TCP/IP

TCP/IP详解

（第二版）

Special Edition Using TCP/IP Second Edition

Ramadas Shanmugam
[美] R. Padmini S. Nivedita 著
NIIT公司
尹浩琼 李 剑 等译

que
PHEI
電子工業出版社
Publishing House of Electronics Industry
http://www.phei.com.cn

TCP/IP 详解

（第二版）

Special Edition Using TCP/IP

Second Edition

Ramadas Shanmugam
R. Padmini
S. Nivedita
NIIT 公司

［美］ 著

尹浩琼 李 剑 等译

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内容简介

本书是一本讲述TCP/IP基本原理的技术参考书，从网络发展史入手，逐步展开对TCP/IP参考模型的讨论，详细剖析了包含于其中的各种网络协议。本书主要内容包括：TCP/IP参考模型、IP网络的编址机制、用户数据报协议、传输控制和数据流、文件传输和访问、域名系统（DNS）及地址解析与逆向地址解析等，并且对IP路由协议、IP协议应用和IP网络安全进行了深入探讨。本书的附录部分则提供了与TCP/IP相关的技术文档资料和故障处理等内容。

本书讲解由浅入深，内容完整实用，比较适合于那些想全面深入了解TCP/IP的工程人员使用，同时也可作为专业技术人员的参考书。

版权贸易合同登记号：图字：01-2002-6168

图书在版编目（CIP）数据

TCP/IP详解：第二版/（美）尚穆盖姆（Shanmugam, R）等著；尹浩琼等译. -北京：电子工业出版社，2003.8
书名原文：Special Edition Using TCP/IP，Second Edition
ISBN 7-5053-8980-7

Ⅰ.T... Ⅱ.①尚... ②尹... 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（2003）第067756号

责任编辑：赵红燕 贺瑞君
印 刷 者：北京兴华印刷厂
出版发行：电子工业出版社 http://www.phei.com.cn
北京市海淀区万寿路173信箱 邮编：100036
经 销：各地新华书店
开 本：787 × 1092 1/16 印张：20.5 字数：525千字
版 次：2003年8月第1版 2003年8月第1次印刷
定 价：33.00元

译 者 序

互联网从它的雏形ARPA网发展到今天的Internet，中间经历了无数的变革。每一种新技术的开发，新协议的提出，新标准的采用，都给互联网带来了深刻的变化。而在互联网飞速发展的时代，一直被人们视为网络互联核心的正是TCP/IP。虽然它只是一个用于在网络中通信的协议族，但是作用却非同一般，称之为Internet的灵魂一点也不为过。经过三十多年的发展，TCP/IP已经相当成熟和完善。TCP/IP，从名字上就可以看出，它由两个协议组成，即传输控制协议（Transfer Control Protocol，TCP）和Internet协议（Internet Protocol，IP）。这两个协议既独立工作，又互相作用，共同完成网络中的数据传输功能。虽然TCP/IP是作为Internet中的协议演进而来的，但也可以用于其他互联网络。

本书前7章介绍了基本的网络互联概念以及构成TCP/IP协议族基础的核心协议，第8章至第14章主要讲述TCP/IP参考模型应用层中的软件应用，第15章至第20章讨论了子网提供的IP编址机制和IP地址会话特性，以及TCP/IP提供的关于路由体系结构和路由机制的信息，接下来的两章内容虽然相对较少，但却是本书中很重要的一部分，讲述了TCP/IP协议族提供的安全特性。最后的5章除了展望TCP/IP技术的前景，还讨论了TCP/IP使用的先进联网技术。另外，不要忽略了本书的附录，它提供了很多重要的知识，比如局域网基础知识、TCP的端口号、请求注释（RFC）以及检测、排除故障的技巧等。

本书的作者都是有很多年计算机和网络培训经验的专家，他们经常和用户打交道，因此知道用户在想什么，当然也就知道用户最需要了解什么了。本书内容丰富全面，基本涵盖了TCP/IP的全部内容，并且讲解由浅入深，层次分明，又贴近读者，不失为TCP/IP方面一本不可多得的读本。

本书适用于那些想完整地了解TCP/IP知识的读者。如果读者是网络管理员，想知道平时经常与之打交道的网络事务后台究竟怎样运行，也可以在本书中找到答案。本书可能需要读者具备一定的计算机和网络基础知识，但不是必需的。关于网络基础知识的简单介绍，可以参考本书的附录。

