WANGLUO ANQUAN

网络安全

理论及实战研究

尚玉莲◎著

LILUN JI SHIZHAN YANJIU

中国水利水电出版社
www.waterpub.com.cn

网络安全理论及实战研究

尚玉莲　著


中国水利水电出版社
www.waterpub.com.cn

·北京·

内 容 提 要

随着科技的发展，网络在现代人的生活中已经必不可少，它不仅加快了信息的传播速度，还极大地丰富和便利了现代人的日常生活。与此同时，网络所产生的安全问题也日益受到关注。本书本着由一般到个别的逻辑顺序对网络安全及信息网络安全中的信息安全的相关理论与实战技术展开深入分析讨论，内容主要涉及四部分，第一部分主要就网络安全的一般概念及安全问题展开分析，包括网络概念与威胁、网络协议等；第二部分主要就相关的网络安全实战技术展开研究，包括密码及加密技术、电子邮件安全、网络攻击检测与识别相关技术等；第三、第四部分主要讨论网络信息安全问题及应对措施，内容涉及信息网络安全问题、信息网络面临的不安全因素等。

本书可供网络安全相关专业的教师和学生阅读，也可供相关研究人员参考阅读。

图书在版编目（CIP）数据

网络安全理论及实战研究 / 尚玉莲著. -- 北京 : 中国水利水电出版社, 2018.11
ISBN 978-7-5170-7074-0

Ⅰ. ①网… Ⅱ. ①尚… Ⅲ. ①计算机网络－网络安全－研究 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2018)第254642号

责任编辑：陈　洁　　封面设计：王　斌

书　名	**网络安全理论及实战研究** WANGLUO ANQUAN LILUN JI SHIZHAN YANJIU
作　者	尚玉莲　著
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路1号D座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（营销中心）、82562819（万水）
经　售	全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	三河市元兴印务有限公司
规　格	170mm×230mm　16开本　17.5印张　310千字
版　次	2019年1月第1版　2019年1月第1次印刷
印　数	0001-3000册
定　价	**75.00元**

凡购买我社图书，如有缺页、倒页、脱页的，本社营销中心负责调换

前　言

互联网在全世界的发展和普及，给人们的生活和学习方式、思维方式等带来了巨大的改变。各行各业都越来越需要网络来传输信息，网络信息安全的重要性越来越突出。网络安全不仅会影响到网络信息社会的个人生活，还会影响到电子现金支付、电子商务、网络银行以及电子政务等政治和经济活动。

本着把握实质，注重思想，优化结构，体现思维，与时俱进，理论与实际相结合的撰写思想，作者力图从网络安全的基本理论出发，进而分析相关应用，以激发读者的阅读兴趣，增强读者对网络安全的理解，同时达到学以致用的目的。很多基本概念都是通过实际问题引入，从而增强了本书的应用特色。从内容的安排上，本书第 1 章介绍了网络安全的基本概况，包括网络体系结构、网络协议、网络信息安全概述等内容；在此基础上，第 2 章阐述了网络威胁，包括网络漏洞、常见的网络攻击方法以及常用的对策等内容；第 3 章就信息加密技术展开分析讨论，包括对称加密算法、非对称加密算法、量子密码技术等内容；第 4 章对电子邮件安全技术进行了讨论分析，包括电子邮件安全技术的发展现状、电子邮件安全保护技术和策略、安全电子邮件系统等内容；第 5 章探讨了网络攻击检测技术，包括入侵检测技术与产品、漏洞检测技术与工具等内容；第 6 章分析了防火墙技术，包括防火墙技术的概念与分类、防火墙新技术、防火墙安全技术指标等内容；第 7 章分析和讨论了计算机病毒防范技术，包括计算机病毒防范技术与软件、反垃圾邮箱技术等内容；第 8 章探讨了网络安全体系，包括网络安全防护体系、网络安全信任体系、网络安全保障体系等内容；第 9 章分析了信息网络安全问题与管理，包括信息网络安全问题、网络安全自查与督导检查、公安机关的监督检查、对网络服务机构的监督检查、信息安全等级保护、信息安全等级测评等内容。整体上说，全书内容丰富，逻辑清晰，尽量用通俗的语言来阐述深奥的概念与定理，希望可以为广大读者提供一定的帮助。

