NT Network Plumbing: Routers, Proxies, and Web Services

计算机网络基础与应用系列丛书

由经验丰富的专家撰写

内容全面、覆盖面广

教你连网技术

(美) Anthony Northrup 著
宇尘翻译组 译

Windows NT网络实现——路由器、代理和Web服务

机械工业出版社

IDG BOOKS WORLDWIDE

CMP

本书并不是针对初学者的，而且针对那些想深入理解Windows NT和互联网的人士。

本书讲述了互联网基础、连接、著名产品等内容，并包括了大量的细节，从而使读者能在遇到问题之前预料并计划如何处理它。

本书注重于Microsoft和其他软件开发商所实现的协议以及底层标准，并包括了对新软件的解释和关于下一版的大量信息。

通过阅读本书，读者能真正理解Windows NT网络是如何实现的，并得到基于Windows NT的高层系统和网络工程以及底层排错所需的知识。

本书版权登记号：图字：01-98-1423

图书在版编目(CIP)数据

Windows NT网络实现——路由器、代理和Web服务/(美)诺思拉普(Northrup, A.)著；宇尘翻译组译. - 北京：机械工业出版社，1998

(计算机网络基础与应用系列丛书)

书名原文：NT Network Plumbing: Routers,Proxies, and Web Services

ISBN 7-111-06930-7

Ⅰ.N... Ⅱ.① 诺... ②宇... Ⅲ.互联网络 Ⅳ.TP393

中国版本图书馆CIP数据核字(98)第32421号

出 版 人：马九荣 (北京市百万庄大街22号 邮政编码100037)

责任编辑：温莉芳 李云静

北京市密云县印刷厂印刷·新华书店北京发行所发行

1999年1月第1版第1次印刷

787mm × 1092mm 1/16 · 21印张

定价：38.00元

前　言

理解复杂系统的关键在于细节。而细节的理解则因人而异。一般来讲，对细节的理解来自于经验。经验是一个可怕的老师，传授的过程中常常伴随痛苦和代价。更糟糕的是，经验只在学生需要知识时才进行传授。

《Windows NT网络实现——路由器、代理和Web服务》一书所讲授的经验能使你更好地理解复杂系统，并更好地完成工作。希望本书能成为一个比经验更敏捷、更慈祥的老师。

技术原则——特别是系统和网络工程——需要理解大量的细节。这些细节是可怕的，而且大多数人只在需要时才学习它们。《Windows NT网络实现——路由器、代理和Web服务》一书中充满着大量的细节，从而使你能够遇到问题之前预料并计划复杂系统中的问题。

本书适合的读者

《Windows NT网络实现——路由器、代理和Web服务》一书不是针对初学者的；而是针对那些想深入理解Windows NT和互联网的人士。当然，雄心勃勃的初学者也可能从本书中受益匪浅，但是阅读起来相当困难，因为我没有在必要的地方提供背景信息。本书没有关于如何使用Windows NT用户界面的逐步描述，而是假设你已熟悉Windows NT和网络的基础知识或者可以很方便地得到联机帮助。《Windows NT网络实现——路由器、代理和Web服务》一书的独特之处在于它不是为初学者准备的。

Windows NT是从Microsoft的桌面操作系统演化而来的，或许这就是迄今为止Windows NT的网络方面被忽视的原因。关于Windows NT网络方面的文档一直是深奥的，似乎只有那些Microsoft内部的开发者才需要真正理解其工作原理。实际上，研究是最困难的部分，而大部分研究只是靠协议分析器之类的工具手工完成的。

我希望能拓宽读者的知识，以便能够真正深入理解本书所覆盖的主题；也希望使读者真正理解Windows NT网络是如何工作的。读完本书后，读者应得到基于Windows NT的高层系统和网络工程以及底层排错所需要的知识。当然。高层工作依赖于底层的理解；好的网络体系结构能够进行分解，以便更深入地理解。

