

The Complete Guide to NetWare LAN Analysis (3rd ED)

NetWare 局域网分析大全

(第三版)



[美] Laura A. Chappell 著
Dan E. Hakes

顾文铮 包振山 等译

邱瑞华 孙宏伟 校



電子工業出版社

Publishing House of Electronics Industry

URL: <http://www.phei.co.cn>

The Complete Guide to NetWare LAN Analysis (3rd ED)

NetWare局域网分析大全



〔美〕 Laura A.Chappell 著
Dan E.Hakes

顾文铮 包振山
冯国臻 姜庆林 等译
邱瑞华 孙宏伟 校



電子工業出版社

Publishing House of Electronics Industry

770163

内 容 提 要

本书是劳拉所著的《NetWare局域网分析》的第三版，他的前两个版本很受欢迎。本书在前面版本的基础上增补了有关NetWare网络系统新版本的知识，全面介绍了各种网络结构、协议标准、故障诊断、测试优化等方面的内容。基于多年的网络管理及授课的经验，本书为网络管理员提供了如何充分发挥网络性能，正确预测网络发展趋势，如何分析电缆故障、服务器过载以及各种传输控制方式等有益的指导信息。对于长期使用和管理NetWare网络系统的网络管理员和用户，本书是一本实用性较强的工具书。

本书适用于计算机网络用户和管理员，大专院校相关专业的师生。



Copyright©1996 SYBEX Inc., 1151 Marina Village Parkway, Alameda, CA 94501. World rights reserved. No part of this publication may be stored in a retrieval system, transmitted, or reproduced in any way, including but not limited to photocopy, photograph, magnetic or other record, without the prior agreement and written permission of the publisher.

本书英文版由美国SYBEX公司出版，SYBEX公司已将中文版独家版权授予中国电子工业出版社及北京美迪亚电子信息有限公司。未经许可，不得以任何形式和手段复制或抄袭本书内容。

书 名：NetWare局域网分析大全（第三版）

著 者：〔美〕Laura A.Chappell Dan E.Hakes

译 者：顾文铮 包振山 冯国臻 姜庆林 等

审 校：邸瑞华 孙宏伟

责任编辑：吴琴

印 刷 者：北京顺义颖华印刷厂

装 订 者：三河金马印装有限公司

出版发行：电子工业出版社出版、发行

北京市海淀区万寿路173信箱 邮编：100036 发行部电话：68219077

北京市海淀区万寿路甲15号南小楼三层 邮编：100036 发行部电话：68215345

URL:<http://www.phei.co.cn>

经 销：各地新华书店经销

开 本：787×1092 1/16 印张：22.75 字数：595千字

版 次：1997年7月第1版 1997年7月第1次印刷

书 号：ISBN 7-5053-4158-8/TP·1846

定 价：39.00元

著作权合同登记号 图字：01-96-1498

凡购买电子工业出版社的图书，如有缺页、倒页、脱页者，本社发行部负责调换
版权所有·翻版必究

引 言

工作在LAN环境下和在独立的环境下差别是很大的。电缆是网络传输的动脉，通信协议用于在两个系统之间传输数据和管理信息。随着NetWare LANs不断地普及，用户们需要有关协议标准，故障诊断，测试及优化等方面更为详细的信息。

在过去的几年里，我们已经研究、讲授并出版了关于Ethernet、Token Ring，以及NetWare的协议。很多读者提出了再版的要求，特别需要得到关于NetWare设备管理特性和最新发布的管理协议方面的信息。本书收集了我们全日制协议讲习班学员们所提出的一些最为常见的问题。

哪些用户需要阅读本书呢？

本书是为那些对NetWare协议分析有兴趣的用户准备的，协议分析将从基础知识一直讲到高级应用，以便使用户们能够诊断故障，测试和优化所使用的NetWare Ethernet和Token Ring LANs。不管读者是否具备多年的NetWare管理经验或者精通控制方面的应用，本书都会帮助读者学习并掌握处理“表面现象下所隐藏的”NetWare通信故障。

如果你是一位网络管理员，本书将教会你如何充分发挥网络性能，正确预测网络发展趋势，识别电缆连接、服务器过载以及有关Ethernet，Token Ring和NetWare方面的错误问题。

