

Introdução ao Protocolo Modbus TCP

Curso: Supervisão e Controle de SEP

Duração Estimada: 2 horas

Professor: Lucas Silveira

Janeiro de 2025

Objetivos da Aula

- Compreender o funcionamento do protocolo Modbus TCP.
- Diferenciar Modbus TCP de Modbus RTU.
- Conhecer a estrutura das mensagens Modbus TCP.
- Realizar configurações básicas em sistemas que utilizam Modbus TCP.

O que é Modbus?

- Protocolo de comunicação industrial criado em 1979 pela **Modicon** para uso em CLPs.
- **Arquitetura Mestre-Escravo** (ou Cliente-Servidor em TCP).
- Simples, robusto e amplamente adotado em ambientes industriais por ser aberto e livre de royalties.

Principais Tipos:

- **Modbus RTU** (Serial - RS-485)
- **Modbus TCP** (Ethernet - TCP/IP)

O que é Modbus?

- Many of the data types are named from industrial control of factory devices, such as a **ladder logic** because of its use in driving relays:
 - a single-bit physical output is called a *coil*;
 - a single-bit physical input is called a *discrete input* or a *contact*.

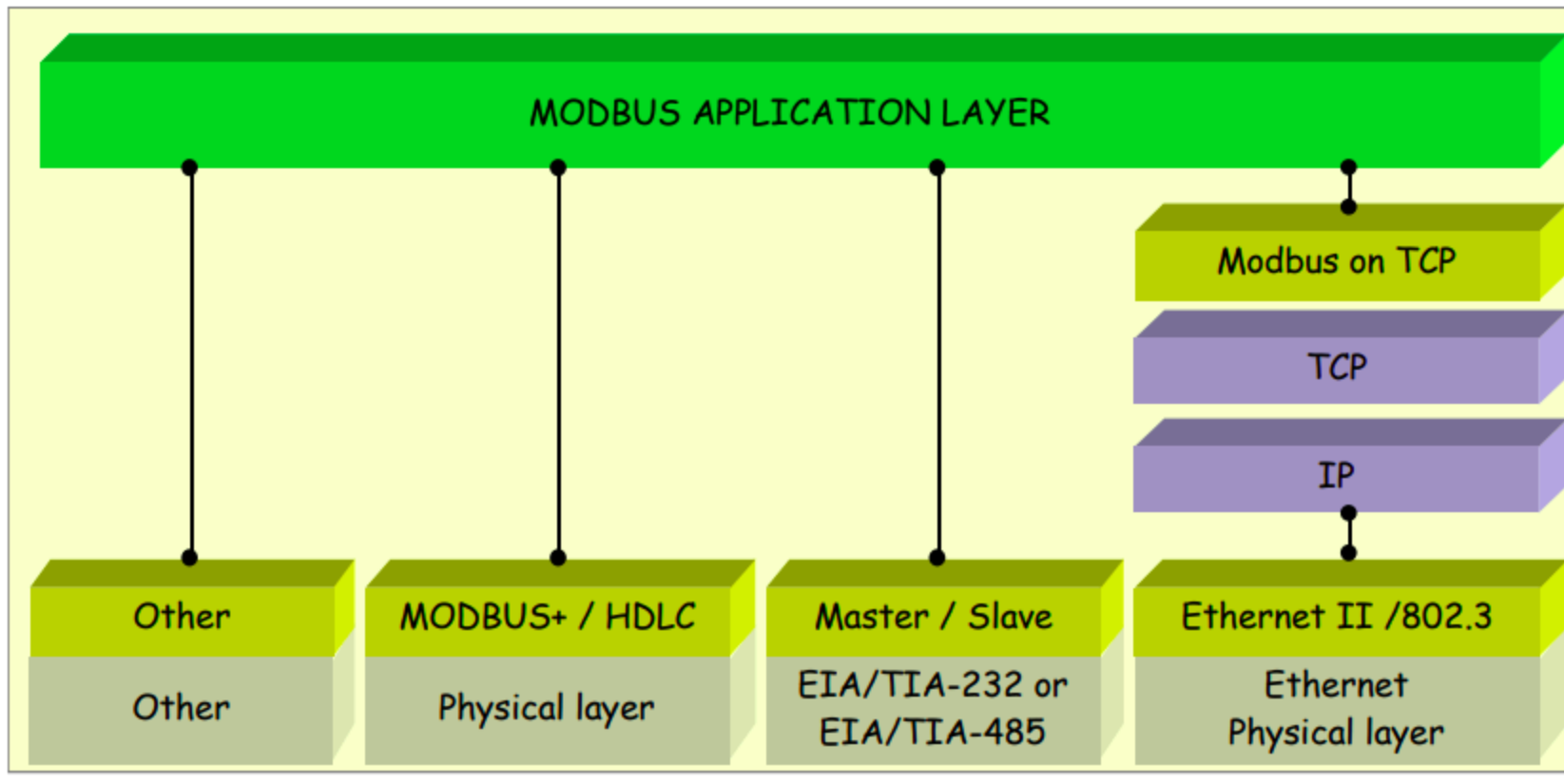
O que é Modbus TCP?

