



新编应用型系列技能丛书

计算机

网络实践教学教程

余小华 李慧芬 ● 编著



清华大学出版社

新编应用型系列技能丛书

计算机网络实践教程

余小华 李慧芬 编著

清华大学出版社

北京

内 容 简 介

本书详细介绍了计算机网络实践教学方面的知识。全书由3篇共9章组成,内容包括网络命令的使用、组网基础知识、双绞线制作、网络抓包软件(Wireshark)、网络设备基本操作、交换机MAC地址转发、交换机VLAN基础实验、静态路由配置、RIP路由配置、OSPF路由配置、广域网数据链路层协议、三层交换机实现VLAN间路由、STP协议、端口聚合、端口安全、RIP进阶配置、OSPF进阶配置、访问控制列表(ACL)、网络地址转换(NAT)、DNS服务器、Active Directory域服务器、Web服务器、FTP服务器、DHCP服务器等。

本书取材新颖,包含了主流网络设备生产商Cisco和H3C的设备配置步骤以及Windows 2008服务器配置内容,适合读者自行选取相应章节进行实验教学。各项实验既可以在真实物理设备上完成,也可以在Packet Tracer、GNS3和HCL等软件上实现。本书内容丰富,叙述由浅入深,重点突出,概念清晰易懂,应用性、实践性强。

本书可作为高等学校计算机网络相关课程的教材或配套实验教材,也适合网络设计与管理人员、系统集成人员、工程技术人员阅读和参考。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。
版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

计算机网络实践教程/余小华,李慧芬编著. —北京:清华大学出版社,2017
(新编应用型系列技能丛书)
ISBN 978-7-302-45839-5

I. ①计… II. ①余… ②李… III. ①计算机网络—教材 IV. ①TP393

中国版本图书馆CIP数据核字(2016)第288554号

责任编辑:苏明芳
封面设计:刘超
版式设计:李会影
责任校对:赵丽杰
责任印制:宋林

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦A座 邮 编:100084

社总机:010-62770175

邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质量反馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

印 装 者:河北新华第一印刷有限责任公司

经 销:全国新华书店

开 本:185mm×260mm 印 张:14.5 字 数:348千字

版 次:2017年2月第1版 印 次:2017年2月第1次印刷

印 数:1~2500

定 价:35.00元



前言

Foreword

互联网极大地改变了人们的学习、工作、生活和生产方式。目前，世界上每天有超过 30 亿人在使用互联网，人们根本无法想象回到一个没有网络，不能随时随地与朋友聊天、发布动态、浏览资讯、观看视频或者在线购物的时代将会是什么样子。计算机网络是“互联网+”社会的重要基础设施。培养一批谙熟计算机网络原理与技术，具有综合应用和研发创新能力的人才，是“互联网+”社会信息化的需要，也是高等院校相关专业的教学目标。

编者在应用型本科院校工作多年，一直从事计算机网络等课程及其实践课程的教学工作。包括编者所在学校在内的许多本科院校采用了谢希仁编著的《计算机网络》作为网络基础课程的教材，该教材内容丰富，讲解透彻。针对应用型本科院校学生的特点，计算机网络教学中应将基础理论和实践并重，大多数院校都开设计算机网络实践课程。为规范实践内容，严格实训训练，达到计算机网络实践教学的目的，经过编者多年来对应用型本科院校的计算机网络实践教学的探索，研究在有限课时的情况下，如何组织计算机网络实践教学的内容，使之既能配合课堂教学，加深对所学知识的理解，又能紧跟网络前沿技术的发展，培养和提高学生的实际操作技能。在教学实践中，编者一直坚持编写和完善实验指导书，并与同类兄弟院校的教师多次交流，修订完成了本书。

本书内容涵盖诠释网络基本原理，组网技术，交换机、路由器进阶配置和服务器配置等几方面的实践内容。本书以设计“基础篇→进阶篇→服务器篇”为主线，以 H3C 设备和 Cisco 设备为例，具体内容如下：

基础篇：从网络命令的使用着手，了解网络基本故障所在。组网技术主要介绍了局域网中常见的子网划分方法、双绞线的制作和网络抓包软件 Wireshark 的基本使用。然后进一步从 H3C 和 Cisco 设备基本操作、VLAN 划分、静态路由配置、RIP 路由配置、OSPF 路由配置和广域网配置等方面进行了重点介绍。完成该篇实验后，基本上能够组建中小型局域网。

