

SIEMENS

(下册)

西门子工业网络通信指南

Siemens Industrial Communication Guide

崔坚 主编 李佳 杨光 副主编

guide

Industrial Communication Guide



西门子(中国)有限公司
自动化与驱动集团



机械工业出版社
CHINA MACHINE PRESS

西门子工业网络通信指南

(下 册)

崔 坚 主编 李 佳 杨 光 副主编



机械工业出版社

本书从网络通信的实际应用出发,以西门子常用的工业协议为脉络,基于西门子工业控制产品和系统,分上、下两册分别以清晰易懂的理论、丰富详实的通信实例,并结合多年的实践经验,全面地介绍了西门子工业自动化控制系统基于各种协议的通信方式及其具体应用。

上册分为三章,从第4章到第10章分别介绍了MPI和PROFIBUS协议及各种通信方式。

下册分七章,分别对工业以太网通信、网络路由功能、PROFINET I/O与CBA、ASI通信、S7-200的PPI通信、串行通信和SINAUT远程通信等多种通信方式进行了详细的介绍,详述了相关网络协议和网络通信的各种形式、网络组件及各种通信方式的组态、编程和故障诊断方法,每种方式均配以具体案例加以说明。

书中每个通信案例互为独立单元、深入浅出、条理清晰、内容完整,并配有大量的例图与程序,深入细致地阐述了通信协议的各个方面,便于读者学习和掌握。

随书附带的光盘提供了书中所有的应用实例、程序源代码以及技术文档等。

本书适合广大工业产品用户、系统工程师、现场工程技术人员、大专院校相关专业师生,以及工程设计人员借鉴和参考。

图书在版编目(CIP)数据

西门子工业网络通信指南.下册/崔坚主编.一北京:
机械工业出版社,2005.6

ISBN 7-111-16508-X

I.西... II.崔... III.计算机网络-计算机通信
-指南 IV.TN915-62

中国版本图书馆CIP数据核字(2005)第043009号

机械工业出版社(北京市百万庄大街22号 邮政编码100037)

责任编辑:林春泉 版式设计:张世琴 责任校对:刘志文

责任印制:陶湛

北京铭成印刷有限公司印刷·新华书店北京发行所发行

2005年5月第1版第1次印刷

787mm×1092mm 1/16·28.5印张·704千字

00 001—10 000册

定价:58.00元(含1CD)

凡购本书,如有缺页、倒页、脱页,由本社发行部调换

本社购书热线电话(010)68326294

封面无防伪标均为盗版

编委会名单

主 编：崔 坚
副主编：李 佳 杨 光
编 委：陈 志 柳 杰 龚笠宁
 李 凯 王 威 葛 蓬
 刘 错

序

“自动化是工业现代化取得成功的要素。”虽然自动化技术只有 50 年的历史，但是它在确保生产高效、优质和精确等各个方面扮演着举足轻重的角色，并成为衡量工业现代化水平的重要标志。西门子公司致力于自动化和驱动产品以及系统的不断创新，并将西门子技术的各种应用汇集在《西门子工业网络通信指南》一书中，呈现给读者，希望能为设计院的设计人员和工厂的工程师以及高校相关专业的广大师生提供有力的支持和帮助。

工业的现代化，很大程度体现在工业生产过程的自动化，其中信息的传输，数据的交换也成为评判工业自动化水平的因素。从 20 世纪末到 21 世纪初，随着计算机与计算机网络技术的不断进步，工业网络在此期间展开了一场轰轰烈烈的革命。20 年来计算机技术的不断发展，使计算机网络有着非常成功的历史，现在将它们借鉴到工业自动化的领域中来，使其应用范围更加广泛，也使工业用户有了更多可以选择的解决方案。

现场总线技术的出现，现场设备的智能化以及 IT 技术与自动化技术的日趋融合，使得工业自动化产业面临变革性的挑战。网络技术在工业中所占的比重越来越大。西门子作为工业自动化的知名厂商，引领着工业自动化与驱动技术发展的方向，与此同时满足各个行业用户的不同需求。丰富的产品类型，多元化的通信方式为工业用户提供支持，同时也为自动化与驱动领域的发展提供了动力。

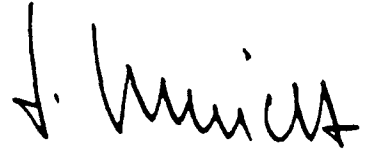
工业网络知识已经成为当今自动化过程应用中的重要内容，并深入到工业自动化的各个层次当中，从现场设备、可编程控制器、I/O 设备等硬件组件到操作系统、驱动设备以及人机接口、网络的应用可谓无处不在。

