21世纪高等院校网络工程规划教材

21st Century University Planned Textbooks of Network Engineering

计算机网络实验教程

Guidence of Experiments for Computer Networks

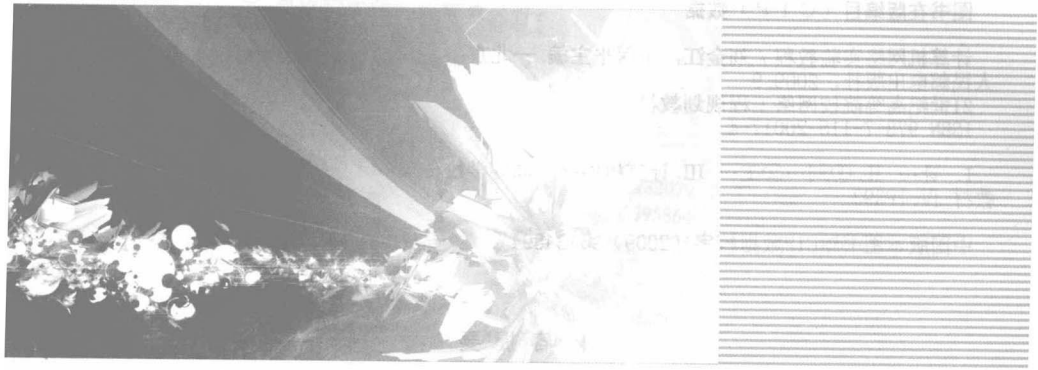
刘金江 王保平 主编

- 紧扣当前主流的网络设备和常用命令
- 精心设计与应用密切联系的实验范例
- 提高解决实际网络问题的能力

人民邮电出版社
POSTS & TELECOM PRESS

21世纪高等院校网络工程规划教材

21st Century University Planned Textbooks of Network Engineering



计算机网络实验教程

Guidence of Experiments for Computer Networks

刘金江 王保平 主编

人民邮电出版社

北京

图书在版编目（CIP）数据

计算机网络实验教程 / 刘金江，王保平主编. —北京：人民邮电出版社，2009.9
21世纪高等院校网络工程规划教材
ISBN 978-7-115-20017-4

Ⅰ. 计… Ⅱ. ①刘…②王… Ⅲ. 计算机网络－高等学校－教材 Ⅳ. TP393

中国版本图书馆CIP数据核字（2009）第134894号

内 容 提 要

本书是一本适用多种网络设备的计算机网络实验教材，主要介绍计算机网络实验过程中如何配置交换机、路由器、硬件防火墙等知识。全书由20个基础实验和9个综合实验组成，内容涵盖交换机的基本配置、VLAN的划分、MAC地址和IP地址与端口的绑定、配置生成树、链路聚合、三层交换机路由配置、DHCP服务器配置、基础路由配置、广域网协议封装、RIP路由协议、OSPF多区域路由和标准访问控制列表技术、防火墙的用户管理、透明模式配置、路由模式配置、混合模式配置、NAT转换、VPN配置等。

本书实验的设计具有很强的可操作性和针对性，通过这些实验，可以提高学生处理网络实际问题的能力。

本书可作为高等院校及高职高专院校计算机网络实验教学的指导教材，也可供从事计算机网络管理的人员学习参考。

21世纪高等院校网络工程规划教材

计算机网络实验教程

◆ 主　　编　刘金江　王保平
责任编辑　邹文波

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街14号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京华正印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：15.25
字数：386千字　　2009年9月第1版
印数：1－3 000册　　2009年9月北京第1次印刷

ISBN 978-7-115-20017-4

定价：25.00元

读者服务热线：(010)67170985　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前　言

计算机网络课程随着社会信息化的深入对实践操作能力要求越来越高。过去价格高不可攀的交换机、路由器、硬件防火墙等网络设备也在高等院校的网络实验室普及开来。学生通过在网络实验室中实际动手配置网络设备，加深了对网络理论知识的理解，提高了解决网络问题的能力。然而，市场上针对整个网络实验室、适用于多种网络设备的计算机网络实验教材相对匮乏。因此，作者以网络实验室为依托，针对主流网络设备，综合多年的网络实验教学经验，编写了这本计算机网络实验教材。

