

BOOK RAMMING

NetBIOS, IPX, and SPX C 程序员指南

Schwaderer gives clarity and stability to a heretofore illusory de facto standard. It illustrates principles and techniques for developing the growing variety of NetBIOS applications..."

—Dr. Robert M. Metcalfe
Founder, 3Com Corporation
Publisher, InfoWorld Magazine

W. David Schwaderer

SAMS
PUBLISHING

BOOK
ODISK

Contains vital source and executable code you can use right away

科学出版社
龍門書局

希望

4, 6, 5.

NetBIOS, IPX, SPX C 程序员指南

W. David Schwaderer 著

徐光贤 译

燕卫华 校

科学出版社
龍門書局

1995

(京)新登字 092 号

内 容 简 介

本书详细介绍了用 C 语言开发 NetBIOS 应用程序的原理和技术,这些 NetBIOS 应用程序可以运用在许多不断涌现的 LAN 系统上。本书适用于有一定 NetBIOS 使用经验的读者。

需要本书的用户,请直接与北京海淀 8721 信箱书刊部联系。电话:2562329,邮政编码:100080。

版 权 声 明

Authorized translation from the English language edition published by Sams Publishing Copyright © 1994.

本书英文版名为“C Programmer's Guide to NetBIOS, IPX, and SPX”,由 Sams Publishing 出版,版权归 Sams Publishing 所有。本书中文版由 Simon & Schuster (Asia) Pte Ltd 授权出版。未经出版者书面许可,本书的任何部分不得以任何形式或任何手段复制或传播。

NetBIOS, IPX, SPX C 程序员指南

W. David Schwaderer 著

徐光贤 译

燕卫华 校

责任编辑 朱培华

科学出版社
龙门书局 出版

北京东黄城根北街 16 号

邮政编码:100717

双青印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

*

1995 年 10 月第 一 版 开本:787×1092 1/16

1995 年 10 月第一次印刷 印张:22 5/8

印数:1—5000 字数:518 000

ISBN 7-03-005013-4/TP·511

定价:33.00 元

序 言

NetBIOS 是一个很重要的网络编程接口。在 PC DOS 领域,NetBIOS 特别是为使用 IBM、XNS、TCP、IEEE 和 OSI 协议的各种通信系统提供一个一致的通信接口。当网络用户要从原系统过渡到新的协议,例如 OSI,或者新的 LAN 操作系统,例如 OS/2 LAN Manager,或者新的硬件平台,例如 PS/2 和 Macintosh II 时,NetBIOS 的重要性就更加显示出来了。

Schwaderer 编著的本书将使读者对一个被广泛采用但又似虚幻的事实上的标准有一个清晰而牢固的认识。本书给出了发展史透视,而且本书也可以作为 NetBIOS 的工作手册。本书揭示了开发正在不断增长的各种 NetBIOS 应用的原理及技术,这些 NetBIOS 应用可以运行在许多不断涌现的 LAN 系统上。

3Com 公司以太网的发明者和奠基者
Dr. Robert M. Metcalfe

前 言

网络基本输入/输出系统(NetBIOS)几乎使得一个通信程序编程员的梦想变成现实。NetBIOS 完美无缺吗?尽管我怀疑这一点,但是我们只要做小小的努力就可以掌握并提供一个功能如此强大的 LAN 通信编程平台,因而我认为必须与尚未入门的人员分享我的一些认识,我们要讨论有关 NetBIOS 过于简略及某些含糊不清的内容。

本书包括如下内容:

- NetBIOS 的历史以及它与其他 IBM 软硬件的关系
- NetBIOS 的命令
- Ncb 域
- 命名、数据报、会话支持程序
- LAN 数据的安全性及完整性
- CRC 基础

全书的大量例子揭示了应用编程的准则,附录中提供了可用的参考表及程序。

致 谢

这里要专门提到我的两个朋友。首先是 Jim Brady,他目前是我的上一级经理。在 IBM 磁盘驱动部门工作的两年半的大部分时间,我非常感谢他将我安排到与 LAN 有关的工程中工作。我的工作使我能跟踪 LAN 技术的发展,这对我们的部门发展大概有用处。幸运得很,Jim 对通信领域涉足很深,否则我的工作会加倍困难。