《西门子工业网络通信指南》一书，正是在网络应用日益广泛的环境下，本着全面而清晰、服务用户、方便用户的原则，以西门子公司工程师多年积累的经验潜心编写的，是西门子自动化与驱动集团提供给广大工业用户的有力网络技术支持之一。在产品覆盖方面，内容全面而具代表性，50 余个精心挑选的实例，从 PLC 可编程控制器、PC 通信模板到变频器、上位机，以及 HMI 人机界面，各种通信方式与步骤都包含其中；在通信类型方面，从 MPI、PROFIBUS 到工业以太网、ASI 通信以及 SCADA 远程通信，以便给更多用户提供工业网络技术和应用的参考与支持。

目前，在世界范围的工业总线标准中，PROFIBUS 总线在工业现场中的应用已经达到 10 000 000 个节点。它符合国际标准 IEC 和欧洲标准 EN50170，清晰简单的接线、标准化的接口和精简的协议结构，使设备之间保持可靠而高速的数据交换。在中国，PROFIBUS 总线是当今总线标准中最早成为中国机械行业标准的总线之一，在中国的过程自动化和工厂自动化领域都有着成功而广泛的应用。同时，工业以太网也是工业用户多为选用的网络模式。它提供了针对制造业控制网络数据传输的以太网标准，具有更多的安全性、可操作性和实用性，更大程度地满足了用户和生产厂商的需要。非常高兴地看到，即将付梓的《西门子工业网络

通信指南》一书中，对用户经常用到的几种网络类型在不同产品之间的配置和应用进行了详细的介绍。

希望《西门子工业网络通信指南》一书能为更多的工业用户提供有力的支持和有效的解决方案，同时也为工业网络的进一步发展发挥它的一份作用。



施密特

西门子(中国)有限公司

执行副总裁

自动化与驱动集团总经理

2005年5月

Preface

“Automation is the key to success for industrial modernization.” It plays a key role in all kinds of process of production, for example, it ensures high efficiency, good quality, accurate logistic control, even though it is still a young technology with only about 50 years history. Siemens committed a lot as innovation trendsetter in the field of automation and drives with reliable product and system. This book presents readers the collection of dedicated applications of Siemens technology, which we hope quite helpful for electric designers of design institute, engineers of factory of engineering company and students.

To a large extent, industrial modernization is reflected in the automation of industrial production processes, of which information transmission and data exchange have become factors to consider in evaluating the level of industrial automation. With the steady progress in computer and computer network technologies, a dynamic revolution has been taking place in industrial networks from the late 20th century to the early 21st century. The steady development of computer technology in the past twenty years has led to the successes in the technological advance of computer networks. Now these technologies have been used in the field of industrial automation, which broadens the range of applications of these technologies and provides industrial customers with more solutions to choose.

The appearance of field bus technology, the development of intellectual field devices, and the blending of IT and automation technology have brought transforming challenges for industrial automation. Network technology is playing an increasingly important role in industries. As a prestigious manufacturer in the field of industrial automation, Siemens has been leading the technological development of industrial automation and drives, meeting the different needs of customers in different industries. With a large variety of products and plural communication methods, Siemens provides technological support for industrial customers and gives impetus to development in the field of automation and drives.

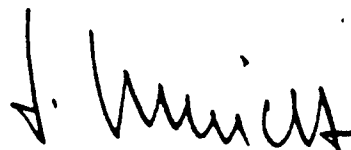
Industrial network technology has become an important part in the automation process in modern times and has been used in different levels in industrial automation, ranging from hardware components like field devices, PLCs and I/O devices to operation systems, drive devices and human machine interfaces. The application of networks can be found everywhere.

Siemens Guidebook for Industrial Network Communication is written by diligent Siemens engineers with their accumulated experience of many years in the context of increasingly widespread network applications and under the principles of “completeness and clarity” and “offering convenient services to customers”. It is a powerful support in network technology from Siemens Automation and Drives for industrial customers. In the aspect of product coverage, over 50 complete and representative practical cases have been carefully selected, ranging from PLCs and PC communication templates to frequency converters, host computers and to HMI, different communication methods and procedures; and in the aspect of types of communication, from MPI, PROFIBUS to industrial Ethernet, ASI communication and SCADA telecommunication, in order to provide more customers with references and support in industrial network

technology and application.

