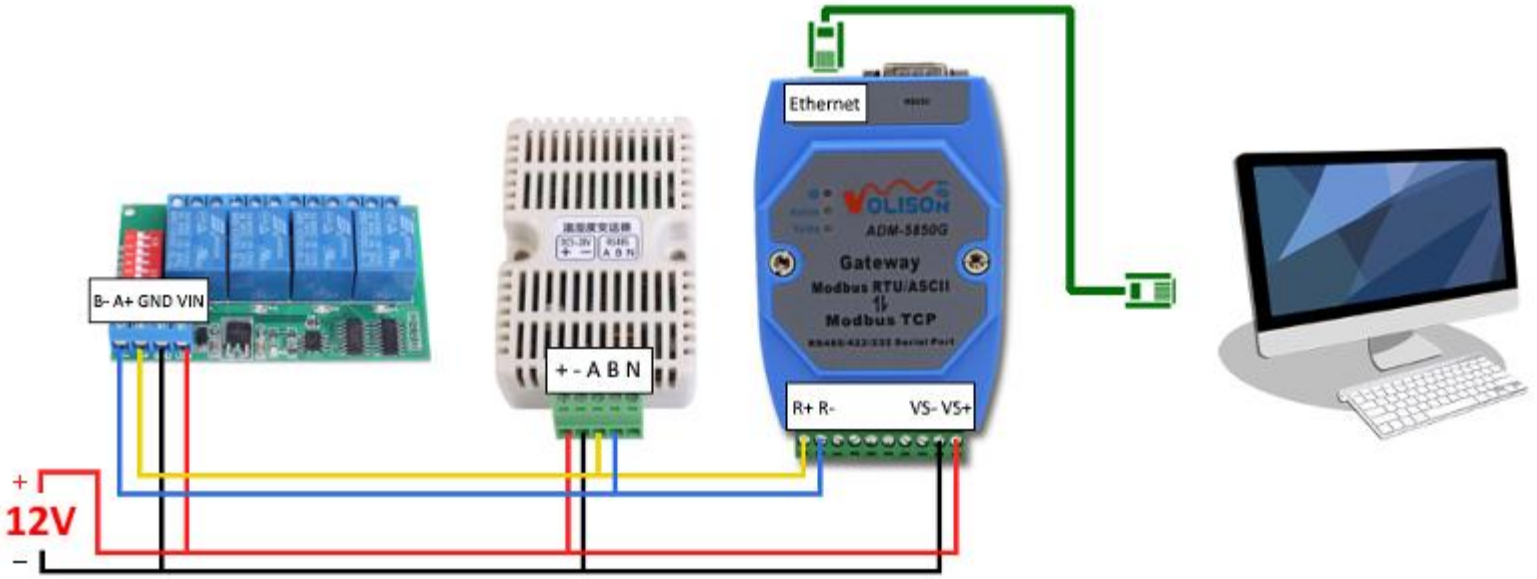
Modbus Protocol

Yogesh M Iggalore

What is modbus

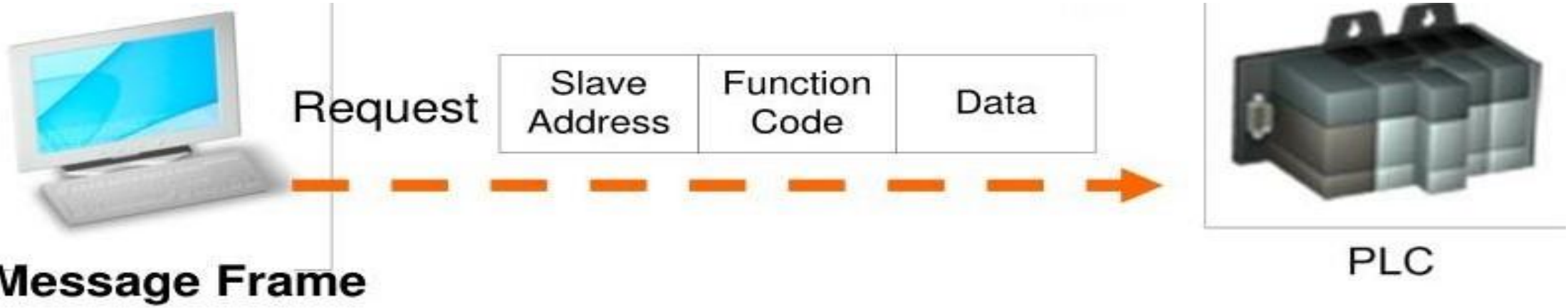
- Modbus is a open source protocol developed by modicon.
- Developed in year 1979 to communicate with PLC.
- Standard communication protocol in industry.
- The device which request the data are called modbus master.
- The device which response the data are called modbus slave.
- In standard network, there is one master and can be up to 247 slaves.
- Modbus is often used to connect SCADA systems.

