

# 基金会现场总线的 HSE 网络连通性动态监测

鹿玲杰 邵 庆 大庆石油学院计算机科学与工程学院(163318)

### Abstract

The dynamic monitoring of the network's connectivity is one of the important aspects of the Fieldbus Control System (FCS).Through the analysis of network model of Fieldbus Foundation's (FF) High Speed Ethernet (HSE),a Ping software is implemented via TCP/IP and ICMP (Internet Control Message Protocol) to monitor the connectivity of HSE dynamically,and provide the foundation for management of HSE network.

Keywords:FCS,FF,HSE,TCP/IP,ICMP

### 摘 要

网络连通性的动态监测是现场总线控制系统(FCS)的重要方面之一。通过对基金会现场总线(FF)的高速部分(HSE)网络模型的分析,从 TCP/IP 入手,利用网际控制报文协议(ICMP)实现一个 Ping 功能的软件,对 HSE 网络的连通性进行动态监测,为 HSE 网络的管理提供基础。

关键词:现场总线,基金会现场总线,高速以太网,TCP/IP,ICMP

FF 现场总线分为 H1 低速部分和 HSE(High Speed Ethernet)高速部分。FF(现场总线基金会)于 2000 年 3 月 29 日公布了高速以太网的最终技术规范 FS1.0 (100Mbps),HSE 本身只定义了物理层和数据链路层,作为一套完整的网络传输协议,必须具有高层控制协议,以太网使用了 TCP/IP 协议,IP(internet protocol)用来确定信息传递路线,而 TCP(transmission control protocol)则是用来保证传输的可靠性。虽然 TCP/IP 并不是专为以太网而设计的,但它已经成为了事实上的标准。

TCP/IP 协议族提供给网络管理员一种管理网络、排除网络差错和解决网络拥挤等方法,也提供了获得网络拓扑结构的一种途径。本文从 ICMP(网际控制报文协议)着手加以探讨,通过 Ping 功能来动态检测 HSE 网络的连通状态,并确定网络上的各结点是否运行正常。

## 1 HSE 与 TCP/IP 网络模型的结合

以太网自身只提供一系列的物理介质定义和一个共享的构架,构架包括物理介质、帧格式和 LAN 设备数据的寻址格式,即它只提供物理层和数据链路层。而 TCP/IP 则包含 IP 协议(层三)、TCP 或 UDP 协议(层四),当以太网用于信息技术时,第七层含有 HTTP(超级文本传输协议)、FTP(文件传输协议)、SNMP(简单网络管理协议)、SMTP(简单电子邮件传送协议)和 Telnet(远程登录)等。但当它用于工业控制时,体现在第七层的是实时通信、用于系统组态的对象以及工程模型的应用协议。

以太网是 TCP/IP 使用最普遍的物理网络,TCP/IP 支持基于异种操作系统的异种网络间的互联,包括:令牌总线、令牌环、FDDI(光纤分布式数据接口)、SLIP(串行线路 IP)、PPP(点到点协议)、X.2.5 数据网等。它是真正的开放系统通信协议,已成为目前国际上进行异种网络互联的事实上的标准。

与 ISO/OSI 参考模型不同,TCP/IP 网络只使用 ISO/OSI 分层的五层。图 1 给出了一个简单的五层网络模型和与其相对应的在 FF 中的分层结构,其中每层都采用 TCP/IP 协议。图 1 中有箭头的线表示不同的网络软件和硬件组件之间可能的通信通道。

HSE 在底层采用了互联网上流行的以太网+TCP/IP 族协议,这样使 HSE 的开发难度相对减小,同时降低了使用成本。为了保证 HSE 的硬实时特性,可以通过限制报文总量使网络工作

在较轻的负载率下。一般情况下,以太网在小的负载率下延迟时间小于令牌网络,而采用 100M 以太网更有助于使这个条件得到满足。另一方面,由于采用了 IP 协议,因此理论上 HSE 能支持跨网关的、覆盖范围很大的大型控制系统。

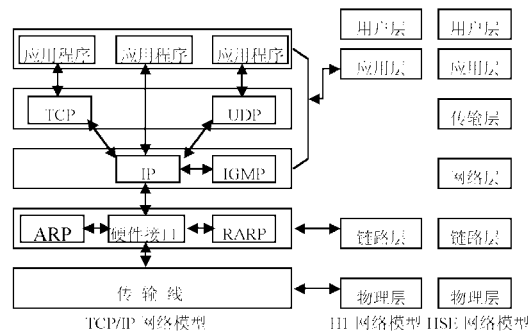


图 1 TCP/IP 网络和 FF 网络模型图

使用 TCP/IP 协议族作为 HSE 的网络传输协议,扩展了 HSE 协议的开放性,便于基于 HSE 的设备与外界的交流,同时也便于 HSE 协议本身的推广使用。