Presently, in the standards of industrial buses worldwide, the field application of PROFIBUS in industries has reached 10,000,000 nodes. It conforms to IEC Standards and EN 50170 Standards. With its clear and simple wire splices, standardized interfaces and concise protocol structure, it ensures reliable and high-speed data exchange between different devices. In China, PROFIBUS is one of the first buses among the present bus standards to become the standard of Chinese machinery industry and is successfully and widely used in the fields of process automation and factory automation in China. In the mean time, the Industrial Ethernet is also one of the most popular network chosen by industrial users. It provides Industrial Ethernet standard for data transfer in all kinds of automatic control network. Especially, the high security, operability and real time data transfer can meet the demand well of different automatic system. It is pleasing to see that the configuration and application of several networks in different products that customers frequently use are detailedly described in Book II of *Siemens Guidebook for Industrial Network Communication*, which is to be sent to press soon.

It is hoped that *Siemens Guidebook for Industrial Network Communication* can provide powerful support and effective solutions for more industrial customers and meanwhile contribute to the further development of industrial networks.



Siegfried Schmidt
Executive Vice President
GM of A&D Group
Siemens Ltd., China
May, 2005

前 言

随着现代信息技术和计算机技术的不断发展，分布式控制系统在工厂自动化和过程自动化中的应用迅速增长，现场总线技术已成为工业通信中的佼佼者。网络通信方式的多样化和通信速度的提高，使信息交换领域从现场设备控制层到企业管理层的不断扩大。信息技术的飞速发展，引起了自动化系统结构的变革，以网络为主干的自动化分布式控制系统成为行业趋势。由此，网络通信的实时性和可靠性，以及网络故障的智能诊断和排除都成为工业通信关注的焦点。通信在自动化系统中无处不在，它是整个自动化控制系统的灵魂。

作为全球先进自动化技术的引领者，不论在控制系统的核心部分——可编程控制器，还是自动控制系统的神经系统——通信网络，西门子公司都引领着技术创新的潮流。由于网络通信要同时兼顾其稳定性、快速性、灵活性和相互之间的兼容性，因而网络往往成为自动控制系统设计和实施中的难点，为此西门子的资深工程师们凭借多年现场经验和基于对西门子自动化系统的认识，以实例的方式编写了《西门子工业网络通信指南》。本书从 MPI 协议、PROFIBUS 总线到功能强大的工业以太网以及灵活的 ASI 总线等，以清晰明了的实例，结合多年积累的应用经验，将西门子工业网络技术的原理及应用娓娓道来。

《西门子工业网络通信指南》在内容的编写上力求实用性与先进性并举。它以通信协议为主要脉络，覆盖从现场到控制器和人机界面的各级工控产品。因此，《西门子工业网络通信指南》一书并非只涉及通信，而是在梳理通信脉络的同时，将西门子全集成自动化(TIA-Totally Integration Automation)的理念贯穿于整个系统中。本书重点突出，覆盖全面，它具有如下特点：

1. 全面性

本书分为上下两册，涵盖西门子网络通信中常用的各种通信方式。上册主要以 MPI (Multi Point Interface) 通信和 PROFIBUS (PROCESS FIELD BUS) 通信协议为主。在下册中，则以工业以太网、ASI 总线、串口通信以及其他特殊通信方式等为主线，以实例的形式全面展开，深入浅出，将各种通信方式从原理到编程、组态进行了详细阐述。

工业以太网是许多大型工业控制系统中常用的通信方式。在工业以太网一章中，介绍了 S7-200、S7-300、S7-400 以及 S5 之间的以太网通信实例。

网络路由功能详细地说明了网络路由的特点和使用方法，为工业用户的使用提供了更多的方便。

ASI 通信是连接传感器与执行器机构常用的通信方式。PPI 网络和串行通信也是工业网络用户较常接触的通信模式。特别针对用户的应用和经常提出的问题构建了网络模式，并提供了解决方案。

在本书下册中，用一章的篇幅介绍了新一代的自动化总线标准——PROFINET，为工业网络用户提供了最先进的技术方案，以方便用户选择。下册中列举了各种协议在不同产品之间的通信实例 40 余例，给予用户在网络通信上的更多支持。

2. 实用性

由于工业网络的覆盖范围不断地扩大,从现场设备、现场仪器仪表到上位监控系统,通信贯穿整个自动化系统的始终。本书的编写以通信为主线,辅以大量的图示进行说明,具有指导性强,适用范围广的特点。从控制器与控制器、控制器与变频器以及控制器与人机界面产品等之间的通信,通过已实现的具体实例,将通信的连接和组态步骤作了清晰描述,具有较强的实用性。每个例子自成一个独立单元,方便读者直接学习和引用。它既适用于具有先进设备的大型厂家和企业,又适用于一些规模较小的企业;既阐述了现场级设备之间的通信,又阐述了现场级与车间级系统之间的通信。

