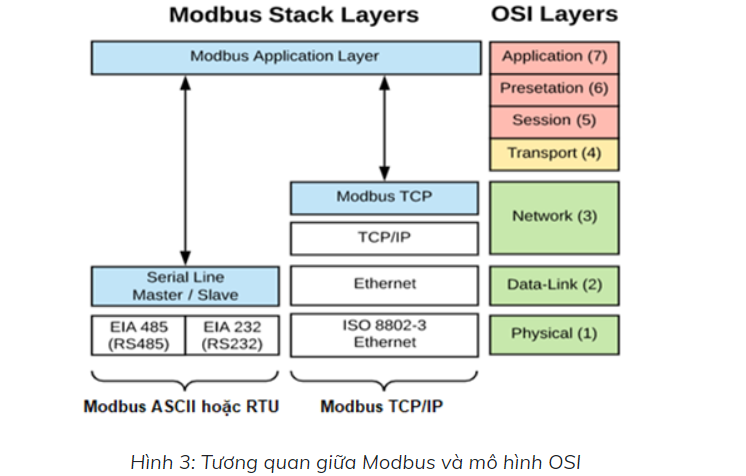
- Truyền thông Modbus, với **truyền thông nối tiếp** có 3 lớp (Vật lý, liên kết dữ liệu, ứng dụng), với **truyền thông TCP/IP** có 4 lớp (Vật lý, liên kết dữ liệu, mạng, ứng dụng).



**1. MODBUS ASCII VÀ MODBUS RTU**

-   Modbus ASCII sử dụng kết nối truyền thông nối tiếp, mã hóa Hex

- Modbus RTU sử dụng kết nối truyền thông nối tiếp, mã hóa nhị phân.

- Giao thức Modbus hỗ trợ tối đa 247 thiết bị Slave được kết nối nối tiếp vào Master (không qua các thiết bị chuyển tiếp). Với cổng kết nối RS232, Modbus có khoảng cách truyền tối đa là 200m; với cổng kết nối RS485 khoảng cách này là 1200m.

- Kích cỡ tối đa của tin nhắn Modbus là 256 bytes và tuân theo format dưới đây:



-  Các thành phần nêu trên được kết hợp để tạo nên Modbus Frame format gồm một ADU (Application Data Unit) và một PDU (Protocol Data Unit).

ADU: Additional address + PDU + Error check

PDU: Function code + Data

**2. MODBUS TCP/IP**

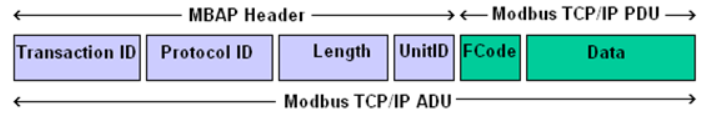
- Modbus TCP/IP: Sử dụng truyền thông TCP/IP để gói (wrap up) **gói phần Function code và Data của Modbus nối tiếp vào gói tin TCP/IP**, cho phép định tuyến việc truyền gói tin, hỗ trợ nhiều thiết bị hơn, đồng thời tăng khoảng cách truyền tin.

- Modbus TCP/IP sử dụng khối PDU của khung tin nhắn Modbus RTU



- Sau đó chèn thêm phần MBAP (Modbus Application Protocol), được khung tin nhắn Modbus TCP/IP

-   MBAP Header, 7 bytes được thêm vào đầu của khung tin nhắn.



Transaction ID: 2 bytes

Protocol ID: 2 bytes

Length: 2 bytes

UnitID: 1 byte

- Có thể hiểu đơn giản Modbus TCP/IP là giao thức Modbus RTU với giao diện TCP chạy trên Ethernet. TCP/IP cung cấp phương tiện truyền cho tin nhắn Modbus TCP/IP. Nói cách khác, TCP/IP cho phép khối dữ liệu nhị phân được trao đổi giữa các máy tính. Chức năng chính của TCP là đảm bảo rằng tất cả các gói dữ liệu được nhận chính xác, trong khi IP đảm bảo rằng các thông điệp được xử lý và định tuyến chính xác. Sự kết hợp TCP/IP chỉ là một giao thức truyền tải và không xác định ý nghĩa của dữ liệu và nội dung dữ liệu. Modbus TCP/IP sử dụng TCP/IP và Ethernet để mang dữ liệu của cấu trúc tin nhắn Modbus giữa các thiết bị tương thích với chuẩn mạng (TCP/IP). Thông điệp Modbus TCP/IP là một giao tiếp Modbus được gói gọn trong TCP/IP Ethernet. Trong thực tế, Modbus TCP nhúng khung dữ liệu Modbus vào khung TCP, đã bỏ đi CRC của Modbus.  Mã CRC của khung tin nhắn Modbus được loại bỏ, địa chỉ khung Modbus được thay thế bởi mã định danh đơn vị trong Modbus TCP/IP và trở thành một phần của tiêu đề giao thức ứng dụng Modbus (MBAP). ADU được nhúng vào trường dữ liệu của khung TCP tiêu chuẩn và được gửi qua TCP port 502. Cổng này được dành riêng cho các ứng dụng Modbus, tất cả các thiết bị Modbus Server và Modbus Client nhận và truyền dữ liệu Modbus thông qua port 502