本书为山东省教育厅课题资助项目，课题名称：灰色半解生成算法在医学动态影像安全认证中的应用研究，课题编号：J14LN22。在本书的撰写过程中，得到了许多专家学者的帮助，同时参考了许多相关的文献，在这里表示真诚的感谢。同时，限于的水平，虽经多次细心修改，书中难免会有疏漏，恳请广大读者批评指正。

作者

2018 年 5 月

目　录

第 1 章　网络安全概述

随着人类社会对信息的依赖程度越来越大，人们对信息的安全性越来越关注。随着应用与研究的深入，信息安全的概念与技术不断得到创新。在计算机网络广泛使用之前主要是开发各种信息保密技术，在 Internet 全世界范围商业化应用之后，进入网络信息安全阶段。近几年又发展出了“信息保障”（Information Assurance，IA）的新概念。下面从网络体系结构、网络协议、网络信息安全概述三个方面来阐述网络安全。

1.1　网络体系结构

网络体系的结构是一个逐渐形成、逐渐完善的过程。下面从网络体系层结构的形成、网络体系层结构的功能和网络体系层结构的模型三个方面进行探讨。

1.1.1　网络体系层结构的形成

网络体系层结构的形成有一个历史发展的过程。首先，我们简要回顾一下网络发展历史的各个阶段，如图 1 - 1 所示。过去几十年间发生了许多变化，网络的规模与复杂性都在增加。早期网络设计只提供连通性，并不支持安全性。20 世纪 70 年代第一个网络仅限于几个研究机构与大学之间，且互连的每一方都是可信任的，安全问题并不突出。1988 年，针对网络上的计算机攻击首次出现，直到今天采用相同方法的某些攻击仍然有用。推动网络更新与增长的是网络的简单易用与互连。

网络是如何实现的，网络是如何发挥其功能的。一个网络可以划分为不同的功能模块，这些功能模块称为“层”。而每一层都被赋予相应的职能，这些层就构成现代网络的全部功能。层可以由软件或硬件实现，但网络上的每一台设备并不对应所有网络层。例如，路由器的设计就不是针对每一层的，因为它不负责数据端到端的传输，它只关心把网络上送来的数

据传输到下一个节点。网络层的结构是通过其在因特网上提供的服务与功能来表现的。

图1－1　网络发展的历史阶段

计算机通信的第一个例子，是由两台希望通信的设备通过点对点的连接构成的。在这个例子中，通信需要的软件是自带的，且由销售商独家开发。物理连接既可能是直接采用专线，也可能是采用电话线加调制解调器。其数据速率与今天的网络速率相比是很低的，应用往往基于简单的文本通信。这些早期应用一般用于简单的文件传输或远程访问。由于早期的文件传输系统使用专用软件进行通信，因此异种计算机之间的电子邮件通信很困难。

20世纪70年代，业界开始着力制定标准，旨在让网络上不同种类的设备实现通信。早期标准的制定者决定把问题分成功能模块，即不同的计算

机采用不同的方法使之互相通信。每一个模块或每一层执行一组功能，并为它上面的那一层提供一组服务，本层使用它下面那一层提供的服务。图 1 -2 是采用黑匣子方法定义的一个层，图 1 -2（a）表示任何一个黑匣子的设计方法，输入和输出定义为一组服务和要实现的功能。由某一层提供的服务称为服务访问点（Service Access Point，SAP），每层实现标准中规定的一组功能，这些功能用于支持一组服务，这些服务通常涉及希望交换数据的两个设备对应层之间的通信。这个内部层之间的通信称为协议。实现这个层的具体方法在标准中没有规定，这一点会导致一些值得关注的安全问题。这种定义每一层的黑匣子方法，使得不同的提供商能够实现相同的功能与服务。

