网络安全核心技术及其软件编程理论研究

WANGLUO ANQUAN HEXIN JISHU
JIQI RUANJIAN BIANCHENG LILUN YANJIU

桑志国　金　峰　著

中国原子能出版社

网络安全核心技术及其软件编程理论研究

桑志国　金　峰　著

中国原子能出版社

图书在版编目(CIP)数据

网络安全核心技术及其软件编程理论研究/桑志国，金峰著. --北京：中国原子能出版社，2018.9
ISBN 978-7-5022-9428-1

Ⅰ.①网… Ⅱ.①桑… ②金… Ⅲ.①计算机网络－网络安全－程序设计－研究 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字(2018)第 235904 号

内 容 简 介

处于互联网时代，网络安全在信息领域中的地位从一般性的防卫手段变成了非常重要的安全防御措施。本书主要围绕网络安全研发的主要领域与方向，对涉及网络安全的技术展开讨论，在介绍技术的同时，还会对相关软件编程理论进行讨论。本书主要内容包括：套接字 Socket 网络编程、防火墙部署及编程理论、网络端口扫描技术及程序设计、TCP/IP 数据包安全技术及编程理论、E-mail 安全技术及编程理论、网络信息加密传输技术及编程理论、客户机/服务器程序设计等。本书结构合理，条理清晰，内容丰富新颖，是一本值得学习研究的著作。

网络安全核心技术及其软件编程理论研究

出版发行 中国原子能出版社(北京市海淀区阜成路 43 号 100048)
责任编辑 张 琳
责任校对 冯莲凤
印 刷 三河市铭浩彩色印装有限公司
经 销 全国新华书店
开 本 787mm×1092mm 1/16
印 张 19.5
字 数 349 千字
版 次 2019 年 3 月第 1 版 2019 年 3 月第 1 次印刷
书 号 ISBN 978-7-5022-9428-1 定 价 78.00 元

网址：http://www.aep.com.cn E-mail:atomep123@126.com
发行电话:010－68452845

前　言

Internet 应用技术、无线网络技术和网络安全技术的研究与发展，使得计算机网络技术进入了一个更高的阶段，正在对社会产生着前所未有的影响。计算机网络已经和电力、电话一样，成为支持现代社会整体运行的基础设施。目前，网络技术发展迅速、应用广泛、知识更新快、产业发展势头强劲，是一个充满活力与机遇的领域。

社会对网络人才的需求十分强烈，但是真正懂得网络安全技术、具备深入网络协议内部的高层次网络应用系统设计和网络软件编程的人才非常缺乏，他们也是社会急需的高级专业人才。基于这样的认识，作者写作了本书，旨在让读者了解网络安全核心技术的同时提高软件编程能力。

由于网络安全的内容非常丰富，本书以加强实践性、提高实用性为目的进行写作，讲究知识性、系统性、条理性、连贯性，注重知识概念，强调深入浅出。本书以清晰的思路、合理的体系、通俗的语言，向读者介绍计算机网络核心技术的基本理论、基本知识和常用技术，在注重网络安全基础理论上，又着眼提高读者软件编程能力。本书的特点是技术性和编程方法的结合，实践性很强，既基于编程又不限于编程。本书文字简明、图表准确、通俗易懂，用循序渐进的方式叙述网络安全知识，对网络信息安全技术难点的介绍适度，内容安排合理。

全书分为 8 章，第 1 章绪论，第 2 章套接字 Socket 网络编程理论，第 3 章防火墙部署及编程理论，第 4 章网络端口扫描技术及程序设计，第 5 章 TCP/IP 数据包安全技术及编程理论，第 6 章 E-mail 安全技术及编程理论，第 7 章网络信息加密传输技术及编程理论，第 8 章客户机/服务器程序设计。

本书的撰写凝聚了作者的智慧、经验和心血，在撰写过程中参考并引用了大量的书籍、专著和文献，在此向这些专家、编辑及文献原作者表示衷心的感谢。由于作者水平有限以及时间仓促，书中难免存在一些不足和疏漏之处，敬请广大读者和专家给予批评指正。