本书主要介绍计算机网络实验过程中如何配置交换机、路由器和硬件防火墙。全书共分5章，由20个基础实验和9个综合实验组成，每个实验都包括前置知识、实验目的、实验设备、实验规划和拓扑结构、实验步骤、思考题、相关配置命令的详解等几部分。第1章介绍计算机网络的基础知识；第2章介绍交换机的配置实验，由9个实验组成，包括交换机的基本配置、交换机VLAN的划分、MAC地址和IP地址与端口的绑定、配置生成树、链路聚合、三层交换机路由配置、DHCP服务器配置等实验项目。第3章是路由器的配置实验，由5个实验组成，包括组建路由网络的基础路由配置、广域网协议封装、RIP路由协议、OSPF多区域路由和标准访问控制列表技术。第4章介绍了网络安全中的硬件防火墙的配置实验，由6个实验组成，包括防火墙的用户管理、透明模式配置、路由模式配置、混合模式配置、NAT转换、VPN配置。第5章是9个综合实验，综合了交换机、路由器和防火墙的链路聚合、生成树协议、链路负载均衡、端口认证、端口地址绑定、PAP和CHAP封装验证等重要内容，给出了解决这些网络难题的方法。

本书的特点是紧密结合网络设备，介绍的各种配置命令和方法在绝大部分网络设备上通用。通过认真学习实践本书的内容，可以锻炼实际解决网络问题的能力。

本书主要面向高等院校及大中专院校计算机相关专业、通信相关专业的教师和学生，可以作为教师开展实验教学的指导教程，也可作为其他专业学生和社会认证的实验指导书。同时为各级网络管理员提供了一本入门与提高的专业书籍。

本书按54个学时编写，教师可以根据实际需要灵活安排教学内容。自学者在学习过程中，需要有一定的计算机基础知识和网络基础知识。

本书由刘金江、王保平任主编，王兴、郝身刚任副主编。第1章由黄河涛编写，第2章由程宁、张坤编写，第3章由刘金江编写，4.1节～4.2节由郝身刚编写，4.3节～4.6节由张丽编写，5.1节～5.2节由王兴编写，5.3节～5.4节由李争艳编写，5.5节～5.6节由梁晶晶编写，5.7节～5.9节由王保平编写。全书由刘金江统稿。

由于编者水平有限，书中不妥与疏漏之处在所难免，敬请广大读者批评指正。

编　者

2009年7月

目　录

试读结束，需要全本PDF请购买 www.ertongbook.com

第 1 章　计算机网络基础

现在，人们的生活、工作、学习等方面都离不开计算机网络。假如某一天计算机网络突然不能工作，我们将面临什么样的结果呢？人们将无法出行，因为无法买到车票、机票；银行不得不关门；人们无法上网查询自己所需要的资料；整个社会将会是一片混乱。计算机网络已经成为一个国家的战略基础设施，世界各国纷纷研究和制定本国建设信息基础结构的计划，同时也推动计算机网络进入了一个新的历史阶段。

1.1　计算机网络基本概念

1.1.1　计算机网络的定义

计算机网络没有统一的精确定义。

关于计算机网络最简单的定义是：通过同一种技术相互连接起来的一组自主计算机的集合。如果两台计算机能够交换信息，则称这两台计算机是相互连接的。以后我们将会看到，计算机网络可以有不同的大小、形状和形式。

1.1.2　计算机网络的分类

关于计算机网络的分类有两个因素非常重要：传输技术和距离尺度。不同的因素带来不同的分类结果。

1. 按传输技术分类

按照传输技术不同，可以将计算机网络分为广播式网络和点到点网络。

（1）广播式网络（broadcast networks）只有一个通信信道，网络上所有计算机都共享该信道，任何一台计算机发送的消息都可以被其他所有计算机收到。在传输的分组中有一个地址域，指明了该分组的目标接收者。一台计算机收到一个分组以后，检查地址域。如果该分组正是发送给它的，它就处理该分组，否则该分组就被丢弃。

例如，一个人来到教室大声喊“张三，有人找，请出来一趟。”虽然很多同学都听到了这个消息，但是只有张三会应答，别的同学都忽略了。另外一个可以类比的例子是，火车站候车室广播：“乘坐 T116 的旅客到三号检票口检票进站”。

（2）点到点（point-to-point）网络则是由许多连接构成的，每一个连接对应一台计算机。在这种网络中，为了将一个分组从源端传送到目的地，该分组可能首先要经过一台或者多台

中间计算机，通常有可能存在多条不同长度的路径。所以，找到一条好的路径对于点到点网络是非常重要的。

2. 按距离尺度分类

按照距离尺度可以将计算机网络分为局域网、城域网和广域网。

（1）局域网（Local Area Network，LAN）是专有网络，可以位于一个建筑物内，或者一个校园内，也可以远到几千米的范围。局域网通常用来将办公室或者实验室中的计算机连接起来，能够共享资源和交换信息。局域网由于覆盖范围有限，使得数据在网内的传输速度很快，这样可以简化网络的设备和管理模式。

（2）城域网（Metropolitan Area Network，MAN）的作用范围一般是一个城市，其作用距离为 5km～50km。许多城市的有线电视网就是城域网。目前很多城域网采用的是以太网技术，因此有时也常将其并入局域网的范围进行讨论。