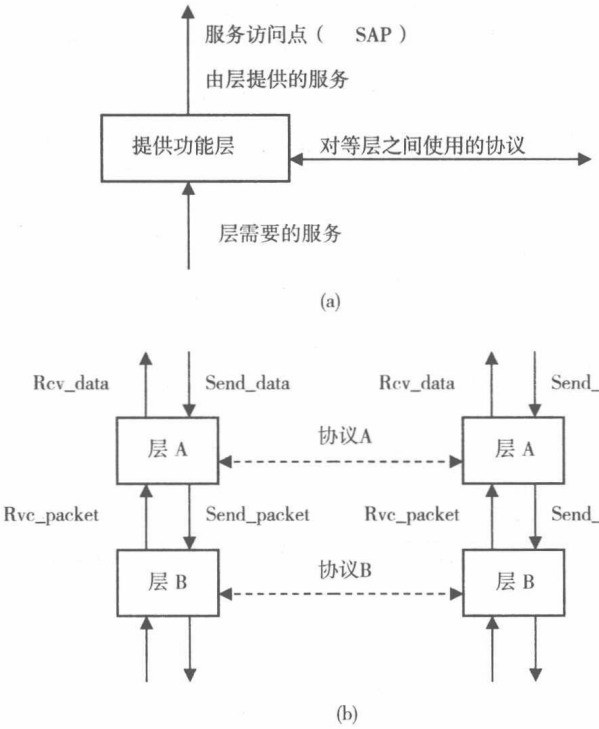

图 1 -2　网络的层

由图 1 -2（b）可以看到，层 A 为上一层提供服务，层 B 为层 A 提供服务，这些服务通常被规定为子程序调用。例如，这里有一个由层 A 提供的 Send_data（目标、源数据、选项和长度）服务，这个服务用于发送一个数据块到与其对应的层 A，即由目标地址指定的另一台设备。这个服务有几个参数，用于指定层如何处理服务请求，同时包括要传送到对等层的信息。参数 data 包含层 A 要发送到目标设备上的对应层 A 的数据，每一层利

用它的下一层提供的服务实现它要提供的功能。同样，在图 1 - 2（b）中，层 B 提供的服务为 Send_packet（目标、源、数据和选项）。注意，在这个例子中，层 B 提供发送一个固定长度数据的 Send_packet 子程序，它上面的层 A 提供一个发送较大数据量的服务，这就是某一层要提供的功能所在。在这个例子中，层 A 需要提供一个功能，把从上一层收到的数据分成较小的数据包，并发送到下一层，收到数据的对应层 A 需要提供一个功能，把这些小的数据包收集到一起成为一个数据块，并发送给它的上一层。当某一层和它对应的层通信时，它必须把数据发送到它的下一层。当某一层执行其功能时，它也必须能将控制信息传递到对应的层。根据图 1 - 2（b）所示的例子，层 A 需要发送控制信息，用于接收层 A 把数据重新组装起来。对等层之间的交互有对应的交互规则，如最大的数据包的尺寸、控制信息和数据格式以及控制消息的计时与顺序等。这些规则即是协议，而控制信息用于执行协议。每一层定义为服务、功能与协议的集合，图 1 - 3 说明了控制信息如何封装到数据中，从而每一层依据它处理来自上一层的请求。

