Cisco专业技术丛书

Cisco 安全体系结构

Cisco Security Architectures

(美) Gilbert Held Kent Hundley 著
陈彦海 张巧莉 等译

机械工业出版社
China Machine Press
McGraw-Hill

Cisco专业技术丛书

Cisco安全体系结构

(美) Gilbert Held
Kent Hundley 著

陈彦海 张巧莉 等译

机械工业出版社
China Machine Press

本书详细叙述了对Cisco路由器和Cisco PIX防火墙进行配置的方法。全书首先对网络的一些基础知识进行了介绍，考虑用户的需要，重点介绍了TCP/IP。本书介绍了NetWare的一般性知识，对Cisco路由器的软硬件知识进行了讲解，并说明了Cisco路由器的一般配置方法。全书的重点部分是介绍Cisco路由器和Cisco防火墙的安全配置，重点阐述了访问表、反访问表、动态访问表以及基于上下文的访问控制等，作者对其他的一些安全知识也进行了阐述。

本书叙述清晰，实用性强，是网络管理员和对Cisco安全策略感兴趣的读者不可多得的一本好书。

本书版权登记号：图字：01-1999-2374

图书在版编目（CIP）数据

Cisco安全体系结构／（美）海尔德（Held,G.），（美）亨得利（Hundley,K.）著；陈彦海等译. -北京：机械工业出版社，1999.10

（Cisco专业技术丛书）

书名原文：Cisco Security Architectures

ISBN 7-111-07448-3

Ⅰ.C… Ⅱ.①海… ②亨… ③陈… Ⅲ.计算机网络－安全技术 Ⅳ.TP393

中国版本图书馆CIP数据核字(1999)第37468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：郭东青

北京市南方印刷厂印刷·新华书店北京发行所发行

1999年10月第1版第1次印刷

787mm×1092mm 1/16·12.75印张

印数：0 001－5 000册

定价：28.00元

译 者 序

近几年来，网络的发展非常快。网络底层的带宽正在快速增加，几个大的网络公司已经能够在广域的SDH上传输2.4G（OC-48/STM-16）的IP报文。与此同时，网络软环境（网络管理和网络安全）的发展却相对滞后于带宽的发展，就如同计算机软件的发展滞后于硬件的发展一样。

开展政府上网工程以来，国内对网络安全的呼声越来越高，对于国家而言，真正的网络安全必然是使用自主开发的网络设备。译者很幸运地参加了网络安全方面的一些研究工作，近两年的时间里，也花费了很多时间研究Cisco和3COM网络设备的安全结构，对网络安全有一定的认识和见解。对于用户（网络管理员）而言，熟练掌握所使用设备的安全特征是必要的，只有这样才能较好地保护自己所在单位的网络安全。

目前，我国使用最多的路由器是Cisco公司生产的，大量的随机文档虽然对管理员有一定的帮助，但阅读英文毕竟是一件让人心烦的事情，因此我们翻译了本书，以满足用户对网络安全的需要。

本书全面地介绍了Cisco的安全思想，以及这些思想在Cisco设备中的应用。作者简单明了地说明了对Cisco路由器、Cisco PIX防火墙以及内嵌于Cisco路由器中的安全特征的操作和使用。书中还包含了一些现实生活中的示例，以便读者可以参照进行设备配置。书中还提到了一些可以用来增强网络安全的要点和技术。

译者在翻译的过程中，对原书存在的一些明显错误进行了修改，对于不太清楚的地方也与网络研究方面的一些人士进行了交流。

有些术语为Cisco的专用术语，尚无非常一致的翻译方法，如FACL等。译者根据自己的经验，进行了翻译。

有一些平常很少用到的协议，对于其英文说法，读者可能比较清楚，如果硬要译成中文，反而不确切，因此有一些协议名没有翻译。

本书由陈彦海、张巧莉组织进行翻译，参加本书翻译、录排、校对工作的人员还有：赵军锁、龚波、田丽韫、邓波、邓涛、潇东、李士心、李林、李卓林、聂宛析、田敏、金光、小光、龚露娜等。本书的出版是集体劳动的结晶，在此特别感谢前导工作室的全体工作人员。

