

高等学校计算机类国家级特色专业系列规划教材

计算机网络 实验教程（第2版）

王盛邦 编著
农 革 审



清华大学出版社

高等学校计算机类国家级特色专业系列规划教材

计算机网络 实验教程（第2版）

王盛邦 编著

清华大学出版社
北京

内 容 简 介

本书覆盖了交换技术、路由技术、网络安全技术、网络编程技术、协议分析技术、设备管理、无线网络等技术,共13章,主要内容有实验基础、网络嗅探与协议分析、网络编程、网络安全、双绞线、VLAN技术、端口聚合、端口镜像、生成树协议、路由器技术、NAT技术、ACL访问控制技术、IPv6技术、无线网络、综合实验等。

本书以实际网络应用为出发点,提供了大量实验,每个实验都包括网络拓扑结构、实验环境说明、实验目的和要求、配置步骤、测试结果等。

本书可作为计算机网络专业本专科教材,也可作为网络专业从业人员的自学教材。

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

计算机网络实验教程/王盛邦编著.—2版.—北京:清华大学出版社,2017

(高等学校计算机类国家级特色专业系列规划教材)

ISBN 978-7-302-46123-4

I. ①计… II. ①王… III. ①计算机网络—实验—高等学校—教材 IV. ①TP393-33

中国版本图书馆CIP数据核字(2016)第315954号

责任编辑:汪汉友

封面设计:傅瑞学

责任校对:李建庄

责任印制:何 芊

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

课件下载: <http://www.tup.com.cn>, 010-62795954

印 装 者:三河市少明印务有限公司

经 销:全国新华书店

开 本:185mm×260mm

印 张:27.5

字 数:669千字

版 次:2012年10月第1版 2017年5月第2版

印 次:2017年5月第1次印刷

印 数:1~1200

定 价:59.50元

产品编号:071554-01

前 言

作者在本书第1版的基础上,对原内容做了一些调整。原第1章不变,但内容有删减。原第9~11章调整为第2~4章,原第2~8章调整为第5~11章,并增加了新的第12章无线网络,原综合实验调整为第13章。

本书第1版大部分内容的操作系统是基于Windows XP的,第2版修改了不适用于Windows 10的部分。交换机与路由器的端口也从百兆升级为千兆端口,以锐捷的S5750、RSR20为参考设备,但实际上对于网络设备的配置管理命令并没有太大改变。书中交换机与路由器等网络设备的配置实验,对于不具备硬件实验环境的可以采用第1章实验基础所介绍的Cisco仿真软件模拟实现。针对目前无线网络比较流行的情况,本版增加了相关内容,供读者学习参考。本书内容覆盖较为广泛,将网络知识和技术融于网络配置实验中,每章均配有用于巩固所讲授内容的思考与练习题和上机实验题,本版还增加了一些有挑战性的实验。本书可作为计算机网络专业应用本科的实验教材,也可作为网络专业从业人员的自学教材。

全书共有13章,主要内容包括实验基础(第1章)、网络嗅探与协议分析(第2章)、网络编程(第3章)、网络安全(第4章)、双绞线实验(第5章)、交换机技术(第6章)、路由技术(第7章)、访问控制列表(第8章)、网络地址转换(第9章)、VPN技术(第10章)、IPv6技术(第11章)、无线技术(第12章)、综合实验(第13章)。

本书重点突出,结构层次清晰,语言通俗易懂,有众多的网络实验,每个实验针对性很强,叙述和分析透彻,包括网络拓扑结构、实验环境说明、实验目的和要求、配置步骤、测试结果等,具有可读性、可操作性和实用性强的特点。本书十分重视实验前后的验证,同时在实验中插入了许多思考和讨论环节。

在本书的编写过程中,参考了大量锐捷网络的技术资料和培训教材,借鉴了许多网络工程和网络同仁的宝贵经验,在此表示诚挚的谢意。由于作者水平有限,书中的不妥和错误在所难免,诚请各位专家和读者批评指正。