## 2 网际控制报文协议 ICMP

在 TCP/IP 协议族中,IP 提供一种不可靠的无联接报文分组递送服务,报文分组通过一个又一个网关,直到最后一个网关,这个网关把报文分组直接递交给报宿主机。如果一个网关不能为数据报选择路由,或者不能递交数据报,或者这个网关测试到某种不正常状态,例如网络拥挤影响到主机,就需要通知主机采取措施,避免或者纠正这类问题。为了使网络上的设备能够报告错误,或者提供有关意外情况的信息,在网际协议(IP)中加上了一种特殊用途的报文机制,这种机制就是网际控制报文协议(Internet Control Message Protocol,ICMP)。这个协议作为 IP 的一部分,在每个 IP 实施中都必须包括在内。网关和主机使用这种机制传送控制信息或差错信息,网关使用这种机制报告递送过程中的问题,主机使用这种机制测试报宿主机是否可到达。

ICMP 报文的格式如图 2 所示,开始都有下面三段:一个 8 位整数报文 TYPE(类型)段,一个 8 位 CODE(码)段,提供更多的报文类型信息,一个 16 位 CHECKSUM(校验和)段,ICMP 所用校验和算法与 IP 相同,但只包含 ICMP 报文。此外,报告差错的

ICMP 报文总包含产生问题数据报的网际报头及前 64 位数据。返回的信息比数据报报头还多的原因是为了使接收者更准确地确定用了什么协议,以及什么应用程序对此数据报做出了响应。

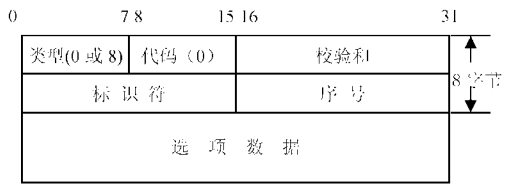


图2 ICMP 回应请求(类型“8”)/应答(类型“C”)报文格式

尽管 ICMP 报文也封装起来,并且用 IP 协议发送,但 ICMP 不是高层协议的内容,它只是 IP 中要求的一部分。ICMP 报文的封装如图 3 所示。每个 ICMP 报文都在 IP 数据报的数据部分中

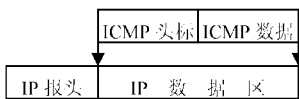


图3 ICMP 数据的封装

通过网际进行传输,而数据报本身又在帧的数据部分中穿过每个物理网。数据报载送 ICMP 报文经过选择的路由,完全像数据报载送用户信息一样,没有附加的可靠性与优先级。因此,差错报文本身也可能丢失或被弃掉。此外,在已经拥挤的网络中,差错报文可能造成额外拥挤。一个例外情况是,如果载送 ICMP 报文的 IP 数据报也出了差错时的差错处理过程,规定,当载送 ICMP 差错报文出了差错,不产生对应的 ICMP 报文,该例外是为了避免差错报文出了差错而产生差错报文的问题。

ICMP 报文在 IP 数据报的数据部分之中,像所有其他流通信息一样,经过网际进行传输。ICMP 报文最终报宿不是报宿计算机上的一个用户进程,而是那个计算机上的网际软件。也就是说,当一个有错误的 ICMP 报文到达时,IP 软件模块就处理本身问题,并不把这个 ICMP 报文传递给应用程序。

### 3 HSE 网络连通性自动监测

FF 的 HSE 系统中,通信出现故障时,如何判断网络是否连通是非常重要的,因为一旦通讯中断,生产线将陷于停顿,会直接影响到生产。此时的关键问题就是如何判断并发现网络不通,如何发现成组的失去联系的设备。这就要求主机或者设备具有 TCP/IP 协议中 Ping 程序的功能。而难题是如何快速发现网络不连通,一般我们可以通过 Ping 命令来及时的判断网段连通性,确保更快的发现网络故障。Ping 是一个 DOS 下的可执行文件,这个术语来源于网络互联报文探索(Packet Internetwork Groper)的缩写。Ping 报文是 IP 网络中能够生成和寻址的最小报文,在 Ping 程序执行过程中,双方计算机所消耗的资源都很少。其基本原理就是利用 TCP/IP 协议包中 ICMP 的 echo-request 和 echo-reply 功能进行工作,即向所指定的计算机发送一个请求,收到请求的计算机返回一个应答,借此来判断该计算机是否在网上运行或者检查网络连接是否稳定可靠。