（3）广域网（Wide Area Network，WAN）跨越了一个很大的地理区域，通常是一个国家或者一个州。广域网是因特网的核心部分，由主机和通信子网组成。其任务是通过长距离运送主机所发送的数据。连接广域网各结点交换机的链路一般都是高速链路，具有较大的通信容量。

1.1.3 计算机网络的性能指标

计算机网络有几个重要的性能指标，从不同的方面来衡量计算机网络的性能。

（1）速率。计算机发出的信号都是数字形式的。网络技术中的速率指的是连接在计算机网络上的主机在数字信道上传送数据的速率，单位是 bit/s（比特每秒），可以用 kbit/s、Mbit/s、Gbit/s。

（2）带宽。在计算机网络中，带宽用来表示网络的通信线路所能传送数据的能力。就是在单位时间内从网络中的某一点到另一点所能通过的“最高数据率”，单位是 bit/s（比特每秒）。

（3）时延。时延是指数据（一个报文或分组）从网络的一端传送到另一端所需的时间。

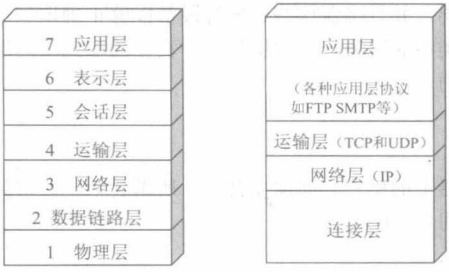
网络中的时延由发送时延、传播时延、处理时延和排队时延组成。数据在网络中经历的总时延就是这 4 种时延之和，即

总时延=发送时延+传播时延+处理时延+排队时延

（4）往返时间（RTT）。往返时间表示从发送方发送数据开始，到发送方收到来自接收方的确认（接收方收到数据后便立即发送确认），总共经历的时间。

1.2 计算机网络的参考模型

计算机网络是一个非常复杂的系统，为了降低网络设计的复杂性，在最初的 ARPANET 设计时就提出了分层的方法。分层将庞大而复杂的问题，转化为若干较小的局部问题，这样就比较容易研究和处理。在现在网络理论中，有两种重要的参考模型：OSI 参考模型和 TCP/IP 参考模型。尽管与 OSI 模型相关的协议已经很少在使用了，可是该模型本身是非常通用的，在每一层上讨论到的特性也仍然非常重要。而 TCP/IP 模型正好相反：模型本身并不常用，但是协议却被广泛使用。二者的参考模型如图 1-1 所示。



（a）OSI 参考模型　　（b）TCP/IP 参考模型

图 1-1　计算机网络参考模型

1.2.1　OSI 参考模型

OSI 参考模型是以国际标准化组织的一份提案为基础的。它本身并不是一个网络体系结构，因为它并没有定义每一层上所用到的服务和协议。它只是指明了每一层上应该做些什么事情。

1. 物理层

物理层涉及在通信信道上传输的原始数据位。在设计的时候必须要保证：当一方发送了“1”时，在另一方收到的也是“1”，而不是“0”。这就要求考虑：应该用多少伏的电压来表示“1”，用多少伏的电压表示“0”，每一位持续多少纳秒（ns），传输过程是否在两个方向上同时进行，初始连接如何建立，当双方结束之后如何撤销连接，网络连接器有多少针以及每一针的用途是什么。这里的设计问题主要涉及机械、电子和接口，以及位于物理层之下的传输介质等。

2. 数据链路层

数据链路层的主要任务是将一个原始的传输设施转变成一条逻辑的传输线路。在该层上，发送方将输入的数据拆开，分装到数据帧中，然后顺序地传送这些数据帧。如果是可靠的服务，则接收方必须确认每一帧都已经正确地接收到了，即给发送方送回一个确认帧。数据链路层另一个功能是流量解调，以便让发送方知道接收方当前时刻有多大的缓存空间。

3. 网络层

网络层控制子网的运行过程。主要功能是确定如何将分组从源端路由到目标端。从源端到目标端的路径可以是静态的也可以是高度动态的。网络层还有进行拥塞控制和控制提供服务质量的功能。当分组在不同网络中传输的时候，网络层要确定不同网络之间的编址方案和所使用的协议。

4. 传输层

传输层的基本功能是接收来自上一层的数据，并且在需要的时候把这些数据分割成小的

单元，然后传送到网络层，并且确保这些数据片段都能够正确地到达另一端。传输层还决定了将向会话层提供哪种类型的服务。传输层是一个真正的端到端的层，所有的处理都是按照从源端到目的端来进行的。