编 者
2017年2月

目 录

第 1 章 实验基础	1
1.1 常用网络命令	1
1.1.1 ping 命令	1
1.1.2 tracert 命令	5
1.1.3 ipconfig 命令	7
1.1.4 netstat 命令	8
1.1.5 arp 命令	10
1.1.6 net 命令	11
1.1.7 netsh 命令	13
1.2 IPv4 地址基础	16
1.2.1 IPv4 地址表示	16
1.2.2 IPv4 地址结构	16
1.2.3 IPv4 地址分类	17
1.2.4 网络掩码	17
1.2.5 子网掩码与子网划分	18
1.2.6 子网划分实例	18
1.3 网络包分析工具 Wireshark	20
1.3.1 Wireshark	20
1.3.2 Wireshark 常用功能	21
1.3.3 Wireshark 的过滤规则	25
1.3.4 Wireshark 命令行抓包	26
1.3.5 Wireshark 数据包捕获实例	26
1.4 网络模拟软件 Packet Tracer	29
1.4.1 Packet Tracer 界面	29
1.4.2 设备管理	33
1.4.3 通过 Packet Tracer 分析协议	35
1.4.4 Packet Tracer 使用实验	38
1.5 绘制网络拓扑图	40
1.5.1 网络设备图例	40
1.5.2 拓扑图绘制工具	41
1.6 实验与实验测试	44

1.6.1	实验前后的对比	44
1.6.2	对实验过程进行监控	44
1.6.3	实验截图	44
1.6.4	撰写实验报告	45
习题 1	45
第 2 章	网络嗅探与协议分析	50
2.1	网络嗅探.....	50
实验 2-1	嗅探实验	51
2.2	协议分析.....	51
2.3	TCP/IP 协议	52
2.3.1	IP 协议	52
2.3.2	TCP 协议	54
实验 2-2	TCP/IP 协议分析	58
2.4	HTTP 协议	60
实验 2-3	HTTP 协议分析实验	62
2.5	FTP 协议	64
2.5.1	FTP 客户/服务器	64
2.5.2	数据连接主动方式/被动方式.....	65
2.5.3	用户名和口令的明文传输	65
2.5.4	FileZilla	66
实验 2-4	FTP 协议分析	66
2.6	Telnet 协议	69
2.6.1	Telnet 的基本服务	69
2.6.2	选项协商	70
2.6.3	Telnet 客户机和服务器	71
实验 2-5	Telnet 协议分析	71
2.7	DNS 协议	73
实验 2-6	DNS 协议分析	76
2.8	ARP 协议	78
实验 2-7	ARP 协议分析.....	80
2.9	QQ 协议	82
实验 2-8	QQ 协议分析	83
2.10	迅雷下载协议	85
实验 2-9	迅雷协议分析	86
习题 2	87
第 3 章	网络编程	91
3.1	利用套接字建立逻辑信道.....	92

3.2	Client/Server 工作模式分类	93
3.3	面向连接的 Client/Server 模式	93
3.3.1	面向连接的服务器工作流程	93
3.3.2	面向连接的客户端工作流程	95
3.4	无连接的 Client/Server 模式	97
3.5	编程实验	97
	实验 3-1 TCP 通信程序设计	102
	实验 3-2 UDP 通信程序设计	103
	实验 3-3 网络嗅探器设计	104
	实验 3-4 停等协议通信	106
	实验 3-5 GBN 协议编程	107
	实验 3-6 IPv4 组播通信	108
	实验 3-7 应用层组播	113
	习题 3	115
第 4 章	网络安全	117
4.1	Linux 防火墙配置	117
4.1.1	netfilter/iptables	118
4.1.2	建立规则和链	119
4.1.3	其他 NAT 配置	123
	实验 4-1 Linux 防火墙设计	123
4.2	ARP 欺骗	126
4.2.1	同一网段的 ARP 欺骗	126
4.2.2	不同网段的 ARP 欺骗	127
4.2.3	ARP 欺骗的防御	129
	实验 4-2 ARP 测试与防御	129
4.3	盗链与反盗链技术	131
4.3.1	盗链原理	131
4.3.2	反盗链技术	131
	实验 4-3 分析某下载软件的盗链行为	132
4.4	蜜罐技术	133
	实验 4-4 简单蜜罐陷阱的配置	134
4.5	入侵检测技术	136
	实验 4-5 入侵检测实验	137
	习题 4	138
第 5 章	双绞线实验	142
5.1	双绞线	142
5.2	RJ-45 连接器	145