如果你是一位网络技术专家，本书将会让你了解以太网和令牌环网的帧结构以及电缆系统。在以太网部分，你将熟悉帧差错，这可能是由于网络过载，电缆接线问题或是网络驱动器以及收发器出了点毛病。在令牌环网部分，你会看到如何管理令牌环网，数据帧并通过分析通信情况来确定叶瓣线（lobe wire）、MSAV端口，或者适配器的故障。最后，通过分析NetWare通信协议，你会完全理解NetWare的客户机/服务器系统的工作特点以及优化技术。

对于那些要提供NetWare操作系统技术讲座和技术支持的人员来说，本书提供了很多课堂中使用到的问题。作为补充材料，无论是初学者还是高级学员，本书都将会让你深入了解以太网和令牌环网的访问途径以及NetWare的通信技术。

用户将会学到哪些东西呢？

在本书中读者将会学到Ethernet和Token Ring电缆连接的基础，帧结构及功能。读者将会对NetWare LAN上发生的故障及其表现有一个充分的了解。

读者也会学到诸如路由、服务器信息、文件和打印机访问、装订数据库（bindery）存取、面向连接的以及无连接的通信、大文件传送、诊断配置信息、连接有效性、串号化信息、网络信息等方面的NetWare通信内容。

本书也提供了有关协议分析的特点的综合说明以及用于检查网络完整和性能，测试电缆及服务器的性能，优化网络，排除Ethernet和Token Ring NetWare通信故障等方面的工具。

本书中提到的工具

本书将介绍两种协议分析器：LANalyzer for Windows（Novell公司）和NCC LANalyzer（网络通信公司）。每个分析器都具有在一定范围内分析联网协议的能力。

LANalyzer for Windows是基于MS Windows的产品，图形界面，使用直观，价格也比较便宜。用一个屏幕画面可表现出该界面的特点，请看LANalyzer for Windows的一个实例，如图1.1。

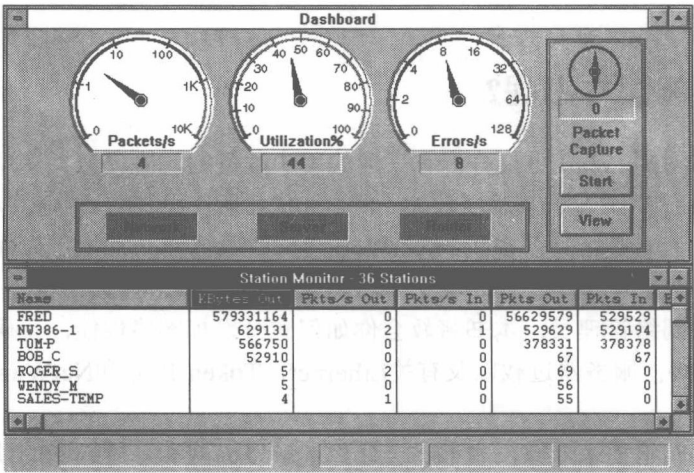


图1.1 使用Windows图形界面的LANalyzer for Windows

另一方面，NCC LANalyzer也使用传统的C-Worthy界面，它提供文本方式的界面。如图1.2。

要得到关于LANalyzer for Windows更详细的信息，请参阅附录C。

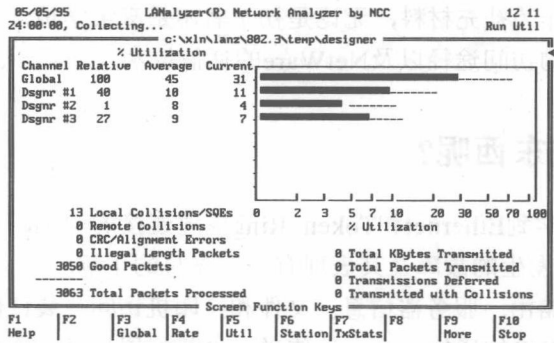


图1.2 使用传统的C-Worthy界面的NCC LANalyzer

Novell的NetWare LANalyzer Agent是分布式的网络分析器。NetWare LANalyzer Agent能够帮助用户分析并捕获网桥、路由器或者广域链路另一端的通信信息。NetWare管理系统提供了一个控制界面，它可从各个网络上收集数据并显示，如图1.3。