由于时间仓促，且译者经验和水平有限，译文难免有不妥之处，恳请读者批评指正！

译者

1999年7月

前　言

过去，衡量一个国家或者组织是否强大的标准是它的产值，如多少多少吨钢材，多少多少桶石油，并以此与其对手进行比较。现在，一个国家或组织的强大更依赖于它传输信息的能力。这些信息可以是关于阿富汗某个小村里恐怖分子的卫星图像，或者各组织之间的财务信息，甚至消费者对ATM机的使用等。如果这些信息流被破坏或者修改，它对国家或组织等所造成的影响是严重的，有时甚至是灾难性的。假设某人可以截取金融信息，并将别人的资金打到他在瑞士或巴哈马群岛的户头上。不管被改变的帐户是国家的、公司的，或者其他实体的，这些受害者都会面临被颠覆或者破产。

保证网络安全的关键在于使用适当的设备，并用适当的策略来管理这些设备。当我们谈论进行Internet访问并保证网络安全时，大多数人毫无疑问会想到Cisco系统公司，因为该公司为Internet上的组织提供了大约80%的路由器。因此，本书集中讲述Cisco设备的思想和方法，包括对公司的路由器和防火墙进行操作和配置的详细知识。

真正完全安全的网络只能是被隔离的，并且锁在实验室或储藏室里。本书介绍的信息提供了一些相关的基础工具和技术，以使读者可以用来保证基于Cisco系统的网络的安全。读者通过对如何配置访问表，以及如何开启各种防火墙的功能有了详细的了解后，就能避免一些导致网络弱点的经常出现的错误。在适当的时候，我们介绍一些现实生活中的示例，这些示例都来源于几十年咨询经验的总结。为了避免对以前或现在的客户造成不必要的麻烦，我们将在书中使用的都是假的名称。因为保证安全需要一个学习的过程，读者要注意错误和疏忽都可能导致潜在的安全问题，所以一定要避免这些错误和疏忽。因此，我们会通过集中讲述对设备的配置，来达到为读者提供尽可能减少网络弱点的必要信息。但是没有人能够非常完善地保证网络的安全。本书所包含的信息应该能够帮助读者获取减少网络潜在弱点的基本知识。

作为专业的作者，我们非常重视读者的反馈意见。如果您希望将您对本书所涉及主题的看法与我们分享，或者您对本书的将来版本有什么期望，请通过我们的出版社或直接通过电子邮件与我们进行联系。

Gilbert Held
Macon, GA
235-8068@mcimail.com

Kent Hundley
Stanford, KY
Kent_hundley@ins.com

目　录

第1章 引 言

我们在本书的前言中讲过，在现代社会中，国家、组织或其他实体的强大与否很大程度依赖于其信息流。信息流必须要以可靠的方式从源端传输到目的端，这样接收者才能确定所接收的信息与发送的信息是一致的，即接收到的数据没有被窜改。而且，某些类型的信息不应该被网络上的其他机器所识别。因此，在信息传输的过程中，至少有几个与安全相关的问题需要考虑，如鉴别和加密等。

当组建一个数据网络时，鉴别和加密可能只是需要考虑的安全特征和技术的一部分。要得到对不同安全特征和技术的客观评价，需要首先考虑对安全的需要以及导致这些安全需要的潜在威胁，以保护现代组织的网络。

1.1 对安全的需求

图1-1展示了一个公司网络连上Internet的示例。许多人可能认为安全设备对于保护私有网络上的计算机免受来自Internet的攻击是必要的，其实网络边界保护只是网络安全的一部分。私有网络，不管其结构如何，都可能需要安全设备、技术和策略来避免网络上的雇员有意或无意造成的危害。因此，本节主要考虑来自网络外部和内部两方面的安全需求。