其次是 Larry Raper,他偶尔在半夜给我打电话,对我正在写的程序提出建议。这一点之所以让我印象深刻,是因为 San Jose 的深夜是 Larry 所在东海岸的凌晨 3 点。附录 B 中的 Post C 语言程序就直接源于 Larry 的深夜电话。Larry 是工业界一个最闪光的编程艺术家和系统设计者。Larry 程序内部的清晰、设计的优美和冲击会使最天才的编程员感到沮丧。

祝你使用 NetBIOS 时好运,如果你乐意,可以对书中有问题的部分划线。我将乐意知道你如何让本书变得更好,以及你如何使用 NetBIOS 来改进你的工作。如果你发现错误或有什么建议,请给我或出版商写信。我将尽个人所能回答您,并在下次出版时更正,在此先表示感谢。

W. David Schwaderer
San Jose, CA

商 标

本书涉及到的商标或服务标志全部列在下面。另外,有些术语可能是商标或服务标志,这在印刷时已适当大写。Sams 出版社不保证这些信息的准确性。本书中这些术语的使用不会影响任何商标或服务标志的有效性。

下面是已经注册的商标或 IBM 的商标:

IBM, PS/2, OS/2, OS/2 EE, PC DOS, XT, IBM AT

EtherNet 是 3Com 公司的注册商标。

Microsoft 和 Microsoft C 是 Microsoft 公司的注册商标。

UNIX 和 AT&T 是美国电话电报公司的注册商标。

Xerox 是 Xerox 公司的注册商标。

目 录

序言	(VI)
前言	(VII)
致谢	(IX)
商标	(X)

第一部分 NetBIOS 引论

第一章 综述	(3)
1.1 NetBIOS 处于模型图的哪一层	(3)
1.2 NetBIOS 从何而来	(4)
1.3 “True NetBIOS”是什么	(4)
1.4 如何获得 NetBIOS	(5)
1.5 IBM NetBIOS 参考资料包括些什么	(7)
第二章 NetBIOS 和 IBM 的 LAN 适配器	(9)
2.1 令牌环环境	(9)
2.2 IBM PC 宽带网络环境	(10)
2.3 IBM PC 基带网络环境	(11)
2.4 以太网环境	(11)
2.5 IBM LAN 编程接口	(11)
第三章 应用服务	(14)
3.1 NetBIOS 命名支持	(14)
3.2 数据报及会话的支持	(17)
3.3 一般命令	(22)
3.4 NetBIOS 命令的调用	(23)
3.5 测试 NetBIOS 是否存在	(25)
第四章 Ncb/Mcb 域	(26)
4.1 命令	(28)
4.2 返回码	(28)
4.3 本地会话编号	(29)
4.4 名字编号	(29)
4.5 缓冲区地址	(29)
4.6 缓冲区长度	(29)

4.7	调用(远端)名.....	(29)
4.8	(本地)名.....	(29)
4.9	接收超时.....	(30)
4.10	发送超时	(30)
4.11	POST 例程地址	(30)
4.12	LANA 编号	(30)
4.13	命令结束标志	(30)
4.14	保留域	(30)
4.15	测试 NetBIOS 存在的 C 样板程序.....	(31)
第五章	IBM PC DOS LAN 支持程序	(34)
5.1	IBM LAN 支持程序的作用	(34)
5.2	NetBIOS 参数总结.....	(35)
第六章	NetBIOS 同其它 IBM 产品的关系	(41)
6.1	IBM PC DOS 版本的要求.....	(41)
6.2	IBM PC LAN Program 的考虑	(41)
第七章	LAN 上数据的完整性和完全性	(47)
7.1	LAN 上数据的完整性	(47)
7.2	LAN 上数据的安全性——给聪明人的话	(47)
7.3	永久节点名的骗局.....	(48)
7.4	令人不安的结论.....	(48)
第二部分 NetBIOS 支持的编程		
第八章	一般支持的编程	(51)
8.1	NetBIOS RESET 样板程序	(51)
8.2	NetBIOS 适配器状态样板程序	(58)
8.3	NetBIOS Reset 和 Adapter Status 命令的协同	(67)
8.4	NetBIOS Cancel 样板程序.....	(67)
8.5	NetBIOS Unlink 样板程序	(72)
第九章	命名支持的编程设计	(74)
9.1	NetBIOS 命名活动的样板程序.....	(74)
第十章	数据报支持的编程	(79)
10.1	main()函数	(82)
10.2	InitDatagramNcb()和 XmitDatagram()	(82)