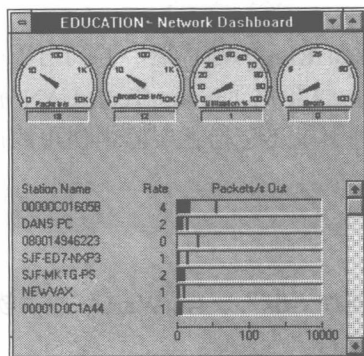


图1.3 NetWare管理系统控制台界面；
和LANalyzer for Windows相似

本书的组织

本书有5部分，包括Ethernet的访问方法；Token Ring介质的访问方法；NetWare协议；性能基准；测试、优化以及协议分析器的特点。

第1部分“Ethernet/802.3 LANs”，详细描述了NetWare环境中Ethernet帧的结构，包括Ethernet_802.3（“纯”以太网）、Ethernet_802.2、Ethernet_SNAP以及Ethernet_II。该部分也详细描述了电缆接线系统的配置要求以及限制，还有电缆测试。最后，列举了很多NetWare LANs中出现的帧差错，以及这些差错中潜在的原因和可能的解决办法。

第2部分“Token Ring/802.5 LANs”详细描述了Token Ring网络的组成部分，功能管理站和地址，功能过程和管理帧。该部分还比较了4Mb/s、16Mb/s和Early Token Release的性能，分析了帧的构造、源路由（Source Routing）/生成树（Spanning Tree）协议以及令牌环网的故障诊断技术。

第3部分“NetWare协议”，探讨了NetWare协议，如路由信息协议（RIP）、服务广告协议（SAP）、网间包交换（IPX）、顺序包交换（SPX和SPX II）、大的网间包、NetWare链路服务协议（NLSP）、NetWare目录服务（NDS）和NetWare核心协议（NCP）。第Ⅲ部分中还包括监视器（Watchdog）序列化协议的分析。最后，定义了诊断响应者的配置请求（Diagnostic Responder Configuration Request）和响应格式（Response formats）来诊断NetWare LAN的故障。

第4部分“性能基准、测试及优化”，彻底地解释了如何确定网络的性能基准，测试网络的能力，以及优化局域网。该部分还有一章详细地阐述了与一台服务器连接、登录进入、产生及清除文件时所遇到的各种通信状况。

第5部分“协议分析器——综述和特性”，通过研究各种特点，包括网络上长短期的统计数字累积、站的监视、报警阈值的设置和动作、数据包的过滤、包的捕获、网络传输以及协议解码等，总结出许多协议分析工具的使用方法。本部分还提供了许多利用特征来诊断故

障和提高网络性能的例子。

附录A汇编了本书中使用的术语。附录B列出了本书所使用的参考资料及文献，建议读者对它们作深入研究。附录C提供了有关Windows的LANalyzer和Software Developer Kit的信息。

附录D详细描述了各种Token Ring的帧构造，并列出了计时器。附录E是一个十六进制—十进制—二进制的转换表。附录F提供了Imagi Tech LAN分析实验室研究Ethernet、Token Ring和NetWare的详细情况。该附录还包括在实验中使用的产品的详细情况。

本书使用的符号规则

在本书中，十六进制值前面加“0x”。NetWare环境中软硬件的地址用它们的十六进制格式表示，前面并没有“0x”字符。

当出现新的名词术语时，用英文正体，括号中为译文。这些新名词在附录A中均能找到。需要用户输入的信息用黑体。

有了本书，可以很容易地解决大多数NetWare通信，Ethernet和Token Ring的性能问题。结合本书在网络上使用协议分析器，将能够追踪网络的变化趋势、配置和性能特性。读过本书后，读者将会掌握书中提供的许多分析技术，并将彻底了解Ethernet及Token Ring LANs上NetWare的通信系统技术。

目 录

第1部分 Ethernet/802.3 LANs	1
第1章 Ethernet LANs概述	2
Ethernet的优缺点	3
CSMA/CD如何工作：发送	3
CSMA/CD如何工作：接收	7
测试站的发送和接收能力	10
第2章 CSMA/CD的性能	13
定义带宽的效用	13
介质访问测试（负荷）	21
电缆系统的压力测试	21
第3章 接线规范及性能	26
10Base5	26
10Base2	27
10BaseT	27
不正确的电缆接线问题	28
第4章 NetWare Ethernet帧构造	31
NetWare LANs上帧类型	31
Ethernet_802.3	33
Ethernet_802.2	37
Ethernet_SNAP	40
Ethernet_II	42
多个协议/多种帧	45
帧类型之间的差别	45
“找不到文件服务器”	45
配置NetWare v3.x使用多种帧类型	47
过滤帧类型	47
第5章 数据链路层的故障诊断	49
监视本地和远端的冲突	49
确定本地及远端冲突过多的原因	50
监视后来的冲突和CRC/对齐差错	51
确定后来的冲突和CRC/对齐差错的原因	53
监视帧长度差错	53

