



TOP Server Addressing

Modbus Addressing Support

Software Toolbox
International Corporate
Headquarters, USA

148A East Charles Street
Matthews, NC 28105 USA
www.softwaretoolbox.com

TOLL FREE: 888-665-3678
GLOBAL: 704-849-2773
FAX: 704-849-6388



Table of Contents

INTRODUCTION	3
TYPES OF MODBUS ADDRESSES	4
OFFSET ADDRESSING: IS THERE A DIFFERENCE BETWEEN 4001 AND 400001	5
WHAT TYPE OF MODBUS ADDRESS DO YOU NEED?	7
CONTACT US	8



Introduction

The intent of this paper is to explain the nature of addressing tags using the Modbus protocol with respect to addressing tags in the TOP Server for any Modbus device. Given the large number of Modbus protocol implementations in the world, device documentation can sometimes be unclear about what numerical address should be requested for a particular piece of data.

With the tendency towards non-standard explanations of how to address Modbus, the goal of this document is to provide a standard explanation for looking at Modbus addressing to make it easier to understand how to access data in your Modbus devices.

This document assumes that you have some familiarity with the Modbus protocol and that you have some reference resource for how the data in your particular device is mapped to Modbus addresses.



Types of Modbus Addresses

When we discuss the Modbus protocol and how to address particular locations of data, there are generally four different types of Modbus addresses:

1. **Holding Registers** – 16-bit addresses with read/write access (4xxxxx)
2. **Internal Registers** – 16-bit addresses with read only access (3xxxxx)
3. **Input Coils** – 1-bit (Boolean) addresses with read only access (1xxxxx)
4. **Output Coils** – 1-bit (Boolean) addresses with read/write access (0xxxxx)

Since some device documentation does not provide a detailed listing of Modbus addresses containing the type of address such as 4xxxxx or Holding Register, it is useful to think of Modbus addresses in terms of the type of data a particular address will contain and whether or not it can be read from and written to or only read from.



Offset Addressing: Is There a Difference between 4001 and 400001

The Modbus protocol has been around for decades and is arguably the most widely used protocol for device communications in the world. That being said, with the birth of the Modbus protocol occurring when memory sizes were still modest, the total amount of memory on a device was small compared to the large quantities of memory available today.

One of the most common questions asked when considering if the TOP Server Modbus Suite is compatible with a device is whether a particular address range is supported by TOP Server. The listed address ranges supported by TOP Server are as follows:

- **Holding Registers – 400001- 465536**
- **Internal Registers – 300001- 365536**
- **Input Coils – 100001- 165536**
- **Output Coils – 000001- 065536**

For many devices, the supported address ranges are much smaller than this. With holding registers, for example, in a device like this, an address of 4001 comes nowhere close to 400001 as a starting address. So how can TOP Server claim to have such wide support for Modbus devices given this data?

Modbus Holding Register Addressing			
Modbus Document Says:		TOP Server Says It Supports:	
4	001	4	00001

The TOP Server Modbus Suite does, in fact, support 4001 and even 400001. TOP Server effectively supports all Modbus addresses because Modbus uses a type of addressing referred to as offset addressing. Notice how, in the figure above, we have separated the starting number from the rest of the address. This is done to illustrate how an offset address works.

The address, "4001", in the figure contains two pieces of information that we are interested in:

1. What type of address should be requested from the device, represented by the starting number "4".
(Holding Register = 4)
2. Which address offset should be requested from the device, represented by the rest of the number "001". (Offset = 1)

Given this knowledge, let's apply the same principle to the starting Holding Register address supported by TOP Server, "400001".

1. Our starting number is "4", as before, meaning we are requesting a Holding Register.
2. The remaining number, with the "4" removed, is "00001", which is numerically the same as "001", and represents the same Offset of "1".

What this means is that, if your documentation or address reference for your Modbus device uses a "smaller" range of numbers for its supported addressing, it is still supported by TOP Server. Just use the address suggested by your device reference. TOP Server automatically accounts for the "extra" zeroes in the middle.

This same principle is true for all of the different Modbus address types (Internal Register=3, Input Coil=1, Output Coil=0).

The reason this is true is because Modbus requests do not contain "400001" or "4001" when sent to the Modbus device when making a request. Only the address offset is sent as part of the command along with a function code that specifies a read or write operation and the type of Modbus address (Holding Register, etc.)



What Type of Modbus Address Do You Need?

That being said, the easiest way to determine what address to use in the TOP Server is to determine what kind of address you are trying to access in the device:

1. Your documentation specifies that a particular piece of data will be analog (non-boolean/binary/discrete) and you will have read and write access to this data:
 - You need to access a **Holding Register**.
 - You would add a "4" at the beginning of any address offset that the documentation specifies.
2. Your documentation specifies that a piece of data will be analog and you will only have read access to this data:
 - You need to access an **Internal Register**.
 - You would add a "3" at the beginning of any address offset that the documentation specifies.
3. Your documentation specifies a Boolean/binary/discrete value and you will have read only access to this address:
 - You would need to access an **Input Coil**.
 - You would add a "1" at the beginning of any address offset that the documentation specifies.
4. Your documentation specifies a Boolean/binary/discrete value and you will have read and write access to this address:
 - You would need to access an **Output Coil**.
 - You would add a "0" at the beginning of any address offset that the documentation specifies.



Contact Us

If you have any questions, or seek further information and help:

- **Online Support:** <http://support.softwaretoolbox.com/>
- **Documentation:** <http://docs.softwaretoolbox.com/>
- **E-Mail Support:** support@softwaretoolbox.com
- **Phone Support:** +1 (704) 849-2773
- **Fax:** +1 (704) 849-6388
- **Mailing Address:** Software Toolbox, Inc. – 148A East Charles Street, Matthews, NC 28105 USA