Windows NT的版本

写本书时，最流行的Windows NT是Windows NT 4.0(带有Service Pack 3)，因而《Windows NT网络实现——路由器、代理和Web服务》一书注重于NT 4。即便NT升级以后本书仍有用，因为本书注重于Microsoft 和其他软件开发商所实现的协议以及底层标准。标准通常有几年的生命期，而Microsoft 可能在版本之间的协议实现上做细小的调整，并保持大部分一致。为了扩展本书的使用期限，我在书中包括了对新软件的解释和关于下一NT版本的大量信息。

本书的组织

本书分为四个部分和五个附录。

第一部分　互联网基础，提供了基本信息，尽管绝大多数读者已经了解了大部分材料，但是该部分填充了他们现有知识之间的空隙。

第二部分　连接，覆盖了网络的设计和实现方面。

第三部分　实现，提供了使特定产品有效正常工作所需的信息。

第四部分　著名产品，检查了基于Windows NT 的几种特殊产品。

最后，五个附录提供了重要的参考信息。附录A 描述了已知的TCP/UDP端口号。附录B 列出了request for commands 各项。附录C 列出了重要的头信息。附录D 定义了常用的缩写。附录E 列出了CIDR(classless interdomain routing)名。

读者可以自始至终地阅读本书的各个主题，以便得到大量的有用信息。但是本书也可以用于排错和研究过程，所以，如果遇见了路由和远程访问服务的问题，可以直接阅读第13章。如果你正在实现常用Internet文件系统(CIFS)，可以阅读第14章。如果理解某章时需要用到其他部分的信息，本书会告诉你阅读哪些章节。

读者反馈

希望收到每个读者的信息，您的意见有助于提高本书下一版本的内容。与我联系最方便的途径是northrup@ultranet.com。我会尽力回复所接收的每封E-mail。

(本书英文原名：NT Network Plumbing:Routers, Proxies,and Web Services,)

ISBN:0-7645-3209-X

作者：Anthony Northrup

目　录

第三部分 实 现

第四部分 著名产品

第五部分 附 录

第一部分　互联网基础

第1章　网 络 基 础

本章重点：

- ◆ 使用OSI模型组织网络
- ◆ 了解Windows NT 支持的各种网络协议
- ◆ 理解路由和路由协议

本章介绍几个关键的网络概念并试图提供技术概览，用于填充技术与经验之间的空隙，并引入一些理解本书所需要而在网络业界并不常见的概念。那些具有丰富的网络和工程经验的人员可以越过本章。但是就我本人而言，我总是喜欢阅读所熟悉的材料。首先，它使我能够更新记忆中过时的主题；其次，每个作者都试图在每个主题中引入自己的观点；最后，我总是觉得对于网络，仍有很多不知道的内容。我常常从某篇文章或某本书籍中学到新的东西。

1.1　OSI模型

开放系统互联(Open System Interconnection, OSI)模型是由国际标准化组织(International Standards Organization, ISO)于1983年开发的网络的概念模型。在开发该框架过程中，ISO建立了一个词汇表为全球工程师描述那些已经理解并想当然的概念提供了一组词汇。OSI模型将通信功能分解成七个层次。这些层次辅助网络应用程序和用户之间的通信的可视化，允许开发商和软件工程师在某个时刻按照清楚的指南对通信模型的某个片段进行工作。

OSI模型的每个层次都有一个简单的任务，即为该层的直接上层提供服务。每层都知道下一层由其支配，正在等待命令。同时，每层都以标准方式从上层接收数据，并提供赋予该层的服务。按照该模型，每层就像与远程对等层次进行直接通信。

OSI使用了几个在网络业界并不常见的主要术语。例如，每层通过网络与对等层次通信时传送的数据称为协议数据单元(Protocol Data Unit, PDU)。而当每层将数据传送到下一层次时，数据称为服务数据单元(Service Data Unit, SDU)。图1-1解释了这个概念。

每个网络和系统工程师都应该深入理解OSI模型。对大多数人而言，OSI并没有启发性，而且对很多人来讲，只有在业界经历几年之后才有意义。但是，其词汇表在现实世界中相当普遍并广泛用于本书中。表1-1列出了OSI模型的各个层次。