5. 会话层

会话层允许不同机器上的用户之间建立会话。所谓会话，通常是指各种服务，包括对话控制、令牌管理，以及同步功能。

6. 表示层

表示层定义了所传递的信息的语法和语义。不同的计算机可能会使用不同的数据表示法，为了让这些计算机能够进行通信，它们所交换的数据结构必须以一种抽象的方式来定义；同时，表示层还定义一种标准的编码方法，用来表达网络线路上所传递的数据。表示层管理这些抽象的数据结构，并允许定义和交换更高层的数据结构。

7. 应用层

应用层包含了各种各样直接针对用户需求的协议，如 HTTP、FTP、SMTP 等。

1.2.2 TCP/IP 参考模型

TCP/IP 参考模型就是 Internet 所使用的参考模型。

1. 连接层

连接层负责建立电路连接，是整个网络的物理基础，典型的协议包括以太网、ADSL 等。

2. 网络层

网络层将整个网络体系结构贯穿在一起。它的主要任务是：允许主机将分组发送到任何网络上，并且让这些分组独立地到达目标端。这些分组到达的顺序可以与它们被发送时候的顺序不同。网络层定义了正式的分组格式和 IP，任务是将 IP 分组投递到它们该去的地方。在这里，需要解决分组路由和避免拥塞问题。

3. 运输层

运输层的主要任务是允许源和目标主机上的对等体之间可以进行对话，通过已经定义好的两个端到端的传输协议完成。一个是 TCP（Transport Control Protocol，传输控制协议），它是一个可靠的、面向连接的协议；另一个是 UDP（User Datagram Protocol，用户数据报协议），它是一个不可靠的、无连接的协议。

4. 应用层

应用层包含了所有的高层协议。其中有虚拟终端协议（TELNET）、文件传输协议（FTP）和电子邮件协议（SMTP），后来又加入了域名系统（DNS）和 HTTP。

1.2.3　OSI 参考模型和 TCP/IP 参考模型的比较

OSI 参考模型是在协议出现之前就已经产生的，这意味着 OSI 不会偏向于任何某一组特定的协议，因而该模型更加具有通用性。但是由于 OSI 参考模型出现的时机太晚，相应的服务定义和协议都极其复杂，很难实现，无法真正投入应用。

TCP/IP 正好相反，协议先出现，TCP/IP 模型是对这些已有协议的描述，所以协议一定符合模型。但是该模型没有清楚地区分服务、接口和协议的概念，不能用到 TCP/IP 之外的其他协议栈。

总而言之，OSI 模型对于讨论计算机网络是非常有用的，虽然它并没有流行起来。而 TCP/IP 模型本身实际并不存在，但是协议却被广泛使用了。

1.3　计算机网络协议

网络协议是一种网络软件，是指通信双方关于如何进行通信约定的规则的集合。要使两台计算机彼此之间进行通信，必须使两台计算机使用同一种“语言”。网络协议正像两台计算机交换信息所使用的共同语言，它精确地定义了计算机在彼此通信过程中的所有细节。例如，每台计算机发送的信息格式和含义，在什么情况下应发送规定的特殊信息，以及接收方的计算机应做出哪些应答等。在网络的各层中存在着许多协议，本节介绍部分常用的网络协议。

1.3.1　网际协议

网际协议（Internet Protocol，IP）是 Internet 上使用的一个关键的底层协议。利用这个共同遵守的协议，才使得 Internet 成为一个允许连接不同类型的计算机和不同操作系统的网络。IP 具有能适应各种各样网络硬件的灵活性，对底层网络硬件几乎没有任何要求，任何一个网络只要可以从一个地点向另一个地点传送数据，就可以使用 IP 加入 Internet。

IP 利用发送 IP 数据报进行通信。每个 IP 数据报包含一个头部和一个正文部分，头部有一个 20 个字节的定长部分和一个可选的变长部分，其中包含有源地址和目的地址两个域，也就是我们常说的 IP 地址，它表示网络号和主机号。利用 IP 地址，数据报才能正确地到达指定位置。我们将在下一节中介绍 IP 地址。

1.3.2　传输控制协议

传输控制协议（Transmission Control Protocol，TCP）是一种端对端协议。这是因为它为两台计算机之间建立连接起了重要作用：当一台计算机需要与另一台远程计算机连接时，TCP 会让它们建立起一个连接、发送和接收数据，以及终止连接的过程。

TCP 利用重发技术和拥塞控制机制，向应用程序提供可靠的通信连接，使它能够自动适应网上的各种变化。Internet 是一个庞大的国际性网络，网路上的拥挤和空闲时间总是交替不定的，加上传送的距离也远近不同，所以传输数据所用时间也会变化不定。TCP 具有自动调

整“超时值”的功能，能很好地适应 Internet 上各种各样的变化，确保传输数值的正确。因此，从上面我们可以了解到：IP 只保证计算机能发送和接收分组数据，而 TCP 则可提供一个可靠的、可流控的、全双工的信息流传输服务。