进阶篇：针对大中型局域网对交换机和路由器配置的要求，本篇重点介绍了三层交换机实现 VLAN 间路由、STP 配置、端口聚合及链路冗余配置、端口安全配置、单臂路由配置、RIP 和 OSPF 的进阶配置、访问控制列表和网络地址转换等原理和具体配置。

服务器篇：网络是基础，应用是目标。本篇以 Windows Server 2008 作为服务器操作系统，对常见的网络应用服务器进行配置，包括 DNS 服务器、Active Directory 域服务器、Web 服务器、FTP 服务器和 DHCP 服务器。这些网络应用服务仍然是网络的常见应用服务，完成该部分实验后，能够搭建基本的的应用服务。

本书由余小华、李慧芬和陈放编写。

感谢所有同仁和朋友对本书编写和出版所提供的意见、建议和热忱帮助。

由于时间仓促和编者水平所限，不足之处在所难免，恳请各位读者不吝批评指正，万分感谢！

编者

2016年8月

于华南理工大学广州学院

E-mail:yuxh@gcu.edu.cn

目 录

Contents

基础篇

第 1 章 网络命令的使用.....2	2.5.3 使用 H3C 设备的实验过程.... 34
1.1 ping 命令.....2	2.5.4 使用 Cisco 设备的实验 过程..... 40
1.2 netstat 命令.....5	2.5.5 实验中的命令列表.....44
1.3 ipconfig 命令.....7	2.5.6 实验总结.....45
1.4 arp 命令.....8	2.6 交换机的 MAC 地址转发表....45
1.5 tracert 命令.....9	2.6.1 原理简介.....45
1.6 nbtstat 命令..... 11	2.6.2 实验环境.....46
第 2 章 组网技术..... 12	2.6.3 使用 H3C 设备的实验过程....46
2.1 基础知识..... 12	2.6.4 使用 Cisco 设备的实验过程..48
2.2 双绞线制作..... 15	2.6.5 实验中的命令列表..... 49
2.2.1 实验器材..... 15	2.6.6 实验总结..... 50
2.2.2 实验步骤..... 15	2.7 交换机 VLAN 基础实验.....50
2.2.3 实验总结..... 18	2.7.1 原理简介..... 50
2.3 网络抓包软件的使用..... 18	2.7.2 实验环境..... 50
2.3.1 原理简介..... 18	2.7.3 使用 H3C 设备的实验过程....51
2.3.2 实验步骤..... 19	2.7.4 使用 Cisco 设备的实验过程..54
2.3.3 实验总结..... 24	2.7.5 实验中的命令列表..... 59
2.4 网络设备基本操作.....25	2.7.6 实验总结..... 60
2.4.1 原理简介..... 25	2.8 静态路由配置.....60
2.4.2 实验环境..... 25	2.8.1 原理简介..... 60
2.4.3 使用 H3C 设备的实验过程.... 26	2.8.2 实验环境..... 60
2.4.4 使用 Cisco 设备的实验 过程..... 30	2.8.3 使用 H3C 设备的实验过程....61
2.4.5 实验中的命令列表..... 32	2.8.4 使用 Cisco 设备的实验 过程..... 64
2.4.6 实验总结..... 33	2.8.5 实验中的命令列表..... 66
2.5 网络设备的信息查看与 调试.....33	2.8.6 实验总结..... 67
2.5.1 原理简介..... 33	2.9 RIP 路由配置.....67
2.5.2 实验环境..... 33	2.9.1 原理简介..... 67

2.9.2	实验环境.....	68	2.11.2	实验环境.....	85
2.9.3	使用 H3C 设备的实验过程....	68	2.11.3	使用 H3C 设备的实验 过程.....	85
2.9.4	使用 Cisco 设备的实验过程... 72		2.11.4	使用 Cisco 设备的实验 过程.....	89
2.9.5	实验中的命令列表.....	74	2.11.5	实验中的命令列表.....	90
2.9.6	实验总结.....	75	2.11.6	实验总结.....	91
2.10	OSPF 路由配置.....	75	2.12	广域网数据链路层协议.....	91
2.10.1	原理简介.....	75	2.12.1	原理简介.....	91
2.10.2	实验环境.....	76	2.12.2	实验环境.....	92
2.10.3	使用 H3C 设备的实验 过程.....	76	2.12.3	使用 H3C 设备的实验 过程.....	93
2.10.4	使用 Cisco 设备的实验 过程.....	80	2.12.4	使用 Cisco 设备的实验 过程.....	99
2.10.5	实验中的命令列表.....	83	2.12.5	实验中的命令列表.....	100
2.10.6	实验总结.....	84	2.12.6	实验总结.....	101
2.11	广域网接口和线缆.....	84			
2.11.1	原理简介.....	84			