表1-1　OSI模型的各个层次

层　次	功　　能	应　　用
应用层	为应用程序访问网络提供接口	Telnet、FTP、HTTP
表示层	提供应用层之前的最后抽象层次，屏蔽了来自于会话层的应用程序的细节	工作站服务，网络转向器

（续）

层　次	功　　能	应　　用
会话层	提供复杂的会话控制，很少被引用	基于TCP/IP的NetBIOS
传输层	提供连接、错误检查和有保障传送	TCP，UDP，SPX
网络层	提供网络之间的寻址、导航和路由	IP，IPX
数据链路层	提供网段内的寻址、冲突避免和某些错误检查	Ethernet，令牌环(Token Ring)，FDDI
物理层	指定同一网段内主机之间的物理信号发送、接收和携带方式	第五类双绞线，光纤，集线器

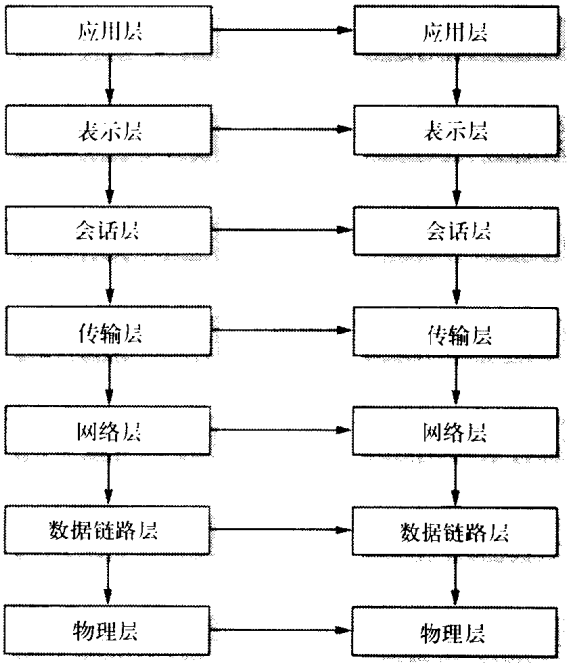

图1-1　PDU在不同主机的对等层次之间通信，SDU在同一主机的各个层次之间通信

OSI模型并不同于每个协议，它只是一个简单的理论模型。实际上，很少有协议真正遵从OSI规范。例如，TCP/IP是在OSI之前设计的基于各层互不相关的四层模型。现在，已经设计了一组遵从OSI模型的协议，包括在功能上大致等价于IP的无连接网络协议(Connectionless Network Protocol, CLNP)和称为媒介系统到媒介系统(Intermediate System to Intermediate System, IS-IS) 的路由协议。本书很少引用这些协议；在业界中也很少遇到，而且在Windows NT中并没有实现。

以下各节分别详细描述各个层次。较其他层次而言，我在某些层次中，如网络层和传输层，加入了更多的细节。这是对现实世界各个层次重要性的一种反映，并且反映了我认为整体理解OSI模型的关键所在。我还试图讲述“会话式OSI”，一种同其他工程师交流的重要技巧。

1.1.1　第一层：物理层

物理层包含了网络中所有的网线、电气特性、针孔和连接器，通常被称为第一层。那些实际接触和感觉的东西(包括电振)都属于该层。对本层我讲述得很少。物理拓扑因网络而异；OSI模型的优美之处在于能够不考虑具体的网络物理实现而讨论高层网络。

1.1.2 第二层：数据链路层

第二层数据链路层定义了网络连接的拓扑结构(例如，星型、环型或总线)和单个网段内的机器标识。LAN中最常见的第二层协议是Ethernet，但是令牌环和FDDI也很普遍。帧(frame)传递常用于数据链路层的WAN协议并提示其他的术语。

注意 数据在网络中带有数据链路层的头尾发送时称为帧。使用协议分析器调查网络通信时，如果数据链路层的头尾很重要，可以将分析的数据看作帧。例如，排除媒体访问控制(Media Access Control, MAC)地址故障时，就是对帧进行分析。