Modbus protocol modes



Modbus RTU
Modbus ASCII
Modbus TCPIP

Modbus RTU frame



RTU Message Frame

START	Slave Address	Function Code	Data	CRC Check	END
T1–T2–T3–T4	8 BITS	8 BITS	n x 8 BITS (0-252 Bytes)	16 BITS	T1–T2–T3–T4

>= 3.5 char — Maximum size of RTU Message Frame is 256 Bytes — >= 3.5 char

Modbus Function codes

Code	1/16-bit	Description	I/O Range
01	1-bit	Read coils	00001 – 10000
02	1-bit	Read contacts	10001 – 20000
05	1-bit	Write a single coil	00001 – 10000
15	1-bit	Write mulitple coils	00001 – 10000
03	16-bit	Read holding registers	40001 – 50000
04	16-bit	Read input registers	30001 – 40000
06	16-bit	Write single register	40001 – 50000
16	16-bit	Write mulitple registers	40001 – 50000
22	16-bit	Mask write register	40001 – 50000
23	16-bit	Read/write mulitple registers	40001 – 50000
24	16-bit	Read FIFO queue	40001 – 50000

Read Coil Status (FC=01)

ON/OFF status of discrete coils

Request command:

Slave id	Function code	Start register	Number of coils	CRC
11	01	0013	0025	0E84

- 11: slave address
- 01: fun code read coil status
- 0013: data address to start read from
- 0025: total 25 number of coil status requested
- 0E84: CRC value

Response data:

Slave id	Function code	Data byte follow	data	CRC
11	01	05	CD6BB20E1B	45E6

- 11: slave address
- 01: fun code read coil status
- 05: number of bytes followed by
- CD6BB20E1B: coil status
  - CD coil 27 to 20 (b'11001101)
  - 6B coil 35 to 28 (b'01101011)
  - B2 coil 43 to 36 (b'10110010)
  - 0E coil 51 to 44 (b'00001110)
  - 1B coil 56 to 52 (b'00011011)
- 45E6: CRC value

Read Input Status (FC=02)

ON/OFF status of discrete input

Request command:

Slave id	Function code	Start register	Number of input	CRC
11	02	00C4	0016	BAA9

- 11: slave address
- 02: fun code read input status
- 00C4: data address to start read from
- 0016: total 25 number of input status requested
- BAA9: CRC value

Response data:

Slave id	Function code	Data byte follow	data	CRC
11	02	03	ACDB35	2018

- 11: slave address
- 02: fun code read input status
- 03: number of bytes followed by
- ACDB35: input status
  - AC input 204 to 197 (b'10101100)
  - DB input 212 to 205 (b'11011011)
  - 35 input 218 to 213 (b'00110101)
- 2018: CRC value

Read Holding Registers (FC=03)

the content of analog output holding registers

Request command:

Slave id	Function code	Start register	Number of register	CRC
11	03	006B	0003	7687

- 11: slave address
- 03: fun code read holding register
- 006B: start register address
- 0003: number of registers
- 7687: CRC value

Response data:

Slave id	Function code	Data byte follow	data	CRC
11	03	06	AE4156524340	49AD

- 11: slave address
- 03: fun code read holding register
- 06: number of bytes followed by
- AE4156524340: register values
  - AE41 value of register 108
  - 5652 value of register 109
  - 4340 value of register 110
- 49AD: CRC value

Read Input Registers (FC=04)

the content of analog input registers

Request command:

Slave id	Function code	Start register	Number of register	CRC
11	04	0008	0001	B298

- 11: slave address
- 04: fun code read holding register
- 0008: start register address
- 0001: number of registers
- B298: CRC value

Response data:

Slave id	Function code	Data byte follow	data	CRC
11	04	02	000A	F8F4

- 11: slave address
- 04: fun code read input register
- 02: number of bytes followed by
- 000A: register values
  - 000A value of register 8
- 49AD: CRC value

Force Single Coil (FC=05)

Writing content of discrete coil

Request command:

Slave id	Function code	Start register	Coil value	CRC
11	05	00AC	FF00	4E8B

- 11: slave address
- 05: fun code force single coil
- 00AC: coil address
- FF00: FF00 (ON) 0000 (OFF)
- 4E8B: CRC value