此外,由于在实际应用中,可能出现的多种多样的通信故障,所以本书单独辟出一节,介绍了通信故障的检测、诊断及排除方法,内容丰富详实、方法简单有效。

3. 先进性

随着各种技术的发展,自动化产品以及通信技术都在更新换代,所以许多自动化厂家是新、老系统同时运行,本书兼顾用户的利益和需求,在阐述新一代先进控制系统之间通信的同时,也详述了新老产品之间的通信(如在 Ethernet 通信中的 S7 与 S5 控制器的通信)。

为了帮助读者了解英文缩写,作者将在本书中涉及到的缩写词及具体解释列在书后的缩略语注释表中,并进行了说明。随书附带的光盘中提供了书中所有的通信例子和源程序代码,用户可直接用 STEP 7 软件解压缩并打开这些项目,作进一步解析。

在本书即将出版时,特别要感谢西门子(中国)有限公司副总裁,前自动化与驱动集团总经理 Mr. Siegfried Schmidt 为本书撰写序言。同时,本书还得到了西门子(中国)有限公司自动化与驱动集团相关部门领导及众多同事的大力支持和指导,他们是西门子(中国)有限公司自动化与驱动集团技术支持与服务总经理王平先生、自动化系统部总经理安晓杰先生、市场部总经理于缨女士、OEM 总经理刘志生先生、自动化系统部经理陈海东先生、张劲松先生、华东区技术支持部经理叶时针先生、北方区技术支持部经理李劲松先生和西门子武汉分公司自动化与驱动集团总经理谢兵先生等,在此特别鸣谢。

本书主编——西门子(中国)有限公司自动化与驱动集团技术支持与服务部高级工程师崔坚先生和副主编李佳女士、杨光先生,以及编委陈志先生、柳杰先生、龚笠宁先生和李凯先生等对本书的编写和审核付出了辛勤汗水,并致以诚挚的谢意。本书的编写还得到了西门子(中国)有限公司自动化与驱动集团的相关工程师和产品经理给予的大力支持,在此一并表示深深的谢意。

无论您是西门子的工业产品用户、工业自动化领域的工程技术人员,还是学习工业网络通信的设计人员以及各大院校相关专业的师生,《西门子工业网络通信指南》一书都能成为您的良师益友,为您提供相关技术支持,为您的成功助一臂之力。

由于本书编写时间仓促,书中错误和不足之处在所难免。诚恳希望各位专家、学者、工程技术人员以及所有的读者批评指正,我们将衷心感谢您的赐教,谢谢!

西门子(中国)有限公司 自动化与驱动集团
技术支持与服务部系统支持经理
王 威
2005年5月于北京

目 录

序
前言

第 4 章 工业以太网通信

4.1 以太网简介	1
4.1.1 以太网的诞生	1
4.1.2 以太网的发展历史	2
4.1.3 以太网技术	2
4.2 工业以太网	6
4.2.1 与传统以太网络的比较	6
4.2.2 以太网应用于工业自动化中的 关键问题及发展方向	7
4.2.3 以太网为用户带来的利益	7
4.3 西门子工业以太网	8
4.3.1 什么是 SIMATIC NET	8
4.3.2 SIMATIC NET 工业以太网	8
4.4 S7-200 的以太网解决方案	31
4.4.1 硬件连接	32
4.4.2 硬件需求和软件需求	32
4.4.3 网络组态及参数设置	32
4.5 S7-200 的以太网 IT 解决方案	65
4.5.1 硬件连接	65
4.5.2 硬件需求和软件需求	65
4.5.3 网络组态及参数设置	66
4.6 S7-300/400 的以太网解决方案	85
4.6.1 西门子支持的网络协议和服务	85
4.6.2 网络连接	87
4.6.3 硬件需求和软件需求	87
4.6.4 S7 通信 (S7 Communication) 网络组态及参数设置	88
4.6.5 S5 兼容的通信网络组态及 参数设置	95
4.7 S7-300/400 的工业以太网 IT 解决方案	110

4.7.1 IT-CP 的属性和服务	110
4.7.2 E-mail 功能	111
4.7.3 FTP 通信	117
4.7.4 IT-CP 的 Web Server 功能	132
4.8 SIMATIC S5 和 SIMATIC S7 通过 工业以太网 SEND/RECEIVE (ISO 连接) 方式进行通信	138
4.9 SIMATIC S5、S7 系统间 通过工业以太网 FETCH/WRITE 连接进行通信	149
4.10 WinCC 通过 Layer 4 通道与 SIMATIC S5 的通信	164
4.11 SIMATIC S5 PLC 通过工业以太网 Send/Receive 接口与 SIMATIC Net OPC Server 通信	172

