文章编号: 1002-0411(2003)02-113-05

基于 OPC 的以太网网络管理

范兴刚[1] 王 智[1] 孙优贤[1] 汪 琳[2]
(1. 浙江大学工业控制国家重点实验室 杭州 310027; 2. 扬子石化设计院 南京 210048)

摘 要: 在工业以太网中, 如何进行网络管理使其具有高效率、高性能, 这是一个很复杂的问题. 简单网络管理协议是管理分布式网络的主要手段; OPC 是一种用于不同数据源通信的工业标准, 它为了不同设备间互通信息提供标准统一接口. 本文先简单介绍了 SNMP 和以太网的网络管理, 然后描述了基于 OPC 技术的信息获取和网络管理. *

关键词: 工业以太网; 网络管理; 简单网络管理协议; 抽象语法符号 1; 管理信息库; OPC
中图分类号: TP393 文献标识码: B

OPC BASED ETHERNET CONTROL AND MANAGEMENT

FAN Xing-gang[1] WANG Zhi[1] SUN You-xian[1] WANG Lin[2]
(1. *National Key Laboratory of Industry Control Technology, Zhejiang University, Hangzhou* 310027, *China*;
2. *The Design Institute of Yangzi Petrochemical Company, Nanjing* 210048, *China*)

Abstract: The network management control is a process that makes network high-efficiency. SNMP is the most popular network management. Its key is the group of objects that was stored in management agency and controlled by management station. ASN.1 defines and encodes the objects. All of objects are in MIB. OPC(OLE for Process Control) provides standard interface for different equipment. It makes it easy to obtain information from other equipment. This is the basis for ethernet control.

Keywords: industrial ethernet, network control, SNMP, ASN.1, MIB, OPC

1 简介(Introduction)

在传统控制系统中, 每个自动化系统都是一个信息孤岛, 相互之间很难实现相互通信. 近年来, 以太网应用于管理层、监控层、现场设备层之间的相互通信, 形成工业以太网, 构成各层之间的无缝连接, 以消除这种现象.

现在工业以太网已成为当今的研究热点之一, Field Bus 基金会已推出以高速以太网为基础的新一代现场总线标准 HSE. IEEE(美国电气和电子工程师协会) 正在着手制订现场总线和以太网通信的新标准[1]. IAONO(工业自动化开放网络联盟) 是研究工业以太网应用和推广的专门国际组织. 工业以太网协会(Industrial Ethernet Association) 与美国的 ARC、Advisory Group 等单位合作, 开展工业以太网关键技术的研究.

以太网是一种成型的网络技术, 但移植到工业控制领域必须解决实时性、快速故障探测与自恢复、网络管理、网络安全等关键技术问题.

网络管理是对一个复杂的计算机网络进行控制和调节, 使其具有高性能、高效率的过程. 根据网络管理系统的能力, 这一过程通常包括数据收集、数据处理等. 它从功能上主要分为[1]: 对网络中的问题和故障进行定位的失效管理; 发现和配置设备各种参数的配置管理过程; 控制信息访问的安全管理过程; 检测网络中各个设备和网络的性能管理, 它主要涉及差错率、响应时间延迟、吞吐量、网络利用率、网络流量等网络性能参数; 还有跟踪网络资源的利用情况, 对用户收取合理费用的计费管理. RFC1157[11] 定义了简单网络管理协议, 用于对网络进行监控与管理.

以太网的控制管理系统是与其网络性能密切相关的一个重要问题. 以太网的网络管理包括[2]:

• 网络拓扑结构搜索, 自动搜寻以太网的拓扑图, 监视当前网络各个控制节点的连通性、以及启动

* 收稿日期: 2002-04-09
基金项目: 国家自然科学基金项目(60203030, 60084001); 中法先进研究计划项目(PRAS101-04)

和关闭状态, 并能适应控制节点即插即用的要求;

• 控制节点的网络接口数据, 节点的网络接口数据包括物理地址、状态、接收/发送包总数、包差错率等;

• 系统管理涉及到控制节点上接入设备的参数、性能与运行状态.

OPC(OLE for the process control)是一个工业标准. 它由一些世界上占领先地位的自动化系统和硬件、软件公司与 Microsoft 紧密合作而建立的(http://www.opcchina.org/). 这个标准定义了应用 Microsoft 操作系统在基于 PC 的客户机之间交换自动化实时数据的方法. 管理这个标准的国际组织是 OPC 基金会. OPC 是当前 DCS 与上位机进行通讯的一个标准. 而且现在的主流 DCS 厂家都支持 OPC 标准. 在实时控制网络中, 通过 OPC 技术获得数据对其进行管理可以提高网络的效率和性能.