作　者

2018 年 7 月

目　录

第1章 绪 论

网络安全(network security)是抵御内部和外部各种形式的威胁,以确保网络安全的过程。当今大部分的现代网络都有很多资源需要被保护,这是因为大多数企业都部署了网络系统,并通过网络以数字形式而不是其他形式(比如纸质印刷形式)向用户提供信息。因而,需要保护的资源数量显著增长。

1.1 网络安全策略的要素

为了透彻了解什么是网络安全策略,我们可以对网络安全策略最重要的元素进行分析以帮助理解。RFC 2196 列出以下内容作为一个安全策略的要素。

①计算机技术购买准则,指明了需要的或者涉及的安全特性。这些特性应该是对现有企业的 IT 产品采购计划的补充。

②保密策略,定义例如监控电子邮件、记录键盘输入和访问用户文件等与保密相关的、合理的期望行为。

③访问策略,用于定义访问权限,制订最终用户、运营部门的员工和管理者可接受的使用准则,以便保护网络资产不会丢失或者泄密。它应该为外部连接、数据通信、向网络中连接设备和向系统中添加新的软件提供指导准则。它还应该包括所有的提示信息(例如,访问设备的提示信息应提供关于授权使用的警告信息和在线监控信息,而不是只简单地说“欢迎”)。

④职责策略,用于定义最终用户、运营部门和管理者的职责。它应该规定审计能力并且提供事故处理准则(例如,如果检测到一个可能的入侵的话,应该做什么以及和联系谁)。

⑤认证策略,通过一个有效的密码策略建立信任机制,以及为认证远程用户和设备使用提供准则(例如一次性密码和产生一次性密码的设备)。

⑥可用性声明,用来定义用户对资源可用性的期望值。它应该包含地

址冗余和故障恢复等问题，也指明操作时间和维护停机时间。它还应包括报告系统和网络故障的联系人等信息。

⑦信息技术系统和网络维护策略，描述为允许内部和外部维护人员处理和访问网络资源时所使用的技术。这里提出的一个重要议题，是否允许远程维护以及怎样控制这样的访问，这时需要考虑的另一个领域是外包以及怎样管理它。

⑧违规行为报告策略，用以指明哪种类型的违规是必须汇报的（例如，保密和安全，内部的和外部的），以及报告生成后向谁汇报。在不具威胁性并且允许匿名报告的前提下，侦测到某种违规行为并且进行汇报的概率会增加。

⑨支持信息，它针对每种违反策略的行为而提供给用户、员工和管理者相关的联系信息；当遇到一个安全事故时如何处理来自外部的咨询，或者哪些信息应被当成保密或是私有的；以及安全程序的交叉引用和所有与其相关的信息，比如公司策略和政府的法律法规。

1.2 构建及部署网络安全策略

1.2.1 构建网络安全策略

网络安全策略定义了一个框架，它基于风险评估分析以保护连接在网络上的资产。网络安全策略对访问连接在网络上的不同资产定义了访问限制和访问规则，它还是用户和管理员在建立、使用和审计网络时的信息来源。

网络安全策略在范围上应该是全面和广泛的。这也就意味着当我们要基于这个策略做安全方案的时候，它应该提供一些摘要性的原则，而不是这个策略实现的具体细节等内容。这些细节可能一晚上就变了，但是这些细节所反映的一般性原则是保持不变的。

S. Garfinkel 和 G. Spafford 在 *Practical Unix and Internet Secwrity* 一书中，定义了一个策略应该完成的 3 个任务：

①阐明保护什么和为什么保护它。

②规定谁负责提供这种保护。

③为解释和解决以后可能出现的任何冲突打下基础。

第一点是关于资产确定和风险评估的一个分支。风险评估在本质上就是一个阐明为什么网络上的资产需要得到保护的客观的方法。第二点阐述了由谁来确保网络上的安全需求都得到了满足，可以是下面的一个或多个：

- 网络的用户；
- 网络管理员和主管；
- 审计网络使用的审计员；
- 拥有网络和相关资源全部所有权的管理人员。

重要的是第三点，因为对于策略中不包括的问题，它把职责指定到某些特定个人，而不是让他们任意解释。为了使安全策略落到实处，它必须是通过现有的技术可以实现的策略。如果构建了一个非常全面的策略但在技术上却无法实现，那也毫无用处。