5.3	双绞线跳线的制作标准和跳线类型	147
5.3.1	T568-A 标准与 T568-B 标准	147
5.3.2	跳线线序	148
5.3.3	直连线和交叉线	148
	实验 5-1 双绞线跳线的制作和测试	149
5.4	信息模块	152
	实验 5-2 信息模块的压制和测试	154
	习题 5	156
第 6 章	交换机技术	157
6.1	交换机技术基础	157
6.1.1	以太网交换机	157
6.1.2	交换机的工作原理	157
6.1.3	交换机的基本功能	159
6.1.4	交换机的交换方式	159
6.1.5	交换机的分类	160
6.1.6	交换机的接口与连接线缆	160
6.1.7	交换机配置基础	161
6.1.8	交换机的命令模式	162
6.2	VLAN 技术	163
6.2.1	基本概念	163
6.2.2	VLAN 的分类	164
6.2.3	VLAN 数据帧的标识	165
6.2.4	VLAN 中的端口	165
6.2.5	VLAN 的基本配置	166
	实验 6-1 单交换机实现 VLAN	169
	实验 6-2 跨交换机实现 VLAN	172
6.2.6	三层交换机 VLAN 间路由	174
	实验 6-3 通过三层交换机实现 VLAN 间路由	177
6.2.7	单臂路由实现 VLAN 间路由	179
	实验 6-4 单臂路由实现 VLAN 间路由	180
6.3	端口聚合	183
6.3.1	基本概念	183
6.3.2	端口汇聚配置命令	184
6.3.3	配置 Aggregate Port 的流量平衡	185
	实验 6-5 端口聚合配置实验	187
6.4	端口镜像	190
6.4.1	基本概念	190
6.4.2	本地端口镜像	190

实验 6-6 交换机端口镜像配置	192
6.4.3 基于 VLAN 的镜像	194
6.4.4 远程端口镜像	195
实验 6-7 交换机端口远程镜像	197
6.4.5 基于流的远程端口镜像配置	199
6.5 生成树协议	199
6.5.1 基本概念	199
6.5.2 生成树协议的定义	203
6.5.3 快速生成树协议	204
实验 6-8 快速生成树协议配置	204
6.5.4 多生成树协议	208
实验 6-9 多生成树协议配置	208
6.5.5 生成树协议小结	215
6.6 交换技术的发展前景	215
习题 6	216
第 7 章 路由技术	223
7.1 路由器技术基础	223
7.1.1 路由的基本概念	223
7.1.2 路由器的功能	225
7.1.3 路由器的分类	226
7.1.4 路由的分类	226
7.1.5 路由器的接口和线缆	227
7.1.6 路由器配置	228
7.1.7 路由器端口配置原则	229
7.1.8 路由器的常见命令模式	230
7.2 静态路由	230
7.2.1 静态路由	230
7.2.2 静态路由配置步骤	232
7.2.3 静态路由配置主要命令	232
实验 7-1 静态路由	233
7.3 RIP 路由	235
7.3.1 RIP 概述	235
7.3.2 路由环路	236
7.3.3 有类路由与无类路由	239
7.3.4 RIP 的工作过程	239
7.3.5 路由汇总	240
7.3.6 RIP 配置步骤	242
实验 7-2 RIP 路由协议	243