本文介绍了简单网络管理协议, 对基于嗅探器、OPC 技术的网络管理实现进行了描述. 最后对本文进行了总结.

2 基本网络管理(The basic network management)[3~6]

简单网络管理协议 SNMP(Simple Network Management Protocol) 是一种监控和管理计算机网络的系统方法. 近几年来, SNMP 已成为管理分布的网络设备的主要手段. 实践中, 常用 SNMP V2 对网络进行管理.

2.1 SNMP 模型

SNMP 模型如图 1 所示, 主要包括: 管理节点、管理站、管理信息和管理协议.

管理节点是指可以与外界交换信息的设备. 为了便于 SNMP 直接管理, 节点内必须运行 SNMP 代理, 用于维护一个本地数据库, 存放节点的状态、历史并影响它的运行.

网络管理由管理站完成, 管理站实际上是一台运行特殊管理软件的普通计算机. 它包括一个或多个进程, 这些进程在网络上与代理通信, 发送命令以及接收应答. 由于实际网络采用多个制造商的设备, 为了使管理站能与多个设备通信, SNMP 严格定义了每种代理应维护的确切信息以及提供信息的确切格式.

这样, 每个设备都具有一个或多个变量来描述其状态. 这个状态称为对象. 网络中所有的对象都存放在一个叫做管理信息库(Management information base, MIB)的数据结构中. 一个 MIB 描述了一个设备或部件内部的目标数据和结构.

管理站使用 SNMP 协议与代理通信.

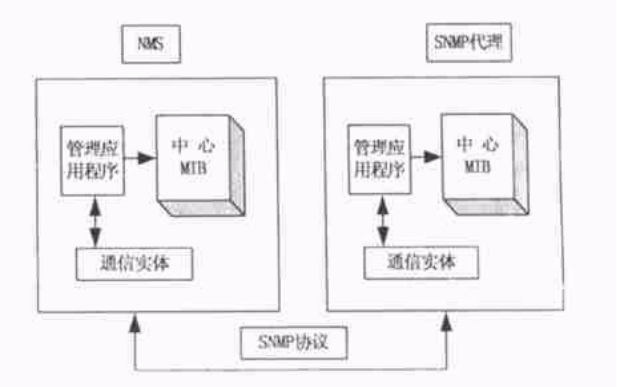

图 1 SNMP 原理图

Fig. 1 The Principle of SNMP

2.2 ASN.1—— 抽象语法符号 1

SNMP 的核心是由代理管理、由管理站读写的对象集合. 为了使不同厂家的设备相互通信, 用一种与制造商无关的方式来定义这些对象是非常关键的. ASN.1(Abstract Syntax Notation One)就是一种专门定义对象和编码规则的语言.

SNMP 使用了 ASN.1 的五种基本数据类型: INTEGER(任意长度的整数), BIT STRING(一个 0 或更多比特的串), OCTET STRING(一个 0 或更多无符号字节), NULL(一个位置符), OBJECT IDENTIFY(一个正式定义的数据类型). 其中的 OBJECT IDENTIFY 定义了一棵标准树, 每个对象对应于树上的一个唯一位置.

ASN.1 采用基本编码规则 BER (Basic Encoding Rules) 将 ASN.1 类型的值转化为适于传输的字节序列. BER 规定, 每个传输的值最多有 4 个字段组成:

• 标示符, 有 3 个字段, 最高 2 位是标记位, 可以是通用的、应用程序的、上下文相关的或私有的. 第二个字段指出是否是基本类型. 最后 5 位对标记值编码;

• 以字节为单位的数据字段的长度;

• 数据字段;

• 结束标志.

在 SNMP 中只采用前三项来完成其控制管理功能.

2.3 管理信息库 MIB

SNMP 管理的对象集合定义在 MIB 中. 对象共有 175 个, 被分为十种. 如表 1.

表 1　SNMP 的管理对象

Tab. 1　The objects of SNMP

组别	描述
System	名字、位置和设备描述
Interface	网络接口和它们的测定通信量
AT	地址转换
IP	IP 分组统计
ICMP	已收到 ICMP 消息的统计
TCP	TCP 算法、参数和统计
UDP	UDP 通信量统计
EGP	外部网关协议通信量统计
Transmission	保留为与介质有关的 MIB
SNMP	SNMP 通信量统计

管理信息库由 MIB 变量构成, 组织成树型结构(MIB 树), 每个 MIB 变量遵循上面的 ASN.1 的对象标识命名规则, 保证整个系统的标准性, 适应不同设备的管理. 对 MIB 变量的存取由应用程序完成, 每一类的 MIB 变量对应程序的某个模块, 这些模块对 MIB 变量进行存取、维护, 并且定期刷新. 它使用一个层次型、结构化的形式, 包括一些标准库及一些私有库. 在 SNMP 中, 主要使用 RFC1213[12]定义的 MIB-II 及一些私有库.