综上所述，虽然 IP 和 TCP 这两个协议的功能不尽相同，也可以分开单独使用，但它们是在同一时期作为一个协议来设计的，并且在功能上也是互补的。只有两者的结合，才能保证 Internet 在复杂的环境下正常运行。凡是要连接到 Internet 的计算机，都必须同时安装和使用这两个协议，因此在实际中常把这两个协议统称为 TCP/IP。

1.3.3 用户数据报协议

用户数据报协议（User Datagram Protocol，UDP）和 TCP 都属于传输层协议，主要用来支持那些需要在计算机之间传输数据的网络应用，包括网络视频会议系统在内的众多的客户/服务器模式的网络应用都需要使用 UDP。

UDP 使用端口号为不同的应用保留其各自的数据传输通道。UDP 和 TCP 正是采用这一机制实现对同一时刻内多项应用同时发送和接收数据的支持。数据发送一方（可以是客户端或服务器端）将 UDP 数据报通过源端口发送出去，而数据接收一方则通过目标端口接收数据。有的网络应用只能使用预先为其预留或注册的静态端口；而另外一些网络应用则可以使用未被注册的动态端口。因为 UDP 报头使用两个字节存放端口号，所以端口号的有效范围是从 0 到 65535。一般来说，大于 49151 的端口号都代表动态端口。

与 TCP 不同，UDP 并不提供数据传送的保证机制。如果在从发送方到接收方的传递过程中出现数据报的丢失，协议本身并不能做出任何检测或提示。因此，通常人们把 UDP 称为不可靠的传输协议。

UDP 由于排除了信息可靠传递机制，将安全和排序等功能移交给上层应用来完成，极大地降低了执行时间，具有 TCP 望尘莫及的速度优势。而 TCP 由于植入了各种安全保障功能，在实际执行的过程中会占用大量的系统开销，无疑使速度受到严重的影响。

1.3.4 点对点协议

点对点协议（Point to Point Protocol，PPP）是为在同等单元之间传输数据包这样的简单的链路而设计的。这种链路提供全双工操作，并按照顺序传递数据包。PPP 为基于各种主机、网桥和路由器的简单连接提供一种共通的解决方案。

PPP 封装提供了不同网络层协议同时通过统一链路的多路技术，具有对常用支持硬件的兼容性。

1.3.5 路由信息协议

路由信息协议（Routing Infomation Protocol，RIP）是最早的路由协议之一，从类别上属于内部网关协议（IGP）类。它是距离向量路由式协议，这种协议在计算两个地方的距离时只计算经过的路由器的数目，如果到相同目标有两个不等速或带宽不同的路由器，但是经过的路由器的个数一样，RIP 认为两者距离一样，而实际传送数据时，很明显一个快一个慢，

试读结束，需要全本PDF请购买 www.ertongbook.com

这就是 RIP 的不足之处，而 OSPF 在它的基础上克服了 RIP 的缺点。

1.3.6　优先开放最短路径协议

优先开放最短路径协议（Open Shortest Path First Protocol，OSPF）也是一种内部网关协议，用于在同一个自治域（AS）中的路由器之间发布路由信息。区别于距离矢量协议（RIP），OSPF 具有支持大型网络、路由收敛快、占用网络资源少等优点，在目前应用的路由协议中占有相当重要的地位。

1.4　计算机网络中的地址

数据在网络中从源端传送到目的端，就必须有标识系统。在标识系统中，地址就是为了识别某个系统的一个非常重要的标识符，如文献【SHOC78】给出的定义：名字指出我们所要寻找的那个资源，地址指出那个资源在何处，路由告诉我们如何到达该处。

在 IEEE 802 标准中为局域网规定了一种固化在网络适配器的 ROM 中的地址，我们称为硬件地址或 MAC 地址。在 TCP/IP 体系中，提出了 IP 地址，是给 Internet 上的每一个主机的每一个接口分配在全世界范围唯一的标识符。

1.4.1　MAC 地址

MAC（Media Access Control）地址是烧录在网卡里的，也叫做硬件地址，是一种 48 位的全球地址，通常是由网卡生产厂家烧入网卡的 EPROM，它存储的是传输数据时真正赖以标识发出数据的计算机和接收数据的主机的地址。在网络底层的物理传输过程中，是通过 MAC 地址来识别主机的。

要获取本机的 MAC 地址，在 Windows 2000/XP 中，依次单击“开始”→“运行”→输入“CMD”→回车→输入“ipconfig /all”→回车（或者依次单击“开始”→“所有程序”→“附件”→“命令提示符”→输入“ipconfig /all”→回车）即可看到 MAC 地址。