虽然第二层协议各不相同，但是大部分都包含一个MAC地址。Ethernet MAC地址是一个分配给特定网络接口的扁平48位二进制数字。数字的分配是由Internet分配数字的权威组织统一管理，从而保证分配给每块网卡的数字都是唯一的。第二层常见的其他字段包括指明帧大小的字段和用于确认帧中数据没有被改动的循环冗余检验(Cyclical Redundancy Check, CRC)字段。

数据链路层包含访问多个系统的能力。这是通过在目的MAC地址中使用特定的广播地址实现的。

OSI模型的第二层存在两种常见的网络设备：网桥和交换器。近几年来，因为路由协议较网桥协议更为流行，而且第三层的交换代价逐步降低，网桥渐渐不再流行。网桥连接两个在物理上分离的网络，倾听从某个网段发出的必须转发到另一网段的帧。网桥存在于OSI模型的第二层，从定义上讲不包含分析第三层通信的智能。这是它的一个局限性，但这种简单性带来了速度上的优势。通过减少分析帧的次数，网桥能在网络之间转发更多的通信量。从内部讲，网桥在其直接连接的网络及其主机的MAC地址之间建立了一个映射，如图1-2和表1-2所示。

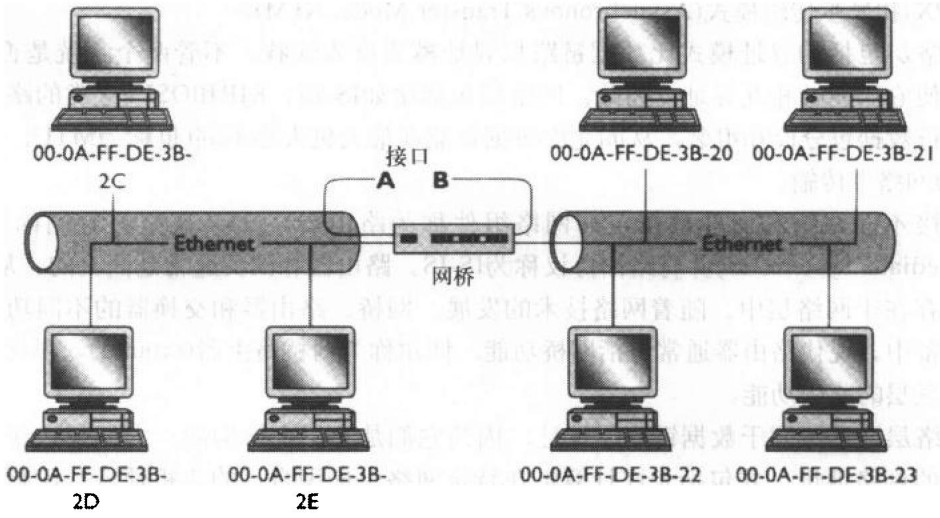

图1-2 网桥按照帧中的MAC地址转发网段之间的通信

网桥倾听网段中的每一帧并将目的MAC地址与内存中的表进行比较。通过查阅RAM中的表，网桥能够判断目的MAC地址是否处在正确的网段。如果是一个广播帧或是属于另一网段的帧，就复制该帧。

表1-2 网桥路由表的例子

MAC地址	接 口
00-0A-FF-DE-3B-2C	A
00-0A-FF-DE-3B-2D	A
00-0A-FF-DE-3B-2E	A
00-0A-FF-DE-3B-20	B
00-0A-FF-DE-3B-21	B
00-0A-FF-DE-3B-22	B
00-0A-FF-DE-3B-23	B

交换器执行许多与网桥相同的功能，并在许多网络中取而代之。网桥按照MAC地址转发帧，但是必须拥有八个或八个以上网络接口。每个接口必须直接连到主机，或者能够连接到其他的交换器或集线器。近几年来，交换器端口的价格已降到足够低，以至于交换器能够真正替代在物理层上操作的集线器。Windows NT只是在远程访问服务(Remote Access Service, RAS)中包含很弱的网桥功能。因为网桥不是NT的关键组件，本书中将不再讨论。