- Modbus TCP é uma versão do Modbus que utiliza o protocolo **TCP/IP** sobre redes **Ethernet**.
- Funciona no modelo **Cliente-Servidor**.

Características principais:

1. Alta velocidade (10/100 Mbps ou superior).
2. Usa endereçamento IP.
3. Compatível com equipamentos Ethernet modernos.

O que é Modbus TCP?



Estrutura da Mensagem Modbus TCP

Campo	Tamanho	Descrição
Transaction ID	2 bytes	Identificador da transação.
Protocol ID	2 bytes	Sempre 0x0000 para Modbus TCP.
Length	2 bytes	Número de bytes restantes.
Unit ID	1 byte	ID do dispositivo escravo (servidor).
Function Code	1 byte	Código da função (ex: 03, 06).
Data	Variável	Dados da requisição/resposta.

Estruturas de Dados do Modbus

Primary tables	Access	Size	Features
Contact (Discrete input)	R	1 bit (0–1)	Read on/off value
Coil (discrete output)	R/W	1 bit (0–1)	Read/Write on/off value
Input register	R	16 bit words (0–65,535)	Read measurements and statuses
Holding register	R/W	16 bit words (0–65,535)	Read/Write configuration values

Principais Códigos de Função

Código	Função	Descrição
01	Read Coils	Lê saídas digitais (liga/desliga).
02	Read Discrete Inputs	Lê entradas digitais.
03	Read Holding Registers	Lê registradores de 16 bits.
04	Read Input Registers	Lê registradores de entrada.
05	Write Single Coil	Escreve em uma saída digital.
06	Write Single Register	Escreve em um registrador de 16 bits.

Diferenças entre Modbus RTU e Modbus TCP

Aspecto	Modbus RTU	Modbus TCP
Meio Físico	RS-485 / RS-232 (Serial)	Ethernet (TCP/IP)
Modelo	Mestre-Escravo	Cliente-Servidor
Velocidade	Limitada (até 115,2 kbps)	Alta (10/100 Mbps ou mais)
Endereçamento	IDs dos escravos (1 a 247)	Endereçamento IP
Verificação de Erro	CRC (RTU)	Verificação nativa TCP/IP

Exemplo Prático de Requisição

Requisição: Mestre lê 2 registradores de um servidor

Campo	Valor Hexadecimal	Descrição
Transaction ID	00 01	Identificador da transação.
Protocol ID	00 00	Protocolo Modbus (0x0000).
Length	00 06	Tamanho da mensagem.
Unit ID	01	ID do servidor.
Function Code	03	Lê Holding Registers.
Start Address	00 10	Endereço inicial (4097).
Quantity	00 02	Quantidade de registradores.

Resposta do Servidor

Resposta para a requisição anterior

Campo	Valor Hexadecimal	Descrição
Transaction ID	00 01	Igual ao da requisição.
Protocol ID	00 00	Protocolo Modbus.
Length	00 07	Tamanho da mensagem.
Unit ID	01	ID do servidor.
Function Code	03	Confirmação da leitura.
Byte Count	04	2 registradores x 2 bytes.
Data	00 0A 00 14	Valores dos registradores.

Aplicações do Modbus TCP

- Automação industrial.
- Sistemas SCADA.
- CLPs, sensores e atuadores.
- Inversores de frequência.
- Integração entre redes de TI e OT (Operações).

Exercícios

1. Qual a principal diferença entre Modbus RTU e Modbus TCP em relação ao meio de comunicação?
2. Qual o tamanho do cabeçalho TCP na estrutura de uma mensagem Modbus TCP? Explique seus campos principais.
3. Um cliente envia um código de função 03 para ler 4 registradores a partir do endereço 0x0020. Quantos bytes de dados espera-se na resposta?
4. Cite três vantagens do Modbus TCP em relação ao Modbus RTU em sistemas industriais.

Encerramento

- **Revisamos:** Introdução ao Modbus TCP, estrutura das mensagens, códigos de função e aplicações.
- **Próxima Aula:** Configuração prática de redes Modbus TCP com sistema SCADA-LTS.

Obrigado!

Dúvidas?