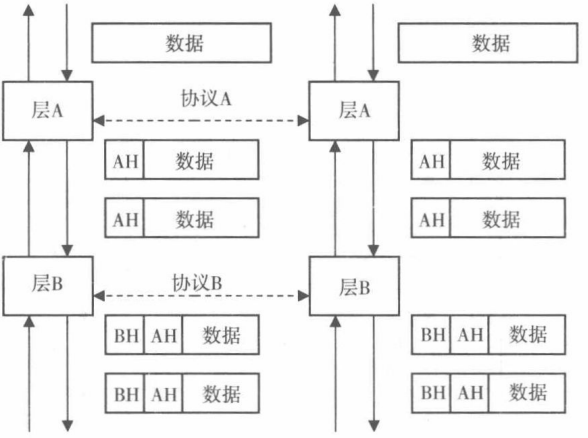

图 1 - 3　控制信息封装

由图 1 - 3 可以看到，层 A 表示的数据由层 A 分成两个数据包，每一个包都加上了控制信息。该控制信息包含当目标设备对应层 A 收到信息后如何恢复两个数据包的信息。数据包的控制信息段称为头部，层 A 使用层 B 提供的服务传送两个数据包给层 B，层 B 把自己的控制信息（头部）添加到每个数据包，以便和目标设备的对应层 B 进行通信，如此继续下去，数据包经过网络层，直至物理层的传输介质上。当目标设备收到数据包时，接收设备上的每一层将利用控制信息决定如何处理数据包，对应层会去掉

与其相关的控制信息，并将剥离后的数据包传送到它的上一层。

图 1 -2 与图 1 -3 说明了当数据被送到下一层的协议栈，并在接收方备份时，层之间的交互动作。另一部分层规范是相应层之间使用的协议。例如，图 1 -3 所示的每一个设备上的层 A 需要理解如何处理数据包，即需要知道控制信息的格式。协议就是用来提供这个功能的。如果一个数据包发生错误或丢失，层能够请求数据包重发。为了实现这个功能，这个层需要确定数据包是什么时候出错或丢失的。这就要求使用协议的层之间的协同工作。协议定义控制信息和数据在层之间是如何交互的，还定义层之间信息交互的格式。协议就是要实现这些功能和服务，在网络安全方面要注意防范由层提供的这些功能可能被黑客利用。

当然要明晰一些定义：协议就是一组规则，用于控制网络体系结构中两个对等层之间的交互，用于执行层的功能；重组就是由层提供的一个功能，用于合并数据包，即把对等层拆分的数据包重新组装成原来的数据包；路由器就是一种网络设备，负责把数据从一个网络传送到另一个网络，路由器可以解读从发送端到接收端的数据的路由；拆分就是由层提供的一种功能，它把从上一层接收的数据包分成多个较小的数据元素；服务访问点就是由网络层提供的一组服务，服务访问点通常被定义为一系列的子程序。

1.1.2　网络体系层结构的功能

网络体系结构中的一个功能组件，包含一组确定的输入和输出，并提供一组功能协助网络的运行，这就是网络层。网络层结构的功能是在和网络中的对方设备的对等层协同时提供网络服务。这些功能使面向层提供的服务能够执行并依赖下一层提供的服务。数据包就会在层之间传输一组数据。数据包头部则由层添加到数据包的那部分数据，它用来执行协议。网络层结构的功能表现为拆分与重组、封装、连接控制、顺序递交、流控制、出错控制、复用等方面。

1. 拆分与重组

在有些情况中，某一层对它上一层来的数据大小是有限制的，限制的原因可能是缓冲区、协议头部空间或物理链路有限制。例如，许多物理局域网（如以太网）限制数据包的尺寸为几千字节，以确保物理链路能正常传输。如图 1 -3 所示，如果某一层从它的上一层收到的数据超过下一层的处理能力时，数据包必须分成较小的数据包（拆分），最终再由接收层组合

到一起（重组）。执行拆分的层要负责把重组指令放在它的头部，指令内容包括数据包的数目及数据的相对位置等。

2. 封装

封装是指将控制信息以头部的形式添加到数据包中，如图 1 - 3 所示。头部包括下列典型信息：

（1）地址，即发送端和接收端的地址。

（2）出错校验码，常常包括一些用于错误校验的某种类型的代码。

（3）协议控制，执行协议需要的附加信息。

3. 连接控制

层既可采用无连接（传输数据不需要连接）数据传输，也可以采用面向连接（在数据传输之前，通信双方必须确立连接再通信）的数据传输。在面向连接的数据传输中，数据在传输之前，必须在实体间建立一种逻辑联系（即连接）。这类似于电话系统，一个人必须先拨号，并等待对方拿起电话后，双方才可以通话。在面向连接的数据传输模式中，双方必须同时准备对话。连接是根据数据包头部的信息确定的。在多数情况下，用于确定连接的数据包是不含数据的。连接控制（Connection Control）的三个数据项是：请求/连接项、数据传输项与终止项。许多基于网络的攻击就发生在连接控制交换时。在无连接的数据传输中，数据包与数据包是独立的，数据包的传递是无序的，也可能数据包根本就没被送出去。这类似于邮件系统，寄信人发出一封信，信在某个时间到达，信与信之间是独立的。