就用户对网络资源使用的易用性而言，有两种类型的安全策略。

- 许可性的(permissive)——任何没有明确禁止的都是允许的。
- 限制性的(restrictive)——任何没有明确允许的都是禁止的。

从安全的角度来说一个比较好的办法是，首先部署一个限制性的策略，然后基于日后的实际使用再对合法的用户进行允许操作。要知道无论计划得多么周密，许可性的策略总还是会有漏洞存在的。

安全策略需要平衡易用性、网络性以及在规则中定义的安全问题。这一点是重要的，因为与那些不太严格但不会耗费太多网络性的安全策略相比，限制性过高的安全策略会导致成本增加。当然，风险分析所确定的最小安全需求在部署安全策略时必须得到满足。

1.2.2　部署网络安全策略

定义了安全策略之后，下一步要做的就是部署它。部署安全策略不是一件简单的事情，它包括技术性和非技术性两方面的内容。找到能够互相兼容的设备，并且通过这些设备真正地实现安全策略极具挑战性，同时对所有相关团队提出一个切实可行的设计也同样困难。

在开始实现安全策略之前，有几点需要记住：

①公司中所有的风险承担者，包括管理人员和终端用户，必须都同意或者一致同意这个安全策略。如果不是每个人都相信这个安全策略是必须的话，那么维护这个安全策略将非常困难。

②用“为什么安全是重要的”来培训用户和相关的团体(包括管理人员)是至关重要的。必须确保所有的团体都理解制定的安全策略及其实现它的原因。这种培训必须是持续性的，以便让新加入的员工知道网络安全相关

的问题。

③安全不是凭空得来的。实现安全的代价是昂贵的，并且需要经常性投入，而不是一次性支出就一劳永逸了。因此让企业管理者和财务人员了解安全策略中计划的费用和风险分析是很重要的。

④必须为不同的人清楚地定义他们在网络中的职责分工及相互之间的报告关系。

部署一个安全策略的时候，牢记这些问题将能够帮助你实现一个物理设备和用户思想上的双重安全策略。

1.3 网络体系结构及协议

1.3.1 协议与划分层次

在计算机网络中要做到有条不紊地交换数据，就必须遵守一些事先约定好的规则。这些规则明确规定了所交换的数据的格式以及有关的同步问题。这里所说的同步不是狭义的(即同频或同频同相)而是广义的，即在一定的条件下应当发生什么事件(例如，应当发送一个应答信息)，因而同步含有时序的意思。这些为进行网络中的数据交换而建立的规则、标准或约定称为网络协议(network protocol)。网络协议也可简称为协议。更进一步讲，网络协议主要由以下三个要素组成：

①语法，即数据与控制信息的结构或格式。

②语义，即需要发出何种控制信息、完成何种动作以及做出何种响应。

③同步，即事件实现顺序的详细说明。

由此可见，网络协议是计算机网络不可缺少的组成部分。实际上，只要想让连接在网络上的另一台计算机做点什么事情(例如，从网络上的某台主机下载文件)，就必须要有协议。但是当我们经常在自己的个人电脑上进行文件存盘操作时，就不需要任何网络协议，除非这个用来存储文件的磁盘是网络上的某个文件服务器的磁盘。

协议通常有两种不同的形式。一种是便于人来阅读和理解的文字描述，另一种是让计算机能够理解的程序代码。这两种不同形式的协议都必须能够对网络上的信息交换过程做出精确的解释。

ARPANET 的研制经验表明，对于非常复杂的计算机网络协议，其结构应该是层次式的。我们可以举一个简单的例子来说明划分层次的概念。

现在假定在主机 1 和主机 2 之间通过一个通信网络传送文件。这是一项比较复杂的事情，因为需要做不少的工作。例如，发送端的文件传送应用程序应当确信接收端的文件管理程序已做好接收和存储文件的准备。若两台主机所用的文件格式不一样，则至少其中的一台主机应完成文件格式的转换。这两项工作可用一个文件传送模块来完成。这样，两台主机可将文件传送模块作为最高的一层(图 1-1)。在这两个模块之间的虚线表示两台主机系统交换文件和一些有关文件交换的命令。