第 5 章 网络路由功能

5.1 概述	188
5.2 支持网络路由功能的设备	188
5.3 网络路由的编程功能	188
5.4 组态编程器的网络路由功能	190
5.5 HMI 的网络路由功能	193
5.5.1 OP/TP 的网络路由功能	193
5.5.2 组态 OP/TP 的网络路由功能	193
5.5.3 上位机网络路由功能	194
5.5.4 组态 S7 OPC Server 的网络路 由功能	196
5.6 网络路由功能小结	198

第 6 章 PROFINET IO 与 CBA

6.1 什么是 PROFINET	199
6.2 PROFINET 的实时性	199
6.3 PROFINET 的主要应用	201
6.4 在 PROFINET 网络中集成	

现有总线系统	201	7.7.3 使用 DP/ASI Link 的 ASI 通信	267
6.5 PROFINET IO	201	第 8 章 S7-200 的 PPI 通信	
6.6 PROFINET CBA	207	8.1 概述	277
6.6.1 PROFINET 组件	207	8.2 S7-200 的 PPI 通信举例	278
6.6.2 SIAMTIC IMAP	207	8.3 S7-200 的 OPC 通信	284
6.6.3 PROFINET 的数据类型	207	第 9 章 串行通信	
6.6.4 PROFINET 组件的设备类型	208	9.1 串行通信概述	287
6.6.5 PROFINET 设备	209	9.2 串行通信接口类型	287
6.6.6 PROFIBUS 设备	209	9.3 ASCII 驱动	291
6.6.7 PROFINET 组件的生成	211	9.3.1 通信方式的参数化	291
6.6.8 生成 PROFIBUS 设备的组件	218	9.3.2 ASCII 驱动通信举例	294
6.6.9 连接各组件的通信接口	222	9.3.3 ASCII 驱动常用通信方式	300
6.6.10 连接上位监控软件	227	9.3.4 DP/232C LINK ASCII 驱动应用	302
6.6.11 PROFINET 设备间的 实时通信	230	9.4 3964 (R) 协议	308
第 7 章 ASI 通信		9.4.1 3964 (R) 协议报文格式	308
7.1 ASI 概述	235	9.4.2 3964 (R) 通信协议的参数化	309
7.1.1 ASI 产生原因	235	9.4.3 3964 (R) 协议通信举例	311
7.1.2 ASI 总线特点	236	9.5 RK512 协议	316
7.2 ASI 系统构成	236	9.5.1 RK512 协议报文格式	316
7.2.1 ASI 主站	236	9.5.2 RK512 通信协议的参数化	318
7.2.2 ASI 从站	237	9.5.3 RK512 协议通信举例	321
7.3 ASI 总线拓扑结构	241	9.6 CP441 通信处理器的应用	327
7.3.1 ASI 总线拓扑类型	241	9.6.1 ASCII 协议与 3964 (R) 协议 调用的通信功能块	327
7.3.2 ASI 总线连接方式	242	9.6.2 RK512 协议调用的通信功能块	331
7.4 ASI 传输机制	243	9.7 MODBUS 通信	336
7.4.1 信号调制过程	243	9.7.1 MODBUS 通信协议 串行接口类型	336
7.4.2 数据解耦	244	9.7.2 西门子 PLC 支持 MODBUS 的 通信处理器 (CP)	337
7.4.3 访问方式和报文结构	244	9.7.3 MODBUS 通信协议简介	337
7.4.4 传输故障特征	244	9.7.4 MODBUS RTU 主站通信 协议及参数化	338
7.5 ASI 从站编址	245	9.7.5 MODBUS RTU 主站通信举例	341
7.5.1 通过手持编址单元编址	245	9.7.6 MODBUS RTU 从站通信 协议及参数化	345
7.5.2 通过 ASI 主站编址	246	9.7.7 MODBUS RTU 从站通信举例	349
7.6 ASI 主站的操作模式	246		
7.7 ASI 通信举例	247		
7.7.1 S7-200 系统的 ASI 通信	247		
7.7.2 S7-300 系统主站 CP343-2P 的 ASI 通信	257		