本书由尹浩琼、李剑主译，参与翻译工作的人员还有欧阳宇、李明、石朝江、盛海燕、艾杨、谢小花、谢俊、冯奇、武堂、方净。由于时间仓促，再加上译者水平有限，书中错误在所难免，欢迎专家和读者批评指正。

前　言

TCP/IP是一个保证网络中或网络间能可靠、安全地即时通信的协议族。随着过去几十年间网络的迅猛发展，TCP/IP提供了一个标准化的通信和数据交换机制，该机制包含维持互联网络中平稳通信所需的硬件和软件需求。

TCP/IP简单地说只是一组通信标准，经过三十年的发展才变成今天的样子。这些标准是以请求注释（RFC）的形式发布的，它们除了规定很多软件规范外，还提供了设计网络体系结构的指导和规则。由于网络界先驱和专家们的辛勤努力，TCP/IP已发展成为最重要的互联网络通信机制，并经受住了时间的考验。目前，该协议族提供了用于实现移动通信、实时多媒体传输、服务质量和高度数据通信安全等方面的规范。

读者对象

如果读者想完整地了解TCP/IP知识，本书是最好的选择。阅读本书可能需要具有一定的计算机和网络基础知识，但不是必需的（关于网络基础知识的简单介绍，可以参考本书附录B“局域网基础”）。在各种不同操作系统中使用TCP/IP实现的网络管理员可能想知道幕后的技术原理，对于这些网络管理员，本书也是首选。

本书的组织结构

本书首先介绍了网络互联的概念，以及构成TCP/IP协议族基础的核心协议；讲述了使用TCP/IP进行网络通信的一些软件应用协议和实用程序；讨论了TCP/IP提供的子网和路由功能；也讲述了该协议族内在的安全特性；最后提到了一些先进的TCP/IP技术，并展望了TCP/IP的未来。

前七章介绍了基本的网络互联概念以及构成TCP/IP协议族基础的核心协议。

- 第1章“网络互联和TCP/IP介绍”，讲述互联网络的基础，当然也提到了TCP/IP的基础知识。
- 第2章“网络接口与链路层”，介绍了TCP/IP参考模型中的网络层和链路层。
- 第3章“Internet层协议”，讲述了一个叫做Internet协议的核心TCP/IP协议。
- 第4章“ICMP协议”，研究了TCP/IP通过Internet控制报文协议提供的错误跟踪和隔离功能。
- 第5章“传输控制和数据流”，让我们认识了TCP/IP协议族中的另一个核心协议——传输控制协议。
- 第6章“定时数据传输和性能的概念”，继续探讨传输控制协议的特性。本章研究了定时数据传输以及传输控制协议提供的性能增强特性。

- 第7章“用户数据报协议”，研究了如何利用用户数据报协议实现不可靠的数据传输。

第8章至第14章主要介绍工作在TCP/IP参考模型的应用层中的软件应用协议。

- 第8章“文件传输和访问”，讨论了利用诸如文件传输协议（FTP）、普通文件传输协议（TFTP）和网络文件访问（NFA）等协议来实现的远程文件传送和访问。
- 第9章“远程登录”，讲述了诸如Telnet和Rlogin等允许远程计算机登录的协议。
- 第10章“邮件传送协议”，讨论了TCP/IP如何利用简单邮件传输协议实现邮件传输功能。
- 第11章“超文本传输”，让读者了解TCP/IP如何利用超文本传输协议提供超文本数据传输功能。
- 第12章“简单网络管理协议”，讨论了利用TCP/IP的简单网络管理协议实现的网络管理功能。
- 第13章“域名系统”，介绍了TCP/IP利用域命名服务实现的域命名和域名解析功能。
- 第14章“自举协议：BOOTP和DHCP”，讨论了BOOTP和DHCP等应用协议，这些协议提供了自举和动态主机配置功能。

第15章至第20章主要讨论子网技术提供的IP编址机制和IP地址会话功能，以及TCP/IP提供的关于路由体系结构和机制的信息。

- 第15章“子网和无类编址”，讨论了用来解决IP地址短缺问题的IP编址机制和无类地址分配功能。
- 第16章“IP路由”，介绍了路由的概念以及TCP/IP实现的路由错误处理功能。
- 第17章“路由机制”，简要地描述了TCP/IP实现的路由机制。
- 第18章“自治系统路由”，研究了自治系统，以及在自治系统内部实现的路由机制。
- 第19章“自治系统间路由协议：EGP和BGP”，讨论了如何利用外部网关协议和边界网关协议在自治系统之间实现路由。
- 第20章“多播”，介绍了多播的概念以及如何在TCP/IP网络中实现多播。本章还讨论了多播数据报中Internet组管理协议所扮演的角色。