7.4	OSPF 路由	246
7.4.1	OSPF 概述	246
7.4.2	Loopback 地址	247
7.4.3	OSPF 数据包类型	247
7.4.4	OSPF 协议工作过程	249
7.4.5	OSPF 区域	250
7.4.6	OSPF 配置步骤	251
	实验 7-3 OSPF 单区域	252
	实验 7-4 OSPF 多区域	255
7.4.7	OSPF 虚连接	258
7.4.8	OSPF 的认证	259
	实验 7-5 OSPF 虚链路	260
7.4.9	路由重发布	263
	实验 7-6 路由重发布	266
7.5	动态路由协议小结	269
	习题 7	269
第 8 章	访问控制列表	279
8.1	基本概念	279
8.2	ACL 匹配性检查	280
8.2.1	ACL 的匹配过程	280
8.2.2	配置 ACL 的基本原则	280
8.2.3	通配符掩码	281
8.2.4	入站过滤分组和出站过滤分组	282
8.3	标准 ACL	282
8.3.1	标准 ACL 的工作过程	282
8.3.2	标准 ACL 的配置	282
	实验 8-1 利用标准 IP 访问列表进行网络流量的控制	284
8.4	扩展 ACL	286
8.4.1	扩展 ACL 的工作过程	286
8.4.2	扩展 ACL 的配置	287
	实验 8-2 利用扩展 IP 访问列表实现应用服务的访问限制	288
8.5	MAC 扩展访问控制列表	291
8.5.1	MAC 扩展访问控制列表工作过程	291
8.5.2	配置命名的 MAC 扩展 ACL	291
	实验 8-3 配置基于 MAC 的 ACL	292
8.6	基于时间的访问列表	295
8.6.1	基于时间的访问列表的工作过程	295
8.6.2	配置基于时间的访问列表	295

实验 8-4 配置基于时间的 ACL	296
习题 8	298
第 9 章 网络地址转换	304
9.1 地址转换	304
9.2 静态转换	304
9.2.1 基本概念	304
9.2.2 静态转换的配置	305
实验 9-1 利用静态转换实现内外地址的转换	306
9.3 动态转换	307
9.3.1 基本概念	307
9.3.2 动态转换的配置	308
实验 9-2 配置动态转换实现内外地址的转换	308
9.4 端口地址转换	310
9.4.1 基本概念	310
9.4.2 端口地址转换配置	310
实验 9-3 端口地址转换的配置	311
9.5 TCP 负载均衡	312
9.5.1 基本概念	312
9.5.2 配置 TCP 负载均衡	313
实验 9-4 配置 TCP 负载均衡	314
9.6 网络地址转换小结	317
习题 9	317
第 10 章 VPN 技术	323
10.1 基本概念	323
10.2 VPN 协议	324
10.2.1 VPN 安全技术	324
10.2.2 VPN 的隧道协议	324
10.2.3 VPN 的类型	325
10.3 加密系统	327
10.4 IPSec 协议	328
10.4.1 IPSec 体系结构	328
10.4.2 IPSec 的主要协议	329
10.4.3 IPSec 的工作模式	332
10.4.4 IPSec 中的对等体	333
10.4.5 IPSec VPN 的配置步骤	333
实验 10-1 IPSec VPN 简单配置	335
实验 10-2 Site To Site IPSec VPN 多站点配置	339

习题 10	342
第 11 章 IPv6 技术	346
11.1 IPv6 报头结构	346
11.2 IPv6 地址技术	346
11.2.1 IPv6 地址表示法	346
11.2.2 IPv6 地址分类	347
11.2.3 IPv6 地址配置方法	348
11.2.4 IPv6 数据包	349
11.3 IPv6 邻居发现协议	349
实验 11-1 IPv6 邻居发现	353
11.4 IPv6 路由	356
11.4.1 静态路由	356
实验 11-2 IPv6 静态路由	356
11.4.2 IPv6 RIPng	360
实验 11-3 IPv6 RIPng	362
11.4.3 IPv6 OSPFv3	363
实验 11-4 IPv6 OSPFv3 单区域	364
11.5 IPv6 访问控制列表	366
实验 11-5 IPv6 访问控制列表	367
11.6 IPv6 过渡技术	369
11.6.1 双协议栈技术	369
11.6.2 隧道技术	370
实验 11-6 IPv6 手动隧道	372
实验 11-7 6to4 隧道	377
实验 11-8 IPv6 ISATAP 隧道	381
11.6.3 网络地址转换/协议转换技术	384
习题 11	386
第 12 章 无线网络	392
12.1 无线网络概述	392
12.2 无线接入设备	393
12.3 无线网络分类	396
12.4 无线局域网	396
12.5 无线局域网结构	398
12.5.1 点对点 Ad-Hoc 结构	398
实验 12-1 搭建 Ad-Hoc 模式无线网络实验	399
12.5.2 基于 AP 的 Infrastructure 结构	400
实验 12-2 搭建基于 AP 的 Infrastructure 模式无线网络	402