进阶篇

第 3 章	交换机进阶配置.....	104	3.3.1	原理简介.....	111
3.1	基于 MAC 地址的 VLAN 划分.....	104	3.3.2	实验环境.....	112
3.1.1	原理简介.....	104	3.3.3	使用 H3C 设备的实验 过程.....	112
3.1.2	实验环境.....	104	3.3.4	使用 Cisco 设备的实验 过程.....	118
3.1.3	使用 H3C 设备的实验 过程.....	105	3.3.5	实验中的命令列表.....	122
3.1.4	实验中的命令列表.....	107	3.3.6	实验总结.....	123
3.1.5	实验总结.....	107	3.4	端口聚合及链路冗余配置.....	123
3.2	三层交换机实现 VLAN 间 路由.....	107	3.4.1	原理简介.....	123
3.2.1	原理简介.....	107	3.4.2	实验环境.....	123
3.2.2	实验环境.....	108	3.4.3	使用 H3C 设备的实验 过程.....	124
3.2.3	使用 H3C 设备的实验 过程.....	108	3.4.4	使用 Cisco 设备的实验 过程.....	126
3.2.4	使用 Cisco 设备的实验 过程.....	109	3.4.5	实验中的命令列表.....	128
3.2.5	实验中的命令列表.....	110	3.4.6	实验总结.....	128
3.2.6	实验总结.....	111	3.5	端口安全配置.....	128
3.3	配置交换机 STP 协议.....	111	3.5.1	原理简介.....	128
			3.5.2	实验环境.....	129

3.5.3	使用 H3C 设备的实验 过程	129	4.3.2	实验环境	149
3.5.4	使用 Cisco 设备的实验 过程	132	4.3.3	使用 H3C 设备的实验 过程	150
3.5.5	实验中的命令列表	132	4.3.4	使用 Cisco 设备的实验 过程	159
3.5.6	实验总结	133	4.3.5	实验中的命令列表	168
第 4 章	路由器进阶配置	134	4.3.6	实验总结	169
4.1	单臂路由配置	134	4.4	访问控制列表	169
4.1.1	原理简介	134	4.4.1	原理简介	169
4.1.2	实验环境	134	4.4.2	实验环境	170
4.1.3	使用 H3C 设备的实验 过程	135	4.4.3	使用 H3C 设备的实验 过程	170
4.1.4	使用 Cisco 设备的实验 过程	136	4.4.4	使用 Cisco 设备的实验 过程	173
4.1.5	实验中的命令列表	137	4.4.5	实验中的命令列表	175
4.1.6	实验总结	138	4.4.6	实验总结	176
4.2	RIP 进阶配置	138	4.5	NAT 配置	176
4.2.1	原理简介	138	4.5.1	原理简介	176
4.2.2	实验环境	139	4.5.2	实验环境	176
4.2.3	使用 H3C 设备的实验 过程	140	4.5.3	使用 H3C 设备的实验 过程	177
4.2.4	使用 Cisco 设备的实验 过程	144	4.5.4	使用 Cisco 设备的实验 过程	181
4.2.5	实验中的命令列表	148	4.5.5	实验中的命令列表	185
4.2.6	实验总结	148	4.5.6	实验总结	186
4.3	OSPF 进阶配置	149			
4.3.1	原理简介	149			

服务器篇

第 5 章	DNS 服务器的部署	188	6.2.1	Active Directory 域控制器的 安装	197
5.1	DNS 概述	188	6.2.2	创建域用户账户	199
5.2	DNS 服务器的部署	189	6.2.3	使用域共享资源	202
5.2.1	DNS 服务器的安装	189	第 7 章	Web 服务器的部署	205
5.2.2	DNS 服务器的配置	190	7.1	万维网概述	205
第 6 章	Active Directory 域服务器的 部署	196	7.2	Web 服务器的配置	206
6.1	Active Directory 概述	196	7.2.1	Web 服务器的安装	206
6.2	Active Directory 域服务的 配置	197	7.2.2	Web 站点的配置	207
			第 8 章	FTP 服务器的部署	210
			8.1	FTP 协议概述	210