1.1.1 公共网络的威胁

本节我们将考虑来自公共网络的安全问题，并展示其潜在的或实际的威胁。这些威胁出现在那些连到公共网络上的私有网络中。因为Internet是没有边界的互连网络，一个组织的网络对成千上万的可以访问Internet的人就变成了可访问的。如果没有一种方法来控制访问组织的路由器后面的网段，每一个被操作的工作站和服务器就可能被来自全球的有意的或恶意的行为所破坏。这些恶意的行为可能包括企图侵入某个服务器或通过电子邮件给工作站用户发送病毒，病毒可能以宏的方式或文件附件的方式嵌入到电子邮件中。

另一个需要考虑的方面如图1-1所示，涉及到两个连接：将组织的路由器连到Internet服务提供者（Internet Service provider, ISP）路由器的传输线，以及ISP与Internet的连接。一旦数据流离开了组织，保证传输过程不被别人所读取和修改是非常困难的。这是因为在组织内部，通过建筑物封闭和雇员重视等物理安全措施还可以防止人们进入配线间，或使用协议分析仪来记录传输的数据；而一旦数据流离开组织管理的范围，就只能依靠鉴别和加密来证实消息的来源，以及其内部没有被泄露了。

另一个应该引起重视的问题是：当连接到一个公共网络，如Internet时，这些网络上潜在着一系列的行为，通常会导致拒绝服务（denial of service）一类的攻击。考虑其简单的情况，一个或多个恶意的人可以书写一个程序，并随意选择一个源地址，将报文请求发送到组织的一个或多个服务器。由于被传送了连续的服务请求流，服务器会做程序指示其所做的工作：响应这些请求。因为响应数据流被传送到一个并不存在的地址，服务器会将一个会话保持比平常长得多的时间，直到超时。大量的服务请求和被延长的会话连接时间，积累起来就会导

致服务器资源的耗尽，结果是对合法用户反而拒绝服务。

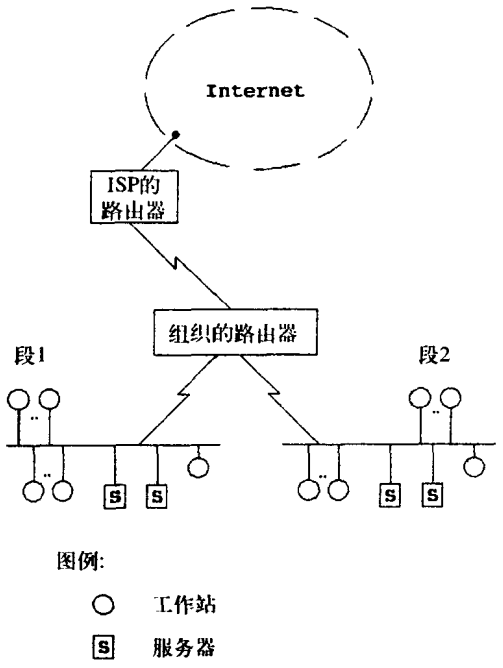

图1-1 公共网络的威胁

这种可能性还可能出现在当别人能非常容易地让组织的公用网络服务器超载时，有时候并不一定要书写一个特定的软件。例如，假设读者所在的组织拥有一个或多个FTP服务器，并且支持匿名FTP访问。某个有意或无意的人可能访问FTP服务器，并敲入命令“MGET *.*”，以传输当前目录的所有文件。如果该FTP服务器有几千G字节的文件和一个56Kbps的Internet连接，一个MGET命令就会导致Internet连接的饱和，结果可能妨碍客户们从Web服务器上获取报价单或放置定单。所以说，在将私有网络连上Internet时，有大量的因素需要考虑。在对来自公共网络的威胁有一个客观的认识后，下面不妨了解一下来自私有网络的威胁。