4. 顺序递交

在某些情况下，层提供的服务要求数据包按序递交，但数据包在下一层也许是无序递交的。在互联网上就是这样，数据传输是采用无连接协议传递的。但应用程序要求数据包按照发出时的顺序接收到。为了使层提供这项服务，需要向数据包的头部增加控制信息，以对数据包进行编号，从而接收方能够按原顺序重组。

5. 流控制

流控制是由层提供的一个功能，它用来在接收端开始拥堵时，降低发送端数据包的传送速率。流控制是为了确保传输层不会因为接收信息过多导致接受层溢出的一种技术，一般在几个层中都要实现流控制，在大多数面向协议的连接中也采用。

6. 出错控制

数据包传输中的出错控制是指由层提供的一个功能，用来侦查并纠正数据包的丢失或损坏。无论数据包是丢失还是损坏，层应该负责侦查丢失或者损坏的数据包，并负责重新层传输这些数据包。不是每一层都要负责数据包的重新传输，但是大多数层在头部都有某种类型的错误侦查（一般使用校验和方法）。攻击者有时通过向一个设备发送出错的数据包，引起层重新动作，从而利用出错的控制协议攻击。

7. 复用

复用是某一层提供的服务访问点面向多个上一层，反之，仅由一个下一层提供的服务访问点为多个上一层发送或接收数据包。复用是在由多个上层过来的数据包共享同一个下层时发生的，最典型的例子就是某台计算机连接到单条物理链路，如图 1 - 4 所示。当多个应用（如 Web、E - mail 及 IM 等）同时使用这个物理链路时，每个信息源都要向物理链路上发送数据包，然而，只能有一个层来控制对物理层的访问。因此，在计算机的多个网络层中的某处需要设置一个或一个以上的层使用层 B 提供的服务。对于接收层 B，为了知道是哪个层 A 发来的数据包，层 B 需要在数据包头部包含一个地址指出每个上一层的识别号。