接下来的两章内容虽然相对较少，但却是本书中很重要的一部分，它描述了TCP/IP协议族提供的安全特性。

- 第21章“安全概念和专用网连接”，介绍了专用网的体系结构和通过专用网络互联实现的安全概念。
- 第22章“IP安全”，研究了TCP/IP如何通过使用IPSec框架解决基本的安全问题。

最后5章除了展望TCP/IP技术的前景，还讨论了TCP/IP使用的先进联网技术。

- 第23章“异步传输模式上的IP”，介绍了利用ATM实现的异步数据传输，以及IP如何才能在ATM框架上实现。
- 第24章“VoIP”，研究了TCP/IP提供的能够进行实时语音传输的标准和协议。
- 第25章“移动IP”，讨论了如何利用移动IP框架实现IP的移动支持。
- 第26章“IPv6”，介绍了下一代Internet协议实现，即IPv6。

- 第27章“服务质量”。随着网络互联逐渐成为一个有利可图的商业领域，提供服务质量成为一项很重要的生存策略。本章向读者介绍TCP/IP如何在互联网络中实现服务质量。

本书的附录提供了以下参考内容：

- RFC。
- 局域网基础。
- TCP/IP故障检测及解决。
- HTTP状态码和报头字段。
- 数据格式的编程结构。
- TCP应用端口。

本书的使用约定

为使本书内容更易理解，帮助读者更好地掌握和应用书中知识，本书使用了如下辅助格式：

注意： 本书的“注意”表示一些能帮读者更好地理解主题，或者避免出现与当前话题有关的问题的额外信息。

警告： “警告”主要是提示危险的操作（例如，潜在地危害系统安全性的操作）。

本书使用了大量形如下例的交叉参考，以帮助读者快速找到其他章节中的相关信息。

参考： 关于FDDI的更多信息，请参见附录B“局域网基础”。

目　录

第1章　网络互联和TCP/IP介绍

1.1　TCP/IP和Internet的发展史

人类为了生存下去，具有一些与生俱来的本能，与周围环境相联系的能力便是其中之一。这种本能促使了原始的家庭、部落、公社、村庄、城市和国家的产生。最后，人类又用道路连接了各个地点，用船连接了各个大陆，用火箭和卫星连接了外部空间，通过这一系列方法，使这种本能发展到了空前的程度。在20世纪的后50年中，这种本能是通过互联计算机的形式来体现的。在计算机时代的早期，每台计算机就是一个独立的信息单元，它对输入信息进行处理，并输出结果，但人们很快就意识到有必要将计算机互相连接起来，于是一些计算机就被连接起来，组成了一个称为网络的计算机集合体。

和任何一个集合体一样，网络中的每台计算机与其他计算机共享公共的可用资源。为了使用这些共享资源，各个计算机间通过一些像电缆、集线器和交换机这样的硬件设备连接在一起。然而，计算机要共存于网络中，首先必须能够互相通信。尽管计算机之间互相交流的语言只是0和1而已，但还是需要遵循一些规则。例如，当有人跟你说话时，很重要的一点是你先倾听，然后再向他表达你的观点。我们只是将其作为与人交谈的一条不成文的规则，而计算机却需要明确地编程指定要使用这些规则，以便与其他计算机进行平稳的通信。我们把这样的一组通信规则称为协议。

通常，协议为计算机间通信的建立、维持及终止定义了一整套方法和手段。当联网的概念产生后，使各种协议实现标准化的需求也被提上了日程。所有计算机必须以同一种语言通信，以确保数据交换的一致性。于是，一种称为传输控制协议/Internet协议（Transmission Control Protocol/Internet Protocol，TCP/IP）的标准化联网协议应运而生。

顾名思义，TCP/IP是一组提供了两种服务的协议族，即对数据进行打包并路由这些已打包的数据。试想一下，当你从一个城市搬到另一个城市时，需要让包装和搬运公司来负责将所有家具搬到新地点。包装和搬运公司除了负责在搬家前对你的所有财产提供安全可靠的包装服务，还要负责在一定时间内以尽可能短的路程运送你的财产，将其搬到你的新地址。TCP/IP协议族与包装和搬运公司相似，但不同的一点是，数据不仅仅被打包和运送到正确的目的地，而且需要被解包并分发给目标计算机上的正确的应用程序。TCP提供了打包、重组、流控制和错误检测等服务，而IP负责确定到达目标计算机的最短路径。需要注意的一点是，TCP/IP本质上并不是一个软件，而是人们提出的一个包含一定的规则和格式、有助于创建协议软件的框架。