1.1.2 私有网络的威胁

在本节中，我们将讲述私有网络中实际的和潜在的威胁。我们仍然引用图1-1所示的网络结构，集中讲解组织的路由器之后的两个网段。

假设该私有网络被分段，以使得记帐和个人操作从其组织功能中分离出来。这样，一个网段上的一台或多台服务器就只限于自己网段的用户使用。这种情况意味着某个好奇的或恶意的雇员，可以通过访问记帐或个人服务器来增加其朋友的报酬，修改雇员的级别，或者进行其他更有破坏性的活动。因为路由器是防止用户从一个网段访问另一个网段的第一个连接，如果不采用访问表，数据就可能自由地在两个网段之间流动。即使使用了访问表，某个不满的雇员也可能使用另一台工作站（其地址在访问表中是允许的）来访问另一个网段。或者，拥有一定的技术知识的话，该雇员如果能够访问到路由器的命令端口，他就能修改访问表。

假设某个不满的雇员可以访问其他网段，那么使用电子字典来获取对服务器帐号的访问就变得简单了。事实上，就像本书稍后要说明的，路由器并不检查报文信息域中的内容。这意味着一旦对服务器的访问被接受，不管该访问是来自公共网络还是私有网络，路由器不能从一系列的重复登录请求中区分客户/服务器方式的请求/响应。

因此，路由器自身只提供了有限的安全措施，许多组织通常附带使用防火墙、认证服务器和病毒扫描软件等。监视对电话的使用以及公司的Internet来防止雇员无意识地下载包含病毒的文件，这样做即使不说不可能，也是很困难。而且，许多恶意的人开发了一些基于病毒的宏和可执行程序，他们将这些病毒程序嵌入到电子邮件中，或附加到他们的电子消息中，这带来了另一种潜在的安全危害，而这种安全危害必须引起网络管理者、LAN管理员和网络用户的高度重视。在对网络中存在的一些安全威胁有一个明确的认识之后，下面将讲述路由器在保护网络方面担当的角色。

1. 路由器的角色

从操作的观点看，路由器的主要功能是将报文从一个网络传输到另一个网络。路由器在网络层操作，对应于OSI参考模型的第三层。通过检测报文的网络地址，路由器作出转发报文的决定。与路由报文一起存在的另一个功能是创建和维护路由表。一些协议，如路由信息协议（Routing Information Protocol, RIP）、开放式最短路径优先（Open Shortest Path First, OSRF），以及边界网关协议（Border Gateway Protocol, BGP），只是过去20年来开发的50多种路由协议中的代表。在安全方面，路由器是保证网络安全的第一关。其保护是以访问表的形式进行的，被创建的访问表可以用来允许或拒绝信息流通过一个或多个路由器接口。

Cisco公司的路由器支持两种类型的访问表：基本访问表和扩展访问表。基本访问表控制基于网络地址的信息流。扩展访问表通过网络地址和传输中的数据类型进行信息流控制。尽管访问表可以认为是保护网络的第一关，当前实现的路由器并不实际检验报文中的信息域，也不维护关于连接状态的信息。换句话说，每一个报文被分别检验，路由器并不判断某个报文是否为一个合法对话流中的一部分。

上述规则有两个例外，它们是基于上下文的访问控制（Context-Based Access Control, CBAC）和反访问控制表（Reflexive Access Control List, Reflexive ACL）。CBAC是Cisco防火墙特征集的核心，它是Cisco1600和2500系列路由器的一个特殊代码版本。从IOS 12.0T开始，CBAC出现在3600系列路由器中，当新版本的Cisco IOS出现时，它可能在其他平台上得以体现。其特征是能够维护一个已有连接的状态信息，并对有限的TCP和UDP协议进行应用层信息检验。反访问控制表是Cisco IOS 11.3开始出现的新特征。反访问控制表维护一定程度的“伪状态（pseudostate）”信息，一旦合法的对话建立，它就在传统ACL中创建动态的表项。以后的报文在反访问控制表中与动态条目进行比较评估，以确定这些报文是否为已存在连接的一部分。会话结束后，ACL中的动态条目被删除。但是，反访问控制表不能理解高层协议，并且不适宜于与FTP等多通道协议一起使用。CBAC和反访问控制表将在本书稍后进行详细阐述。

