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。

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

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	指定要求的服务类型(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