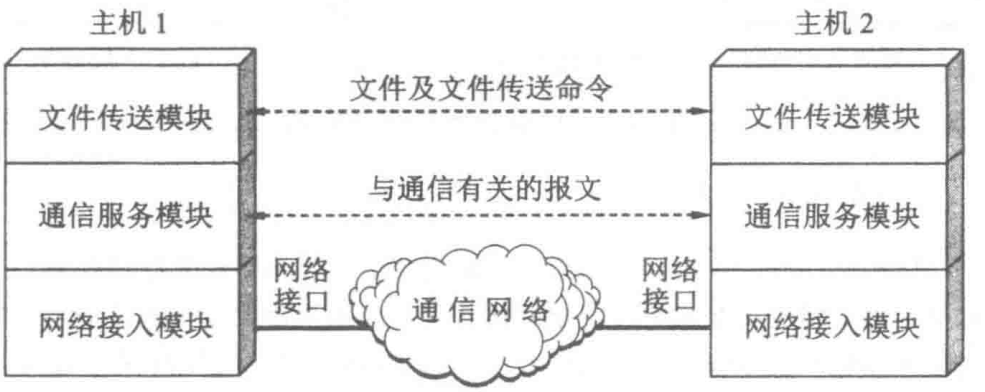

图 1-1　划分层次的举例

1.3.2　具有五层协议的体系结构

OSI 的七层协议体系结构[图 1-2(a)]的概念清楚，理论也较完整，但它既复杂又不实用。TCP/IP 体系结构则不同，它得到了非常广泛的应用。TCP/IP 是一个四层的体系结构[图 1-2(b)]，它包含应用层、运输层、网际层和网络接口层(用网际层这个名字是强调这一层是为了解决不同网络的互连问题)。不过从实质上讲，TCP/IP 只有最上面的三层，因为最下面的网络接口层并没有什么具体内容。因此在学习计算机网络的原理时往往采取折中的办法，即综合 OSI 和 TCP/IP 的优点，采用一种只有五层协议的体系结构[图 1-2(c)]，这样既简洁又能将概念阐述清楚。有时为了方便，也可把最底下两层称为网络接口层。

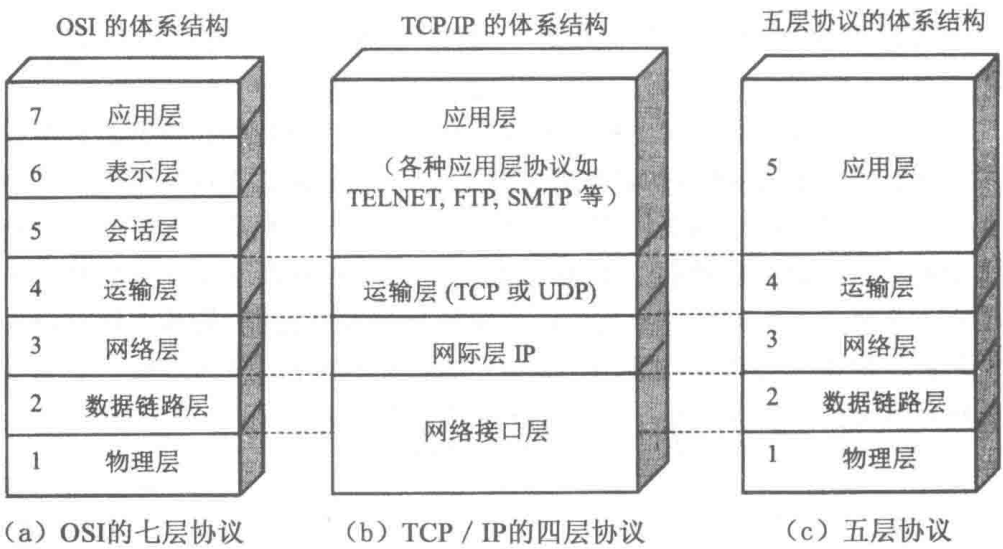

图 1-2　计算机网络体系结构

1. 应用层

应用层(application layer)是体系结构中的最高层。应用层的任务是通过应用进程间的交互来完成特定网络应用。应用层协议定义的是应用进程间通信和交互的规则。这里的进程就是指主机中正在运行的程序。对于不同的网络应用需要有不同的应用层协议。在互联网中的应用层协议很多，如域名系统 DNS、支持万维网应用的 HTTP 协议、支持电子邮件的 SMTP 协议等等。我们把应用层交互的数据单元称为报文(message)。