虽然拥有这样的一些特征，ACL仍不能认证数据是否未经修改。认证过程要求加密报文的信息域以隐藏其内容。正因为意识到访问表的局限性，Cisco系统公司和其他软硬件厂商开发了其他一系列的安全设备。

2. 其他安全设备

与路由器ACL相关的局限性导致人们开发了一些附加的安全设备。这些设备包括防火墙、代理服务器、加密服务器、认证服务器以及病毒扫描服务器等。因为某些防火墙可以配置以支持一种或多种功能，而其他服务器一般只支持一种功能，所以我们将在本节集中阐述防火墙及其通用特征。

防火墙的特征

许多防火墙包含大量的安全相关特征，这些特征包括报文过滤（在某种程度上类似于对路由器访问表进行操作）、网络地址转换、认证服务、基于报文的目的地址对报文内容进行加密，以及代理服务等。因为读者对这些特征可能不是十分清楚，我们在这里简单地描述一下每一项功能。本书稍后，当我们讨论Cisco的安全产品时，会更加详细地阐述每一种防火墙功能。

1) 报文过滤。虽然许多防火墙执行报文过滤的方式与路由器访问表有些相似。实际上，它们包含很多基本访问表和扩展访问表所不包含的功能。这些附加的功能一般以策略创建的方式表现出来，使得防火墙管理员可以将特定过滤类型与特定用户组联系起来。这种联系还能包括某一天中的某一个时刻，某一个星期中的某一天等控制方式，这两个附加的功能在许多防火墙的报文过滤机制中都得到了体现。

2) 网络地址转换。网络地址转换的目的是将IP报文中的第3层源地址和（或）目的地址进行转换。这项功能让管理员能隐藏其设备的IP地址，以防止防火墙外部的计算机用户发现其真实的地址。该功能能保护网络中的设备免遭直接的攻击，因为所有的响应都发往防火墙，所以防火墙要作一个反向的地址转换。

3) 认证服务。认证服务的目的是验证数据流是否为“原创”。认证的常用方法，也是为大多数读者所接收的方法是用户ID口令方式。不幸的是，许多流行的应用程序，如FTP服务器都使用明码的口令，这种口令是很容易被截获和读取的。另外，口令自身并不能说明口令的给出者具有拥有口令的资格。

一种非常流行的认证方式是智能卡（smart card），智能卡与身份证大小差不多，它有一个伪随机数产生器和6个数字的显示屏。这种卡每分钟都能产生一个新的6个数字的随机数。支持这种认证方式的防火墙拥有相似的伪随机数产生器，该产生器通过个人身份标识号（Personal Identification Number, PIN）与每个用户相联系。需要进行认证的远程用户被要求输入其PIN号，并附上其安全卡上的6位伪随机数，以用来被防火墙所认证。

4) 加密。要有效加密报文，防火墙必须有方法能识别出这些报文。这一任务一般通过将一个或多个目的地址与一种或多种加密方法相关联来实现。加密必须选择性地进行，其原因在于大多数时间里用户访问不同的目标。有些目标可能不需要进行加密，而另一些目标可能要通过公共网络才能访问，所以可能只能接受加密数据。这种两个组织通过公共报文网络进行数据交流的情形导致了虚拟私有网（Virtual Private Network, VPN）的产生。加密数据流的过程，在VPN中建立了一条安全通道。

5) 产生警报。许多防火墙拥有管理特定条件门槛值的能力。一旦门槛值达到，防火墙可以配置用以产生可听到的警报，给一个或多个人发送电子邮件，执行预定义的程序，甚至可能在凌晨3点给局域网（Local area network, LAN）管理员发送一条消息。

6) 代理服务。代理就是中间媒介。对于网络而言，代理服务可以让防火墙接收应用请求，并检测这些请求，如果配置了的话，可以将这些请求发送到实际执行服务的设备。代理服务包括FTP代理和Telnet代理等。在对防火墙的许多特征有一个认识之后，本章后面部分将介绍全书的后续章节。