9.8 PLC 与驱动装置串行通信			
(USS 协议)	352		
9.8.1 USS 通信功能块	353		
9.8.2 驱动装置 USS 端口的设置	355		
9.8.3 USS 通信举例	357		
第 10 章 SINAUT 远程通信			
10.1 概述	363		
10.1.1 SINAUT ST7 系统	363		
10.1.2 SINAUT ST7 系统结构	364		
10.1.3 SINAUT ST7 系统特点	365		
10.2 SINAUT ST7 系统组件	366		
10.2.1 SINAUT ST7 系统硬件	366		
10.2.2 SINAUT ST7 系统标准软件包	374		
10.2.3 SINAUT ST7cc 系统			
		标准软件包	376
		10.3 SINAUT 网络拓扑结构	377
		10.4 SINAUT 系统硬件设置	379
		10.4.1 连接和设置 TIM3 模块	379
		10.4.2 连接和设置 TIM4 模块	387
		10.4.3 MD 的设置方法	391
		10.4.4 CPU300/400 连接 TIM 的方法	397
		10.5 SINAUT 站点间通信	397
		10.6 上位控制中心与 SINAUT	
		远程站间通信	410
		10.7 路由编程功能	434
		10.8 GPRS 通信	434
		缩略语	436
		参考文献	439

第 4 章 工业以太网通信

随着信息技术的发展,信息交换技术覆盖了各行各业。在自动化领域,越来越多的企业需要建立包含从工厂现场设备层到控制层、管理层等各个层次的综合自动化网络管控平台,建立以工业控制网络技术为基础的企业信息化系统。

工业以太网提供了针对制造业控制网络的数据传输的以太网标准。该技术基于工业标准,利用了交换以太网结构,有很高的网络安全性、可操作性和实效性,最大限度地满足了用户和生产厂商的需求。工业以太网以其特有的低成本、高实效、高扩展性及高智能的魅力,吸引着越来越多的制造业厂商。

4.1 以太网简介

4.1.1 以太网的诞生

以太网技术的思想渊源最早可以追溯到 1968 年。以太网的核心思想是使用共享的公共传输信道,这个思想来源于夏威夷大学。

上个世纪 60 年代末,夏威夷大学的 Norman Abramson 及其同事研制了一个名为 ALOHA (夏威夷人问候语,即“欢迎、再见”的意思)系统的无线电网络。

Metcalfe 是在世界著名的研究机构—Xerox 的帕洛阿尔托研究中心(PARC)的计算机科学实验室工作的网络专家。

1972 年底, Metcalfe 和 David Boggs 设计了一套网络,用于将不同的 ALTO 计算机连接起来,同时又把 NOVA 计算机连接到 EARS 激光打印机。在研制过程中, Metcalfe 将其命名为 ALTO ALOHA 网络,因为该网络以 ALOHA 系统为基础,同时连接了众多的 ALTO 计算机。这个世界上第一个个人计算机局域网——ALTO ALOHA 网络首次在 1973 年 5 月 22 日开始运转。这一天, Metcalfe 写了一段备忘录,称他已将该网络改名为以太网(Ethernet),其灵感来自于“电磁辐射是可以通过发光的以太来传播的这一想法”。最初的实验型 PARC 以太网以 2.94Mbit/s 的速度运行。

1976 年, PARC 的实验型以太网已经发展到 100 个节点,在长 1000m 的粗同轴电缆上运行。1976 年 6 月, Metcalfe 和 Boggs 发表了题为《以太网:局域网的分布型信息包交换》的著名论文。1977 年底,多点传输系统被称为 CSMA/CD (Carrier Sense Multiple Access with Collision Detection network,带碰撞检测的载波侦听多址访问)。从此,以太网诞生了。1979 年, DEC (Digital Equipment Corp,数字设备公司(美国)、Intel 和 Xerox 共同将此网络标准化,正式定名为以太网。

4.1.2 以太网的发展历史

- Xerox PARC 创建首个以太网(1972 ~ 1977)
- DEC、Intel 和 Xerox 将以太网标准化(1979 ~ 1983)
- 1989 年 ISO 以标准号 ISO8023 采纳 802.3 以太网标准,至此,IEEE (Institute of Electrical and Electronics Engineers, 电工与电子工程师学会)标准 802.3 正式得到国际上的认可
- 交换式和全双工制以太网出现(1990 ~ 1994)
- 快速型以太网出现(1992 ~ 1995)
- 工业趋势(1995)
- 千兆位以太网出现(1999)

4.1.3 以太网技术

在局域网家族中,以太网是指遵循 IEEE 802.3 标准,可以在光缆和双绞线上传输的网络。以太网也是当前主要应用的一种局域网(LAN——Local Area Network,局域网)类型。目前的以太网按照传输速率大致分为以下四种:

- 10Base-T 以太网——传输介质是同轴电缆,传输速率为 10Mbit/s;
- 快速以太网——传输速率为 100Mbit/s,采用光缆或双绞线作为传输介质,兼容 10Base-T 以太网;
- Gigabit 以太网——扩展的以太网协议,传输速率为 1Gbit/s,采用光缆或双绞线作为传输介质,基于当前的以太网标准,兼容 10Mbit/s 以太网和 100Mbit/s 以太网的交换机和路由器设备;
- 10Gigabit 以太网——2002 年 6 月发布,是一种速度更快的以太网技术。支持智能以太网服务,是未来广域网(WAN——Wide Area Network)和城域网(MAN——Metropolitan Area Network)的宽带解决方案。

1. OSI 参考模型

通信网络的核心是 OSI (OSI——Open System Interconnection,开放系统互联)参考模型。为了理解互联网络的操作方法,为创建和实现网络标准、设备和网络互联规划提供的一个框架。1984 年,国际标准化组织(ISO——International Organization for Standardization)提出了开放系统互联的七层模型,即 OSI 模型。该模型自下而上分别为:物理层、数据链路层、网络层、传输层、会话层、表示层和应用层,如图 4-1 所示。

OSI 参考模型的上三层通常称为应用层,用来处理用户接口、数据格式和应用程序的访问;下四层负责定义数据的物理传输介质和网络设备。OSI 参考模型提供了大多数协议栈共有的基本框架,如图 4-2 所示。

物理层——定义了传输介质、连接器和信号发生器的类型,规定了物理连接的电气、机械功能特性如电压、传输速率、传输距离等特性。

数据链路层——确定传输站点物理地址以及将消息传送到协议栈,提供顺序控制和数据流控制。该层可以继续分为两个子层:介质访问控制层(MAC——Medium Access Control,介

质访问控制层)和逻辑链路层(LLC——Logical Link Control(layer)逻辑链路控制(层)),即层2a和2b。其中IEEE 802.3(Ethernet,CSMA/CD)就是MAC层常用的通信标准。

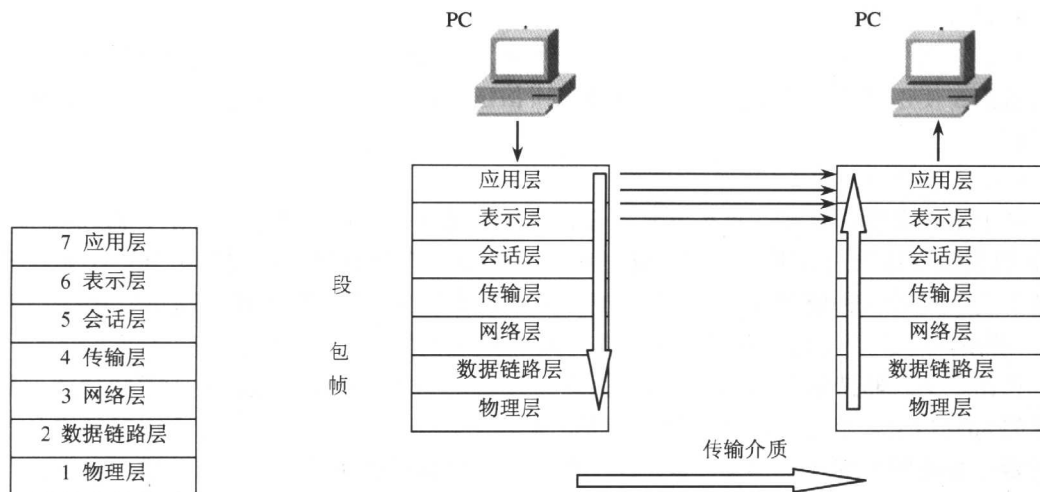


图 4-1 OSI 参考模型

图 4-2 数据传输过程

网络层——定义设备间通过逻辑地址(IP——Internal Protocol,因特网协议地址)传输数据,连接位于不同广播域的设备,常用来组织路由。

传输层——建立会话连接。分配服务访问点(SAP——Service Access Point,服务访问点),允许数据进行可靠(TCP——Transmission Control Protocol,传输控制协议)或不可靠(UDP——User Datagram Protocol,用户数据报协议)的传输。可以提供通信质量检测服务(QoS——Quality of Service,服务质量)。

会话层——负责建立、管理和终止表示层的实体间通信会话,处理不同设备应用程序间的服务请求和响应。

表示层——提供多种编码用于应用层的数据转化服务。

应用层——定义用户及应用程序接口与协议对网络访问的切入点。目前各种应用版本较多,很难建立统一的标准。在工控领域常用的标准是MMS(Multimedia Messaging Service,多媒体信息服务)(制造业消息规范),用来描述制造业应用的服务和协议。