2.4　SNMP 协议

SNMP 使用方法为: 管理站向代理发送一个请求, 索要信息或命令它以特定方式修改其状态. 理想情况下, 代理发回所要信息, 或证实它按要求修改了自己的状态. 数据用 ASN.1 转换语法发送. SNMP 定义了七种可发送信息. SNMP 的命令和响应在协议数据单元(Protocol Data Unit-PDU)中编码. 其中常用的消息类型如表 2.

表 2　常用的消息类型

Tab. 2　The common style of messages

消息	描述
Get— request	从设备请求一个或多个目标数据的值
Get— next— request	用来从一个设备中顺序请求当前数据的下一个数据的值
Get— bulk— request	用来改变一个或多个目标数据的值
Inform — request	描述本地 MIB 的管理者至管理者的消息
SnmpV2— trap	代理向管理者的陷阱报告

2.5　SNMP 管理的实现[1]

SNMP 引擎实现网络管理, 它为上层应用提供 SNMP 消息的构造、发送、接收以及消息的鉴别, 加密、存取控制等. 它主要包括:

- 发送器子系统, 它将包含有控制信息的协议数据单元 PDU 分发给相应的应用程序, 并负责管理消息的发送;
- 消息处理子系统, 它对收到的消息解码, 取得现场的信息和数据, 并对要发送的 PDU 编码, 对网络形成控制;
- 安全子系统, SNMP 采用基于用户的安全模型(User-based Security Model)对网络数据进行完整性、机密性、合时性的检查;
- 存取控制子系统 SNMP 控制用户对 MIB 的访问, 不同的用户分配不同的访问权限.

SNMP 内核在 Windows 平台上以动态连接库 SNMP.DLL 文件的形式实现, 包括导出函数和内部函数. 导出函数构成 SNMP 的应用编程接口 API. SNMP 内核与应用程序的通信采用回调函数实现.

3　基于 OPC 的以太网控制网络管理(Ethernet management based on OPC)

以太网的网络管理系统是基于 SNMP 的应用系统, 各个子系统之间的通信遵循 SNMP 协议.

3.1　用虚拟设备驱动程序实现嗅探器[1]

以太网的大部分管理工作是由以太网嗅探器来完成的, 它捕获网络报文, 分析网络的流量和性能, 对其进行监督与控制.

在 32 位 Windows 平台上, 网络管理要由网络设备驱动程序来完成, 网络设备驱动程序常用规范为 NDIS(network driver interface specification)[8]. 对应于 OSI 的网络参考模型, NDIS 将协议处理与硬件操作分开考虑, 即协议驱动程序负责协议处理, 介质访问控制驱动程序(即 MAC 驱动程序)负责硬件操作. 协议管理器将各个模块连接在一起. MAC 驱动程序工作在网络设备驱动程序之下, 处于数据链路层的下半部分. 协议驱动程序作用于数据短路层的上半部分, 即在网络设备驱动程序之上. NDIS 不但为这两种驱动程序互相功能调用作了定义, 还给出了一个标准的网络设备接口, 来完成各个驱动程序之间的通信.

在 Windows 98 操作平台上, 一般通过虚拟设备驱动程序 VPACKET VxD 访问内核态, 如图 2.

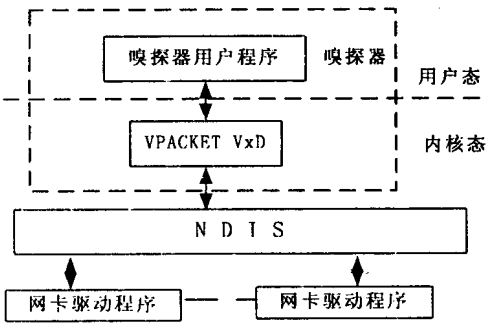

图 2 嗅探器结构

Fig. 2 The Structure of Sniffer

VPACKET VxD 向上层嗅探器的模块提供间接访问网卡的手段. 嗅探器运行时先加载 VxD, 然后用 Bind 接口将 VxD 绑定到某个网卡上, 接着调用 Device Control 接口将网卡设为杂凑模式, 从网卡中不断读取数据, 进行统计分析, 完成网络监视功能.