请记住，将网络通信分层的所有目的在于使各层之间相互独立。因此，网桥和交换器在转发携带TCP/IP的帧或携带IPX/SPX的帧时并无分别。

1.1.3 第三层：网络层

OSI模型的第三层，即网络层，定义通信如何通过网络。其定义的寻址模式包括网络和主机地址、通信控制机制以及校验和。本书后面的章节会更详细地讨论网络层中的几个关键概念：寻址(第2章)、路由(第2章和第13章)和流量控制 (第2章和第9章)。

第三层协议最著名的例子有Internet 协议(Internet Protocol, IP)、Internet控制消息协议(Internet Control Message Protocol, ICMP)、互联网包交换(Internetwork Packet Exchange)、X.25(IPX)和异步传输模式(Asynchronous Transfer Mode, ATM)。

网络层包括的寻址模式比数据链路层寻址模式更为强壮。不管两个系统是否直接相连，网络层使它们能够相互寻址。为此，网络层包括诸如IS-IS、RIP和OSPF之类的路由协议，并能够进行数据包分段和组装，从而允许数据包能在最大包大小不同(也称为MTU，或最大传输单元)的网络中传输。

连接不同网络和交换数据包的网络组件称为路由器。OSI 模型将它们称为媒介系统(Intermediate System, IS)并将路由协议称为IS-IS。路由器和网关通常是同义的。从定义上讲，路由器存在于网络层中。随着网络技术的发展，网桥、路由器和交换器的不同功能将合并到单个设备中。现代路由器通常包括网桥功能，偶尔称为网桥路由器(brouter)。现代交换器通常包括第三层的路由功能。

网络层地址不同于数据链路层地址，因为它们是有层次结构的。它们包括帮助路由器发现目的的网络地址，并包括允许计算机在特定网络中标识自己的主机地址。IP有被网络和主机地址共享的32位，其位数的分配稍有不同。相反，IPX有一个32位的网络地址并用MAC地址作为主机地址的端口号。

1.1.4 第四层：传输层

OSI 模型的第四层，即传输层，负责维护网络两个节点间的会话。它提供错误纠正以及

数据分段和组装的功能。

IP协议组的传输层协议包括传输控制协议 (Transmission Control Protocol, TCP)和用户数据报协议(User Datagram Protocol, UDP)。有序包交换(Sequenced Packet Exchange, SPX)是IPX第三层协议的常用第四层协议。

第四层协议可分为两种：面向连接和无连接。面向连接协议允许主机之间进行双向会话。它们提供有保障的传输和序号。TCP是TCP/IP栈中的面向连接传输协议。TCP的常见应用有World Wide Web请求、Windows NT 文件传输和Telnet通信。

无连接的第四层协议的优点在于开销较小。在无连接的通信中，消息发送后发送者不需要等待包是否正确传输的通知。因为它们不需要为序号维护头字段，而且发送者不需要等待来自目的端的确认，所以无连接协议更有效。但是，它们只适合传输那些并不关键的通信。UDP是TCP/IP栈中的无连接传输协议。UDP的常见应用有DNS查询、Windows NT 浏览器通知和网络广播。

1.1.5 第五层：会话层

OSI 模型的第五层，即会话层，提供复杂的会话控制。它允许管理和协调主机之间的通信。会话层也负责用户认证。

实际中，会话层是OSI层次中最不实用的一层并很少被引用。在基于TCP/IP的美国国防部模型中，并没有与会话层对应的层次。因为本书注重于TCP/IP，而会话层和表示层没有直接的关联，所以本书对它们的讲述很简单，在TCP/IP之上实现的会话层协议是NetBIOS，第10章将详细讨论。

1.1.6 第六层：表示层

OSI 模型的第六层，即表示层，提供了OSI 模型的应用层的抽象。允许应用程序协商数据的标准表示。网络转向器，如工作站服务，通常使用表示层。

该层主要提供不同格式之间的转化，例如，将回车转换成回车换行。诸如压缩和加密之类的任务也应当在本层实施，尽管它们常常在其他层次的协议中实施。像会话层一样，对表示层的讨论也很少。

