HZ BOOKS

Microsoft® Press

Microsoft 核心技术丛书

Windows Server 2008 TCP/IP 协议和服务参考手册

Windows Server 2008 TCP/IP Protocols and Services

（美）Joseph Davies 著
贾笑明 汪国安 等译

机械工业出版社
China Machine Press

Windows Server 2008 TCP/IP 协议和服务参考手册

Microsoft
核心技术丛书

Windows Server 2008 TCP/IP 协议和服务参考手册

Windows Server 2008 TCP/IP Protocols and Services

（美）Joseph Davies 著
贾笑明 汪国安 等译

机械工业出版社
China Machine Press

本书详细介绍 TCP/IP 协议栈中多个协议的概念、原理、处理过程以及 Windows Server 2008 和 Windows Vista 中对于它们的支持，重点讨论 IPv4 以及相关的传输和网络基础结构支持协议，主要是协议本身（通信过程中介质上所见）和处理过程（表层下的工作机制）。本书包含 Microsoft 对于 TCP/IP 实现的处理过程细节以及如何通过注册表值和 Netsh. exe 工具命令来修改默认的行为。

本书可供网络技术人员参考。

Joseph Davies：Windows Server 2008 TCP/IP Protocols and Services（ISBN13：978-0-7356-2447-4，ISBN10：0-7356-2447-X）.

本书版权登记号：图字：01-2009-1587

图书在版编目（CIP）数据

Windows Server 2008 TCP/IP 协议和服务参考手册/（美）戴维斯（Davies，J.）著；贾笑明等译. —北京：机械工业出版社，2009.3

（Microsoft 核心技术丛书）

书名原文：Windows Server 2008 TCP/IP Protocols and Services

ISBN 978-7-111-25652-6

Ⅰ. W…　Ⅱ. ①戴…　②贾…　Ⅲ. 计算机网络－通信协议　Ⅳ. TN915.04

中国版本图书馆 CIP 数据核字（2009）第 009396 号

机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码　100037）

责任编辑：王　玉

北京京北印刷有限公司印刷

2009 年 3 月第 1 版第 1 次印刷

186mm×240mm · 21.75 印张

标准书号：ISBN 978-7-111-25652-6

定价：59.00 元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

本社购书热线：（010）68326294

译 者 序

深入学习 TCP/IP，可以使我们能够更加深入地了解网络上的通信如何发生，各种协议表层之下的任务处理又是如何进行的。本书别出心裁地利用了一些实用工具。在作者的精心组织下，读者能够实际“看到”这些网络上传递的数据包如何进行封装和处理。与当今流行的 Windows Server 2008 和 Windows Vista 操作系统中所用的技术相结合，这使得本书在实用性上得到了进一步提高。

由于 TCP/IP 标准的独立性与平台无关性，本书重点针对协议及协议操作本身进行讨论，使它不仅可以作为 Windows 网络管理员深入学习 TCP/IP 协议并排除网络问题的极佳参考书，也可以作为一部极好的 TCP/IP 深入学习教程供高校师生使用。

另外，书中大量使用 Network Monitor 捕获英文示例，对这些示例的理解与书中所提供的数据包结构示意图有着密切的联系，所以在翻译时，我们并没有像其他图书那样将图中内容一一翻译，而是尽量保持原貌。为了方便读者阅读，在涉及字段及关键术语说明时中英并陈，这样做的目的只有一个——让读者更容易理解书中的示例，并在其指导下进行实践。

参与本书翻译的还有侯彦娥、陈倩、陈霞、张啸风、童广林、李媛、霍俊伟、李俊等。他们的配合与支持，让本书的翻译工作得以顺利完成，在此向他们表示感谢。

感谢我的家人，在本书的翻译中占去了太多与他们在一起的时间，正是他们给了我无微不至的关怀与支持，让我能够全身心地投入到工作中。

虽然已经尽最大努力保证本书在翻译中的精确性，但难免还会有疏漏之处。如果读者朋友发现任何错误，请通过我的博客与我联系，我会将最新的勘误发布到上面，我的博客地址是：http://blog.sina.com.cn/mengmengbug。