2. 运输层

运输层(transport layer)的任务就是负责向两台主机进程之间的通信提供通用的数据传输服务。应用进程利用该服务传送应用层报文。所谓“通用的”是指并不针对某个特定网络应用，而是多种应用可以使用同一个运输层服务。由于一台主机可同时运行多个进程，因此运输层有复用和分用的功能。复用就是多个应用层进程可同时使用下面运输层的服务，分用和复用相反，是运输层把收到的信息分别交付上面应用层中的相应进程。

3. 网络层

网络层(network layer)负责为分组交换网上的不同主机提供通信服务。在发送数据时，网络层把运输层产生的报文段或用户数据报封装成分组或包进行传送。在 TCP/IP 体系中，由于网络层使用 IP 协议，因此分组

也叫做 IP 数据报，或简称为数据报。

4. 数据链路层

数据链路层(data link layer)简称链路层。我们知道，两台主机之间的数据传输，总是在一段一段的链路上传送的，这就需要使用专门的链路层的协议。在两个相邻结点之间传送数据时，数据链路层将网络层交下来的 IP 数据报组装成帧(framing)，在两个相邻结点间的链路上传送帧(frame)。每一帧包括数据和必要的控制信息(如同步信息、地址信息、差错控制等)。

5. 物理层

物理层(physical layer)为数据链路层提供比特传输服务，确保比特在通信子网中从一个节点传输到另一个节点上。物理层协议主要定义传输介质接口的电气的、机械的、过程的和功能的特性，包括接口的形状、传输信号电压的高低、数据传输速率、最大传输距离、引脚的功能以及动作的次序等。

1.3.3　TCP/IP 的体系结构

TCP/IP 的体系结构比较简单，它只有四层。图 1-3 给出了用这种四层协议表示方法的例子。请注意，路由器在转发分组时最高只用到网络层而没有使用运输层和应用层。

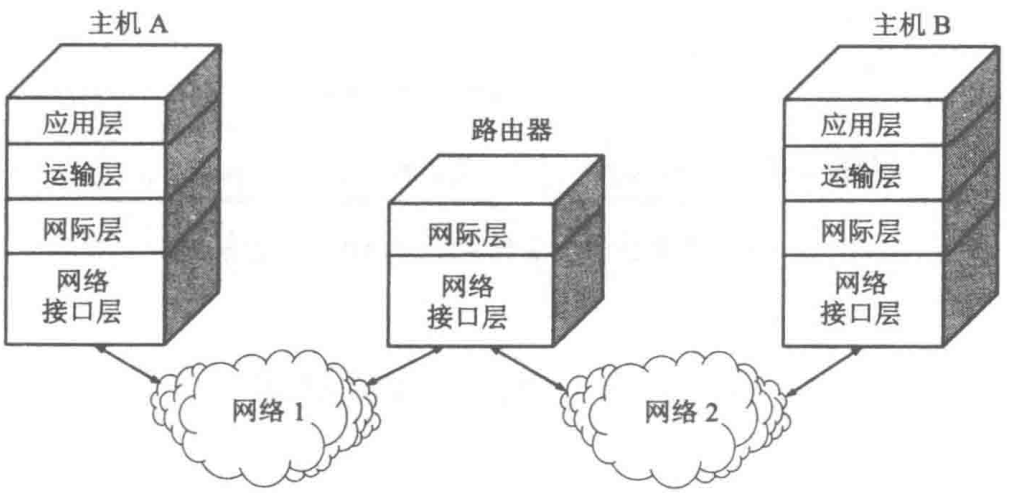

图 1-3　TCP/IP 四层协议的表示方法举例

应当指出，技术的发展并不是遵循严格的 OSI 分层概念。实际上现在的互联网使用的 TCP/IP 体系结构有时已经演变成为图 1-4 所示的那样，即某些应用程序可以直接使用 IP 层，或甚至直接使用最下面的网络接口层，图 1-4 就是这种表示方法。