12.6 点对点无线桥接技术·····	403
实验 12-3 搭建无线分布式系统模式网络·····	404
习题 12·····	407
第 13 章 综合实验 ·····	410
综合实验 1 网络嗅探·····	410
综合实验 2 FTP 流量分析·····	411
综合实验 3 应用层组播拓扑修复·····	411
综合实验 4 网络安全·····	413
综合实验 5 入侵检测·····	415
综合实验 6 网络设计·····	415
综合实验 7 网络规划配置·····	417
综合实验 8 综合组网实验·····	418
综合实验 9 OSPF 与 NAT·····	420
综合实验 10 VLAN+单臂路由+路由重发布+ACL 综合实验·····	421
综合实验 11 IPv6 IPSec·····	422
综合实验 12 IPv6 构建园区骨干网·····	423
综合实验 13 RIP 动态路由协议攻防·····	424
综合实验 14 无线网络中 DNS 和 IIS 服务器的配置应用实验·····	425

第 1 章 实验基础

本章主要介绍与本书后续实验相关的基础知识,包括常用的网络命令、IPv4 基础、网络包分析工具、网络仿真软件、绘制拓扑图以及实验报告的书写要求等。

1.1 常用网络命令

Windows 操作系统中有一个命令行解释器,它类似于 MS-DOS 的命令解释程序,可以在其中输入一些命令,实现用户和操作系统之间的直接通信。命令行解释器提供基于字符的应用程序和实用程序的用户界面,命令的语法多数可以通过在命令后加/? 获得使用帮助。

Windows 似乎已经终结了命令的使用,绝大多数操作者习惯于双击图标和菜单操作。但实际上,命令行是非常重要的管理手段。MS-DOS 时代的大部分命令不仅在 Windows 后续版本中得以保留,还有了新的发展(尤其是与网络相关的命令)。本章仅介绍部分与网络有关的命令。

1.1.1 ping 命令

在进行网络实验与调试的过程中,ping 是最常用的一个命令。ping 命令全称为 Packet Internet Grope(因特网包探测器),一般用于测试源主机到目的主机网络的连通性。ping 命令在 IP 层中利用回应请求/应答 ICMP 报文测试目的主机或路由器的可达性。不同操作系统对 ping 命令的实现有所差异。通过执行 ping 命令主要可获得如下信息:

(1) 监测网络的连通性,检验与远程计算机或本地计算机的连接。

(2) 确定是否有数据包丢失、复制或重传。ping 命令在所发送的数据包中设置唯一的序列号,以此检查其接收到的应答报文的序列号。

(3) ping 命令在其所发送的数据包中设置时间戳(Timestamp),根据返回的时间戳信息可以计算数据包往返的时间(Round Trip Time,RTT)。

(4) ping 命令校验每个收到的数据包,据此可以确定数据包是否损坏。

在 Windows 环境下,ping 命令的语法如下:

```
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count]
    [[-j host-list] | [-k host-list]] [-w timeout] [-R] [-S srcaddr] [-4] [-6]
target_name
```

表 1-1 给出了 ping 命令各选项的具体含义。从表 1-1 可以看出,ping 命令的许多选项实际上是指定互联网如何处理和携带回应请求/应答 ICMP 报文的 IP 数据包。

在这些参数中,使用较多的有 t、l、s 等。t 表示连续 ping 目的主机,直到按下 Ctrl+C 键时手动停止;l 表示发送缓冲区大小(默认值为 32B);s 表示使用时间戳选项(仅适用于 IPv4)。

