

文章编号: 1000 - 8829(2004)12 - 0050 - 02

OMRON PLC 在以太网中的通信及实现

Implementation of OMRON PLC Communication Based on Ethernet

(东南大学 机械工程系, 江苏 南京 210096) **曹 卫**
(扬州大学 信息工程学院电气工程系, 江苏 扬州 225009) **史旺旺, 陈 虹**

摘要: 介绍了一个使用 Visual C++ 的 Socket 与 OMRON PLC 之间的通信程序, 并成功地应用在自动控制系统中, 主要实现上位机与 OMRON PLC 之间的以太网通信, 并对它们之间的通信协议作了描述, 文中所介绍的通信程序的设计方法具有一定参考价值。

关键词: 可编程逻辑控制器; 以太网; FINS; 控制系统

中图分类号: TP393

文献标识码: A

Abstract: A kind of communication program developed with VC is introduced, which is successfully applied in the automatic control system, and mainly carries out the communication between host and OMRON PLC. The communication protocol between them is described in detail. The design method of communication program has some reference value.

Key words: PLC; Ethernet; FINS; control system

在分布式计算机监控系统中, PLC 是常用的现场控制设备, PLC 和微机之间的通信常采用 RS-232/RS-485 串行通信方式, 这种方法对于数据量较大、通信距离较远、实时性要求高的控制系统很难满足通信需要。工业以太网特别是交换式以太网已经广泛用于工业控制中, 是工业控制中的发展趋势^[1]。许多大型 PLC 厂商生产的 PLC 都配备了相应的以太网通信单元, 笔者讨论了 OMRON PLC 的以太网通信体系结构, 并以 CJ1G 型 PLC 的以太网模块 ENT11 为例实现与微机的通信, 上位机利用 Visual C++ 的 CAsyncSocket 类的 UDP 协议实现了微机和 PLC 以太网模块之间的 FINS 通信, 程序实现简单, 并给出了核心程序。

1 PLC 的网络体系结构与 FINS 协议

1.1 FINS 协议与 TCP/IP 协议

OMRON 公司的 ETN11 型以太网单元支持 10Base-T 型以太网, 网络层和传输层采用 TCP/IP 和 UDP/IP 协议, 应用层

协议支持 FTP、SMTP 和 FINS (factory interface network service)。FINS 通信协议是 OMRON 开发的用于工厂自动化控制网络的指令/响应系统, 使用 FINS 指令, 可实现网络间的无缝通信。网络对于每个系统层次都是有效的, 包括用于信息层的 Ethernet, 用于控制器层的 Controller Link 网络和用于器件层的 DeviceNet(CompoBus/D), 而且 Ethernet 和 Controller Link 网络之间的通信, 能够在 3 个网络层次间进行, 像一个网络一样方便。使用 FINS 指令, 上位机程序或 PLC 用户程序通过指令就能够读取另一个 PLC 数据区的数据, 简化了用户程序。

以太网通信使用 IP 地址, 而 FINS 通信使用节点号。节点号为以太网和 Link 网之间提供了一致的寻址方式。以太网单元能在 IP 地址和节点号之间转换, 转换方式有自动转换、IP 地址表和复合地址表。FINS 通信与 TCP/IP 协议之间的关系见图 1。

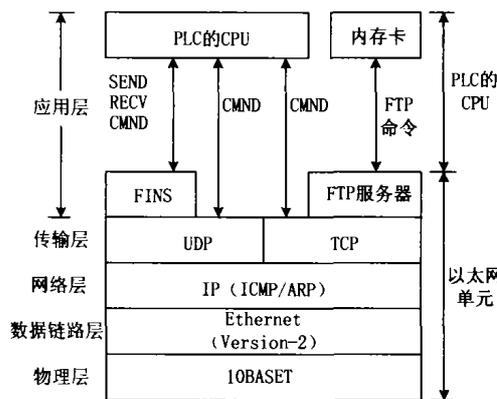


图 1 FINS 协议和 TCP/IP 协议之间的关系

FINS 帧本质上属于链路层, 为了利用 TCP/IP 协议传输 FINS 帧, 将 FINS 信息作为 UDP 的数据区, 封装在 UDP 中, 从 TCP/IP 协议的角度看 FINS 信息, 属于应用层数据。如果在 PLC 上安装以太网单元和 Link 通信单元, 就可以实现以太网和 Link 网之间的数据转发过程, 如图 2 所示。