贾笑明

2008 年 9 月于开封

前　言

本书详细了 TCP/IP 协议栈中多个协议的概念、原理、处理过程以及在 Windows Server 2008 和 Windows Vista 中对于它们的支持。本书重点讨论 IPv4 以及相关的传输和网络基础结构支持协议。虽然书中也包括了 IPv6 的概览，但是不涉及深度技术细节。更多有关 IPv6 及其在 Microsoft Windows Server 2008 和 Windows Vista 中的实现，请参见 Joseph Davies 所著的《Understanding IPv6，2nd Edition》（Redmond，Wash.：Microsoft Press，2008；ISBN 978-0735624467）一书。

本书主要讨论协议本身（通信过程中介质上所见）和处理过程（表层下的工作机制），而不是规划、配置、部署、管理或应用程序的开发。有关 TCP/IP 的规划、配置、部署和管理方面的讨论，请参阅《Windows Server 2008 Networking and Network Access Protection（NAP）》（Redmond，Wash.：Microsoft Press，2008；ISBN 978-0735624221），Windows Server 2008 帮助和支持，以及 Windows Server 2008 技术中心（http://technet.microsoft.com/windowsserver/2008）。关于使用 Windows 套接字进行 TCP/IP 应用程序开发的讨论，请访问 Microsoft 开发人员网络（http://msdn.microsoft.com）。

本书不包含 TCP/IP 在 Windows Server 2008 和 Windows Vista 中实现的代码细节，例如，内部结构、表、缓冲区以及相关的使用或编码逻辑。只有少数读者对这些细节感兴趣，并且出于安全原因和 Microsoft 知识产权的保护，它们不对外公开。不过，本书包含了 Microsoft 对于 Windows Server 2008 和 Windows Vista 中 TCP/IP 实现的处理过程细节以及如何通过注册表值和 Netsh.exe 工具命令来修改默认的行为。

注意　除非特别说明，否则对于注册表值的修改需要重新启动系统才能生效。

本书可用作深入学习 TCP/IP 知识的教材和详细的技术参考。本书不是 TCP/IP 或网络技术的初级读物。

读者对象

本书适合于以下读者：

- **Windows 网络顾问和规划人员**　所有计划或部署 Windows Server 2008 或 Windows Vista 计算机网络的人员。
- **Windows 网络管理员**　目前正在管理 Windows 网络和想获得有关 TCP/IP 及其在 Windows Server 2008 和 Windows Vista 中实现的额外技术知识的人员。
- **微软认证系统工程师（MCSE）和微软认证讲师（MCT）**　本书可作为 MCSE 和 MCT 对于 TCP/IP 协议栈的标准参考。
- **普通技术人员**　由于本书主要讲述 TCP/IP 协议及处理过程，与 Windows Server 2008 和 Windows Vista 中的实现独立，普通技术人员可把本书作为 TCP/IP 协议的深入参考资料。
- **信息技术（IT）专业学生**　可将本书作为教育机构或组织内部全面讲授中高级 TCP/IP 课程的极佳教材。

预备知识

本书希望读者已经了解网络基础知识，包含基本的组网概念和广泛使用的网络技术。例如，尽管本书详细讲述了 IP 数据包在以太网网段上发送时的封装方法，但并不涉及以太网历史或技术细节（如信号编码、布线、拓扑或配置选项等），希望读者已经具备这方面的知识。

本书希望读者对于 TCP/IP 协议栈和基于 Windows 网络所支持的协议集有最基本的了解，包括对于 TCP/IP 体系结构、IP 寻址、IP 路由、域名解析，以及动态主机配置协议（DHCP）和 Internet 协议安全（IPsec）这样的网络基础结构协议作用的基本了解。

本书的组织方式

本书分为 4 个部分，分别对应美国国防部（DoD）高级研究计划局（DARPA）模型中的 4 层：

- **网络接口层** 在这一部分中有两章讲述 Windows Server 2008 和 Windows Vista 支持的局域网（LAN）和广域网（WAN）技术，尤其是对 IP 数据报如何进行封装。该部分中还有一章讲述地址解析协议（ARP），它是为下一跳 IP 地址解析硬件地址（媒体访问控制（MAC）地址）的一个简单协议。该部分中还有一章讲述了点对点协议（PPP）协议栈，它为点对点链路提供了封装、链路协商和协议配置服务。
- **Internet 层协议** 这一部分讲述了 IP、Internet 控制消息协议（ICMP）和 Internet 组管理协议（IGMP）。关于 IPv6 的章节提供了 IPv6 的概览及其 Internet 上当前使用的 IP 版本 IPv4 的对比。
- **传输层协议** 这一部分讲述了发送不可靠消息的一个简单传输层协议，用户数据报协议（UDP）和发送可靠数据的一个复杂传输层协议、传输控制协议（TCP）。
- **应用层协议和服务** 该部分讲述了 TCP/IP 相关的关键基础结构协议和网络基础结构服务，例如，DHCP、域名系统（DNS）、Windows Internet 名称服务（WINS）、远程身份验证拨入用户服务（RADIUS）、IPsec 和虚拟专用网络（VPN）。

