

原创文章，转载请注明出处。

更多实用资料请登录方正智芯官网：www.founderchip.com

作者：北岛李工

西门子S7系列PLC的开放式以太网通信过程包括如下几个步骤：建立连接（Establish connection）、发送/接收数据（Send/receive data）、断开连接（Disconnect）。

与通信伙伴建立连接要使用TCON指令，该指令的“CONNECT”引脚的数据包含了通信伙伴的相关信息（比如：通信协议、IP地址、端口号等等）。在S7-300/400中，CONNECT引脚的数据类型为：TCON_Param。但是，在S7-1500系列PLC的开放式以太网通信中，数据类型TCON_Param会出现通信无法建立的情况。这是怎么回事呢？



我们知道，S7-1500系列PLC有两个以太网端口：X1和X2。其中X1包括2个RJ45口（内置交换机功能）；X2有1个RJ45口。X1和X2是独立的，也就是可以设置成两个不同网段的IP地址，都支持开放式以太网通信协议。当使用数据类型TCON_Param做为连接的参数时，X1口可以建立通信，但是X2口确无法建立通信。

这种情况下，应该使用新的数据类型：TCON_IP_v4。

与TCON_Param相比，数据类型TCON_IP_v4明确了硬件标识符，因此可以指明当前是使用哪个网口进行通信。

TCON_IP_v4的数据结构如下表：

方正智芯——TCON_IP_v4数据结构

字节	参数名称	数据类型	初始值	说明
0~1	interface_id	HW_ANY	64	本地通信的硬件标识符 (范围：0~65535)
2~3	id	CONN_OUC	1	通信连接的标识符 (范围：1~4095)
4	connection_type	BYTE	11	连接的类型：11=TCP；19=UDP；
5	active_established	BOOL	TRUE	是否主动进行通信连接。TRUE=主动;FALSE=被动
6~9	remote_address	ARRAY[1..4] of BYTE		通信伙伴的IP地址
10~11	remote_port	UINT	2000	通信伙伴的端口号 (范围：1~49151)
12~13	local_port	UNIT	2000	本地端口号 (范围：1~49151)
www.founderchip.com				

各部分的含义解释如下：

1) interface_id：本地通信端口的硬件标识符。默认值64表示使用X1端口，若要使用X2端口，则根据硬件配置的标识符数据进行修改；

2) id：用来标识连接，在发送/接收指令中会用到连接的ID；

3) connection_type：表示连接的类型。

- 11(0x0B)=TCP协议；
- 19(0x13)=UDP协议。

出于兼容及程序移植的考虑，17(0x11)也表示TCP协议；

4) active_established：是否主动建立连接。TRUE表示主动；FALSE则表示被动建立连接；

5) remote_address：通信伙伴的IP地址，是一个四个字节的数组。

假设通信伙伴的IP地址为：192.168.0.88，则：

- addr[1]=192；
- addr[2]=168；
- addr[3]=0；
- addr[4]=88；

6) remote_port：通信伙伴的端口号，建议使用大于2000的数值；

7) local_port：本地端口号，建议使用大于2000的数值；

在S7-1500及S7-1200 (V4.0以上) 的以太网通信连接中，建议使用TCON_IP_v4代替TCON_Param！

好了，关于TCON_IP_v4数据类型就先介绍到这里。相关参考文章：

[西门子PLC以太网开放式用户通信连载（1）-TCON](#)

如果你喜欢这篇文章，可以去官网（www.founderchip.com）下载本文PDF版本。

小程序【李工谈工控】提供方便的文章检索功能，欢迎体验：