8.2 FTP 服务器的配置210
8.2.1 FTP 服务器的安装 210
8.2.2 FTP 站点的配置 211

第 9 章 DHCP 服务器的部署 215
9.1 DHCP 协议概述215

9.2 DHCP 服务器的安装与
配置217
9.2.1 DHCP 服务器的安装217
9.2.2 DHCP 服务器的配置219

参考文献223

基础篇

◇ 网络命令的使用

◇ 组网技术

第 1 章

网络命令的使用

1.1 ping 命令

ping (Packet InterNet Groper) 是个使用频率极高的 ICMP 协议的程序, 用于确定本地主机是否能与另一台主机¹交换(发送与接收)数据报。根据返回的信息, 就可以推断 TCP/IP 参数设置是否正确以及运行是否正常。需要注意的是, 成功地与另一台主机进行一次或两次数据报交换并不表示 TCP/IP 配置就是正确的, 必须执行大量的本地主机与远程主机的数据报交换, 才能确信 TCP/IP 的正确性。当然, 对方也有可能通过防火墙等设置对 ping 包进行阻挡。

简单地说, ping 就是一个连通性测试程序, 如果能 ping 通目标, 就可以排除网络访问层、网卡、线缆和路由器等存在的故障; 如果 ping 目标 A 通而 ping 目标 B 不通, 则网络故障发生在 A 与 B 之间的链路上或 B 上, 从而缩小了故障的范围。如果目标 B 设置了对 ping 包的阻挡, 也是 ping 不通的, 但并不存在网络故障。

按照默认设置, Windows 上运行的 ping 命令发送 4 个 ICMP (Internet Control Message Protocol, 网际控制报文协议) 回送请求, 每个 32B 数据, 如果一切正常, 应能得到 4 个回送应答。ping 能够以毫秒为单位显示发送回送请求到返回回送应答之间的时间量。如果应答时间短, 表示数据报不必通过太多的路由器或网络连接速度比较快。ping 还能显示 TTL (Time To Live, 存在时间) 值, 可以通过 TTL 值推算一下数据包已经通过了多少个路由器。TTL 的初值通常是系统默认值, 是包头中的 8 位的域。TTL 的最初设想是确定一个时间范围, 超过此时间就把包丢弃。由于经过每个路由器都至少要把 TTL 域减 1, TTL 通常表示包在被丢弃前最多能经过的路由器个数。当计数到 0 时, 路由器决定丢弃该包, 并发送一个 ICMP 报文给最初的发送者。

1. ping 检测网络故障的典型步骤

正常情况下, 当使用 ping 命令来查找问题所在或检验网络运行情况时, 需要执行多次 ping 命令, 如果所有都运行正确, 就可以相信基本的连通性和配置参数没有问题; 如果某些 ping 命令出现运行故障, 它也可以指明到何处去查找问题。下面就给出一个典型的检测次序及对应的可能故障。

¹ 主机泛指配置有 IP 地址的主机、路由器或交换机等设备。

(1) ping 127.0.0.1

ping 环回地址，验证是否在本地计算机上正确地安装 TCP/IP 协议以及配置是否正确。

(2) ping 本机 IP

这个命令被送到我们计算机所配置的 IP 地址，计算机始终都应该对该 ping 命令做出应答，如果没有，则表示本地配置或安装存在问题。

(3) ping 局域网内其他 IP

这个命令应该离开我们的计算机，经过网卡及网络线缆到达其他计算机，再返回。收到回送应答表明本地网络中的网卡和载体运行正确。但如果收到 0 个回送应答，那么表示子网掩码（进行子网分割时，将 IP 地址的网络部分与主机部分分开的代码）不正确或网卡配置错误或电缆系统有问题。

(4) ping 网关 IP

这个命令如果应答正确，表示局域网中的网关路由器正在运行并能够做出应答。

(5) ping 远程 IP

如果收到 4 个应答，表示成功地使用了默认网关。对于拨号上网用户则表示能够成功地访问 Internet（但不排除 ISP 的 DNS 会有问题）。

(6) ping localhost

localhost 是操作系统的网络保留名，它是 127.0.0.1 的别名，每台计算机都应该能够将这个名字转换成该地址。如果没有做到这一点，则表示主机文件（/Windows/host）中存在问题。