Network Monitor 跟踪

本书中演示的数据包结构和协议操作过程都是通过 Network Monitor 3.1[⊖]显示的数据包捕获。它们演示了线缆上可见的协议或服务的实际行为。本书涉及的所有跟踪都包含在示例文件[⊖]的 \Captures 文件夹下。书中显示或提及的所有 Network Monitor 捕获文件都包含在内。

注意 Network Monitor 的不同版本可以显示的数据包结构也有所差异。

教师须知

如果您是一位讲授 TCP/IP 协议栈高级知识的教师，那么强烈推荐使用本书教授 TCP/IP 课

⊖ Network Monitor 可以捕获并查看网络通信及捕获文件。可以从 http://go.microsoft.com/fwlink/?LinkID=92844 安装 Network Monitor 3.1。有关 Network Monitor 的最新信息，请留意 Network Monitor 博客 http://blogs.technet.com/netmon/。

⊖ 书中的“示例文件”可在华章网站（www.hzbook.com）的本书页面上下载。

程。显然，本书可以用作 Windows 网络管理员和系统工程师补充 TCP/IP 知识的教程，但由于书中的内容大部分是关于 TCP/IP 协议栈数据包结构和协议处理过程的细节，所以本书也可用作为独立于具体实现的 TCP/IP 教程。

同为教师，希望在您的努力下讲授这门有趣而又重要的技术时能够取得成功。

本版新增内容

本书是 Joseph Davies 和 Thomas Lee 所著的《Microsoft Windows Server 2003 TCP/IP Protocols and Services Technical Reference》的更新版，修改和更新如下：

- 第 2 章删除了串行线路 Internet 协议（SLIP）、X. 25 和异步传输模式（ATM）部分的内容。
- 第 3 章新增 Windows Server 2008 和 Windows Vista 中的重复地址检测和邻居不可达检测行为。
- 第 4 章删除了 Shiva 密码身份验证协议（SPAP）、Microsoft 质询握手身份验证协议（MS-CHAP）（也称为 MS-CHAP v1）和可扩展身份验证协议消息摘要 5（EAP-MD5）身份验证协议部分，新增受保护的 EAP（PEAP）身份验证协议。
- 第 5 章新增 RFC 3168 中定义的 IP 服务类型（TOS）字段中显式拥塞报告（ECN）字段的讨论。
- 第 10 章（以前的第 12 章）新增 RFC 3168 中定义的 TCP 段头中 ECN 标志的讨论。
- 第 12 章（以前的第 14 章）新增接收窗口自动调节、复合 TCP、ECN 和受限传输的讨论。
- 第 13 章（以前的第 15 章）增加新的失效网关检测算法、Forward RTO-Recovery 和新的丢失恢复方法。
- 第 14 章（以前的第 16 章）重排和重写，重点放在 DHCP 协议的细节和消息交换上。
- 第 15 章（以前的第 17 章）重排和重写，重点放在 DNS 协议的细节和消息交换上。
- 第 16 章（以前的第 18 章）重排和重写，重点放在 TCP/IP 上的网络基本输入/输出系统（NetBIOS）协议的细节和 WINS 消息交换上。
- 第 17 章（以前的第 20 章）重排和重写，重点放在 RADIUS 协议的细节和消息交换上。
- 第 18 章（以前的第 22 章）新增身份验证 Internet 协议（AuthIP）部分的内容。
- 第 19 章（以前的第 23 章）重排和重写，重点放在点对点隧道协议（PPTP）、第二层隧道协议（L2TP）的细节和消息交换上，并新增了安全套接字隧道协议（SSTP）相关的内容。
- 附录（以前的第 6 章）更新了 Windows Server 2008 和 Windows Vista 中使用的新技术。