1.1.7 第七层：应用层

应用层是OSI模型的第七层。应用层并不描述应用程序；相反，它为应用程序提供网络接口，从而，应用程序可以简单地在网络中进行通信，而不管物理拓扑、网络体系结构和网络协议，按照应用程序的输入，应用层利用其下的层次在网络中通信并在主机之间交换数据。

OSI模型的第七层常用的协议有HTTP(Web请求)、FTP(Internet文件传输)和Telnet(远程控制台)。

1.1.8 OSI 模型的工作方式

为了更好地说明OSI 模型的工作方式，让我们先看一个网络通信的例子。如果你激活了一个Web浏览器并访问某个Web站点，Web浏览器就用应用层协议HTTP发出请求。理论上，HTTP与在应用层上的Web服务器的HTTP服务直接通信。回过头看看图1-1，该图显示了协议

数据单元从客户端的应用层直接水平地传送到服务器的应用层——HTTP协议是该理论实际工作的一个具体例子。

发送请求获取Web页时，该协议并不考虑网络的拓扑结构，而是由底层考虑这些细节。HTTP创建由HTTP服务器接收的请求，如“GET/”，并将该数据传输给传输层协议。此时的传输层协议是TCP。(TCP/IP不包括表示层和会话层，所以该例子没有表示这两个层次。)

如图1-3所示，TCP加入头并将它的SDU传给网络层协议IP。接着IP在从TCP接收的数据中填充头并传给第二层协议，可能是Ethernet、令牌环、FDDI或其他的协议。数据链路层将数据传给第一层协议(第一层协议通常依赖于第二层协议)，第一层协议将数据转换成能够被目的主机网卡接收的实际电气信号。

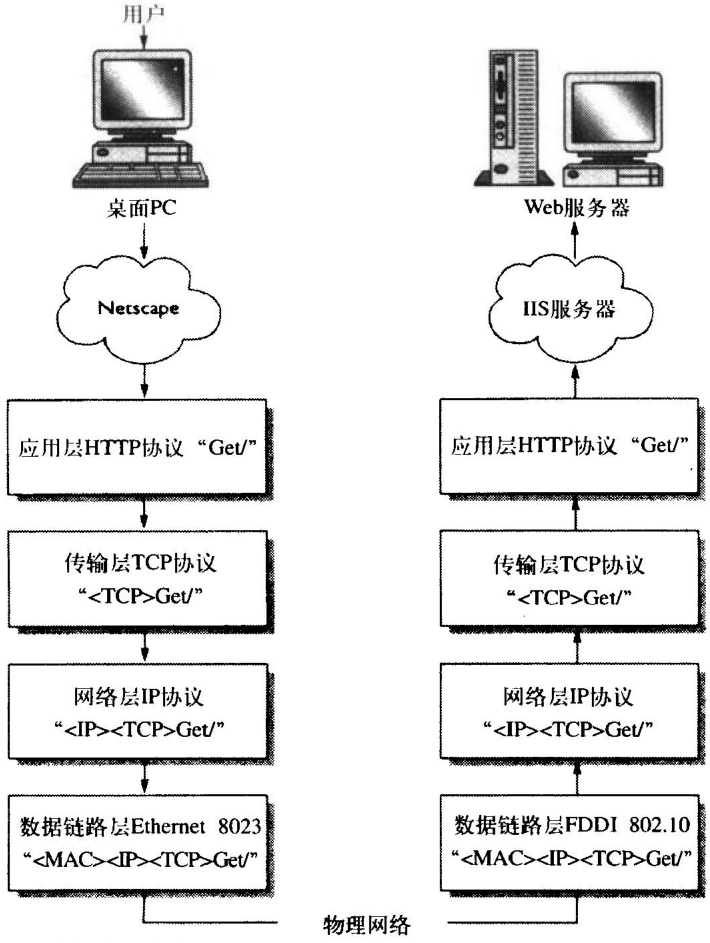

图1-3 来自用户的请求在转换成网络通信之后才在OSI 模型中传输。一旦到达主机，就沿OSI 模型向上移动以使服务器应用程序能够解释该请求

总而言之，OSI 模型对绝大多数网络工程师的最大价值在于提供了交流中描述协议的常用方法。例如，有强大OSI 模型知识背景的网络工程师可以很容易理解诸如“当然TCP不负责通过路由器的通信！它是第四层协议！”之类的谈话。