(7) ping www.xxx.com（如 www.163.com 网易）

执行 ping www.xxx.com 地址，通常是通过 DNS 域名服务器解析域名，如果这里出现故障，则表示本机 DNS 的 IP 地址配置不正确或 DNS 服务器有故障（对于拨号上网用户，某些 ISP 已经不需要设置 DNS 服务器）。顺便说一句，也可以利用该命令实现域名对 IP 地址的转换功能。

如果上面所列出的所有 ping 命令都能正常运行，那么对自己的计算机进行本地和远程通信的功能基本上就可以放心了。但是，这些命令的成功并不表示所有的网络配置都没有问题，例如，某些子网掩码错误就可能无法用这些方法检测到。

2. ping 命令的常用参数选项

- -t: 对指定的计算机一直进行 ping 操作，直到按 Ctrl+C 快捷键中断为止。
- -a: 将 IP 地址解析为计算机 NetBIOS 名称。
- -n: 发送指定数量的 ECHO 数据包。这个命令可以自定义发送数据包的个数，对测试网络速度有帮助，默认值为 4。
- -l size Send buffer size: 定义 echo 数据包大小，在默认的情况下 Windows 的 ping 发送的数据包大小为 32B。也可以自己定义它的大小，如 64B，但最大不能超过 65 500B。
- -i TTL Time To Live: 指定 TTL 值，TTL 的作用是限制 IP 数据包在计算机网络中存在的时间。TTL 的最大值是 255，TTL 的一个推荐值是 64。

3. ping 命令返回结果

如果 ping 命令成功连接到对方,则显示如图 1-1(Windows XP 系统)和图 1-2(Windows 7 系统)所示结果。

```
C:\Documents and Settings>ping www.mit.edu

Pinging e9566.dscl.akamaiedge.net [23.54.203.63] with 32 bytes of data:

Reply from 23.54.203.63: bytes=32 time=291ms TTL=44
Reply from 23.54.203.63: bytes=32 time=274ms TTL=44
Reply from 23.54.203.63: bytes=32 time=288ms TTL=44
Reply from 23.54.203.63: bytes=32 time=299ms TTL=44

Ping statistics for 23.54.203.63:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 274ms, Maximum = 299ms, Average = 288ms
```

图 1-1 Windows XP 系统中 ping 命名连接成功显示结果

```
C:\Users>ping www.mit.edu

正在 Ping e9566.dscl.akamaiedge.net [23.42.190.127] 具有 32 字节的数据:
来自 23.42.190.127 的回复: 字节=32 时间=18ms TTL=49
来自 23.42.190.127 的回复: 字节=32 时间=22ms TTL=49
来自 23.42.190.127 的回复: 字节=32 时间=18ms TTL=49
来自 23.42.190.127 的回复: 字节=32 时间=19ms TTL=49

23.42.190.127 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 18ms, 最长 = 22ms, 平均 = 19ms
```

图 1-2 Windows 7 系统中 ping 命令连接成功显示结果

如果连接对方不成功,则返回以下几种显示结果。

1) Request timed out (请求超时,无响应)

这是常见的提示信息,不仅仅是对方机器设置了过滤 ICMP 数据包,一般有以下几种情况。

- (1) 对方已经关机,或者网络上不存在该地址。
- (2) 对方与自己不在同一网段内,通过路由也无法找到对方,但有时对方确实是存在的。

(3) 对方确实存在,但设置了 ICMP 数据包过滤(如防火墙设置)。判断对方是否存在,可以用带参数 -a 的 ping 命令探测对方,如果能得到对方的 NetBIOS 名称,则说明对方是存在的,且有防火墙设置;如果得不到,多半是对方不存在或关机,或不在同一网段内。

(4) 错误设置 IP 地址。正常情况下,一台主机应该有一个网卡,一个 IP 地址,或多个网卡,多个 IP 地址(这些地址一定要处于不同的 IP 子网)。但如果一台计算机的 TCP/IP 设置中,设置了一个与网卡 IP 地址处于同一子网的 IP 地址,这样,在 IP 层协议看来,这台主机就有两个不同的接口处于同一网段内。当从这台主机 ping 其他机器时,会存在以下问题:

① 主机不知道将数据包发到哪个网络接口,因为有两个网络接口都连接在同一网段。

② 主机不知道用哪个地址作为数据包的源地址。因此,从这台主机去 ping 其他机器,IP 层协议会无法处理,超时后, ping 就会给出一个“超时无应答”的错误信息提示。但从其他主机 ping 这台主机时,请求包从特定的网卡来,ICMP 只需简单地将目的地址、源地址互