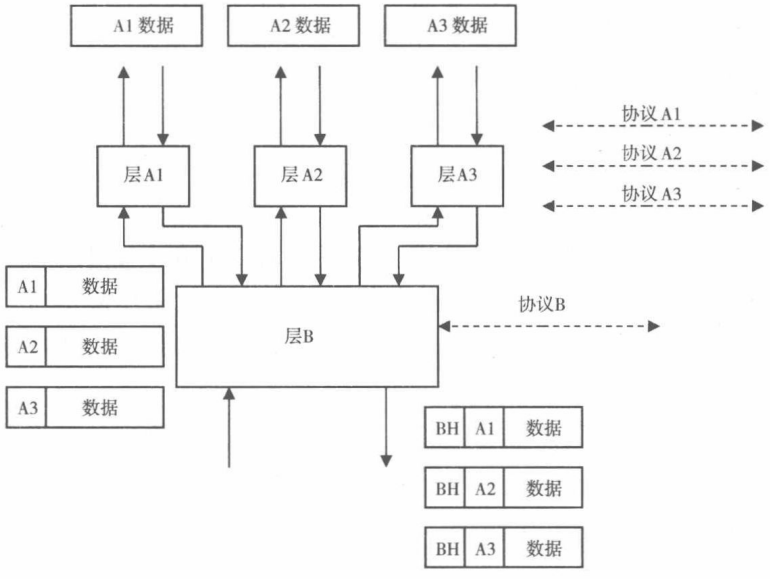

图 1 - 4　层复用

1.1.3 网络体系层结构的模型

网络的功能是分层的，许多技术是按照第一个实现的标准去做的，这样标准就有了竞争，对于网络更是如此。为了更好地了解网络体系结构的模型，首先来认识一些相关定义：帧是用于描述 OSI 模型的数据链路层的数据包；不分层服务通常用于描述网络服务，这些服务不必通过其他层而是直接访问一个或一个以上协议层，常常用于网络管理；OSI 模型是一种描述了每一层需要提供的高层功能且构成完整网络功能的七层模型；TCP/IP 模型是一种描述了高层功能并为因特网实际应用的四层协议模型；用户空间是指运行在用户空间的多种程序，这些程序与正在运行它们的用户具有同样的访问权限，并可以限制指定程序对系统文件的访问。

1984 年，国际标准化组织（International Standards Organization，ISO）提出了七层网络的概念，称为开放系统互连（Open Systems Interconnection，OSI）模型[①]，从此开始了制定每一层的标准。OSI 模型受到电信行业标准的重大影响，电信的关键点是链路交换（面向连接的）技术。这样两个竞争性的标准就有了两股力量在推动各自的进展。在某种程度上联邦政府推动了 OSI 模型的采用，同时 TCP/IP 协议在大学和研究实验室开始实施。Internet采用的是 TCP/IP 协议，除少数情况外，OSI 标准已经被废弃了，保留下来的只是 OSI 模型用于描述网络的层结构。尽管 OSI 标准没被采用，但在任何当前采用的标准总是能对应到 OSI 模型。

我们探究网络体系层结构模型的目的就是了解其功能。接下来简述 OSI 模型与 TCP/IP 模型每一层提供的功能（图 1－5）。

1. OSI 模型及其功能

（1）物理层。物理层负责物理上互连系统之间的比特位的透明传输。物理层必须给数据链路层提供识别终点的方法（一般采用源地址与目标地址）。物理层必须按数据链路层提供的要传输的比特位的同样顺序进行传输。

（2）数据链路层。数据链路层的主要任务是根据物理传输介质的特点屏蔽它的上层。数据链路层要为上层提供基本无误的可靠传输，当然，在数据链路层传输时也会发生错误。由网络层来的每个数据单元映射到含数

① Day，J. D.，H. Zimmermann. The OSI reference model. Proceedings of the IEEE 71：1334－1340，1983.

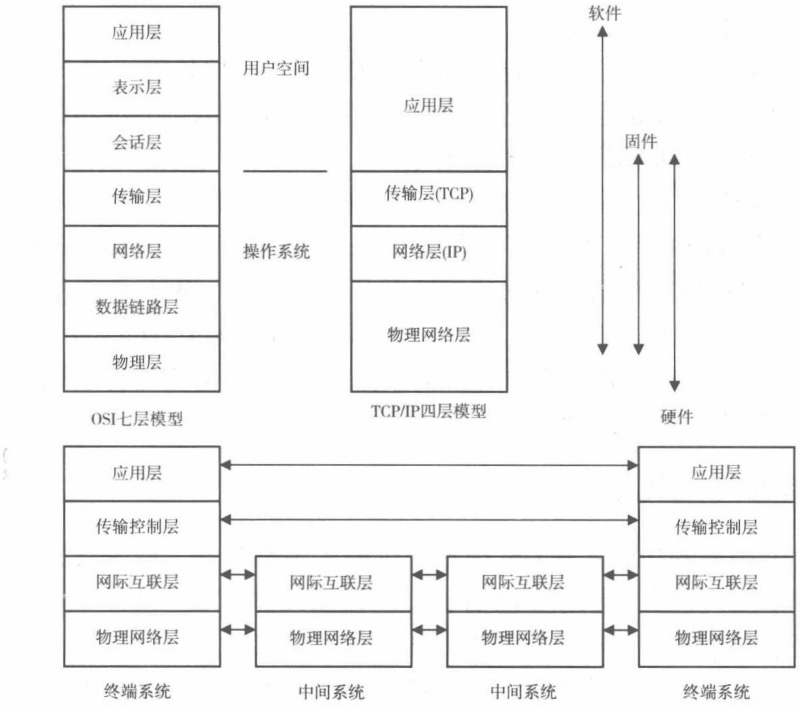

图 1-5　OSI 模型与 TCP/IP 模型

据链路协议信息的数据链路协议单元，称其为帧（frame）。数据链路层必须提供某种方法识别数据帧的开始与结束。这些帧要按其接收顺序提供给物理层。数据链路层也可以进行流控制（flow control）以防数据溢出。