确定引起非法长度帧的原因	54
监测超时发送	54
第2部分 令牌环（Token Ring）/ 802.5	57
第6章 令牌环概述	58
令牌环的优点和缺点	58
令牌环是如何工作的	59
令牌环拓扑结构和硬件概述	62
第7章 功能管理工作站/ 地址	67
活动监视器（必需的）	67
备用的监视器（必需的）	69
环参数服务器（可选）	70
环差错监视器（可选）	71
配置的报告服务器	71
第8章 令牌环的功能进程	73
监视器竞争	73
环轮询进程	77
站的初始化过程	80
环清除过程	83
警告进程	85
第9章 令牌环的帧构造	89
特别的令牌环位形式	89
令牌环帧	90
第10章 MAC帧信息	97
MAC信息格式	97
MAC帧的描述	101
第11章 数据链路层的故障诊断	104
令牌环的差错	104
诊断故障	108
第12章 令牌传递环的性能考虑	116
优化令牌环	116
作出基线和监视令牌环	121
第13章 源路由网桥和生成树协议	124
源路由网桥与透明网桥的比较	124
源路由网桥	125
生成树协议（STP）	131
为源路由配置NetWare服务器和工作站	136

第3部分 NetWare协议	139
第14章 NetWare的IPX、SPX和SPX II 协议	140
IPX、SPX和SPX II 的优缺点	140
IPX头标	141
已通过路由器的分组	144
用传输控制协议优化LAN	145
IPX时限	147
NetWare v3.x和4.x服务器考虑	148
顺序分组交换 (SPX)	149
SPX头标	149
建立和终止SPX连接	150
监视SPX连接	152
SPX时限监视/ 配置	153
新一代SPX、SPX II	154
SPX II 分组格式	155
第15章 NetWare	158
建立NCP连接	158
NCP请求和应答头标格式	159
NCP功能码和子功能码	161
NCP通信样本	171
网络上的特殊分组	174
第16章 大型网间分组 (LIP) 和突发方式协议	180
大型网间协议 (LIP)	180
突发方式特征	181
BNETX功能	181
VLM突发方式功能	183
突发方式帧格式	185
分析突发方式的优点	186
NetWare Shell的历史	187
第17章 服务广告协议 (SAP)	195
SAP功能	195
周期性SAP信息广播	196
SAP服务查询	197
SAP服务响应类型	199
SAP服务响应分组格式	199
监视过多的SAP通信	200
标识服务器和可用性	201

主动收集服务信息	201
“服务器关闭”分组	203
SAP中介网络域	203
第18章 寻径信息协议 (RTP) 和NetWare连接服务器协议 (NLSP)	205
寻径信息协议功能	205
本地广播和最佳信息算法	206
寻径信息分组格式	207
路由器“关机”分组	208
在建立连接时使用RIP	209
测试寻径效率	210
距离向量和连接状态寻径协议	213
第19章 NetWare诊断分组	216
连接性测试	216
收集配置信息	216
诊断请求分组结构	218
诊断响应分组结构	219
部件类型描述	221
创建诊断测试	221
第20章 NetWare目录服务	225
NetWare NDS概览	225
和NDS有关的通信	225
新的NCP和NDS动词	226
第4部分 网络性能的基准化、测试和优化	239
第21章 建立和使用网络基线	240
基线报告中包括些什么?	240
建立基线应在什么时间	244
当前网络性能和基线的比较	244
第22章 强力测试技术	246
哑负载	246
智能型负载	247
强力测试	248
第23章 NCP通信的测试和优化	250
利用NETX.COM的连接过程	250
使用指定服务器选项的NETX.COM的连接过程	251
使用VLMs的连接过程	253
NetWare服务器的连接优先级	254
不用突发模式支持的登录过程	255
突发模式支持的NetWare 4.x登录进程	258