换，并更改一些标志即可，ICMP 应答包能顺利发出，其他主机也就能成功 ping 通这台机器。

2) Destination host unreachable (目的主机不可达)

(1) 对方与自己不在同一网段内，而自己又未设置默认的路由。

(2) 网线出了故障。

这里要说明一下 destination host unreachable 和 time out 的区别，如果所经过的路由器的路由表中具有到达目标的路由，而目标因为其他原因不可到达，这时会出现 time out；如果路由表中连到达目标的路由都没有，就会出现 destination host unreachable。

3) Bad IP address (“坏”的 IP 地址)

这个信息表示可能没有连接到 DNS 域名服务器，所以无法解析这个 IP 地址，也可能是 IP 地址不存在。

4) Source quench received (接收源终止)

这个信息比较特殊，它出现的概率很小，表示对方或中途的服务器繁忙，无法回应。

5) Unknown host (不知名主机)

这种出错信息的意思是，该远程主机的名字不能被域名服务器 (DNS) 转换成 IP 地址。故障原因可能是域名服务器有故障，或者其名字不正确，或者网络管理员的系统与远程主机之间的通信线路有故障。

6) No answer (无响应)

这种故障说明本地系统有一条通向中心主机的路由，但却接收不到它发给该中心主机的任何信息。故障原因可能是下列之一：中心主机没有工作；本地或中心主机网络配置不正确；本地或中心的路由器没有工作；通信线路有故障；中心主机存在路由选择问题。

7) ping 127.0.0.1 (127.0.0.1 是本地循环地址)

如果本地地址无法 ping 通，则表明本地机 TCP/IP 协议不能正常工作。

8) no rout to host (网卡工作不正常)

9) transmit failed,error code (10043 网卡驱动不正常)

1.2 netstat 命令

netstat 用于显示与 IP、TCP、UDP 和 ICMP 协议相关的统计数据，一般用于检验本机各端口的网络连接情况。

计算机有时接收到的数据报会导致出错 (数据删除或故障)，TCP/IP 可以容许这些类型的错误，并能够自动重发数据报。但如果累计的出错情况数目占到所接收的 IP 数据报相当大的百分比，或者出错的数目正迅速增加，那么就应该使用 netstat 查一查为什么会出现这些情况。

1. netstat 命令格式

```
netstat [-a] [-e] [-n] [-s] [-t] [-p protocol] [-r] [-interval]
```

netstat 命令的各参数含义说明如下。

- ❑ -a: 显示一个所有的有效连接信息列表，包括已建立的连接（ESTABLISHED），也包括监听连接请求（LISTENING）的连接。
- ❑ -e: 用于显示关于以太网的统计数据。它列出的项目包括传送的数据报的总字节数、错误数、删除数、数据报的数量和广播的数量。这些统计数据既有发送的数据报数量，也有接收的数据报数量。该选项可以用来统计一些基本的网络流量。
- ❑ -n: 显示所有已建立的有效连接。
- ❑ -s: 显示每个协议的统计。默认情况下，显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6。
- ❑ -t: 能够按照各个协议分别显示其统计数据。如果应用程序（如 Web 浏览器）运行速度比较慢，或者不能显示 Web 页之类的的数据，那么就可以用该选项来查看所显示的信息。需要仔细查看统计数据的各行，找到出错的关键字，进而确定问题所在。
- ❑ -r: 可以显示关于路由表的信息，除了显示有效路由外，还显示当前有效的连接。

2. netstat 命令的典型应用

(1) -e: 显示关于以太网的统计数据。显示结果如图 1-3 所示。

```
C:\>netstat -e
Interface Statistics
```

	Received	Sent
Bytes	177040795	5575226
Unicast packets	185065	123359
Non-unicast packets	115	117
Discards	0	0
Errors	0	0
Unknown protocols	0	

图 1-3 netstat -e 命令的显示结果

(2) -s: 显示所有协议，如 TCP、UDP、IP 等的使用状态。显示结果如图 1-4 所示。

```
TCP Statistics for IPv4
```

Active Opens	= 10
Passive Opens	= 0
Failed Connection Attempts	= 0
Reset Connections	= 10
Current Connections	= 0
Segments Received	= 133619
Segments Sent	= 71914
Segments Retransmitted	= 0

```
UDP Statistics for IPv4
```