第十一章 间接的数据报应用	(83)
11.1 日期及时间的服务器应用程序	(83)
11.2 日期及时间的 client 应用程序	(86)
第十二章 实时的 LAN 会议应用	(96)
12.1 main() 函数	(111)
12.2 EditArgs() 函数	(111)
12.3 NetBIOS 的 Add Name 处理过程	(111)
12.4 Particlipate() 函数	(112)
12.5 ServiceDatagramNcbs() 函数	(112)
12.6 ProcessReceivedDatagram() 函数	(113)
12.7 Servicekeyboard() 函数	(113)
12.8 SendkeyboardMsg() 函数	(113)
12.9 Applykeystroke() 函数	(113)
第十三章 C 语言文件传输应用	(114)
13.1 应用程序概述	(127)
第十四章 无盘工作站、RPL 和重定向	(129)
14.1 客户和服务端	(129)
14.2 数据层	(129)
14.3 重定向器的实现	(131)
14.4 块设备驱动程序的实现	(131)
14.5 INT 13 BIOS 接口	(132)
14.6 NetBIOS RPL 的实现——如何加载 PC DOS	(132)

第三部分 循环冗余校验(CRC)专题

第十五章 CRC 基础	(139)
15.1 CRC 校验的必要性	(139)
15.2 XMODEM 校验和	(139)
15.3 CRC 数学基础	(139)
15.4 CRC 计算	(142)
15.5 常用 CRC 多项式	(144)
第十六章 CRC-16 和产生 CRC 常用方法	(145)
16.1 CRC 硬件	(146)
16.2 通用的 CRC-16 移位	(149)

16.3	查表方法	(151)
16.4	CRC 兼容性	(156)
第十七章	CRC-CCITT 及最小的可查表	(157)
17.1	查表法的实现	(158)
第十八章	CRC-32——令牌环、PC 网及以太网	(164)

第四部分 NetBIOS 技术参考手册

第十九章	网络控制块	(177)
19.1	Ncb 域	(177)
19.2	命令的完成	(182)
第二十章	NetBIOS 命令	(183)
20.1	命令	(183)
20.2	特殊值总结	(203)
20.3	复杂的 Hang up	(204)
20.4	返回码小结	(205)
第二十一章	IPX/SPX 概述	(206)
21.1	Novell Netware 的背景	(206)
21.2	IPX	(206)
21.3	SPX	(207)
21.4	IPX 和 SPX 存在性测试	(207)
21.5	Novell NetWare 的概念	(210)
21.6	为什么知道这些	(214)
21.7	ECB	(222)
21.8	IPX 包头结构	(224)
21.9	SPX 包头结构	(225)
21.10	结论	(226)
第二十二章	IPX 编程	(227)
22.1	结构成员对齐	(227)
22.2	程序的执行	(227)
22.3	包发送	(228)
22.4	AES 例子	(228)
22.5	取消一个 ECB	(229)
22.6	包接收	(229)

22.7 结论.....	(229)
第二十三章 SPX 编程	(260)
23.1 程序的执行.....	(260)
23.2 数据包发送.....	(260)
23.3 数据包接收.....	(261)
23.4 结论.....	(262)
附录 A NetBIOS2.h 程序清单	(305)
附录 B POST 例程 C 语言程序清单	(311)
附录 C 错误代码,原因及解决方案	(314)
附录 D Ncb 命令和域的关系	(324)
附录 E Send No-Ack 和 Chain Send No-Ack	(326)
附录 F OS/2 扩展版本及 LAN Manager	(328)
附录 G IPX-SPX.h 清单	(332)
附录 H Novell NetWare 通信编程参考	(337)

第一部分

NetBIOS 引论

第一章 综 述

网络基本输入/输出系统(NetBIOS)是一个应用程序接口,用于数据源与目的地之间的数据交换。形象点讲,NetBIOS 是一个门槛,让程序员能访问到支持计算机应用和设备通信时要用到的各种服务。应用程序要用特殊的命令序列来调用这些不同的 NetBIOS 服务。因此,NetBIOS 的某些服务有着明确而简单的通信协议。

典型的数据交换发生在两个 NetBIOS 应用之间,这两个应用驻留在通过一个局域网 LAN 连接起来的两台不同机器上。但运行在同一台机器上的两个应用也可以用 NetBIOS 进行数据交换而无需 LAN。因此,尽管所有的 IBM NetBIOS 实现都需要一个 LAN 适配器,但是 NetBIOS 的使用不局限于 LAN 环境。