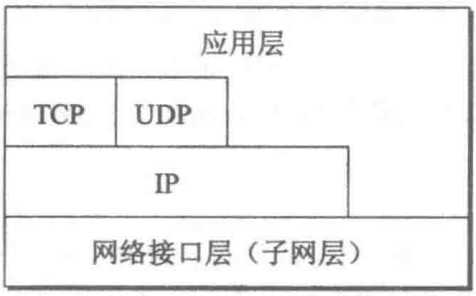

图 1-4　TCP/IP 体系结构的另一种表示方法

还有一种方法，就是分层次画出具体的协议来表示 TCP/IP 协议族（图 1-5），它的特点是上下两头大而中间小：应用层和网络接口层都有多种协议，而中间的 IP 层很小，上层的各种协议都向下汇聚到一个 IP 协议中。

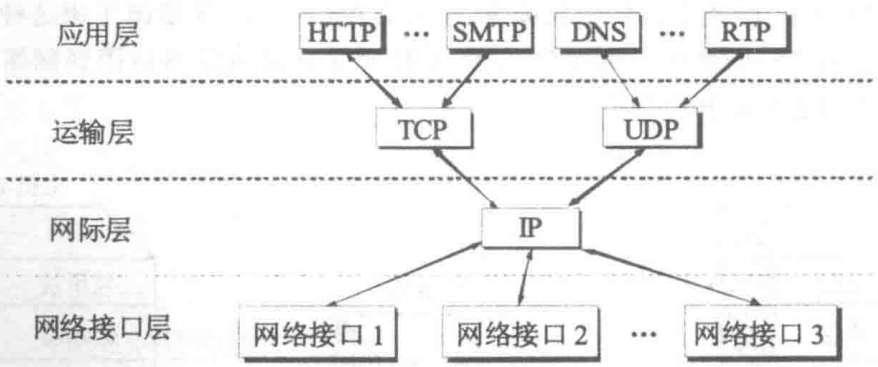

图 1-5　沙漏计时器形状的 TCP/IP 协议族示意

1.4　客户机/服务器模式

客户应用与服务器应用的交互称为客户机/服务器模式，客户机/服务器模式是个定义而不是标准。在互联网中，一个服务器程序定义为一个应用等待另一个应用请求连接。服务器程序常常等待默认客户端口号