1.4.2　IP 地址

在 Internet 中，IP 地址是一个最基本的概念。IP 地址是一个 32 位的二进制地址，为了便于记忆，将它们分为 4 个字节，由小数点分开，可以计算出用点分开的每个字节的数值范围是 0～255，如 211.84.150.1，这种书写方法叫做点分十进制表示法。

最基本的分类将常见的 IP 地址分为 A、B、C 三类。每一类 IP 地址都由网络地址和主机地址两个字段构成，网络地址能够确定这类 IP 地址所在的网络，根据主机地址能够确定这个网络中的一台主机。

A 类地址的表示范围为：0.0.0.0～126.255.255.255，默认网络掩码为：255.0.0.0；A 类地址分配给规模特别大的网络使用。A 类网络用第 1 个字节表示网络地址，后面 3 个字节作为连接于网络上的主机的地址。

B 类地址的表示范围为：128.0.0.0～191.255.255.255，默认网络掩码为：255.255.0.0；B 类地址分配给一般的中型网络。B 类网络用前两个字节表示网络地址，后两个字节代表网络上的主机地址。

C 类地址的表示范围为：192.0.0.0～223.255.255.255，默认网络掩码为：255.255.255.0；C 类网络用前 3 个字节表示网络地址，最后一个字节作为网络上的主机地址。

D 类地址和 E 类地址的用途比较特殊，D 类地址称为广播地址，供特殊协议向选定的结点发送信息时用。E 类地址保留给将来使用。

在 Internet 中，一台计算机可以有一个或多个 IP 地址，就像一个人可以有多个通信地址一样，但两台或多台计算机却不能共用一个 IP 地址。如果有两台计算机的 IP 地址相同，则会引起异常现象，无论哪台计算机都将无法正常工作。

在上述分类 IP 地址中还包含以下几类特殊的 IP 地址。

（1）广播地址目的端为给定网络上的所有主机，一般主机段为全 0。

（2）单播地址目的端为指定网络上的单个主机地址。

（3）组播地址目的端为同一组内的所有主机地址。

（4）环回地址 127.0.0.1 在环回测试和广播测试时会使用。

1.4.3 子网掩码

在网络传输数据时需要确定主机所在的网络，利用掩码的主要的目的就是找到 IP 中的网络地址。针对 A、B、C 三类地址有如下预设的掩码值。

	IP 地址	掩码
A	1.0.0.0～126.255.255.255	255.0.0.0
B	128.0.0.0～191.255.255.255	255.255.0.0
C	192.0.0.0～223.255.255.255	255.255.255.0

这三类地址的网络地址都是整字节的，所对应掩码的位的值都是 1，所以字节的值只有 255，如果把这三类地址拆分成子网时网络地址就不一定是整字节的，掩码值便不一定是 255 了。这时必须通过将 IP 地址和子网掩码作 AND 操作才可以得到网络地址。

例：已知 IP 地址是 141.14.72.11，子网掩码是 255.255.224.0。试求网络地址。

解：注意到掩码的前两个字节全为 1，因此网络地址的前两个字节可以直接确定为 141.14。子网掩码的第 4 个字节全为 0，因此网络地址的第 4 个字节是 0。只需把 IP 地址的第 3 个字节和子网掩码的第 3 个字节转化为二进制数来表示，对它们进行 AND 操作就可得出网络地址。

a. 把 IP 地址的第 3 个字节转换成二进制数：141. 14 . 01001000.11

b. 把子网掩码的第 3 个字节转换成二进制数：255.255.11100000. 0

c. IP 地址与子网掩码逐位相与得出结果：141. 14 .01000000. 0

d. 得到的网络地址点分十进制：141.14.64.0

1.4.4 MAC 地址与 IP 地址的关系

既然每个以太网设备在出厂时都有一个唯一的 MAC 地址了，那为什么还需要为每台主机再分配一个 IP 地址呢？或者说每台主机都分配了唯一的 IP 地址，为什么还要在网络设备（如

网卡，集线器，路由器等）生产时内嵌一个唯一的 MAC 地址呢？主要原因有以下几点。

（1）IP 地址的分配是根据网络的拓扑结构，而不是根据谁制造了网络设置。若将高效的路由选择方案建立在设备制造商的基础上而不是网络所处的拓扑位置基础上，这种方案是不可行的。

（2）当存在一个附加层的地址寻址时，设备更易于移动和维修。例如，如果一个以太网卡坏了，可以被更换，而无须取得一个新的 IP 地址。如果一台主机从一个网络移到另一个网络，可以给它一个新的 IP 地址，而无须换一个新的网卡。

（3）无论是局域网，还是广域网中的计算机之间的通信，最终都表现为将数据包从某种形式的链路上的初始结点出发，从一个结点传递到另一个结点，最终传送到目的结点。数据包在这些结点之间的移动都是由 ARP（Address Resolution Protocol，地址解析协议）负责将 IP 地址映射到 MAC 地址上来完成的。