数据经过封装后通过物理介质传输到网络上,接收设备除去附加信息后,将数据上传到上层堆栈层。

2. CSMA/CD 技术

在传统的共享网络中,由于以太网段中的所有站点采用相同的物理介质相连,这就意味着两台设备同时发送信号时,就会出现信号间的互相冲突。为了解决这个问题,以太网规定,在一个站点访问介质前,它首先必须监听网络上有没有其他的站点在同时使用该介质。如果介质被使用,则该站点在发送前必须等待。这就是CSMA/CD技术。为了减少冲突发生的几率,出现了一些算法,常用的有:

• 1-持续 CSMA

当一个站点要传送数据时,它首先监听信道,看是否有其他站点正在传送。如果信道正忙,它就持续等待,直到当它监听到信道空闲时,便将数据送出。若发生冲突,站点就等待

一个随机长的时间, 然后重新开始。此算法被称为 1-持续 CSMA, 因为站点一旦发现信道空闲就发送数据, 其发送数据的概率为 1。

- 非持续 CSMA

在发送之前, 站点会监听信道的状态, 如果没有其他站点在发送, 它就开始发送。但如果信道正在使用之中, 该站点将不再继续监听信道, 而是等待一个随机的时间后, 再重复上述过程。

- p -持续 CSMA

一个站点在发送之前, 首先监听信道, 如果信道空闲, 便以概率 p 传送, 而以概率 $q = 1 - p$ 把该次发送推迟到下一时隙。此过程一直重复, 直到发送成功或者另外一个站点开始发送为止。在后一种情况下, 该站的动作与发生冲突时一样(即等待一随机时间后重新开始)。若站点一开始就侦听到信道忙, 它就等到下一时隙, 然后开始上述过程。

相比之下, 非持续型 CSMA 可以大大减少冲突可能性, 能使系统的最大吞吐量达到信道容量的 80% 以上。但由于随机延迟侦听的原因, 将会使系统对帧传输的响应时间变长, 也即时延一吞吐特性变坏。相反, p -持续 CSMA 既考虑到尽快使用已空闲的信道, 又考虑到发送帧时的主动退避, 在性能上比非持续型 CSMA 的性能好。需要说明的是, 对于极端时的 1-持续 CSMA 方式, 在通信负载很小时, 帧的发送机会多, 响应也快, 但若站点数增多或总的负载增加时, 冲突的机会急剧增加, 吞吐特性和时延特性均急剧变坏, 其性能比非持续 CSMA 要差, 最大吞吐量只能达到信道容量的 53%。

为了确保 CSMA/CD 访问机制的正常工作, 整个网络的范围就受到数据包传播的最大时间的限制, 例如典型的以太网(10M 网络)的冲突域范围为 4.5km ($< 5\text{km}$)。到了上世纪 90 年代初, 随着计算机性能的提高及通信量的剧增, 传统局域网已经愈来愈不能适应超出自身能力的负荷, 交换式以太网技术应运而生, 大大地提高了局域网的性能。与现在基于网桥和集线器的共享介质的局域网拓扑结构相比, 网络交换机能显著地增加整个网络系统的带宽。交换技术的出现, 使得可以建立地理位置相对分散的网络, 使局域网交换机的每个端口可平行、安全、同时地互相传输信息, 而且使局域网可以高度扩展。

3. 以太网的交换技术

以太网交换机(Switch), 也称为交换器、交换式集线器, 是为了改善以太网负载较重时的网络拥塞问题而出现的。它采用将共享的局域网进行有效的冲突域划分技术, 各个冲突域之间用交换机连接, 以减少 CSMA/CD 机制带来的冲突问题和错误传输, 使每个端口独享整个介质带宽, 使局域网可以高度扩展。

在一个完全的交换网络中, 整个网络只有交换机和通信节点, 没有集线器(Hub), 交换机将首先接收节点发来的数据, 再将数据转发到另一个冲突域。且在交换网络中, 通信节点只同交换机作数据交换而相互之间不直接进行数据通信。

交换网络采用全双工的通信方式, 故可以认为是无冲突的网络。交换机是利用 MAC 地址工作在 OSI 参考模型第二层(数据链路层)的设备, 与集线器或其他工作在第一层(物理层)的网络设备相比, 交换机有许多优点:

- 连接冲突域/子网

中继器(Repeater)和集线器属于物理层的设备, 因而受到冲突域的限制。而交换机可以通过内部交换技术, 将各冲突域进行划分和连接, 从而将局域网的范围扩展到 150km, 同时