请求连接。如图 1-6 所示是几个客户应用通过互联网来请求与服务器程序的连接。

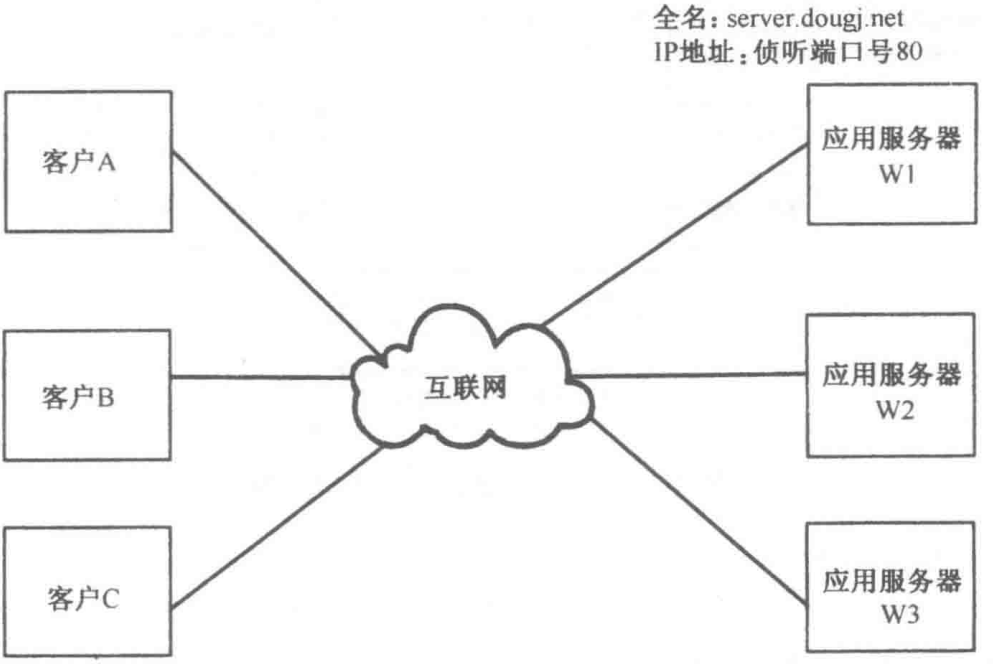

图 1-6　客户应用通过互联网请求与服务器程序连接

如图 1-6 所示，服务器应用驻留在具有全名及 IP 地址的计算机上，这个应用还被分配了应用地址(侦听端口号)。图 1-6 中的 3 个应用都在等待端口 80(Web 服务器使用相同的端口号)。客户应用通过指定目标地址和目标端口号请求与一个等待的服务器程序进行连接。客户也可以使用 DNS 系统把服务器的全域名转换为服务器程序的 IP 地址。

请求一个连接，就是一个服务器程序请求操作系统打开一个与 TCP 层的连接(一个套接字)，并侦听目标为某个端口号的连接(侦听端口号)。如图 1-7 所示是两个客户与两个服务器程序及它们开始通信的过程。同一台主机上的每个服务器程序侦听一个不同的端口号，在建立连接时，客户必须指定目标端口号及目标 IP 地址。套接字是应用与操作系统之间的连接的规定名称，它是由侦听 IP 地址与端口号定义的。一个应用只可以侦听一个与给定的目标 IP 地址有联系的给定端口。如果有多个 IP 地址与计算机联系，应用需要指示正在侦听的目标 IP 地址。

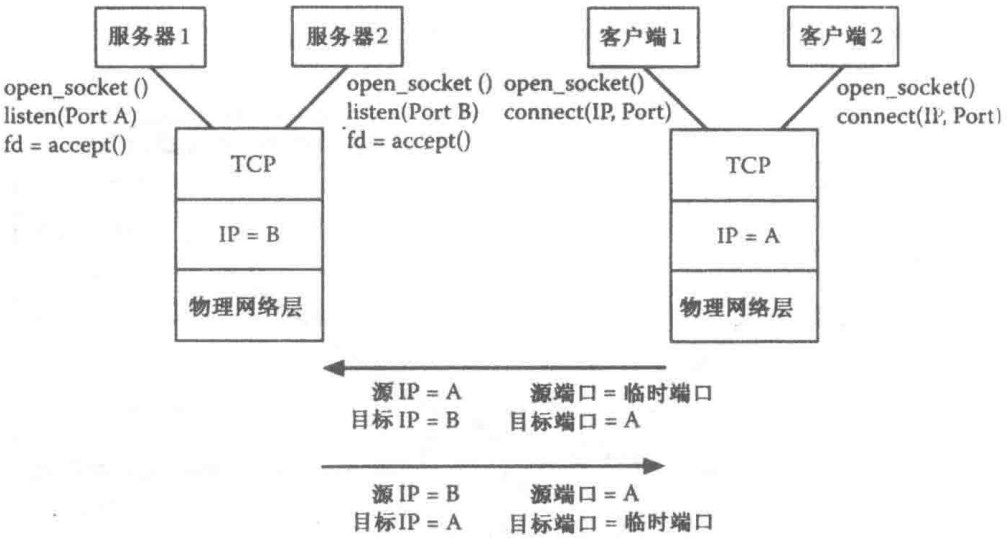

图 1-7　客户机/服务器模式的连接

为了开始一个连接，客户也需要与操作系统进行交互。客户将打开一个套接字，同时客户既可以使用源端口号，也可以让操作系统使用源端口号。当操作系统对客户使用源端口号时，称这个端口号为临时性端口。正像服务器应用一样，一个客户应用只能在某一时间使用一个给定的源端口号。客户应用指定它要连接的应用的目标 IP 地址和目标端口号。