随着TCP/IP被实现为一种标准的联网协议以及网络的普及，联网领域中涌现出大批的网络，结果导致了“网中网”（Network of Networks）的出现，并由此产生了互联网的概念。在深入研究互联网之前，让我们先花点时间，大体上了解一下互联网的历史，特别是Internet的历史。

Internet作为一个全球性的网中网，连接了全世界成千上万台计算机。它是美国为建立一个可靠的信息交换系统（以便让科学家和管理者共享重要数据）的产物。美国国防部高级研究规划局（DARPA）想要创建一个覆盖全国、四通八达的网络，以便监视和控制国内的所有战略重地。因此，这个网络必须是这样的：即使部分网络受到了破坏或者被中断，网络的功能也不应该受到影响，而且网络一定不能有中央控制权，因为一旦控制被集中，对控制中心的任何破坏都会导致整个网络瘫痪。

网络上的每个节点都应该有能力去生成、发送和接收数据。基于这一需求，DARPA设想了一个将数据拆分成分组的网络结构，每一个分组都被标记上目标地址，并且通过网络发送。分组将不停地从网络上的一台机器传送到另一台机器，直到抵达预定的接收者。这些分组采取的路由可能不同。

与此同时，一个与此相似的称为分组交换技术的研究正在DARPA的资助下顺利进行。这项技术最初被使用在一个仅有4台计算机的网络上。该网络被称为ARPA网，连接了高等院校和军方的研究中心。慢慢地，随着数据交换需求的增加，越来越多的大学加入到这个网络中。从此以后，这个原始Internet的发展便一日千里了。DARPA想要建立更多的这种网络并将它们都互联起来，于是就又出现了各种不同类型的网络。

一段时间之后，许多使用不同技术和协议的网络被建立起来。为了能在这些网络之间交换信息，必须创建并遵循一个称为协议的公共通信模式。很多协议正是基于这一需求开发出来的，并最终被组合起来形成了ARPAnet协议族。该协议族是在1978年就初具规模的TCP/IP协议族的前身。TCP/IP协议族是一个为各种用途而开发的协议组合，其中最主要的协议是TCP和IP，TCP/IP协议族正是由此得名。随着Internet的逐渐成型，DARPA逐渐在连接到它的科研网的机器上使用TCP/IP协议。这样一来，以ARPANET为骨干的Internet变成了TCP/IP的试验平台。1983年1月，美国国防部长办公室正式要求所有连到网络上的计算机都使用TCP/IP。

注意： 尽管TCP/IP是作为一种Internet中的协议演变而来的，但也可以用于任何其他类型的互联网络。

1.2 网络互联

联网的概念不只是把两台或多台计算机连在一起那么简单，网络是用来在计算机之间共享软件或硬件设备等资源的。为了使各计算机间能彼此通信，需要将各种不同的网络连接起来组成一个网络。例如，一个公司有很多遍布全国的分支机构，为了能最有效地发挥公司机能，必须让各分支机构的网络能彼此通信。否则，诸如文件和数据库这样的资源就会出现冗余，因为它们将被四处复制。这一问题使得将两个或更多网络彼此互联成为必要。