Datagrams Received	= 51522
No Ports	= 29
Receive Errors	= 0
Datagrams Sent	= 51527

```
C:\>netstat -s
```

图 1-4 netstat -s 命令的显示结果

1.3 ipconfig 命令

ipconfig 命令显示当前所有的 TCP/IP 配置值、刷新动态主机配置协议 (DHCP) 和域名系统 (DNS) 设置。

1. ipconfig 命令格式

```
ipconfig [/all] [/renew [adapter]][/release [adapter]] [/flushdns] [/displaydns] [/registerdns] [/showclassid
adapter] [/setclassid adapter [classid]]
```

ipconfig 命令常用的参数含义说明如下。

- /all: 显示所有适配器的完整 TCP/IP 配置信息。在没有该参数的情况下, ipconfig 只显示 IP 地址、子网掩码和各个适配器的默认网关值。
- /renew [adapter]: 更新所有适配器 (不带 adapter 参数), 或特定适配器 (带有 adapter 参数) 的 DHCP 配置。该参数仅在具有配置为自动获取 IP 地址的网卡的计算机上使用。要指定适配器名称, 请输入使用不带参数的 ipconfig 命令显示的适配器名称。
- /release[adapter]: 发送 DHCPRELEASE 消息到 DHCP 服务器, 以释放所有适配器 (不带 adapter 参数) 或特定适配器 (带有 adapter 参数) 的当前 DHCP 配置并丢弃 IP 地址配置。该参数可以禁用配置为自动获取 IP 地址的适配器的 TCP/IP。要指定适配器名称, 请输入使用不带参数的 ipconfig 命令显示的适配器名称。

2. ipconfig 命令的应用

(1) 使用带/all 选项的 ipconfig 命令, 给出所有接口的详细配置信息, 如本机 IP 地址、子网掩码、网关、DNS、硬件地址 (MAC 地址) 等, 显示结果如图 1-5 所示。

```
C:\>ipconfig/all

Windows IP Configuration

Host Name . . . . . : apache-c172a328
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter 本地连接:

Connection-specific DNS Suffix . :
Description . . . . . : AMD PCNET Family PCI Ethernet Adapter

Physical Address. . . . . : 08-00-27-22-D1-96
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 10.0.2.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.2.2
Dhcp Server . . . . . : 10.0.2.2
DNS Servers . . . . . : 10.10.1.1
                        8.8.8.8
Lease Obtained. . . . . : 2016年1月28日 17:47:39
Lease Expires . . . . . : 2016年1月29日 17:47:39
```

图 1-5 ipconfig/all 命令的运行结果

(2) 对于启动 DHCP 的客户端, 使用 ipconfig/renew 命令可以释放当前 IP 地址配置,

使用 `ipconfig/renew` 命令可以刷新配置，向 DHCP 服务器重新租用一个 IP 地址，大多数情况下网卡将重新赋予和以前所赋予的相同的 IP 地址，如图 1-6 所示。

```
C:\>ipconfig/release

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 

C:\>ipconfig/renew

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 10.0.2.15
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.2
```

图 1-6 `ipconfig/release` 和 `ipconfig/renew` 的运行结果

1.4 arp 命令

ARP (Address Resolution Protocol) 是一个重要的 TCP/IP 协议，对应的命令 `arp` 用于查看和绑定 IP 地址和网卡物理地址。使用 `arp` 命令，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。此外，使用 `arp` 命令，也可以用人工方式输入静态的网卡物理/IP 地址对，可以使用这种方式为默认网关和本地服务器等常用主机进行绑定，有助于减少网络上的信息量。

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。一旦高速缓存的项目被输入，它们就已经开始走向失效状态，失效时间为 2~10 分钟不等。因此，如果 `arp` 高速缓存中的项目很少或根本没有时，请不要奇怪，通过另一台计算机或路由器的 `ping` 命令即可添加。所以，需要通过 `arp` 命令查看高速缓存中的内容时，请最好先 `ping` 此台计算机（不能是本机发送 `ping` 命令）。

1. `arp` 命令格式

```
arp -s inet_addr eth_addr [if_addr]
arp -d inet_addr [if_addr]
arp -a [inet_addr] [-N if_addr] [-v]
arp/?
```

参数说明如下。

- `-s`: 向 `arp` 高速缓存中人工输入一个静态项目。目的是让 IP 地址对应的 MAC 地