

工业以太网中嵌入式 TCP/IP 协议应用技术分析

李怀俊, 张学习, 章 云

(广东工业大学 自动化学院, 广东 广州 510090)

摘要:阐述了以太网主导工业自动化领域的必然性和优越性,给出了工业以太网的架构和实施要点,详细讨论了工业以太网技术中的关键之处——嵌入式 TCP/IP 通信协议栈的特点、开发及应用,最后就当前该技术的应用进一步做了总结和展望.

关键词:工业以太网;TCP/IP 协议;数据报;嵌入式控制模块

中图分类号:TP393.11

文献标识码:A

文章编号:1007-7162(2002)04-0025-05

以太网(Ethernet),既是一种计算机接入局域网络的连接标准,又是一种网络互联设备数据共享的通信协议.以太网采用具有冲突检测的载波监听多点接入(CSMA/CD)技术,主机只有在检测到线路空闲时才能发送数据,如果检测到冲突,即其它主机正在发送数据时,它会过一段时间再试发直至把数据发送出去.1990年9月,802.3i/10BASE-T标准正式通过,依靠新的10BASE-T中继器、双绞线介质(MAU)和NIC网络接口卡,以太网得到广泛应用.随后,快速以太网、交换式以太网等技术的出现使以太网在局域网中占据了主导地位.由于以太网传送速率的大幅度提高,物理层标准的工业化以及以太网集线器技术的形成,千兆以太网技术和无碰撞全双工光纤技术的出现,使得这一先进的网络技术被推进到早先认为不适宜的工业控制网络中,形成了工业以太网技术^[1].与目前基于现场总线的控制网络相比,基于工业以太网技术的控制网络是一种低成本、高性能的控制网络解决方案.这种高度开放、使用灵活方便、功能强大的新型工业控制网络将会以非常高的效率把企业的现场设备层、控制层以及管理层连接在一起,形成以网络集成自动化为基础的企业信息系统.

1 工业以太网技术分析

一般来讲,控制系统网络可分为3层:信息层、控制层和设备层(传感/执行层).传统的控制系统在信息层大都采用以太网,而在控制层和设备层一般采用不同的现场总线或其他专用网络.目前,以太网已经渗透到了控制层和设备层,几乎所有的PLC和远程I/O供应商都能提供支持TCP/IP的以太网接口产品.采用以太网架构以后,控制器的位置也可以突破传统网络架构的限制,可以位于现场,也可以位于中央控制室.目前控制器甚至远程I/O支持以太网的功能越来越强,在有些控制器和远程I/O模块中已经集成了Web服务器,从而允许信息层的用户也可以和控制层的用户一样直接获取控制器和远程I/O模块中的当前状态值.

工业以太网体系结构中(见图1),以太网作为连接智能控制模块的系统总线.集线器技术

收稿日期:2002-04-08

作者简介:李怀俊(1978-),男,2002级硕士研究生,主要研究方向为计算机工业网络控制.

被集成在每个控制器中,通过分配地址空间把内部通讯从外部通讯中分离出来.其中集线器技术和底层协议的集成,确保了以太网的确性、兼容性和整体性.TCP/IP 已成为标准网络协议,这是以太网正常运作的“中枢”.工业以太网技术中关键一环是:在现场级的节点控制模块(如远程 I/O 模块)中实现 TCP/IP 网络通信协议,即建立协议栈.随着电子和信息技术的高速发展,通过软件方式或硬件方式将 TCP/IP 协议嵌入到节点模块

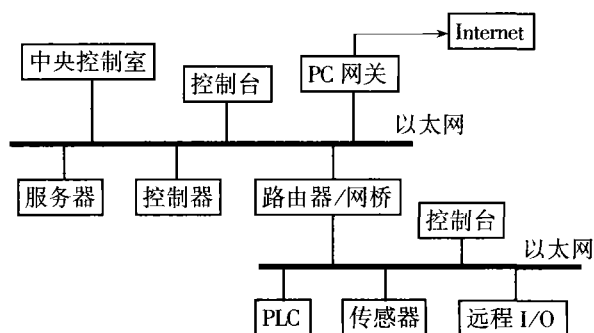


图 1 工业以太网结构图

已经成为可能^[2].软件方式将 TCP/IP 嵌入到微处理器的 ROM 中,硬件方式是设计嵌入式处理器和 ASIC 器件芯片,直接用作网络接口.下面具体分析网络协议栈的实现.