未列出的章节中更新了 Windows Server 2008 和 Windows Vista 中新的特性、行为和设置。

删除了下列章节：

- 第 7 章。
- 第 19 章　有关 Internet 打印协议（IPP）的信息可参阅 RFC 2567、2568、2569、2910 和 2911；有关通用 Internet 文件系统（CIFS）的信息可于 http://www. microsoft. com/downloads /details. aspx? FamilyID = c4adb584-7ff0-4acf-bd91-5f7708adb23c&displaylang = en 的文档《Common Internet File System（CIFS）File Access Protocol》下载。
- 第 21 章　有关超文本传输协议（HTTP）的信息可参阅 RFC 2616；有关文件传输协议

（FTP）的信息可参阅 RFC 959；有关网络新闻传输协议（NNTP）的信息可参阅 RFC 977 和 2980；有关简单邮件传输协议（SMTP）的信息可参阅 RFC 821。

其他在线内容

本书补充的新内容或更新的内容将发布在 Microsoft Press Online Windows Server And Client Web site Web 站点上。根据 Windows Server 2008 的最终发布版本，更新的内容可能包括本书的内容、文章、附带内容链接、勘误和样章等。该站点位于 www. microsoft. com/learning/books/online/serverclient 并定期更新。

支持信息

本书代表了出版时 Windows Server 2008 和 Windows Vista 提供的 TCP/IP 协议栈中诸多协议实现的最新信息快照，其时正值 Windows Server 2008 RC 0 版和 Windows Vista Service Pack 1 的 Beta 1 版。书中的内容不包含之后发布的 Windows Server 2008 和 Windows Vista Service Pack 1 版本，或者 2007 年 11 月 15 日之后 IETF 标准的变化部分。

IETF 标准对于 TCP/IP 的最新信息可参见 IETF 站点：http://www. ietf. org/。

我们尽全力确保书中内容的准确性。Microsoft Press 在 Microsoft 知识库中提供了本书的勘误。要直接访问 Microsoft 知识库并查询书中的问题或错误，可以访问 http://support. microsoft. com/search/? adv = 1，在搜索框中输入 978 - 0735624474，然后点击搜索。

如果对本书有任何意见、问题或看法，请通过邮件或电子邮件发送至 Microsoft Press。邮件地址是：

Microsoft Press

Attn：Windows Server 2008 TCP/IP Protocols and Services Editor

One Microsoft Way

Redmond，WA 98052 - 6399

Email 地址是：MSPInput@ microsoft. com.

请注意这些地址不提供产品支持。有关 Windows 产品的支持信息请访问 Microsoft 支持站点 http://support. microsoft. com/default. aspx。

致谢

感谢参与本书各章节及附录内容技术审校工作的 Microsoft 的工作人员：Boyd Benson、Lee Gibson、Philippe Joubert、Jason Popp、Katarzyna Puchala、Aaron Schrader、Ben Schultz、Murari Sridharan、Brian Swander、Mark Swift 和 Jeff Westhead。特别要感谢 Dmitry Anipko，他是 Windows 网络核心开发团队中的一名软件开发工程师，对于标准的 IPv4 以及在 Windows Server 2008 和 Windows Vista 中 IPv4 的实现细节，他在多个章节给了我非常详细的反馈。

我还要感谢 Maureen Zimmerman（Microsoft Press 内容项目经理）、Kelly D. Henthorne（Abshier House 的项目经理）、Jim Johnson（技术审校）、Kim Heusel（文稿编辑）、Debbie Berman（排版）以及 Johnna VanHoose Dinse（索引）。

最后，我要向我的妻子 Kara 和女儿 Katie 表达我的感谢和感激之情，感谢她们对我为本书所投入的时间与精力上的耐心与宽容。

目　录

第三部分 传输层协议

第一部分　网络接口层

第 1 章　局域网技术

为了成功排除局域网（LAN）中出现的传输控制协议/网际协议（TCP/IP）问题，当使用 Windows Server 2008 或者 Windows Vista 计算机发送 IP 数据报和地址转换协议（ARP）消息时，理解它们是如何在基于以太网（Ethernet）、令牌环（Token Ring）、光纤分布式数据接口（FDDI）和 IEEE 802.11 这样的 LAN 技术链路上进行封装是非常重要的。例如，以太网上发送的 IP 数据报能够以两种不同的方式进行封装，但是如果两个主机使用了不同的封装方法，那么它们之间就无法互相通信。当使用 Microsoft Network Monitor 时，理解局域网封装技术对于正确解释帧中的以太网、令牌环、光纤分布式数据接口和 IEEE 802.11 部分也是非常重要的。