3.2 设置协议数据单元

SNMP 不支持强制的命令, 一般通过设置 MIB 变量, 再由 PDU(Protocol Digital Unit)传给节点实现控制, 每个设置对应于一个控制动作. PDU 如图 3, 其中的 0 表示请求正确, Variable-Bindings 绑定了多个 name-value, name 是 MIB 对象的标识符, value 表示对象的值.

PDU type	Request-id	0	0	Variable-Bindings

图 3 设置协议数据单元

Fig. 3 Set Protocol Digital Unit

3.3 基于 OPC 的现场获取[7~10]

以太网中每一个节点都挂接一些外部设备, 获取这些外部设备的配置信息和运行数据是对网络进行管理的基础. 如何屏蔽不同外界设备之间的差异, 使上层应用软件能采用一致的方式存取下层的设备信息, 是一个非常重要的问题.

OPC 是一种用于不同数据源通信的工业标准, 它基于微软 OLE (object linking and embedding)、COM (component object model) 和 DCOM (Distributed COM) 技术, 由一套用于过程控制和制造业自动化的标准接口、属性、方法组成. OLE 即对象的连接与嵌入技术, 它是把每个应用程序看作一个对象, 通过对象之间的相互协作和协议来共同完成任务. OPC 则是把 OLE 应用在过程控制中的技术. COM 提供了接口和内部组件通信的标准, 它是 DCOM、OLE、ActiveX 的核心. DCOM 把 COM 的技术扩展到网络, 使远程组件看起来就像在本地一样. ActiveX/COM 技术定义了工业软件组件如何才能交互作用和共享数据, 它得到了微软的 NT 技术的支持. OPC 为多种多样的过程控制设备提供了一个公共的接口, 此接口与过程中的控制软件或设备无关.

OPC 采用服务器和客户机模式(CLIENT/SERVER 模式). OPC 服务器是数据源, 它们拥有数据, 或者从各种设备、系统、控制器得到数据, 典型的是用 C 或 C++ 编成. OPC 客户机是数据用户, 他们在应用中使用数据, 典型的是用 VB、Excel、Delphi 等写成. OPC 客户端通过 OPC 接口与 OPC 服务器连接、通信, OPC 服务器对象向 OPC 客户端提供创建和操纵 OPC GROUP 对象的功能, 如图 4 所示.

OPC 标准规定的基本 OPC 服务器对象有: OPC SERVER、OPC GROUP、OPC ITEM 和针对不同厂商的硬件设备编写的 I/O DLL. 每个 SERVER 对象可以包含多个 GROUP 对象, OPC ITEM 对象包含在 OPC GROUP 对象中, 一个 GROUP 对象可以包含多个 ITEM 对象, 它同样由对它们要访问的数据进行组织. 一个 GROUP 可以作为一个单元被激活或失活. 一个 GROUP 也可以提供一种方法允许客户“订阅”ITEM 列表, 以便在 ITEM 变化时它能得到通知. 客户只能看到接口, 所有的 COM 对象只能通过接口进行访问. 这样对象只是逻辑表示, 可能与服务器的内部执行无关. ITEM 定义了从服务器到数据源的连接. 因为不同厂家设备的数据采集方式和现场通信网络的通信协议不同, 需要为不同的硬件设备和通信协议编写不同的 I/O DLL, 实现从具体的现场设备读取数据的功能.

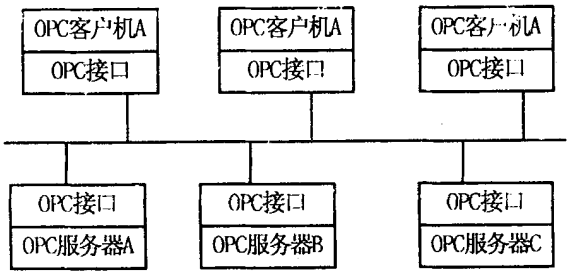

图 4 OPC 的结构

Fig. 4 The Structure of OPC

在不同的数据源通信过程中, OPC 对外部提供统一的接口. OPC 接口为两类: COM 用户化接口(Custom Interface)和 OLE 自动化接口(Automa-

tion Interface). 前者采用低级的 COM 接口, 描述了 OPC 组件和对象的接口, 提供更多的控制功能和较高的性能, 它适用于由 C+ + 语言设计的 OPC 客户端和服务器程序; 后者依赖 OLE 技术, 提供了一个自动配置和存取过程数据的接口, 主要用于象 VB 这样的程序和其它脚本程序. 由于采用统一的外部接口, 各种不同设备和数据源可以以一致的形式对上层应用提供内部数据. 采用 OPC 标准编写的设备驱动程序提供了统一的内部信息存取接口, 为控制网络管理奠定了基础. OPC 对象与接口如图 5 所示.