1.5　网络测试与维护命令

网络应用中经常会遇到网络故障，采用 Windows 系统内置的网络测试工具就能够解决不少常见问题。

1.5.1　Ping 命令

Ping 命令是用于检测网络连通性、可到达性和名称解析问题的主要 TCP/IP 命令。它通过向对方主机发送“ICMP”报文来验证与对方计算机的 IP 连接情况。回响应答消息的接收情况将和往返过程的次数一起显示出来。

Ping 命令格式如下：Ping 目标计算机名（或域名，IP 地址）

最常见的应用如图 1-2 所示。

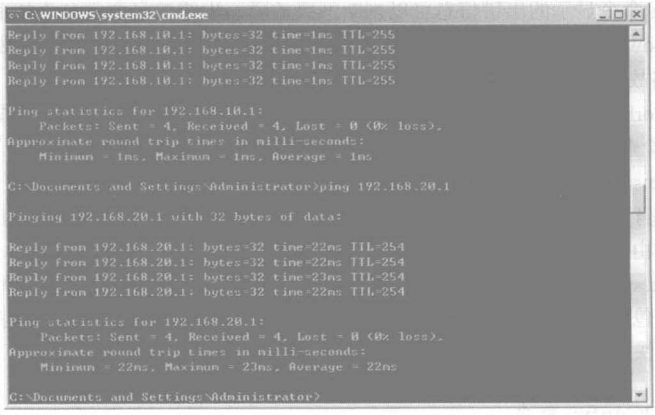


图 1-2　应用 Ping 命令测试网络连通性

Ping 命令的主要参数如下。

-t 不停地 Ping 对方主机，给指定的计算机发送报文，按 Ctrl+Break 组合键可以查看统计信息或继续运行，按下 Ctrl+C 组合键可以中断运行。

-a 解析对方的计算机名。

-n 指定发送的 Echo 数据包数。

Ping 命令在默认情况下只发送 4 个数据包，通过这个参数可以自己定义发送数据包的个数，这对衡量网络速度很有帮助。例如，想测试发送 50 个数据包的返回的平均时间为多少，最快时间为多少，最慢时间为多少，就可以在命令提示符后输入下列命令：

ping -n 50 192.168.1.12

-l：定义 echo 数据包大小。

在默认的情况下 ping 发送的数据包大小为 32 个字节，可以通过这个参数自己定义它的大小，但有一个大小的限制，即最大只能发送 65 500 个字节。示例如下：

ping -l 65500 -t 192.168.1.21

-f：在数据包中发送“不要分段”标志。

-I：指定 TTL 值在对方的系统里停留的时间。

-v：将“服务类型”字段设置为 tos 指定的值。

-r：在“记录路由”字段中记录传出和返回数据包的路由。

发送的数据包是通过一个个路由才到达对方的，但到底是经过了哪些路由呢？通过此参数就可以跟踪经过的路由的个数，不过限制在了 9 个。示例如下：

ping -n 1 -r 9 202.96.105.101 （发送一个数据包，最多记录 9 个路由）

-s：指定 count 指定的跃点数的时间戳。

此参数和-r 差不多，只是这个参数不记录数据包返回所经过的路由，最多也只记录 4 个。

-j：利用 computer-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔（路由稀疏源）IP 允许的最大数量为 9。

-k：利用 computer-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔（路由严格源）IP 允许的最大数量为 9。

-w：指定超时间隔，单位为毫秒。

根据 Ping 命令显示的出错信息可以判断网络故障。出错信息通常分为如下 4 种情况。

（1）unknown host（不知名主机）：该远程主机的名字不能被 DNS（域名服务器）转换成 IP 地址。网络故障可能为 DNS 有故障，或者其名字不正确。

（2）network unreachable（网络不能到达）：这是本地系统没有达到远程系统的路由，可用 netstat-rn 检查路由表来确定路由配置情况。

（3）no answer（无响应）：远程系统没有相应。说明远程主机没有工作，或者本地或远程主机网络配置不正确，或者本地或远程的路由器没有工作，或者通信线路有故障，或者远程主机存在路由选择问题。

（4）Request time out：如果在指定时间内没有收到应答网络包，则 Ping 就认为该计算机不可达。网络包返回时间越短，Request time out 出现的次数越少，则意味着与此计算机的连接稳定和速度快。