Ping 程序的目的是为了测试另一个主机或设备是否可达,该程序传送 ICMP 回应请求报文给主机等,同时等待 ICMP 回应应答。最早的 Ping 程序由 Mike Muuss 编写,目的是为了测试另一台主机是否可达。该程序发送一份 ICMP 回应请求报文给主机,并等待返回 ICMP 回应应答。Ping 程序用到的 ICMP 报文格式如图 2。

一般来说,如果不能 Ping 到某台主机,那么就不能 Telnet 或者 FTP 到那台主机。反过来,如果不能 Telnet 到某台主机,那么通常可以用 Ping 程序来确定问题出在哪里。Ping 程序还能测出到这台主机的往返时间,以表明该主机离我们有多远。

网络管理员在工作中不可能既费时又费力地用手工去反复

执行 Ping 命令,系统必须提供能够对成组的 IP 地址快速地进行 Ping 操作的功能。

利用 DELPHI 编程实现 Ping 功能,首先对编程中需要的动态链接库作一简要说明,在 Windows 的 System 目录下,可以找到 lcmp.dll 文件,该动态链接库提供了 ICMP 协议的所有功能,我们的编程就是建立在对该动态链接库的调用上来实现的。lcmp.dll 文件内的调用函数说明如下: ① lcmpCreateFile: 打开一个句柄,通过该句柄发送 ICMP 的请求回送报文。② lcmpCloseHandle: 关闭通过 lcmpCreateFile 函数打开的句柄。③ lcmpSendEcho: 通过打开的句柄发送 ICMP 请求,在超时或应答报文接收后返回。

本软件构建了一个实现 Ping 功能的类 Tping。Tping 类是从 TObject 类中继承下来的,通过这个类,用户可以发送 ICMP 的请求报文。首先,生成一个 Tsocket 类的实例;接着,在该 Tsocket 类的实例上设置要测试站点的 IP 地址;随后,发送一个 ICMP 请求报文;同时,设置一个超时时间;在超时时限内收到返回的应答报文表明网络线路是正常的,超时未收到应答报文再发第二个请求报文,在一般情况下发送 3 个请求报文后,还未收到返回的应答报文表明网络线路中断,或者其他的网络故障。实现程序流程如图 4 所示。利用这个类可以通过反复设置它的目标地址,进行循环操作来对成组的地址进行 Ping 操作,同时在软件中设置定时器,周期性执行,从而达到对整个 HSE 网络连通性的动态监测。

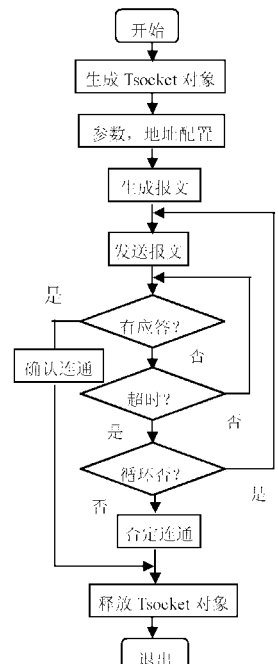


图4 ping 程序流程图

Tping 类有一个 ping 方法,通过这个方法,可以执行对某个 IP 地址的操作。具体使用代码如下:

```

Ping1:=Tping.create; //生成 Tping 的对象
Ping1.IP:=DestionAddress; //给对象指定目标地址
Ping1.OutTime:=3; //指定发送报文的次数
If Ping1.ping then //是否连通
  Showmessage('该地址可以连通')
Else
  Showmessage('该地址不通!');

```

### 4 结束语

随着工业以太网技术的不断完善和发展,HSE 已逐渐成为了现场总线的一个主流方向。本文通过对 HSE 网络模型的分析,利用网际控制报文协议(ICMP)实现一个 Ping 功能的软件,对 HSE 网络的连通性进行动态监测,为推动现场总线的发展作一些有益的探讨。

### 参考文献

- 1 谢希仁. 计算机网络(第 4 版).北京:电子工业出版社,2003
- 2 Steve Teixeira, Xavier Pacheco. Delphi 4 开发大全.北京:人民邮电出版社,1999
- 3 阳宪慧. 现场总线技术及其应用.北京:清华大学出版社,1999

[收稿日期:2004.9.15]