NetWare网络安全的例子	263
对于未授权的网络用户的监控	264
检查访问权限/ 特权	267
第24章 表征服务器性能的特性	270
创建一个服务器工作负载的测试	270
确定过载的服务器	273
确定服务器过载的原因	275
平衡服务器的负载	277
第5部分 协议分析器的概述和特征	279
第25章 协议分析器概述	280
物理层分析	280
数据链路层分析	280
网络层分析	281
上层协议分析	282
硬件/ 软件组合分析器	284
纯软件的解决方案	284
独立式和分布式解决方案	285
第26章 变化趋势和当前统计（基线信息）	286
增加统计计数器的值	286
短期统计	289
长期统计	290
第27章 站的监视、跟踪	292
确定网上最活跃的客户机/ 服务器	292
确定使用最大带宽的站	295
定位网络上产生差错的站	296
名字收集	296
第28章 报警及报警阈值	298
预定义报警阈值	299
用户定义的报警阈值	301
决定报警阈值	303
报警动作	303
第29章 数据包的捕获	306
前过滤的准则	307
后过滤	310
加强的过滤	312
第30章 数据包的发送	315
负载测试	315
部件测试	315

事件的再发生	316
直接产生发送的数据包	317
拷贝和粘贴的方法	317
重现网络事件	319
第31章 协议解码	321
不解码的选项	323
简要的解码选项	323
扩展的解码选项	324
使用模板	325
附录A 词汇	330
附录B 参考书目	335
附录C 用于Windows的LANalyzer产品信息	336
视频磁带培训	336
NetWare专家故障诊断系统	337
NetWare专家培训系统	337
附录D Token Ring计时器	338
T (any-token)	338
T (attach)	338
T (beacon-transmit)	338
T (claim-token)	339
T (escape)	339
T (good-token)	339
T (neighbor-notification)	339
T (notification-response)	340
T (physical-trailer)	340
T (receive-notification)	340
T (response)	341
T (ring-purge)	341
T (soft-error-report)	341
T (transmit-pacing)	341
附录E 十六进制数与十进制数的转换表	343
附录F 分析实验室综述	346
实验室需求	346
实验室的产品制造商和产品信息	348

第1部分 Ethernet/802.3 LANs

第1章 Ethernet LANs概述

当安装NetWare LAN时，用户必须选择适合他们特定需要的网络访问方法。这个网络访问方法决定了在工作站（Ethernet、Token Ring、ARC等）中安装的是何种网络接口以及工作站如何联通电缆接线系统和怎样准备数据在网络上传送。

注意：本书所使用的术语“Ethernet”集中地描述了Ethernet II和802.3网络规范及功能。

现在的NetWare LAN上三种普通的访问方法是：

- 有碰撞检测的载波侦听多重访问（CSMA/CD）
- 令牌传递环
- 令牌传递总线

Ethernet LANs使用CSMA/CD方法，而Token Ring和ARCnet则分别使用令牌传递环和令牌传递总线。

目前，大多NetWare LANs是Ethernet（CSMA/CD）系统；但是过去几年中Token Ring已经在普及应用中稳定增长。ARCnet LANs在网络访问选择之间的“战争”中仍然保持第三名。

三种访问方法在其网络上通信都有唯一的方式。在CSMA/CD网络上，如图1.1所示，所有的工作站共享公共的电缆接线系统。所以有时候在同一时间发送数据，造成数据在网络中的冲突。每个工作站都需要采取必要的措施来避免与其他工作站在同一时刻发送数据，如果最后的信息发生了冲突，就需要再发一次。电气和电子工程师协会（IEEE）规定了这些步骤。本章包括了IEEE 802.3 CSMA/CD的规定。

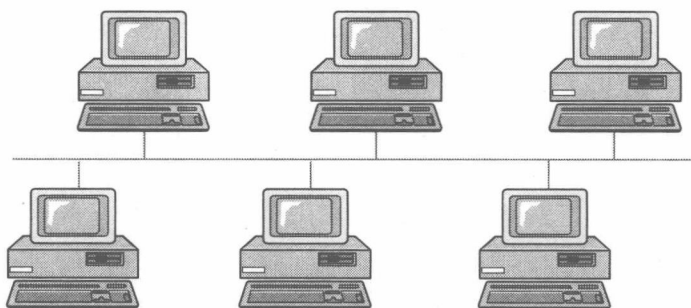


图1.1 Ethernet网络电缆段

在Token Ring及ARCnet LANs上，每个站都在等待令牌以获得允许在电缆接线系统中发送数据，以防止各个工作站同时发送信息。因为令牌在网络上是一个一个地传递的，在站节点地址（ARCnet）或物理接线（Token Ring）的基础上，每个工作站在电缆接线系统中发送机会上是相同的。因为令牌是以确定的过程传递的，所以这种访问方法被称为“确定型”（deterministic），它确保能够实现对网络的访问。