1.5.2 IPConfig 命令

IPConfig 命令用来检验人工配置的 TCP/IP 设置是否正确，对于了解计算机当前的 IP 地

址、子网掩码和默认网关很有用，是进行测试和故障分析的必要命令。

常用的 Ipconfig 命令如图 1-3 所示。

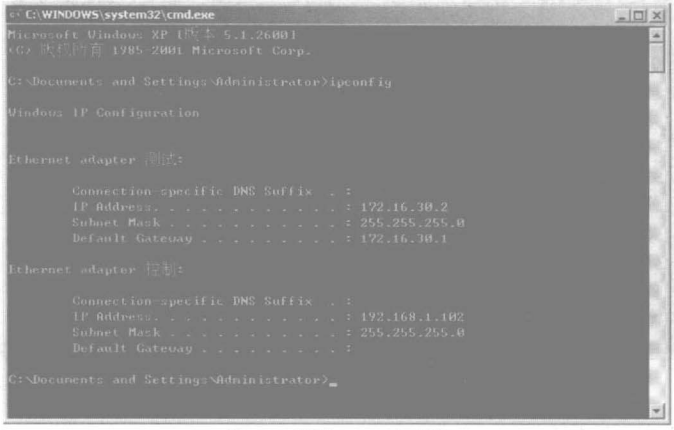


图 1-3　常规的 Ipconfig 用法

其中，最常用的选项如下。

ipconfig：当不带任何参数选项，显示的是 IP 地址、子网掩码和默认网关值。

ipconfig /all：当使用 all 选项时，显示与 TCP/IP 相关的所有细节，包括主机名、结点类型、是否启用 IP 路由、网卡的 MAC 地址、默认网关等。

ipconfig /flushdns：清除本地 DNS 缓存内容。

ipconfig /displaydns：显示本地 DNS 内容。

ipconfig /registerdns：DNS 客户端手工向服务器进行注册。

ipconfig /release 和 ipconfig /renew：这是两个附加选项，只能在向 DHCP 服务器租用其 IP 地址的计算机上起作用。

1.5.3　ARP 命令

ARP 是一个重要的网络层协议，用于 IP 地址与硬件地址解析转换表的管理，能够获得与 IP 地址相对应的网卡物理地址。如果目标主机不在本地网内，则获得默认网关的硬件地址。此外，还能够查看本地计算机或另一台计算机的 ARP 高速缓存中的当前内容。

按照默认设置，ARP 高速缓存中的项目是动态的，每当发送一个指定地点的数据报且高速缓存中不存在当前项目时，ARP 便会自动添加该项目。

ARP 常用命令选项如下。

arp -a 或 arp –g：用于查看高速缓存中的所有项目，用法如图 1-4 所示。

arp -a ip：如果有多个网卡，那么使用 arp -a 加上接口的 IP 地址，就可以只显示与该接口相关的 ARP 缓存项目。

arp -s ip 物理地址：向 ARP 高速缓存中人工输入一个静态项目。该项目在计算机引导过程中将保持有效状态，或者在出现错误时，人工配置的物理地址将自动更新该项目。

arp -d ip：人工删除一个静态项目。

图 1-4 ARP 命令查看缓存中的项目

1.5.4 Tracert 命令

Tracert 命令是路由跟踪命令，用于确定 IP 数据报访问目标所采取的路径。Tracert 命令向目标主机发送包含不同 IP 生存时间（TTL）字段的一系列 Internet 控制消息协议（ICMP）数据包，路径上每个路由器在转发数据包时需将 TTL 递减 1，数据包上的 TTL 到达 0 时，路由器应该将“ICMP 已超时”的消息发送回源系统。Tracert 先发送 TTL 为 1 的 ICMP 数据包，随后每次发送的数据包的 TTL 都递增 1，直到目标响应或 TTL 达到最大值，从而确定路由。

Tracert 参数如下。

-d：指定不将 IP 地址解析到主机名称。

-h maximum_hops：指定跃点数以跟踪到称为 target_name 的主机的路由。

-j host-list：指定 Tracert 实用程序数据包所采用路径中的路由器接口列表。

-w timeout：等待 timeout 为每次回复所指定的毫秒数。

target_name：目标主机的名称或 IP 地址，结果如图 1-5 所示，在跟踪 IP 地址为 172.16.40.2 的主机所经过的路由时，分别通过了路由器 1 172.16.30.1，路由器 2 192.168.10.2 和路由器 3 192.168.20.2。

Tracert 命令按顺序打印出返回“ICMP 已超时”消息的路径中的近端路由器接口列表。如果使用-d 选项，则 Tracert 实用程序不在每个 IP 地址上查询 DNS。

1.5.5 Route 命令

Route 命令用于管理静态路由表，包括对静态路由表的增加、删除、改动、清除以及显示。静态路由表由目标（destination）、网络掩码（netmask）和网关（gateway）组成。

命令格式如下。

Route add [目标][掩码][网关]：增加一个路由。

Route delete [目标][掩码][网关]：删除一个路由。

试读结束，需要全本PDF请购买 www.ertongbook.com