有时一个服务器程序要处理来自一个主机的同一个客户的多个连接请求，要弄明白同一个服务器程序如何处理多个连接请求，需要考察客户应用是如何处理多个连接的。在一个指定的主机上客户的每一个连接请求将由操作系统分发一个不同的临时端口号，这样，两个数据包将有不同的临时端口号，一个具有两个连接的客户应用就可以打开同一个服务器程序。一个很好的例子就是在同一个 Web 服务器上，同一个 Web 浏览器可以同时打开两个窗口。如前所述，每一个客户和服务器连接都是唯一的，这是由 IP 地址和端口号构成的 4 元组进行区分的。图 1-8 给出一个的几个客户向两个 Web 服务器请求连接的例子，它的端口号是默认的 80。

在图 1-8 中有 5 个连接，如表 1-1 所示，每个连接由不同的 4 元组组成。注意，目标服务器的每个数据包的 4 元组是如何不同的，每个返回数据包就将是如何不同的。还应注意，由客户 B 占用的临时端口号与客户 A 占用的临时端口号可以是相同的，因为源 IP 地址是不同的。

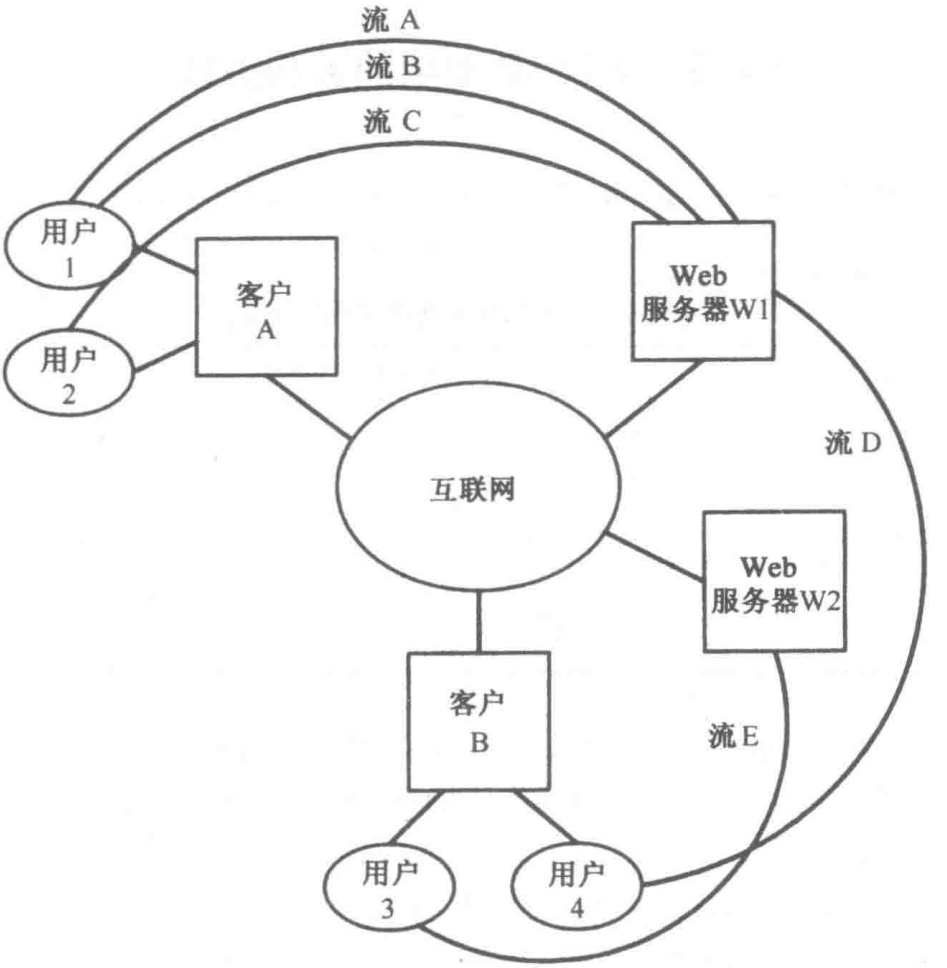

图 1-8　多客户机/服务器模式

表 1-1　流地址

流	源 IP	目标 IP	源端口	目标端口号
A	A	W1	临时端口 A1	80
B	A	W1	临时端口 A2	80
C	A	W1	临时端口 A3	80
D	B	W1	临时端口 B1	80
E	B	W2	临时端口 B2	80