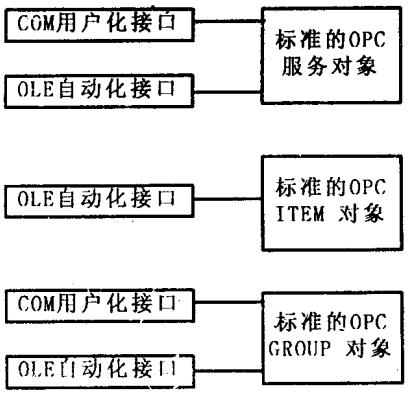

图 5　OPC 对象和接口

Fig. 5　The Objects and Interfaces of OPC

3.4　管理的实现

系统管理代理中, OPC 客户机(即控制节点)通过 OPC 接口与 OPC 服务器(即外部控制设备)交互; 它通过 OPC 接口调用服务器提供的方法. OPC 服务器通过异步通报方式或连接点方式发送数据给 OPC 客户. OPC 服务器通过 I/O DLL 与现场设备交互, 即对现场设备进行读写操作, 从而获得接入设备的静态、动态信息, 完成对网络的监控和管理.

Moore 公司的 Procidia(www. procidia. com)是世界上第一个也是唯一的互联网控制系统(ICS). 其中的 iware 服务器是符合 OPC 标准的数据服务器, 它可自动读取网络信息, 查看所连接的控制器的类型, 生成全局系统数据库. 从而便于控制网络的监督和管理.

中国科学院沈阳自动化研究所的 SIACON-SmartOPC 是国内第一个 OPC 服务器快速开发工具, 该软件可以为现场设备添加 OPC 接口, 实现与各种流行监控组态软件的无缝集成, 定制开发 OPC 数据服务器/客户应用程序.

4　结论(Conclusion)

网络管理协议及实现技术是工业以太网的重要研究领域之一. 目前, 简单网络管理协议已发展到 SNMP V3, 它加强网络的安全性控制, 融合了网络的系统管理. OPC 技术是为了不同设备间互通信息而设计的标准统一接口. 基于 OPC 技术的信息获取是实现网络管理的基础.

参　考　文　献(References)

1　郑文波. 控制网络技术[M]. 北京: 清华大学出版社, 2001

2　Burns T A. Analysis of hard real-time communication[J]. Real-Time System, 1995, **9**(2): 147~ 173

3　Tanenbaum A S. Computer Networks (third edition). Prentice Hall PTR

4　Quinn L, Russell R G. Fast Ethernet, 1998

5　Seifert R. Gigabit Ethernet: technology and applications for high-speed LANs

6　肖明彦, 窦文华. 基于以太网交换机平台的 SNMP 代理实现[J]. 电讯技术, 2000, **4**: 99~ 103

7　OPC 技术综述[Z]. www. opcchina. org/download

8　马龙华. OPC 数据存取规范的研究和应用[J]. 化工自动化及仪表, 2002, (1): 43~ 45

9　苑明哲等. OPC 技术在现场总线控制系统中的应用[J]. 工业仪表与自动化装置, 2000, **3**: 20~ 23

10　许宝祥. 过程控制系统中的 OPC 技术[J]. 冶金自动化, 1999, (6): 20~ 23

11　Case J, *et al*. A simple network management protocol (SNMP). RFC1157

12　McCloghrie K, *et al*. Management information base for network management of TCP/IP-based internets: MIB-II, RFC1213

作者简介

范兴刚(1974-), 男, 博士. 研究领域为网络通信、实时通信, 分布式实时系统的设计.

王　智(1969-), 男, 博士后. 研究领域为网络通信、实时通信, 分布式控制.

孙优贤(1940-), 男, 博士生导师, 中国工程院院士. 研究领域为鲁棒控制、实时通信, 分布式控制.

(上接第 112 页)

5　Kohonen T. Automatic formation of topological maps in self-organizing system[A]. Oja E, Simula O. Proceedings of the 2nd Scand Inavian Conf on Image Analysis[C]. 1981. 214~ 220

作者简介

张义忠(1972-), 男, 博士. 研究领域为计算机信息网络、人工智能和因特网技术的开发和研究.

赵明生(1968-), 男, 博士. 研究领域为信号与信息处理.

梁久祯(1968-), 男, 博士. 研究领域为信号与信息处理.