另外，在连接两个网络时，还需要满足以下两个条件：网络间应该使用相同的通信协议，并且必须使用相同或兼容的硬件技术。

但事实上，大多数需要通信的网络使用的是各种不同的协议和硬件技术。这也促成了一个桥接物理上完全不同的网络，并使之能互相通信的标准。

两个或多个网络彼此连接在一起就组成了互联网络或internet。这些连接成互联网络的各个网络可能各不相同（如图1.1所示）。

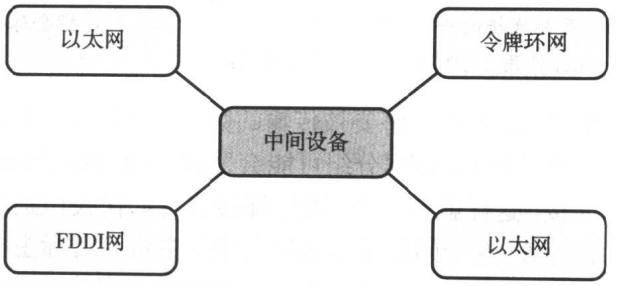
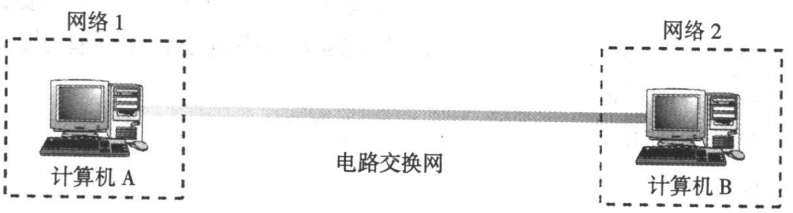


图 1.1　许多不同的网络或硬件技术共同存在，比如那些使用以太网、令牌环和 FDDI 的网络

构建和管理不同网络之间通信的过程被称为网络互联（Internetworking）或因特网互联（Internetting）。网络互联也用来指那些用于连接不同网络的产品、概念和技术，因而网络互联可以保证不管创建网络时用的是何种底层网络技术，网络间都能进行通信。互联网还必须解决那些在网络可靠性、连通性、灵活性和管理方面出现的问题。尽管网络互联听起来很简单，但实际上它是相当复杂的。因为参与的网络可能使用不同的协议、不同的拓扑结构，而且使用的底层技术也有可能不同。

网络可以被分成两种：电路交换网和分组交换网。这种划分是根据源计算机和目标计算机之间数据的传送方式来划分的。在电路交换网中（如图 1.2 所示），发送端和接收端之间建立了一个直接的物理连接。数据只能沿着这个已建立的连接发送。该信道在被释放以前，不能被别的计算机使用。



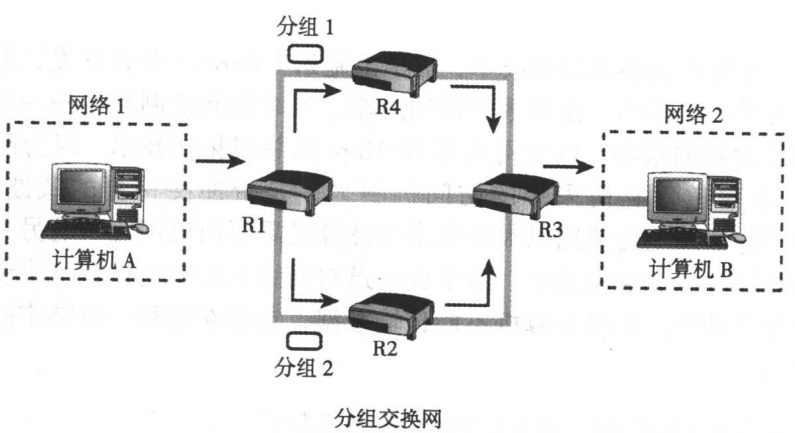


图 1.2　电路交换网中的数据是沿预先确定的直接物理连接传输的，而在分组交换网中，数据分组可以沿不同的路径抵达目的地

注意： 互联网络指那些互相连接的一组网络，而 Internet 或者 Net 则是指全球性的网中网，即最大的互联网络。Internet 使用 TCP/IP 来连接不同的网络。

在分组交换网中（如图 1.2 所示），将要被传输的数据，比如说文件，被分成易管理的数据单元，我们称之为分组或数据分组。数据分组可能会采取不同的路径到达目的地，因为发送者和接收者间并没有建立连接。这样就有一个问题，即接收者如何去识别属于某个组中的所有的数据分组，并将它们重组起来。这个问题可以通过在中间主机和目标主机所用的分组中加入报头重组数据分组的方法来解决。分组交换的优势在于即使在某条路径中断的情况下，数据的传输也不受影响，因为数据分组可以通过另一条不同的路径来传输。另外，被称为路由器的连接设备可以用来确定一条到达目的地的最短路径，并使用此路径来传输数据分组。

注意： 根据覆盖范围的不同，分组交换网还可以再分为局域网（LAN）、广域网（WAN）和城域网（MAN）。局域网是指在一个建筑物内跨越不同楼层的计算机组。城域网是跨越一个城市中的不同地点，而且使用像光纤这样的高速连接的网络。而广域网则运行于不同国家间，并且使用卫星通信。