1.2 全书预览

本节我们将对全书的后续章节作一个概括性的描述。读者可以单独使用本节的信息，或与本书的索引一起使用，以对后面要介绍的知识有一个直观的了解。

1. TCP/IP协议套

第2章后的四章讨论各种不同的协议。本书包含了世界上通用的两大协议套的说明性介绍。之所以要介绍这些信息，是因为理解第2层的帧结构和第3、4层的报文结构对于了解路由器和防火墙如何工作是必要的。

第2章集中阐述TCP/IP协议套。我们首先简单地介绍了国际标准化组织（International Standard Organization, ISO）的开放式系统互连（Open System Interconnection, OSI）参考模型，然后讲述TCP/IP协议套及其与ISO和OSI参考模型的关系。

2. Internet协议

第3章详细介绍Internet协议。在这一章中，我们首先分析了IP报文头的结构，同时阐述了IP寻址方式。随后，介绍了几种类型的IP地址，以及子网屏蔽的目的和创建子网、标识子网的方法。

3. TCP和UDP

第4章转向TCP/IP协议套的上层，集中阐述传输控制协议（Transmission Control Protocol, TCP）和用户数据报协议（User Datagram Protocol, UDP）。因为许多网络安全的措施涉及到TCP和UDP端口号的使用，在介绍完各协议的头格式之后，我们列出了一个完整的通用端口列表，本书的后面部分会引用到这个列表中的端口，以执行安全相关的任务。

4. NetWare

因为在私有网络上，50%的信息是用NetWare协议传输的，所以在开发安全的方法以保护组织的计算设备时，该协议不能被忽略。第5章讲述IPX和SPX的报文头，以及Novell网络实现网络和主机站点寻址的方法。

5. 路由器硬件和软件

Cisco系统公司的路由器就像用来描绘一幅画的工具，它包含各种各样的组成部件，这些组成部件就像用来画画的各种画笔。为了得到对访问表以及安全相关路由器特征的完整认识，就必须对Cisco路由器的软硬件有一个基本的了解，而这正是第6章的目的。

第6章将首先简单介绍Cisco路由器的基本软硬件，然后，读者必须了解如何使用不同的路由器操作模式，最后集中阐述路由器的EXEC命令。

6. 使用访问表

在读者对前面章节所介绍的基础知识有一个完整的了解之后，第7章详细阐述Cisco路由器的访问表。在了解了访问表的语法和格式之后，我们将集中讨论访问表的结构，并使用几个网络实例来阐明如何让访问表成为保护网络的第一关。第8章讲述如何使用增强的IOS安全

特征，如基于上下文的访问控制、反访问控制表，以及网络地址转换等来建造一个Cisco的防火墙。第9章讲述IPX和第2层的访问表。

7. PIX防火墙

第10章作为全书的总结，我们将详细考察Cisco PIX的特征和功能，然后，讲述PIX的配置，并重点讲述其配置命令。这些知识将为读者了解PIX配置，以增强网络的安全提供一个全新的视野。

第2章 TCP/IP协议套

本章的目的是为读者提供一个对TCP/IP协议套的整体印象，为接下来两章对各层的详细描述起一个铺垫的作用。因为TCP/IP描述的是一个层次结构，我们将首先概括性地介绍国际标准化组织（International Standards Organization, ISO）的开放式系统互连（Open System Interconnection, OSI）参考模型。介绍完IOS参考模型的七层功能及相关性之后，我们将重点介绍TCP/IP协议套，TCP/IP虽然也是一个层次协议套，但与ISO参考模型存在很大的不同。通过对TCP/IP和ISO参考模型进行对比分析，我们将对TCP/IP协议栈如何参照国际标准进行操作有一个整体认识。

2.1.1 ISO开放式系统互连参考模型及其层次

ISO的开放式系统互连（OSI）参考模型是为了简化通用的互操作性而推出的。国际标准化组织（ISO）是联合国下属的，包括100多个成员的标准制定实体。ISO是联合国经济与社会理事会的非政府性咨询组织，其制定的七层OSI参考模型是通讯领域著名的体系结构。