表 1-1 ping 命令选项及含义

选 项	含 义
-t	连续 ping 目的主机,直到按下 Ctrl+C 键时手动停止
-a	将 IP 地址解析为计算机主机名
-n count	发送回送请求 ICMP 报文的次数(默认值为 4)
-l size	发送缓冲区大小(默认值为 32B)
-f	在数据包中不允许分段(默认为允许分段),此项仅适用于 IPv4
-i TTL	指定生存时间
-v TOS	指定要求的 service 类型(仅适用于 IPv4)
-r count	记录路由(仅适用于 IPv4)
-s count	使用时间戳选项(仅适用于 IPv4)
-j host-list	利用主机列表指定宽松的源路由(只是指出一个路由表,但并不要求消息必须经过任意两个相邻路由记录,可以经过其他路由器后再到下一跳指定地点)
-k host-list	利用主机列表指定严格的源路由(指发送者指明了必须经过的路由,如果下一跳路由找不到就返回错误)
-w timeout	指定等待每次回复的超时时间,单位为 ms
-R	同样使用路由标头测试反向路由(仅适用于 IPv6)
-S srcaddr	要使用的源地址
-4	强制使用 IPv4
-6	强制使用 IPv6

1. 发送 ping 测试报文

发送 ping 测试报文可以不用选项。如执行命令“ping IP 地址”或“ping 域名”,则向指定的 IP 地址的主机或域名发送 ping 测试报文。这是最常用的一种使用方法。

【例 1-1】 ping 搜狐公司的域名。

```
C:\>ping www.sohu.com
C:\>ping www.sohu.com
Pinging pgderbjt01.a.sohu.com [118.228.148.143] with 32 bytes of data:

Reply from 118.228.148.143: bytes=32 time=69ms TTL=48
Reply from 118.228.148.143: bytes=32 time=69ms TTL=48
Reply from 118.228.148.143: bytes=32 time=64ms TTL=48
Reply from 118.228.148.143: bytes=32 time=67ms TTL=48

Ping statistics for 118.228.148.143:
    Packets: Sent=4, Received=4, Lost=0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum=64ms, Maximum=69ms, Average=67ms
```

【例 1-2】 ping 搜狐公司的 IP 地址。

```
C:\>ping 118.228.148.143
C:\>ping 118.228.148.143
Pinging 118.228.148.143 with 32 bytes of data:

Reply from 118.228.148.143: bytes=32 time=67ms TTL=48
Reply from 118.228.148.143: bytes=32 time=64ms TTL=48
Reply from 118.228.148.143: bytes=32 time=67ms TTL=48
Reply from 118.228.148.143: bytes=32 time=65ms TTL=48

Ping statistics for 118.228.148.143:
    Packets: Sent=4, Received=4, Lost=0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum=64ms, Maximum=67ms, Average=65ms
```

在例 1-1 中,用户知道了域名 `www.sohu.com` 的 IP 地址是 `118.228.148.143`,所以在例 1-2 中改为 ping IP 地址,其结果是一样的。此例说明,可以利用 ping 命令从域名中查找对应的 IP 地址。

在例 1-1(或例 1-2)显示的结果中,都返回了 4 个测试数据包,其中 `bytes=32` 表示测试中发送的数据包大小是 32B,“`time=67ms`”表示与对方主机往返一次所用的时间是 67ms。信息显示这 4 个数据包当中返回速度最快的为 64ms,最慢的为 69ms,平均速度为 67ms。ping 命令能够以毫秒为单位显示发送回送请求和收到回送应答之间的时长。如果应答时间短,表示数据包没有通过太多的路由器或网络连接速度较快。

“`TTL=48`”表示当前测试使用的 TTL 值为 48。因为 ping 命令使用网络层协议 ICMP,所以 TTL(Time To Live,生存时间)指的是一个网络层的数据包(package)的生存周期。