1.2.1 网络互联的优势

网络互联使具有不同网络配置的网络能彼此互相通信。下面是一些网络互联的重要优点：

1. 构成互联网的各个网络的设计结构不需要改动，即便要改，也只需做很小的改动。
2. 网络管理是分布式的，因此效率很高。这是因为网络越小就越好管理，并且网络管理员对网络将有更多的控制权。
3. 即使在速度各异的混合网上数据也能有效地传输。

1.2.2 网络技术

光纤分布式数据接口（FDDI）是一种流行于网络时代早期的重要网络技术。在现今的网络中，以太网（Ethernet）是最普及的网络技术。在下面的章节中我们将探讨这些技术的一些特性。

参考： 关于网络技术的更多信息，请参见附录 B “局域网基础”。

以太网

以太网是一种分组交换局域网技术，最早由施乐（Xerox）公司开发，用来在网络中传输数据。它定义了一组标准，比如数据传输速率、网络访问机制和在任一给定的时间段内网络能传输的最大数据量等。以太网采用 10 Mbps 的总线拓扑技术，因为网络上的所有计算机都共享一条信道。它所采用的访问机制之一是带冲突检测的载波监听多路访问（CSMA/CD）机制。如果一台使用以太网技术的计算机需要向该网络中的另一台计算机传输数据，它将把数据分组放到信道中。由于此信道对网络上所有的计算机来说是公用的，因此有可能发生数据冲突。如果计算机不能传输数据，它将在等待一段特定的时间间隔后重新传输这些数据。

参考： 关于以太网的更多信息，请参见附录 B “局域网基础”。

光纤分布式数据接口（FDDI）

FDDI 也是一种局域网技术，用来在光缆上传输数据。因此使用 FDDI 技术的网络传输数据的速率比用以太网技术的网络快。FDDI 使用最广泛的控制机制是令牌环技术。在此技术中数据的传输由一个在网络上循环传递的令牌控制着。令牌是一个在网络中传递的特殊数据分组。当传输结束后，令牌被释放到网络上，上面的步骤又会重复。由于在同一时刻仅有一台计算机能拥有令牌，所以就避免了数据冲突。

参考：关于 FDDI 的更多信息，请参见附录 B“局域网基础”。

1.2.3　中间设备

为了扩展网络或连接不同的网络以组成互联网，需要一些联网设备，比如中继器、网桥、路由器、局域网交换机和网关等。这些设备统称为中间设备，用来连接那些使用了不同的网络技术、协议和介质类型的网络。

注意：有时为了减轻管理大型网络的难度，可以把它拆分成更小的网络并通过中间设备把它们连接起来。

中继器（Repeater）

如果数据必须远距离传输，那么表示这些数据的电信号在经过网络时其强度有可能减弱，从而可能导致数据的丢失。为了解决这个问题，一种称为中继器的设备被用来再生信号。在以太网这样的网络设计中，中继器扮演了一个重要的角色。需要说明的是，中继器不是一个智能设备。

中继器的功能是从网络中得到数据并再生信号，然后将其送到其他的网络中。由于它不是智能设备，所以不能执行复杂的任务，比如寻找数据传输路由等。另外，如果在网络上传输的数据被破坏，被破坏的信号也被再生。换句话说，中继器不对数据进行错误检查。总之，中继器的优点是线路简单，实现容易。

网桥（Bridge）

网桥可以用来连接相似的或不相似的两个网络。网桥独立于网络结构和网络访问机制。和中继器不同，网桥是一种智能设备。它在收到来自发送端的数据后将其传输到正确的目的地，而中继器只是机械地将数据从一个网络上传输到另一个网络上。使用网桥更优越，因为它们不复制噪声。有一种网桥能确定何种类型的帧必须被转发，我们称这种网桥为自适应网桥。

注意：帧是一种能在物理介质中传输的数据单元，物理介质是指那些在网络上用于连接计算机的电缆。

路由器（Router）

路由器用于连接那些结构不同的两个或多个网络。网络上的数据分组能够采用任何路径到达目的地。如果某个数据分组到达路由器，路由器将会去找一条最佳路径来使数据分组顺利抵达目的地。同时路由器也能用来连接那些使用不同的电缆铺设方法和协议的网络。

路由器跟网桥比较起来有下面一些不同：

- 尽管网桥和路由器都能确定多个到达目的地的路径，但不同的是，网桥仅能利用两个网络间的其中一条路径来传输数据，而路由器则能利用其中的多条路径或路由。网桥使用生成树协议（Spanning Tree Protocol）关闭多余的路径，只留下一条。