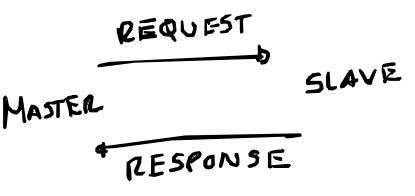
MODBUS

- Client - Server data communications protocol in the application layer

- Uses serial communication lines as a transport layer

- Used often to connect a plant / system supervisory computer with a remote terminal unit (RTU) and data acquisition (SCADA) systems



- Packet format used over Serial to allow the use of TCP/IP and UDP networks

- Data is stored in one of four data banks:
  - coils
  - discrete inputs
  - holding registers
  - input registers

  These define the type and access rights of the entwined data

Modbus Data Model Blocks

Memory	Data Type	Master	Slave
Coils	BOOL	R / W	R / W
Discrete Inputs	BOOL	R	R / W
Holding Register	Unsigned word	R / W	R / W
Input Register	Unsigned word	R	R / W

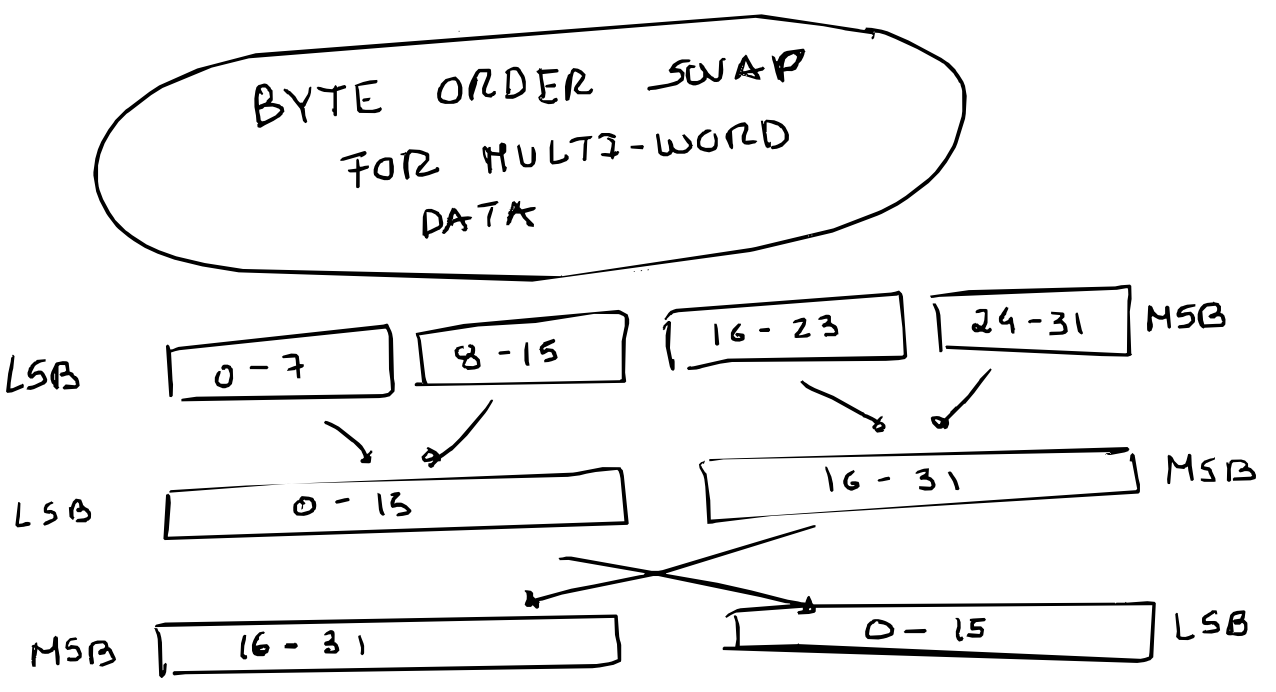
DATA RANGE PREFIXES

DATA BLOCK	PREFIX
Coils	0
Discrete Inputs	1
Input Registers	3
Holding Registers	4

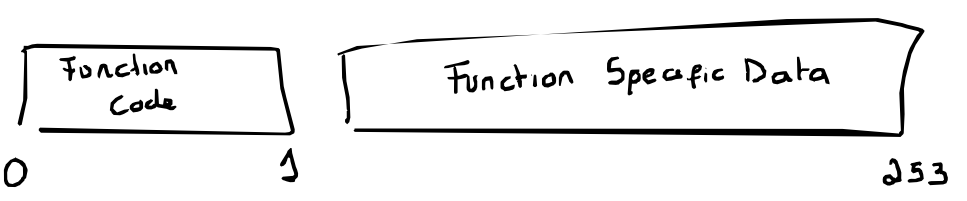
HOLDING REGISTER INDEXING SCHEME

ADDRESS	REGISTER NUMBER	NUMBER (INDEX)
0	1	400001
1	2	400002
2	3	400003

BYTE ORDER SWAP FOR MULTI-WORD DATA



- MODBUS PDU: consists of a one-byte function code followed by up to 252 bytes of function-specific data



STANDARD FUNCTION CODES

CODE	DESCRIPTION
3	Read Multiple Registers
16	Write Multiple Registers
1	Read Coils
2	Read Discrete Inputs
4	Read Input Registers
5	Write single Coil
6	Write Single Register
7	Read Exception Status
15	Write Multiple Coils
20	Read File Record
21	Write File Record
22	Mask Write Register
23	Read / Write Multiple Registers
24	Read FIFO

- Each ADU (application Data Unit) comes with a full PDU (protocol Data Unit)

- Standard Formats (ADU): TCP, RTU, and ASCII