1.1 NetBIOS 处于模型图的哪一层

如果你熟悉数据通信理论,就会知道如图 1.1 所示的国际标准化组织(ISO)开放系统互连(OSI)的参考模型。

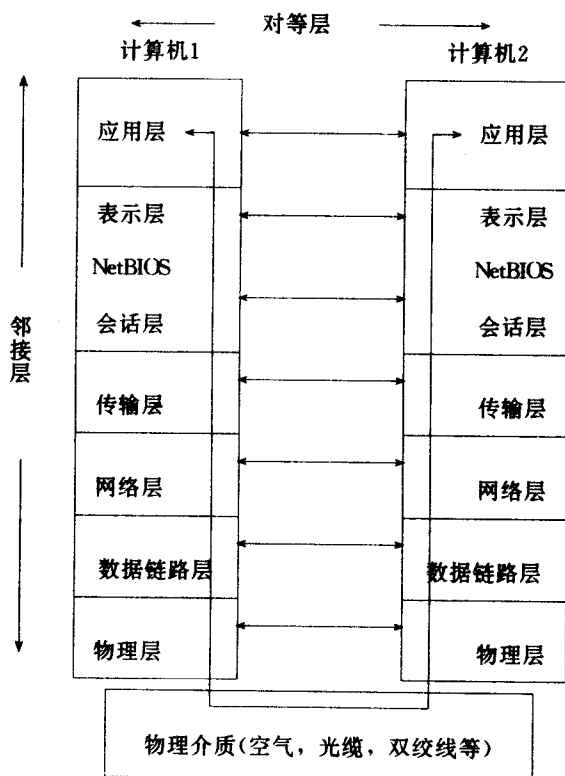


图1. 1 ISO/OSI参考模型

这个概念模型将驻留在不同机器上的两个应用之间一般要实现有序数据通信的不同领域划分成七个层次,NetBIOS 在这个概念模型中的位置也已在图 1.1 中示出。

在通信应用过程中,给定机器上的每一层与它直接相邻的上一层或下一层直接协调工作,进行信息传递。这种传递称为邻接层通信。另外,一台机器的每一层还要与另一台机器上的对等层间接协调工作,以进行信息交换。这种信息交换叫做对等层通信。

NetBIOS 处于参考模型的高层,因此 NetBIOS 接口程序的应用在很大程度上,并且本质上与较低层的各种活动隔离开来。例如,两个 NetBIOS 应用使用 IBM PC 网络适配器通信时,可以用驻留在网络适配器上的会话管理协议(SMP)来实现,也可以用 IBM PC LAN 支持程序来实现,IBM PC LAN 支持程序使用了 IEEE 802.2 的逻辑链路控制(LLC)协议。无论哪种情况,应用程序不必去关心究竟使用了什么协议。

这种不敏感性使得通用的 NetBIOS 应用可以移植到不同的通信环境中去。这种移植通常不是完全照搬。例如,每种类型的 IBM LAN 都有自己特殊的方法来实现 NetBIOS,或者它们将遵循 IBM 的关于发展方向的某个声明,这些声明发表在 IBM PC Network 的简介中。根据 IBM LAN 类型的不同,NetBIOS 某些命令的影响会有所不同。在其他通信环境下实现的 NetBIOS 也有同样的情况。然而,因为 NetBIOS 应用程序明显的可移植性,以及 NetBIOS 的简单直观性,它很快就变成了没有竞争对手的、事实上的工业标准。况且,在它不完善时,其它通信环境也已开始提供 NetBIOS 接口,例如流行的 TCP/IP 环境以及正涌现出的 MAP/TOP 环境。

NetBIOS 正迅速成为不同操作系统环境下普遍使用的数据通信编程平台,这些操作系统中包括 PC DOS,OS/2 和 UNIX。如果你熟悉 NetBIOS 编程,你正在一个正扩展的市场中拥有一项很有市场的技能。

1.2 NetBIOS 从何而来

NetBIOS 首次出现在 1984 年 8 月 IBM PC 网络适配器中,这种网络适配器由 Sytek 公司为 IBM 设计。IBM PC NetBIOS 是 IBM 的第一个 LAN 产品。它采用宽带同轴电缆,提供每秒 2Mb 的数据传输突发速率。使用了流行的工业标准 CSMA/CD(多访问载波侦听/载波检测)作为访问协议,这种访问协议首次出现在 IEEE 802.3 以太网标准中。