1.1　局域网封装

由于 IP 数据报是开放系统互联（OSI）模型的网络层实体，IP 数据包在物理介质中发送前必须通过数据链路层的帧头和帧尾封装。数据链路层的帧头和帧尾提供了下列服务：

- **界定**　数据链路层的帧必须能够相互区别。在每一帧中，帧头和帧尾要标记出来，并且帧的有效负载与数据链路层的帧头和帧尾也能够区分开来。
- **协议标识**　很多组织都在使用诸如 TCP/IP 或 AppleTalk 这样的多协议族，协议之间必须能够相互区分。
- **寻址**　对于以太网这样的共享访问局域网技术，必须标识出源节点和目的节点。
- **比特级完整性**　为了在硬件接收的整个帧中检测比特级错误，需要以校验和的形式进行比特级完整性校验。校验和通过源节点计算并添加到帧头或帧尾。目的节点会重新计算校验和，并与包含的校验和进行比对。如果校验和匹配，那么就认为该帧不存在比特级错误。如果校验和不匹配，该帧会被悄悄丢弃。这种帧校验和附加在像 IP 或 TCP 这样的上层协议所提供的校验和之上。

不同网络类型（例如以太网或者令牌环）封装传输数据的特定方式称为帧格式（frame format）。帧格式对应于 OSI 数据链路层的逻辑链路控制（LLC）和媒体访问控制（MAC）子层置于帧中的信息，它通过帧头和帧尾标识自身。如果提供的网络类型存在有多种帧格式（例如以太网），那么这些帧格式会提供不同的帧头和帧尾结构，并因此互不兼容。换言之，在同一个网段（路由器分界）的所有节点必须使用相同帧格式才能够相互通信。

本章主要讨论以太网、令牌环、FDDI 和 IEEE 802.11 局域网技术，以及它们对于 IP 数据报和

ARP 消息的帧格式。这些内容中并不包含附加资源计算机网络（ARCnet）部分，因为它不是一种广泛使用的网络技术。

1.2　以太网

以太网是美国夏威夷大学开发的9.6 kbps 的 ALOHA 无线传送系统发展演变而成。ALOHA 网络系统的一个关键特性就是所有发送器都共享同一个信道并竞争信道访问进行传送，这就成为我们今天所了解的基于“竞争”的以太网的基础。

1972 年，施乐（Xerox）公司开发出基于 ALOHA 系统原理的 2.94 Mbps 网络。这种新的网络叫做以太网，它的特点是载波检测，也就是发送器在试图传送数据前要先进行侦听。1979 年，数字装备公司（Digital）、英特尔和施乐共同开发出 10Mbps 以太网的业界标准，称为以太网Ⅱ（Ethernet Ⅱ）。1981 年，IEEE Project 802 成立了 802.3 小组委员会，使得 10Mbps 以太网成为一项国际标准。1995 年，IEEE 批准了 100Mbps 版本的以太网，叫做快速以太网（Fast Ethernet）。之后增加的标准定义了更高速率的以太网，包括 1Gbps、10Gbps 和 100Gbps。

在 IEEE 802.3 规范出现之前以太网就已经存在，并且因为有多个以太网的标准，所以在同一个以太网中会有多种数据封装方式进行数据传送。当同一个以太网网段中有两个主机无法进行通信会让人非常困惑，即便它们都使用了正确的通信协议（如 TCP/IP）和应用层协议（如文件传输协议（FTP））。

以太网网段中传送的 IP 数据报和 ARP 消息使用以太网Ⅱ（描述在 RFC 894 中）或者 IEEE 802.3 子网访问协议（SNAP）（描述在 RFC 1042 中）进行封装。

1.2.1　以太网Ⅱ

以太网Ⅱ（Ethernet Ⅱ）的帧格式是在 IEEE 802.3 规范出现之前由数字装备、英特尔和施乐公司共同创建的以太网（Ethernet）规范所定义的。以太网Ⅱ帧格式又称为 DIX 帧格式。图 1-1 显示了对 IP 数据报的以太网Ⅱ封装。