（3）网络层。网络层主要负责由传输层提交的所有数据到网络中的任何传输层的透明传输。网络层必须处理数据包的路由。网络层可以是一个设备中的最高层，如网关或路由设备。在 OSI 模型中，网络层协议最初是设计成面向连接的，因此造成了协议的复杂性。

（4）传输层。传输层负责两个会话实体之间可靠透明的数据传输。传输层只关心会话层之间的数据传输，它并不关心处理层或拓扑层的结构。传输层使用网络层将数据从一个传输实体送到另外一个传输实体。根据网络层提供服务的质量，传输层也会执行附加功能，如按序提交、提供服务等。传输层提供流控制和错误控制。

（5）会话层。会话层并不关心网络，会话层负责协调表示层之间的对话。会话层必须提供会话连接的建立以及在这个连接上对话的管理。在 OSI 模型中，会话层是最后被标准化的三个协议层之一。它可以是没有动作的可选项，作用就是把表示层的数据送到传输层。ATM 机即是一个会话层的

例子，ATM 机负责和银行保持连接（传输服务），当某个用户要办理一笔业务时，一个会话就开始了。

（6）表示层。表示层以某种形式为应用层提供与信息表示相关的服务，这个形式对应用实体是有意义的。表示层要为应用层提供一种机制，以把数据转换成对等层可以翻译的普通格式。

（7）应用层。应用层是最高层，它要提供某种方法，为应用层访问 OSI 堆栈提供应用处理。应用层提供协议以执行应用功能。典型的应用层并不定义用户接口甚至是执行这些功能的用户层命令。Web 就是一个很好的应用层例子，应用协议（超文本传输协议，Hypertext Transfer Protocol，HTTP）定义访问 Web 页面的功能和服务，并给 Web 浏览器传输信息，但并不指定浏览器与用户之间如何交互。

2. TCP/IP 模型及其功能

TCP/IP 模型的功能具有 OSI 模型提供的大多数功能。两者之间最大的区别是 TCP/IP 模型的应用层包括了 OSI 模型的最上面三层，除此之外，TCP/IP 还有模型本身的特点，具体表现如下：

（1）物理网络层。TCP/IP 的物理网络层对应 OSI 模型的物理层与链路层的功能。它提供的服务较简单，只包括数据包的发送与接收。TCP/IP 协议设计的出发点是能在任何网络上运行，因此设计了一组最小的服务集合。

（2）网络（IP）层。网络层提供网际间数据包的路由，并关注全球地址空间，IP 层是无连接的，提供的服务包括数据包的发送与接收。

（3）传输（TCP）层。传输层与 OSI 模型的传输层类似，它负责网络中的端到端的数据传输。TCP 层还使用网络层提供的发送与接收功能与对等的传输层进行通信。TCP 层需要对 IP 层的不可靠的无连接服务进行补偿。

（4）应用层。应用层提供 OSI 协议模型最上面三层同样类型的服务，会话层与表示层的功能是否用或是用多少，取决于具体应用。

当初人们在设计分层协议体系结构时，较少考虑网络的管理、网络安全或网络监控。因为当初网络规模很小，基本由几个机构掌控，并不认为这些功能很重要。随着网络规模的增大与复杂性的增加，对这些功能的需求也随之增加了。当我们审视这些服务需求时，很快发现分层协议模型显然不能满足这些服务需求。这些服务需要访问每一层的内部工作，并且经常需要读取或修改层内部的参数。例如网络管理就常常需要直接控制每一层，这就引出了一个修正型的网络体系结构，如图 1 - 6 所示，它引入几个