图 2 中, 上位机发出带有 FINS 信息的以太网帧被中继 PLC 的以太网单元接收后, 层层分解, 直到抽取出 FINS 信息后, 通过 Link 通信模块转发 FINS 信息, 目的 PLC 收到数据后作出响应, 响应数据也采用 FINS 格式的数据。中继 PLC 收到数据后, 转发给以太网单元, 由以太网单元进行封装后与上位机通信。上位机也作为以太网网段中的一个节点, 也有相应的节点号和相同的地址转换规则。

收稿日期: 2004 - 03 - 02

基金项目: 863 计划课题资助项目 (2001AA411230) 和扬州大学信息科学学科群资助项目 (ISG030604)

作者简介: 曹卫 (1967—), 男, 讲师, 硕士研究生, 主要从事工业自动化及网络通信技术的应用研究工作。

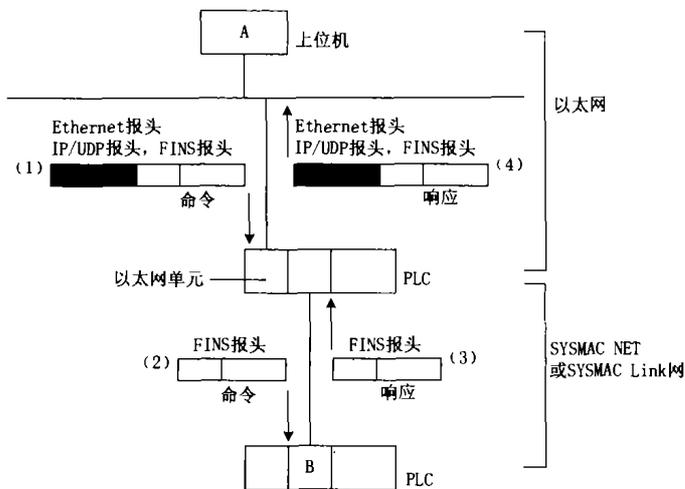


图2 利用 FINS 中继的过程

1.2 FINS 帧格式

在 PLC 之间采用 FINS 协议中的 SEND、RECV 或 CMND 命令进行数据通信时，上述封装和解封过程在通信模块内部自动实现，但对于上位机和以太网单元之间的通信，FINS 的报头和命令应由上位机程序添加，而 UDP 的报头由 Socket 自动完成。FINS 报头的格式见图 3。

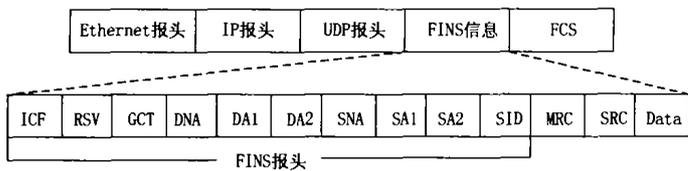


图3 FINS 报头格式

ICF 为信息控制域，主要用于标明命令和响应；RSV 为系统保留；GCT 为网关允许数目；DNA 为目的网络号；DA1 为目的节点号；DA2 为目的节点单元，用于标明 CPU 还是 CPU 总线单元；SNA 为源网络号；SA1 为源网络节点号，对应上位机 IP 地址的主机部分；SA2 为源节点单元，对上位机而言应为 00；SID 为服务和响应的标识，可任意设置，命令和响应有相同的数值；MRC 和 SRC 分别为 FINS 命令的主命令和从命令；Data 域为数据区，用于标明读数据时的地址范围或写数据时的地址和数据。