TTL 的作用是在过长路径情况下,令设备抛弃 ICMP 请求包。因为一个包从一台机器到另一台机器可能需要经过很长的路径,如果无条件的不终止它,它会一直传递下去,如果很多个数据包都这样循环,将会严重影响网络的正常运行。所以需要在包中设置生存时间,并且在包每经过一个节点时,将该值递减 1,最终包在该值还是正数时到达目的地,或者是在经过一定数量的节点后,该值减为 0。前者代表完成了一次正常的传输,后者代表包在生命周期内仍无法到达目的地。当该值为 0 时,网络设备将不会再传递这个包并直接将其抛弃,并发送一个通知给包的源地址。

与 TTL 有关的参数是指定生存时间“-i TTL”,即可以自行定义 TTL 值发送 ICMP 请求包,而忽略操作系统默认的 TTL 值。例如:

```
ping 192.168.1.100 -i 17
```

如果 ping 时 TTL 的值小于 17 仍未到达目的地,将会显示:

```
Request timed out.
```

即在到达目的地之前这个包的生命时间就结束了,由于 TTL 的值减为 0,设备将丢弃包并发送一个 TTL 过期的 ICMP 反馈给源地址。但实际上可能存在如下情况:如果 TTL 的值

大于 17 则可以 ping 通。

2. 连续发送 ping 测试报文

在网络调试过程中,有时需要连续发送 ping 测试报文,一旦配置正确,测试主机可以立即报告目的地可达信息。连续发送 ping 测试报文可以使用-t 选项。如执行命令:

```
ping 192.168.1.100 -t
```

该命令表示连续向 IP 地址为 192.168.1.100 的主机发送 ping 测试报文,可以使用 Ctrl+Break 键显示发送和接收回应请求/应答 ICMP 报文的统计信息,此时 ping 命令仍然继续。结束 ping 命令可以使用 Ctrl+C 键。

3. 自选数据长度的 ping 测试报文

在默认情况下,ping 命令使用的测试报数据长度为 32B,“-l Size”选项可以指定测试数据的长度。如下所示把数据报长度设为 1560B:

```
C:\>ping 192.168.1.100 -l 1560
C:\>ping 92.168.1.100 -l 1560
Pinging 192.168.1.100 with 1560 bytes of data:

Reply from 192.168.1.100: bytes=1560 time<1ms TTL=128
Reply from 192.168.1.100: bytes=1560 time<1ms TTL=128
Reply from 192.168.1.100: bytes=1560 time<1ms TTL=128
Reply from 192.168.1.100: bytes=1560 time<1ms TTL=128

Ping statistics for 192.168.1.100:
    Packets: Sent=4, Received=4, Lost=0 (0%loss),
    Approximate round trip times in milli-seconds:
        Minimum=0ms, Maximum=0ms, Average=0ms
```

虽然-l 参数可以自定义,但是最大值限制为 65500B。超过此值对方就可能因接收的数据包太大而导致死机,这就是著名的“死亡之 ping”。

4. 修改 ping 命令的请求超时时间

默认情况下,系统超时时间为 1000ms。如果超过该时间,系统将显示 request timed out(请求超时)。在使用 ping 命令测试数据报经过延迟较长的链路时,响应可能会花费更长的时间才能返回,这时可以使用-w 选项指定更长的超时时间。如命令 ping 192.168.1.100 -w 6000 指定超时时间为 6000ms。

如果目的地不可达,系统对 ping 命令的响应随不可达原因的不同而异,最常见的有以下两种情况:

(1) Destination net unreachable: 目的网络不可达。说明没有目的地的路由,通常是由于 reply from 中列出的路由器路由信息错误造成的。

(2) Request timed out: 请求超时。表明在指定的超时时间内没有响应测试报文。其原因可能是路由器关闭、目的主机关闭、没有路由返回到主机或响应的等待时间大于指定的超时时间,也有可能是被防火墙阻止或是对方系统设置了安全策略。

5. 不允许路由器对 ping 探测报文分段

主机发送的 ping 探测报文通常允许中途的路由器分段,以便使探测报文通过 MTU 较