Response data:

Slave id	Function code	Start register	Coil value	CRC
11	05	00AC	FF00	4E8B

- 11: slave address
- 05: fun code force single coil
- 00AC: coil address
- FF00: coil ON
- 4E8B: CRC value

Preset Single Register (FC=06)

writing the contents of analog output holding register

Request command:

Slave id	Function code	Start register	Register value	CRC
11	06	0001	0003	9A9B

- 11: slave address
- 06: fun code force single register
- 0001: holding register address
- 0003: write value
- 9A9B: CRC value

Response data:

Slave id	Function code	Register address	value	CRC
11	06	0001	0003	9A9B

- 11: slave address
- 06: fun code force single register
- 0001: holding register address
- 0003: write value
- 9A9B: CRC value

Force Multiple Coils (FC=15)

writing the contents of a discrete coils

Request command:

Slave id	Function code	Start register	Number of coils	Byte followed	Values	CRC
11	0F	0013	000A	02	CD01	BF0B

- 11: slave address
- 0F: fun code force multiple coils
- 0013: start register address
- 000A: number of coils
- 02: bytes followed by
- CD01: coil values
- 9A9B: CRC value

Response data:

Slave id	Function code	Start register	Number of coils	CRC
11	0F	0013	000A	2699

- 11: slave address
- 0F: fun code force multiple coils
- 0013: start register address
- 000A: number of coils
- 2699: CRC value

Preset Multiple Registers (FC=16)

writing the contents of multiple registers

Request command:

Slave id	Function code	Start register	Number of register	Byte followed	Values	CRC
11	10	0001	0002	04	000A0102	C6F0

- 11: slave address
- 10: fun code preset multiple register
- 0001: start register address
- 0002: number of register
- 04: bytes followed by
- 000A0102: registers values
- c6F0: CRC value

Response data:

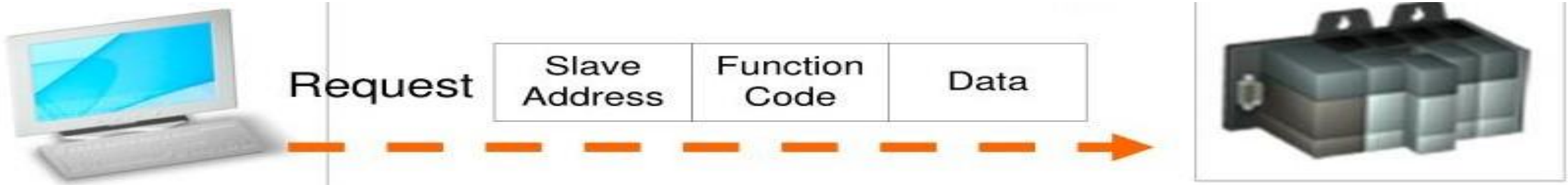
Slave id	Function code	Start register	Number of Register	CRC
11	0F	0001	0002	1298

- 11: slave address
- 10: fun code preset multiple register
- 0001: start register address
- 0002: number of register
- 1298: CRC value

Modbus exceptions

1	Illegal Function	The function code received in the query is not recognized by the slave or is not allowed by the slave.
2	Illegal Data Address	The data address (register number) received in the query is not an allowed address for the slave, i.e., the register does not exist. If multiple registers were requested, at least one was not permitted.
3	Illegal Data Value	The value contained in the query's data field is not acceptable to the slave.
4	Slave Device Failure	An unrecoverable error occurred while the slave was attempting to perform the requested action
6	Slave Device Busy	The slave is engaged in processing a long-duration command. The master should try again later.
10	Gateway Path Unavailable	Specialized use in conjunction with gateways, usually means the gateway is misconfigured or overloaded
11	Gateway Target Device Failed to Respond	Specialized use in conjunction with gateways, indicates no response was received from the target device.

Modbus ASCII



RTU Message Frame

START	Slave Address	Function Code	Data	CRC Check	END
T1–T2–T3–T4	8 BITS	8 BITS	n x 8 BITS (0-252 Bytes)	16 BITS	T1–T2–T3–T4

>= 3.5 char — Maximum size of RTU Message Frame is 256 Bytes — >= 3.5 char

ASCII Message Frame

START	Slave Address	Function Code	Data	LRC Check	END
1 CHAR :	2 CHARS	2 CHARS	n CHARS (0-2x252)	2 CHARS	2 CHARS CRLF

Modbus TCPIP