本章解释了工作站怎样使用CSMA/CD访问方法在网络上送出信息报文（参考第6～第13章，TokenRing/802.5的访问方法）。

Ethernet的优缺点

Ethernet的主要优点包括：

- **容易安装：**所有的工作站都可利用简单的T连接器或收发器连接到网络上。Ethernet不需要集线器。
- **知名技术：**商业普遍采用Ethernet已有多年的。
- **价廉物美：**在前两年中Ethernet卡的价格已明显下降。
- **多种接线配置：**就像第3章所述，可利用不同的电缆类型和电缆设计配置Ethernet LANs。

注意：在第3章中将讨论怎样使用集线器系统和RJ45（电话类型的）连接器。

Ethernet的缺点包括：

- **负荷重的LANs上通信量会下降：**在CSMA/CD LANs上，当网络负荷增大时，性能会下降。虽然有很多人觉得CSMA/CD是Ethernet的最大特点，但其他人却以为它是Ethernet的主要弱点，因为较高的网络中负荷会严重降低它的性能。
- **诊断困难：**由于普通的电缆系统使用的电缆有粗有细，所以Ethernet诊断故障是很困难的。如果电缆中有断裂，整个电缆段都会失效，也许很难找到造成问题的网络节点。新的10BaseT网络已经解决了部分问题。

在开始Ethernet LAN上的工作之前，应着重理解CSMA/CD协议是怎样工作的。这将有助于你了解分析器提供的及本书中其他的统计、差错和效用信息。

注意：在本章中不包括CSMA/CD协议的细节，参考IEEE 802.3规范。

CSMA/CD如何工作：发送

因为CSMA/CD网络使用公共的电缆接线系统，必须制定某些规则以避免工作站同时发送信息。但是，如果有同时发送的，也必须能够查出是否已经发生了数据冲突，并且应该能够决定何时再次发送。（CSMA/CD协议和团体线路的电话相似，许多人可共享同一线路，同时说话。但是如果每个人同时说话，声音就会混乱。而如果大家能够依次轮流，那么每个人的声音都会很清楚。）

当在CSMA/CD网络上发送信息时，站遵照下面5个步骤：

1. 发送之前先听。
2. 如果电缆忙则推迟发送。
3. 发送并同时检查有否冲突。
4. 如果有冲突，则等待再次发送。
5. 再次发送或停止。

步骤1：发送之前先听

如图1.2所示，站连续地监视电缆段上的载波（carried on）信号。通常由电压辨认电缆上的这个信号指出电缆在使用中。如果站未检测到“载波”，它会认为电缆是空的，就开始发送。（就像前面所说的团体电话线路，它相当于在讲之前先听听）。当站发送时如果线路是忙的（有载波），那么数据包会和线上的信号发生冲突。

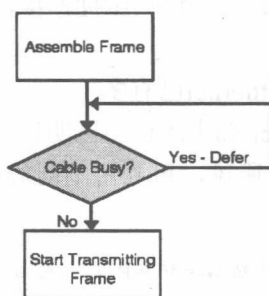


图1.2 站监视电缆的活动

步骤2：如果电缆忙时则推迟（等待）发送

为了避免发生冲突，如果电缆正在使用，如图1.3中所示，站必须推迟（等待）。如果知道电缆正处于忙的状态，工作正常的接口卡将不会有意发送信息。（在团体的线路上，如果你听到有人在讲话，那么你就得等那人讲完以后再说）。推迟的时间（Deferral time）是指线路刚刚空闲而再次发送时所必须等待的时间。

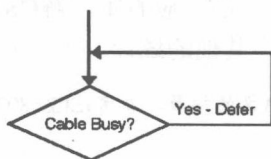


图1.3 如果线路忙站推迟发送

步骤3：发送和检测冲突

当传输媒介空闲时（carrier off）至少有 $9.6\mu\text{s}$ ，就像你在图1.4中见到的，站就可以发送了。帧在电缆系统上同时向两个方向传送。

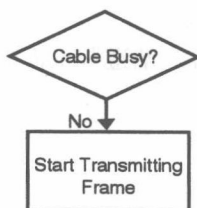


图1.4 如果电缆空闲，站可以开始发送

如果在电缆上另一个站同时已发送了数据包，如图1.5所示，数据包在线路上则会发生