IBM PC NetBIOS LAN 适配器上(LANA)带有一块扩展的 BIOS ROM,这片 ROM 驻留了 LANA 型网络适配器的 BIOS,它占用 8K 内存,起始段地址 CC00h,它包括了 LANA 初始化过程、诊断过程、协处理器以及 PC 内存接口过程,另外还包括部分基本的 NetBIOS 实现,NetBIOS 的其它实现部分驻留在适配器的第二片 ROM 上,这片 ROM 称之为协议 ROM。适配器的 ROM 中还包括允许无引导盘的 IBM PC 工作站从网络引导服务器上引导系统的过程。通过远程程序加载(RPL)和 ROM NetBIOS 提供的服务就可以实现远程引导。

1.3 “True NetBIOS”是什么

工业标准的 TCP/IP NetBIOS 首次发表在 1987 年 12 月。它实际上是一个扩展的 NetBIOS,因为它要解决互连网中的路由问题及命名问题。MAP/TOP NetBIOS 的实现在写本书时仍处于初期,可能也会出现自己的特点。

在 IBM 产品系列中,当前版本的 IBM LAN 支持程序为“true NetBIOS”实现提供保证,它通过不同的 PC DOS 设备驱动程序对所有的 IBM LAN 适配器提供 NetBIOS 支持。

这个程序的一个显著优点是:它通过运行 IBM 的令牌环/PC Network 互连程序的一个中介 PC 或 PS/2,允许 IBM 的不同适配器之间进行通信。除非特别说明,PC 包括 IBM PC 系列(除去 PC Junior)和 PS/2 系列。这样就可以实现 IBM PC Network LAN 工作站与基于令牌环的工作站通信。IBM 仅仅出于战略因素宣布 IBM LAN 支持程序中的 NetBIOS 取代 NetBIOS 的原始实现而成为真正的 NetBIOS 工业标准。

1.4 如何获得 NetBIOS

如果你正使用 IBM LAN,这个问题的答案需要做一个历史产品调查,然后才能得到。如果使用的不是 IBM LAN,请向你的系统供应商寻找答案。

1.4.1 原始的 PC Network LANA 网卡

NetBIOS 自动包含在每块 IBM PC 网络适配器 LANA 网卡中。但是,因为 LANA ROM 是 PC BIOS 的扩充,像 PC-XT 硬盘驱动适配器、EGA 卡等其它适配器一样,所以它要求机器能支持扩充的 PC BIOS。除去原始的 IBM PC,其它型号的 IBM PC 均支持扩充的 PC BIOS(例如,可以使用 IBM PC-XT,IBM PC-AT 等)。

如果使用的是原始的 IBM PC,那么在 NetBIOS 可用之前,要将 PC 的 ROM-BIOS 升级。升级后的结果是:机器加电自检及初始化以后,在加载 PC DOS 之前,PC 机先扫描用于 BIOS 扩充的 PC 内存。BIOS 从内存 C800:0000 处开始执行,每过 2K 内存检查扩充 ROM 的标志值 AA55h。因为 IBM 不再提供 ROM BIOS 升级工具,与系统供应商联系用其它方法来达到上述目的。

如果找到值 AA55h,表明存在扩充的 BIOS,从 AA55h 值后面三个字节的指令开始继续执行。这允许扩充的 ROM BIOS 执行不同的功能,例如适配器及中断向量初始化。每个扩充的 ROM 执行完以后都返回到 PC BIOS,让 PC BIOS 继续对其它扩充的 ROM 进行内存扫描。因此,单个或多个扩充的 BIOS 按一定的顺序进行初始化工作。

LANA NetBIOS 的第一版出现之后,IBM 将网络适配器的 BIOS 升级成另一版本的 ROM BIOS。如果使用的是 LANA 适配器,可以用下面的方法确定该适配器所用的 NetBIOS ROM 是哪一个版本的。用 PC DOS 的 DEBUG.COM 程序显示内存 CC00:0000 的值,该地址周围的值表明了所用适配器的 BIOS 部分编号,第一版的 NetBIOS 编号为 6360715,升级版的编号为 6480417。

也可以看一看实际的 LANA NetBIOS 芯片,它处在适配器 PC 总线连接器左手的紧上边,是上下方向的。图 1.2 标明了 ROM 芯片的位置。

原始版的 ROM BIOS 版权日期是 1984 年,升级版的版权日期为 1985 年。