2 网络协议栈的实现

以太网是基于报文分组的网络,其网络协议通常分不同层次进行开发,每一层分别负责不同的通信功能,进而使相邻层按信息交换一致性原则通信.一个协议族,比如 TCP/IP,是一组不同层次上的多个协议的组合.TCP/IP 这种标准网络协议通常被认为是一个四层协议系统:数据链路层、网络层、传输层、应用层.每一层负责不同的功能.

1)数据链路层,也称为网络接口层.通常包括操作系统中的设备驱动程序和计算机中对应的网络接口卡.它们一起处理与电缆(或其他任何传输媒介)的物理接口细节.

2)网络层,也称作互联网层.处理分组在网络中的活动,例如分组的选路.在 TCP/IP 协议族中,网络层协议包括 IP 协议(网际协议)、ICMP 协议(Internet 互联网控制报文协议)以及 IGMP 协议(Internet 组管理协议).

3)传输层,主要为两台主机上的应用程序提供端到端的通信.TCP 为两台主机提供高可靠性的数据通信.它所做的工作包括把应用程序交给它的数据分成合适的小块交给下面的网络层,确认接收到的分组,设置发送最后确认分组的超时时钟等.由于运输层提供了高可靠性的端到端的通信,因此应用层可以忽略所有这些细节.

4)应用层,用户与网络的界面,负责处理网络信息,沟通各应用程序.应用层可为用户提供多种应用协议:如:HTTP 超文本传输控制协议;TELNET 远程登录;FTP 文件传输协议;SMTP 简单邮件传送协议;SNMP 简单网络管理协议等.

具体网络协议栈实现原理如图 2.因为数据链路层主要是网络接口卡及驱动,由网卡控制芯片(如 Realtek 公司的 RTL8019AS 芯片)来实现,所以下面讨论网络层、传输层和应用层协议栈的实现.

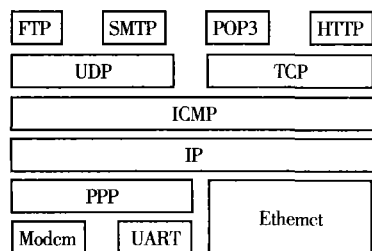


图 2 网络协议栈原理图

2.1 网络层

2.1.1 IP 协议

IP 是 TCP/IP 协议族中最为核心的协议.所有的数据都以 IP 数据报格式传输.IP 协议主要功能有:无连接数据报传送、数据报路由选择和差错控制.IP 不能保证数据报能成功地到达目

的地,仅提供最好的传输服务.若发生某种错误时,如某个路由器暂时用完了缓冲区,IP 有一个简单的错误处理算法:丢弃该数据报,然后发送 ICMP 消息报给信源端.任何要求的可靠性必须由上层来提供(如 TCP).无连接(connectionless)意即 IP 并不维护任何关于后续数据报的状态信息.每个数据报的处理是相互独立的.IP 数据报可以不按发送顺序接收.

IP 数据报的格式如图 3 所示.

0		3		7		15		23		31	
版 本		首部长度		服务类型		数据报长度					
标识						标志		片偏移			
生存时间		传输协议				表头校验和					
源地址											
目的地址											
选择项									填充		
数据											

图 3 IP 数据报格式

版本是指每个数据报所属的 IP 协议的版本号.目前的协议版本号是 4,因此 IP 也称作 IPv4.