OSI模型的目的是提供分离的层，以使某一特定层的协议能够于其他层次的协议“固定和匹配”。但在实际上，第三层协议只与第四、五、六、七层协议一起使用。例如，不能一起使用传输层的TCP协议和网络层的IPX协议。TCP协议只与网络层的IP协议一起使用。不同层次

的协议分组导致了协议群组的发展。下一节描述Windows NT 支持的协议群组。

1.2 最常见的网络协议

随着网络的发展，不同的开发商开发了不同的通信方式。为了使通信成功可靠，网络中的所有主机都必须使用同一语言，不能带有方言。尽管英国人和美国人使用不同的英语，但是，仍然能够交流思想。计算机没有这种灵活性，因而必须开发严格的标准定义主机之间的每个包中每个字节中的每一位。这些标准来自于多个组织的努力，都尽量使通信更容易。

已经开发了许多协议，但是只有少数被保留了下来。那些协议的淘汰有多种原因——设计不好、实现不好或缺乏支持。而那些保留下来的协议经历了时间的考验并成为有效的通信方法。当今局域网中最常见的三个协议是Microsoft的NetBEUI、Novell的IPX/SPX和交叉平台TCP/IP。

1.2.1 NetBEUI

NetBEUI是为IBM开发的非路由协议，用于携带NetBIOS通信。NetBEUI缺乏路由和网络层寻址功能，既是其最大的优点，也是其最大的缺点。因为它不需要附加的网络地址和网络层头尾，所以很快并很有效且适用于只有单个网络或整个环境都桥接起来的小工作组环境。

因为不支持路由，所以NetBEUI永远不会成为企业网络的主要协议。NetBEUI帧中唯一的地址是数据链路层媒体访问控制(MAC)地址，该地址标识了网卡但没有标识网络。路由器靠网络地址将帧转发到最终的目的地，而NetBEUI帧完全缺乏该信息。

网桥负责按照数据链路层地址在网络之间转发通信，但是有很多缺点。因为所有的广播通信都必须转发到每个网络中，所以网桥的扩展性不好。NetBEUI特别包括了广播通信的计数并依赖它解决命名冲突。一般而言，桥接NetBEUI网络很少超过100台主机。

近年来依赖于第二层交换器的网络变得更为普遍。完全的转换环境降低了网络的利用率，尽管广播仍然必须转发到网络中的每台主机。事实上，联合使用100-base-T Ethernet，允许转换NetBIOS网络扩展到350台主机，才能避免广播通信成为严重的问题。。

1.2.2 IPX/SPX

IPX是Novell用于NetWare客户端/服务器的协议群组，避免了NetBEUI的弱点。但是，带来了新的不同弱点。

IPX具有完备的路由能力，可用于大型企业网。它包括32位网络地址，在单个环境中允许有许多路由网络。

IPX的可扩展性受到其高层广播通信和高开销的限制。服务广告协议(Service Advertising Protocol, SAP)将路由网络中的主机数限制为几千。尽管SAP的局限性已经被智能路由器和服务器配置所克服，但是，大规模IPX网络的管理仍是非常困难的工作。

1.2.3 TCP/IP

每种网络协议都有自己的优点，但是只有TCP/IP允许与Internet完全的连接。TCP/IP是在60年代由麻省理工学院和一些商业组织为美国国防部开发的，即便遭到核攻击而破坏了大部分网络，TCP/IP仍然能够维持有效的通信。ARPANET就是由基于协议开发的，并发展成为作为科学家和工程师交流媒体的Internet。