ISO的参考模型定义了一组七层的通讯过程，每一层有其相应的功能，它们互相独立，但又互相联系。通过将复杂的通讯过程分解成七个层次，实现完整的通讯过程就变得相对容易。而且，通过定义各层相关的功能，以及层与层的互操作性，不同的公司在参考模型上开发的同一层和不同层的产品就可以与其它厂商开发的产品互相操作。

图2-1说明了ISO OSI参考模型的七个层次。除物理层之外，每一层都有低层过程，低层与高层的功能相互隔离。通过这种方式，每一层都实现了一组不同的功能，并且为高层提供一组服务。因为有层次上的分隔，如果所支持的服务不变的话，某一层的特性改变不会影响到其他的层次。因此，用户可以使用按照OSI设计的产品来满足特定的需要。

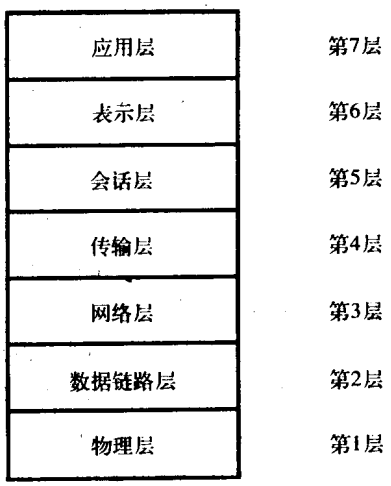

图2-1 ISO的开放式系统互连参考模型

除了第1层和第7层之外，ISO OSI参考模型的每一层都有相邻的低层和高层。第1层，物理层可以认为是与实际传输数据流的物理介质捆绑在一起的。第7层没有相邻的高层，它表示应用程序。这七层中的每一层都拥有相应的功能，并为上层提供一组服务。要对ISO的参考模型有一个整体认识，就必须对模型中的每一层进行分析。

1. 第1层物理层

参考模型中的最低层是物理层（Physical Layer），该层定义了为了互连两个或更多的设备而必须拥有的不同介质上的通讯规则。因此，第1层可以认为是用于支持信息传输的各设备间的电气的和物理的连接。

物理层的一个实例是PC与MODEM的电缆连接。当然，这实际上并非ISO参考模型中的物理层。这种电缆连接定义了PC和MODEM连线接口的每一个引脚及其通讯的方式，这些都被RS-232标准所定义，RS-232是一种物理层的标准。

2. 第2层数据链路层

物理层之上紧接着的是数据链路层（Data Link Layer），该层定义了设备访问物理层介质的方式。

数据链路层的另一关键功能是定义了信息传输的方式。这些定义包括用来保证数据从发送端到接收端正确流动的地址机制，以及用来传输地址、数据和错误检测信息的格式域。通过定义数据的格式，以及纠正传输错误的过程，该层成为了保证信息可靠传输的必要保证。我们在本章稍后将讲到，以太网（Ethernet）、令牌环网（Token Ring）和点到点协议（Point-to-Point Protocol，PPP）就是数据链路层的几种实例。

3. 第3层网络层

ISO的OSI参考模型的第3层是网络层（Network Layer）。就像其名字所显示的，该层为在网络中从源到目的端建立路径而规划一个逻辑的连接。网络层的一个关键功能是网络寻址，它使得数据能在网络与网络之间寻找路径（路由）。

路由过程本身支持网络间信息的传输，以及报文排序和流量控制。之所以需要报文排序，是因为当几个报文在源和目的端传输时，由于走的不同的路径而导致到达目的端时顺序与发送时的顺序不同，因而要重新排序，以产生正确的顺序。而流量控制则用来控制结点和网络之间信息的有序流动。几个通用的网络层协议包括国际电讯联盟（International Telecommunications Union, ITU）的X.25报文交换协议、Novell NetWare的互连网报文交换（Internetwork Packet Exchange, IPX），以及网际协议（Internet Protocol, IP）。