首部长度指的是首部占 32bit 字的数目.由于它是一个 4 位字段,因此首部最长为 60 个字节.在这里,IP 数据报字段的最小值是 5.服务类型字段包括一个 3 位的优先权子字段(现在已被忽略)、4 位的 TOS 子字段和 1 位未用位但必须置 0.4bit 的 TOS 分别代表:最小时延、最大吞吐量、最高可靠性和最小费用.4bit 中只能置其中 1bit.如果所有 4bit 均为 0,那么就意味着是一般服务.数据报长度字段是指整个 IP 数据报的长度,以字节为单位.利用首部长度字段和总长度字段,就可以知道 IP 数据报中数据内容的起始位置和长度.

标识字段唯一地标识主机发送的每一份数据报;标志字段用来指定目的地址是一个完整的主机地址还是一个网络地址;生存时间字段设置了数据报可以经过的最多路由器数;表头校验和字段是根据 IP 首部计算的检验和码;源地址和目的地址都是 32 位的数据;选择项定义安全和处理限制、记录路径、时间戳、宽松的源站选路、严格的源站选路等信息.

2.1.2 嵌入式协议栈对 IP 层的实现

在嵌入式控制模块中开发协议栈,IP 层的实现就是对要发送的消息进行 IP 打包,即加上 IP 包头,使之符合 IP 数据包的格式发送到物理层;将接收到的来自物理层的数据包进行 IP 解包,即去掉包头,送到 TCP 层.对于 MTU(maximum transfer unit)较小的网络,数据报应分片,这也可以通过软件实现.

2.2 传输层

2.2.1 TCP 协议

TCP 提供一种面向连接的、可靠的字节流传送服务,它具有 5 个特征:面向数据流、虚电路连接、有缓冲的传送、无结构的数据流和全双工连接.一旦数据报被破坏或丢失,则由 TCP 将其重新传输.TCP 数据报的结构如图 4 所示.

每个 TCP 段都包含源端和目的端的端口号,用于寻找发端和收端应用进程.这两个值加上 IP 包头中的源端 IP 地址和目的端 IP 地址,唯一确定一个 TCP 连接.序号用来标识从 TCP 发端向 TCP 收端发送的数据字节流.它表示在这个报文段中的第一个数据字节.确认序号包含发

送确认的一端所期望收到的下一个序号;首部长度给出首部中 32bit 字的数目;紧急指针是一个正的偏移量,与序号字段中的值相加表示紧急数据最后一个字节的序号。

0		7		15		23		31	
源端口				目的端口					
序 号									
确认序号									
首部长度		保留		标 志		窗 口			
校验和				紧急指针					
可选项									
数 据									

图 4 TCP 数据报格式

2.2.2 嵌入式协议栈对 TCP 层的实现

在嵌入式模块协议栈中实现 TCP 时,为了保证 TCP 层的数据能有效地传输,在建立 TCP 连接时,用到了三段式握手机制^[3].TCP 协议栈支持同时建立两个 TCP 连接:一个为主动连接,另一个为被动连接.TCP 是基于连接的协议,因为必须保持对 TCP 连接状态的监视和状态有关的信息保存在发送控制块中;而 TCP 连接状态的改变由 TCP 的软件状态机来实现.软件状态机又由事件或用户来触发.比如,当监视到一个带有 SYN 标志的 TCP 包到达时,状态机就将 TCP 连接转换到接收状态;用户也可以手工控制状态机处于发送状态来建立 TCP 连接.建立了 TCP 连接,才可以发送或接收数据.接收数据时,上层协议(ULP)按字节发送,并被划分到 TCP 数据片中,经过状态机去掉 TCP 包头后再送到应用层;发送数据时,软件状态机会在数据前面加上 TCP 包头再发送到 IP 层.发送数据时,有一点值得关注:为了防止接收缓冲区的溢出,相对于发送数据包,协议栈给予接收数据包以更高的优先级.也就是说,协议栈软件会一直处理接收的数据包,直到接收缓冲区中没有任何数据.

