbus Object Types

This section will focus on the structure of the PDU. Check out the table below:

Type of Object	Access to Data		Size	Address	Type of Data
	Master	Slave			
Coil	Read/Write	Read/Write	1 bit	00000 - 09999	Boolean
Discrete Input	Read Only	Read/Write	1 bit	10000 - 19999	Boolean
Input Register	Read Only	Read/Write	16 bit	30000 - 39999	Unsigned Word
Holding Register	Read/Write	Read/Write	16 bit	40000 - 49999	Unsigned Word

Modbus data (PDU) consist of types of data that reserved for some specific function, In theory. But in the practice many brands do not follow that law anymore. It is crucial to read the device manual to ensure you have the right address. In my experiences, some device may offset their modbus address by 1 or -1. you should check with your prefered modbus tools to perform the diagnostic.

Every 1 address in modbus can hold 16 bit of data. If you need to use 32 bit data such as Float, some devices support them by taking 2 address. Doing the address mapping can save your time to make sure that no address overlapped.

References

Modicon Modbus protocol reference guide, Modbus.org, 1st August 2021.

Internet protocol suite, wikipedia.com, 31st October 2021.

Written by Luthfi Arfiansyah on 14 July 2021