1.3 以太网单元的设置

通信测试前必须首先登记 I/O 表，可以用 CX-Programmer 软件在编程模式下自动登记 I/O 表，还要设置 IP 地址、子网掩码、CPU 总线单元、地址转换方法、FINS 的 UDP 端口号，FINS UDP 端口号缺省为 9600。以太网单元属于 CPU 总线单元，单元号旋转开关设定一个十六进制数，作为以太网单元的单元号，范围为 00~15，它决定了分配给以太网单元相应的内存工作区(CIO 区、DM 区)。节点号通过两个旋转开关设定两位十六进制数，作为以太网单元在网络中的节点号，范围为 01~126。以太网单元进行通信前，必须使用编程设备如 CX-P 对以太网单元进行设置。内存工作区分配 CIO 区和 DM 区中的字按照单元号分配给每个单元，每个单元在 CIO 区中

分配 25B，在 DM 区分配 100B。如果设为 0 号单元则分配 CIO1500~CIO1524 共 25B，D30000~D30099 共 100B。

跨网通信时，必须对每一个节点建立路径表，路径表包括本地网络表和中继网络表。本地网络表提供了安装在 PLC 单元上的通信单元的单元号和网络号，中继网络表包括终点网络、中继网络和中继节点 3 项内容，用于 FINS 通信时的数据转发。

2 上位机通信程序设计

为实现上位机的 TCP/IP 通信，采用 Socket 编程。考虑到实现的效率，采用了较低层次的异步 WinSock 即 MFC 中的 CAsyncSocket 类实现并采用 UDP 方式，以提高通信的实时性。在监控系统中，上位机和 PLC 交换数据一般放在 PLC 的内存区即 DM 区，为读取 PLC 数据，编程的关键是 FINS 报头的封装，这里以一台 PLC 和上位机组以太网通信为例，上位机读取 PLC 的 DM 区的 4KB 数据。当发送命令且需要 PLC 响应时 ICF 域为 80H，RSV 域为 00H。GCT 因本例中 PLC 和上位机直接组成以太网，故为 0。GCT 在本例中设置为 2。对于局域网 DNA 应为 0。本例中 PLC IP 地址为 192.168.0.32，对应的 DA1 为 20H。DA2 对于本地 PLC 为 0。SNA、SA1、SA2 与 PLC 地址相似，本例中上位机 IP 地址为 192.168.0.5，上述 3 个字节均为 000500H。SID 可任意设置，本例设置为 EFH。读取内存单元的主命令 MRC 和从命令 SRC 分别为 01H 和 01H。Data 区域格式如图 4 所示。DM 区的内存标识符为 82H，起始地址为内存单元的字地址，由于以太网单元只能处理字数据，比特号单元总是为 0。这样读取起始地址为 100 的 4K DM 区 (2KB) 的 FINS 的数据报格式为：

800002002000000500EF0101820064000800

内存标识	起始字地址	比特号	字长度
------	-------	-----	-----

图4 Data 区域的格式

编程时首先从 CAsyncSocket 类派生出 CUDPSocket 类，在程序初始化时创建 CUDPSocket 类的实例，调用 CAsyncSocket 的 SendTo 函数即可。

3 结束语

运用 VC++ 异步套接字类 CAsyncSocket 与 OMRON PLC 进行以太网通信，由于以太网单元采用广泛使用的 TCP/IP 协议，上位机程序设计简单，除了进行 FINS 报头拼装，其他过程与微机之间的 TCP/IP 程序设计完全一致。用 VC 设计的程序具有实时性好、速度快、可靠性高、运行稳定等优点。此方法已成功应用工程项目中。控制系统中采用以太网单元通信后，使工业自动化与生产管理自动化有机地结合到了一起，简化了系统设计。

参考文献：

- [1] 李炳宇, 萧蕴诗. 以太网在网络控制系统中的应用与发展趋势[J]. 微型机与应用, 2002, (11).
- [2] 宫叔贞, 王冬青. 可编程控制器原理及应用[M]. 北京: 人民邮电出版社, 2002 - 07.