2.3 应用层

2.3.1 HTTP 协议

HTTP 是关于在 Web 上进行文件交换的一组协议.当浏览器端的用户通过打开一个 Web 文件或单击一个超级链接,浏览器就将建立一个 HTTP 请求并把它传送给 URL 所描述的 IP 地址.目的服务端的 HTTP 邮件服务后台程序在收到请求后,进行必要的处理,然后将被请求的文件发送过去,完成信息交换.

2.3.2 嵌入式协议栈对 HTTP 层的实现

HTTP 通信建立在 TCP 连接之上,应用 TCP 的发送和接收函数来实行服务器的请求及相应命令,完成数据传输.Web 服务器运行一个守护进程(HTTP Daemon),始终在端口 80(缺省的 TCP 端口号)监听.对于控制网络模块,所有的 Web 资源都存放在外部存储器(EEPROM)中,HTTP 使用统一资源定位器(URL)来指定返回给客户端的网络资源.一般的解决方案是使用文件系统来管理外部存储器中的资源,另一方面,美国 UBIKOM 公司 SX52 芯片通过一种灵活的 Hush 算法来解决这个问题:当一个请求到来时,一个 8 位的无用信息对统一资源定位器进行运算(8 位字符加运算),再将得到的数据乘以 2,并把这个结果作为一个索引区中的一个值.如果在 EEPROM 中已经建立了查找表,凭着这个值在 EEPROM 中去查表,找到相应的资源并返回.用这种方法的好处是可以避免繁琐的字符串的比较和将 URL 直接存放在服务器中^[4].

3 应用和展望

随着嵌入式技术的发展,工业控制领域越来越多地利用这方面的软、硬件,在单片机系统上实现以太网技术.以嵌入式设备为中心的网络架构正是今后工业网络发展的方向.例如,由美国 UBICOM 公司推出的 SX 系列单片机组成的嵌入式系统,可实现实时多任务操作,可在 MCU 执行数据采集和控制功能的同时把数据打包并传送到网络上.利用其虚拟外设功能可直接驱动 I/O 口实现硬件外设功能,并可直接运行流行的网络协议栈(如 HTTP、TCP、UDP、IP 等).

总之,基于统一的网络平台,开发者可根据各自需要开发软件化或硬件化的不同的 TCP/IP 通信协议栈,并将之与嵌入式微处理器结合,以工业以太网技术标准实现物理层和数据链路层,形成工业网络中控制级智能模块,通过 Internet 接口与上层进行通信,实现与 Internet 的无缝联结和内置 WebServer 的功能,从而建立满足要求的工业以太网.展望未来,现场数据量将越来越大,实时控制的要求也越来越高,控制系统的复杂程度也不断加深,工业以太网可强有力地担负起这一重任.也许在不远的将来,正是这一技术真正实现了工业控制的全面网络化和自动化,我们拭目以待.

参考文献:

- [1] 阳宪惠.现场总线技术及其应用[M].北京:清华大学出版社,2000.70-83.
- [2] Real-time Control on Ethernet, A ControlNet International White Paper [EB/OL]. <http://www.controlnet.org>, 2000, 3.
- [3] 佟震亚,余雪丽,陶世群.现代计算机网络教程[M].北京:电子工业出版社,2001.101-133.
- [4] 许华杰,明健.基于 SX 单片机实现 WebServer 和网络协议栈[J].单片机与嵌入式系统应用.2001,(8):10-13.
- [5] Ethernet SX-Stack Internet Connectivity[EB/OL]. <http://www.UBICOM.com>,000,8.

Technical Analysis Using Embedded TCP/IP Protocol in Industrial Ethernet

LI Huai-Jun, ZHANG Xue-Xi, ZHANG Yun

(Faculty of Automation, GDUT, Guangzhou 510090, China)

Abstract: This paper expatiates the necessity and superiority on Ethernet leading industry automation field, points out the frame of Industrial Ethernet. The specialty, research and use of Key-point(embedded TCP/IP protocol)of industrial Ethernet technology are discussed in detail. Summary and prospect are made on the use of this technology lastly.

Key words: industrial Ethernet; TCP/IP protocol; data package; embedded control module