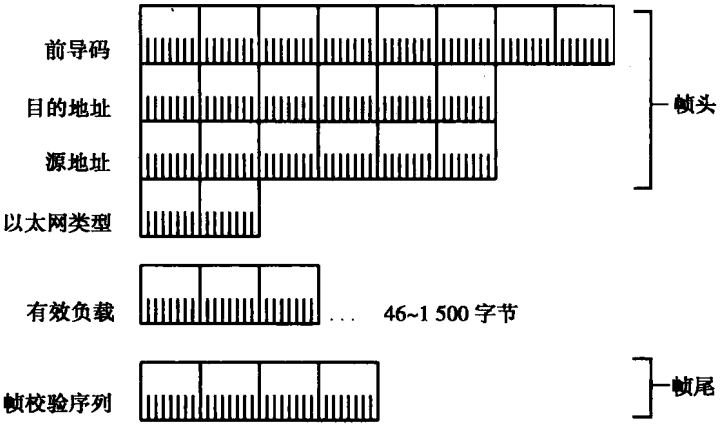

图 1-1　以太网Ⅱ帧格式显示了它的帧头和帧尾

以太网 II 帧头和帧尾

以太网 II 帧头和帧尾的字段定义如下：

- **前导码**（Preamble）　前导码字段长度为 8 字节，包含了 7 字节的 1 和 0 交替（每个字节都是位序列 10101010），用来同步接收站并表示帧起始的 1 字节 10101011 序列。前导码提供了接收端同步和帧界定服务。

注意　前导码字段在 Network Monitor 中不可见。

- **目的地址**（Destination Address）　目的地址字段长度为 6 字节，它表示目的位置的地址。目的位置可以是单播、多播或是以太网广播地址。单播地址又叫做个体、物理、硬件或 MAC 地址。对于以太网广播地址，所有 48 位都设置为 1 来构造地址 0xFF-FF-FF-FF-FF-FF。
- **源地址**（Source Address）　源地址字段长度为 6 字节，它指示发送节点的单播地址。
- **以太网类型**（EtherType）　以太网类型字段长度为 2 字节，指示以太网帧中包含的上层协议。当网络适配器将帧传递到主机的网络操作系统后，以太网类型字段的值用于传递以太网有效负载到合适的上层协议。如果收到帧的以太网类型字段值没有上层协议对其所指的有效负载注册有关联，那么该帧会悄悄丢弃。

  在以太网 II 的帧格式中，以太网类型（EtherType）字段被当作协议标识符使用，对于 IP 数据报该字段被设置为 0x0800，对于 ARP 消息，该字段会被设置为 0x0806。当前以太网类型字段值定义的列表可以从 http：//standards. ieee. org/regauth/ethertype/eth. txt 找到。
- **有效负载**（Payload）　以太网 II 帧的有效负载由上层协议的协议数据单元（PDU）组成。以太网 II 能够发送的最大有效负载是 1 500 字节。因为以太网有冲突检测机制，以太网 II 帧必须发送至少 46 字节的有效负载。如果上层 PDU 少于 46 字节，那么必须填充到至少 46 字节大小。有在以太网最小帧大小的详细讨论可参见本章稍后的“以太网最小帧大小”部分。
- **帧校验序列**（Frame Check Sequence）　帧校验序列（FCS）字段长度为 4 字节，它为以太网 II 帧提供了比特级完整性检验，帧校验序列也称为循环冗余校验（CRC）。源节点计算 FCS 的值，并把结果放到该字段中，当目标节点收到 FCS 时，它使用同样的 CRC 算法并将得到的值与源节点放在 FCS 字段中的值进行比较。如果它们匹配，那么就认为帧有效，目标节点会对它进行处理；如果不匹配，该帧会被悄悄丢弃。

FCS 计算是用 33 位的质数除以帧的位数量（不包括前导码和 FCS 字段）。这个除法计算的结果会得到商数和余数。4 字节的 FCS 字段设置为余数的值，它始终是 32 位值。FCS 能检测到所有的单个位错误。虽然数学上有选择地改变帧中的多个位也许不会改变 FCS 字段值的有效性，但对于随机噪声类型和网络产生的破坏，从而导致帧中位改变但 FCS 仍然有效的情况几乎是不可能发生的。

FCS 计算只提供比特级完整性服务，而不是数据完整性或是身份验证服务。有效的 FCS 并不