4. 第4层传输层

ISO的OSI参考模型的第4层是传输层（Transport Layer），该层负责第三层协议在网络上建立路由之后，信息传输的准确性。传输层在一个会话建立后负责控制其信息流，并在会话完成之后关闭连接。该层还负责控制通讯会话，为了达到这个目的，传输层执行错误控制、顺序检测和其他影响端到端数据传输可靠性的信息功能。

尽管大多数的传输层协议为端到端提供可靠性机制，但这只是与传输层相关联的可选特征。类似地，尽管大多数传输层协议是面向连接的，即在传输会话建立前，发送端必须收到接收端确认的其可以接收信息的应答，这实际上也只是一个可选的特征。除了以面向连接协议的方式工作以外，传输层还可以以高效方式运作，即协议在开始传输数据前无需知道目的结点是否准备接收数据，或者说对方是否是可操作的。尽管这种方式可能带来不良后果，发

送者可以自己设置一个计时器，在发送数据之后，计时器的值递减。如果在时间到达时仍未收到初始报文流的应答，源端就认为目的端是不可达的，并关闭会话。无连接的方法避免了传输层在传输数据前相对较长的握手过程。传输层协议有Novell的NetWare、传输控制协议（Transmission Control Protocol, TCP）和用户数据报协议（User Datagram Protocol, UDP）等。

5. 第5层会话层

会话层（Session Layer）在参考模型中定义了建立和终止底层传输行为的一组规则。会话层所执行的功能包括建立和终止节点连接。进行对话控制，以及端到端数据控制等。

6. 第6层表示层

ISO的OSI参考模型的第6层是表示层（Presentation Layer）。该层主要负责格式交换、数据传输以及语法相关的操作。该层的主要功能之一是在接收设备处将传输来的数据转换成可以显示的格式，而这一功能往往被人们所忽视。考虑一下接收设备，在不同的计算机上驻留的表示层是不同的，所以显示在PC上的数据与显示在其他终端上的数据就可能大相径庭。表示层执行的其他功能包括对数据进行加密/解密，压缩/解压等。

7. 第7层应用层

ISO的OSI参考模型的最高层是应用层（Application Layer）。该层可以认为是应用程序获取模型所提供服务的一个窗口。应用层执行的功能包括电子邮件传输、文件传输、客户/服务器的查询/应答等。

参考模型中的低四层有很好的定义，而高三层的相关功能则根据应用程序、数据传输类型，以及用来表示信息的显示设备的不同而有相应的变化。我们在本章稍后讲述TCP/IP协议套时将会看到，参考模型中的几个高层可以组合成一层。

2.1.2 数据流

进行层次划分的目的在于将一个复杂的通讯过程分解成了不同的实体，在数据从应用层往下直到传输介质的流动过程中，我们需要一种机制来确认每层执行的过程。这种确认机制就是在数据从应用层变成不同层次的报文时，包含一系列的报文头，这些报文头附加在数据上。在接收端，报文以相反的方式被去除掉这些报文头，使得目的端的应用层接收到的是原来的数据。图2-2说明了ISO参考模型理论上的数据流。

注意，图2-2的示例中，ISO参考模型中的数据流除了物理层以外，每一层在往下传送的过程中都增加了报文头。数据在物理层被编码成适合于传输的格式，然后以一串数据流的方式被发送到传输介质上。在接收方，一串数据流被解码，并形成一个个的报文，往参考模型的上层传送。在报文顺着模型往上传递的过程中，相应的层将其相应的报文头去掉，最后使得到达应用层的报文没有任何报文头。

2.1.3 层次再分

在我们将注意力转向TCP/IP协议套以前，先简单地讨论一下电子电器工程师协会（Institute of Electrical and Electronic Engineers, IEEE）的层次细分机制。

IEEE致力于发展局域网（Local Area Network, LAN）标准，其很多成果都被美国国家标准化协会（American National Standards Institute, ANSI）所采用。当IEEE开始制定LAN标准时，它意识到将数据链路层再分成逻辑链路控制（Logical Link Control, LLC）和介质访问控