Handshake TCP: Hàm Connect trong VB6.0

Handshake S7-COMMPlus: Gửi gói tin CR

COTP

TPKT

03 00 00 16 11 0e 00 00 00 0f 00 c1 02 01 00 c2 02 01 02 c0 01 0a

CC Conform là 0x0D

CR Request

Length

Length

Vesion

PLC trả về gói CC

Setup Communication:

VB6 gửi gói Setup

S7-COMM plus

COTP

TPKT

03 00 00 19 02 f0 80 32 01 00 00 02 00 00 08 00 00 f0 00 00 01 00 01 01 e0

Ack\_Data là 3

Job

ID

PLC sẽ trả về gói Ack\_Data

Gửi nhận dữ liệu:

VB6 sẽ gửi 2 gói 1 lúc (KHI READ/WRITE DATA THÌ KHÔNG CẦN GỬI GÓI DT CHỈ GỬI GÓI DATA THÔI)

Gửi gói DT trước

COTP

TPKT

03 00 00 07 02 f0 00

Gửi gói Data

Length

S7-COMM plus

COTP

s

TPKT

03 00 00 1f 02 f0 80 32 01 00 00 00 00 00 0e 00 00 04 01 12 0a 10 02 00 40 00 01 84 00 00 00

Thứ tự vùng nhớ

Địa chỉ

Vùng nhớ

Count

READ

Length

Job

ID

VD DB1.DBX0.0 = 00 01 84 00 00 00

Length

TPKT

COTP

S7-COMM plus

03 00 00 1f 02 f0 80 32 01 00 00 00 01 00 0e 00 00 04 01 12 0a 10 02 00 10 00 00 83 00 00 00

Thứ tự vùng nhớ

Địa chỉ

Vùng nhớ

Count

READ

Length

Job

ID

VD M0.0 = 00 00 83 00 00 00

Byte/word/Dword

S7-COMM plus

COTP

TPKT

03 00 00 27 02 f0 80 32 01 00 00 00 03 00 0e 00 08 05 01 12 0a 10 02 00 04 00 00 83 00 00 20 00 04 00

Địa chỉ

Vùng nhớ

Thứ tự vùng nhớ

Length

Count

Write

20 00 00 01 03

Data

VD M4.0 = 00 00 83 00 00 20 00 04 00 20 00 0 01 03

CHỈ THAM KHẢO DO ĐÓ LÀ GIAO THỨC S7Communication CHO S7-300

CÒN S7-1200 LÀ GIAO THỨC S7CommunicatioPlus

S7 CommunicationPlus cho S7-1200

Bước 1: Gửi gói CR

COTP

TPKT

03 00 00 23 1e e0 00 00 00 06 00 c1 02 06 00 c2 0f 53 49 4d 41 54 49 43 2d 52 4f 4f 54

2d 45 53 c0 01 0a

Bước 2: Lấy ID và Thông tim PLC

//Request

03 00 00 f2 02 f0 80 72 01 00 e3 31 00 00 04 ca 00 00 00 01 00 00 01 20 36 00 00 01 1d 00 04 00 00 00 00 00 a1 00 00 00 d3 82 1f 00 00 a3 81 69 00 15 15 53 65 72 76 65 72 53 65 73 73 69 6f 6e 5f 31 43 39 43 33 38 42 a3 82 21 00 15 38 30 2e 30 2e 30 2e 30 3a 30 49 6e 74 65 6c 28 52 29 20 50 52 4f 2f 31 30 30 30 20 4d 54 20 4e 65 74 77 6f 72 6b 20 43 6f 6e 6e 65 63 74 69 6f 6e 2e 54 43 50 49 50 2e 31 a3 82 28 00 15 00 a3 82 29 00 15 00 a3 82 2a 00 15 17 57 49 4e 2d 34 43 31 32 4c 46 30 42 4a 47 36 5f 31 38 35 32 39 34 38 a3 82 2b 00 04 01 a3 82 2c 00 12 01 c9 c3 8b a3 82 2d 00 15 00 a1 00 00 00 d3 81 7f 00 00 a3 81 69 00 15 15 53 75 62 73 63 72 69 70 74 69 6f 6e 43 6f 6e 74 61 69 6e 65 72 a2 a2 00 00 00 00 72 01 00 00 //Mặc định không cần chỉnh sửa.

//Respone

S7 CommunicationPlus

COTP

ID2

ID1

TPKT

03 00 00 89 02 f0 80 72 01 00 7a 32 00 00 04 ca 00 00 00 01 36 11 02 87 18 87 31 a1 00 00 01 20 82 1f 00 00 a3 81 69 00 15 00 a3 82 32 00 17 00 00 01 3a 82 3b 00 04 82 00 82 3c 00 04 81 40 82 3d 00 04 84 80 c0 40 82 3e 00 04 84 80 c0 40 82 3f 00 15 1b 31 3b 36 45 53 37 20 32 31 34 2d 31 41 45 33 30 2d 30 58 42 30 20 3b 56 32 2e 32 82 40 00 15 05 32 3b 37 39 34 82 41 00 03 00 03 00 a2 00 00 00 00 72 01 00 00

Tính toán Session ID = Byte đầu tiên + 0x80 (87 là byte thứ 2 MẶC ĐỊNH)

VD: ID1 = 0x18 + 0x80 = 0x98

Lúc này Session ID1 (dùng cho các gói tin phía sau) có dạng là 4 byte 00 00 03 98

Mặc định

Tính toán

XONG PHẦN KẾT NỐI VÀ LẤY ID

//RUN

Lệnh RUN

ID1

03 00 00 43 02 f0 80 72 02 00 34 31 00 00 04 f2 00 00 00 44 00 00 03 96 34 00 00 00 34 01 90 77 00 08 03 00 00 04 e8 89 69 00 12 00 00 00 00 89 6a 00 13 00 89 6b 00 04 00 00 00 00 00 00 00 72 02 00 00

Lệnh STOP

// STOP

ID1

03 00 00 43 02 f0 80 72 02 00 34 31 00 00 04 f2 00 00 00 3f 00 00 03 96 34 00 00 00 34 01 90 77 00 08 01 00 00 04 e8 89 69 00 12 00 00 00 00 89 6a 00 13 00 89 6b 00 04 00 00 00 00 00 00 00 72 02 00 00