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

这是S7-1200与S7-200 Smart系列PLC的S7通信教程的第1篇文章。本章我们打算和大家聊聊西门子的S7通信协议。

S7通信协议是西门子S7系列PLC内部集成的一种通信协议，是S7系列PLC的精髓所在。它是一种运行在传输层之上的（会话层/表示层/应用层）、经过特殊优化的通信协议，其信息传输可以基于MPI网络、PROFIBUS网络或者以太网。

S7通信协议的参考模型见下面的表格：

方正智芯——S7 通信协议参考模型		
层	**OSI 模型**	**S7协议**
7	应用层	S7通信
6	表示层	S7通信
5	会话层	S7通信
4	传输层	ISO-ON-TCP(RFC 1006)
3	网络层	IP
2	数据链路层	以太网/FDL/MPI
1	物理层	以太网/RS485/MPI
www.founderchip.com		

S7通信支持两种方式：

1）基于客户端（Client）/服务器（Server）的单边通信；

2）基于伙伴（Partner）/伙伴（Partner）的双边通信；

客户端（Client）/服务器（Server）模式是最常用的通信方式，也称作S7单边通信。在该模式中，只需要在客户端一侧进行配置和编程；服务器一侧只需要准备好需要被访问的数据，不需要任何编程（服务器的“服务”功能是硬件提供的，不需要用户软件的任何设置）。

什么是客户端（Client）呢？

客户端其实是在S7通信中的一个角色，它是资源的索取者；而服务器则是资源的提供者。服务器（Server）通常是S7-PLC的CPU，它的资源就是其内部的变量/数据等。客户端通过S7通信协议，对服务器的数据进行读取或写入的操作。常见的客户端包括：人机界面（HMI）、编程电脑（PG/PC）等。当两台S7-PLC进行S7通信时，可以把一台设置为客户端，另一台设置为服务器。（*这种设置的具体方法我们会在本教程的后续文章中介绍。*）

其实，很多基于S7通信的软件都是在扮演者客户端的角色。比如OPC Server，虽然它的名字中有Server。但在S7通信中，它其实是客户端的角色。

客户端/服务器模式的数据流动是单向的。也就是说，只有客户端能操作服务器的数据，而服务器不能对客户端的数据进行操作。

有时候，我们需要双向的数据操作，这就要使用伙伴（Partner）/伙伴（Partner）通信模式。

伙伴（Partner）/伙伴（Partner）通信模式也称为S7双边通信，也有人称其为客户端（Client）—客户端（Client）模式。不管是什么名字，该通信方式有如下几个特点：

1）通信双方都需要进行配置和编程；

2）通信需要先建立连接。主动请求建立连接的是主动伙伴（Active Partner），被动等待建立连接的是被动伙伴（Passive Partner）；

3）当通信建立后，通信双方都可以发送或接受数据；

在S7-300中，使用FB12（BSend）/FB13（BRecv）进行发送和接收。当一方调用发送指令时，另一方必须同时调用接收指令才能完成数据的传输。

好了，关于S7通信协议就先介绍到这里。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：


李工
谈
工程
扫码关注小程序