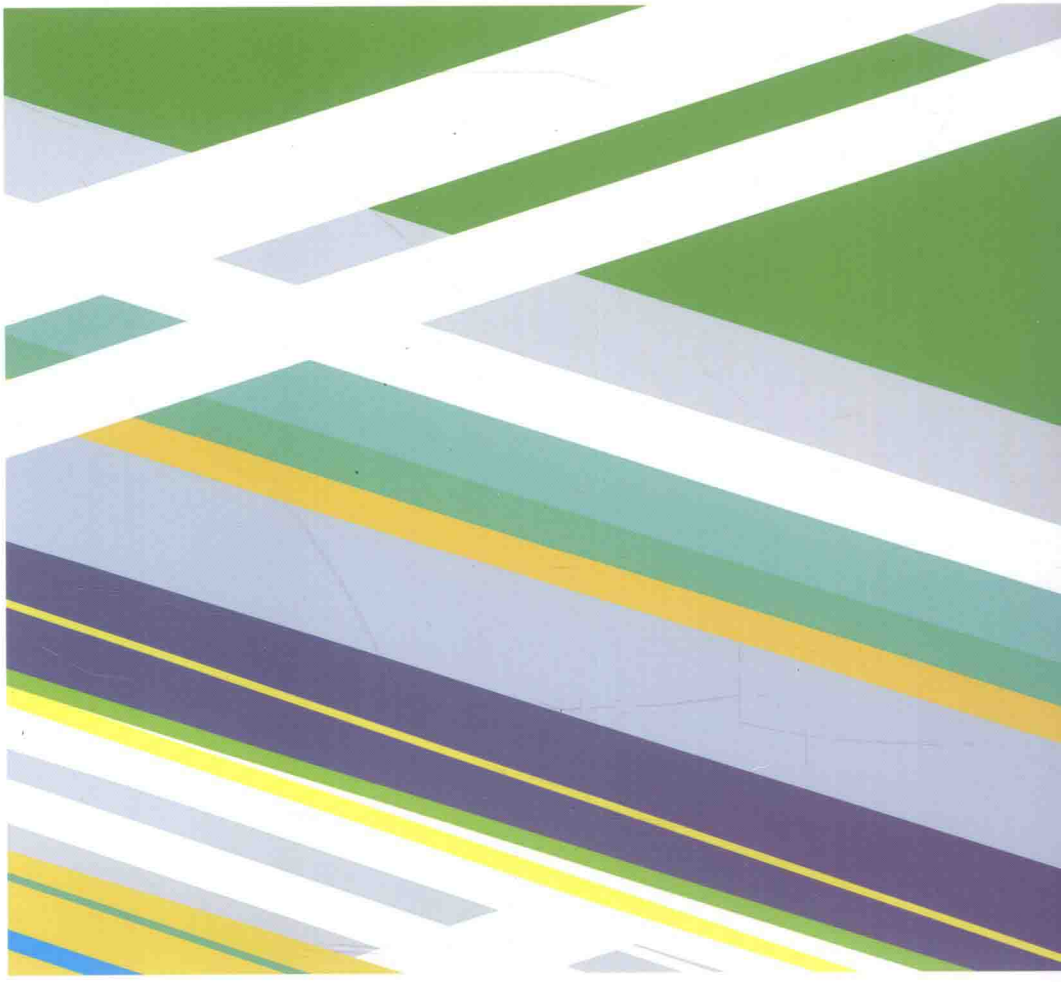


计算机网络课程设计

张晓明　主编

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

计算机网络课程设计

张晓明　主　编

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

内 容 简 介

本教材面向计算机网络课程设计的需要，涵盖了网络设计基础、网络协议模拟和应用设计两部分。前者包括网络环境架设和网络协议分析实例，后者是重点，阐述了各层网络协议的模拟和程序设计内容，精心设计了近 20 道设计案例程序和 27 道课后设计题。其中，物理层、数据链路层和局域网设计示例包括串口通信、组帧、CRC 校验、滑动窗口协议、CSMA/CD 协议、CSMA/CA 协议、透明网桥自学习算法和 ARP 协议等内容； 网络层的设计示例包括 IP 地址校验、IP 协议校验和计算、网络主机扫描、RIP 协议模拟和 OSPF 协议模拟；传输层的设计示例包括端口扫描、UDP 校验和计算、UDP 报文封装、TCP 校验和计算以及 TCP 的拥塞控制等内容。

全书技术性和实用性强，突出工程能力培养，设计示例完整，有较高的参考价值，适用专业包括计算机科学与技术、网络工程、信息安全、通信工程、软件工程等，可以作为计算机网络课程设计和专业实训的教材或参考书。

图书在版编目（CIP）数据

计算机网络课程设计 / 张晓明主编. —北京：北京理工大学出版社, 2016.8
ISBN 978-7-5682-2970-8

Ⅰ. ①计… Ⅱ. ①张… Ⅲ. ①计算机网络-课程设计-教材 Ⅳ. ①TP393-41

中国版本图书馆 CIP 数据核字（2016）第 196371 号

出版发行 / 北京理工大学出版社有限责任公司
社　　址 / 北京市海淀区中关村南大街 5 号
邮　　编 / 100081
电　　话 /（010）68914775（总编室）
　　82562903（教材售后服务热线）
　　68948351（其他图书服务热线）
网　　址 / http://www.bitpress.com.cn
经　　销 / 全国各地新华书店
印　　刷 / 三河市天利华印刷装订有限公司
开　　本 / 787 毫米×1092 毫米　1/16
印　　张 / 11.25
字　　数 / 264 千字
版　　次 / 2016 年 8 月第 1 版　2016 年 8 月第 1 次印刷
定　　价 / 40.00 元

责任编辑 / 钟　博
文案编辑 / 钟　博
责任校对 / 周瑞红
责任印制 / 李志强

前　言

作为网络课程模块的重要组成部分，“计算机网络课程设计”是“计算机网络原理”之后的实践性必修课程，多数设置2～3周集中实践。作者组织本课程设计的教学工作十几年，期间的培养方案更换了3次，课程设计内容也不断更新和完善，教学指导书的版本不断升级，设计项目不断丰富。作者在教学指导过程中体会到，要真正理解某一种网络协议及其数据格式，不是简单的事，最好的解决办法就是做应用设计。这些任务自然就落在了网络课程设计上。为此，作者在2014年即开始教材的规划设计。随着工程教育对本科生系统设计能力的提升要求，本教材在内容和形式上作了进一步调整，针对网络协议描述、设计方法、设计案例、课后项目等都作了精心设计，主要表现为以下几个方面。

1．学术思想

本书以网络协议的模拟设计为核心，以工程实践能力提高为目标，构建网络可操作性、设计性和综合性设计项目，满足网络原理配套实验，特别是网络课程设计实践项目的需要。

2．体系设计

（1）设计基础：它包括网络环境搭建和网络协议分析，本书对此给出了具体的实践案例，可以安排为计算机网络原理课的实验。前者包括网络命令操作、网线制作、无线网配置、小型局域网设计等。对于网络协议分析，本书给出了完整的应用实例，涵盖了ICMP、IP、TCP、UDP、DNS、FTP、SMTP、HTTP等协议的数据包分析。

（2）课程设计项目：以层次化网络协议为划分依据，本书阐述了重要的网络协议模拟设计要点和编程实例，提供了近20道设计案例程序。比如，串口通信程序设计、网络数据校验程序设计、ARP协议程序设计、CDMA/CD协议模拟设计、滑动窗口协议程序设计、透明网桥算法的编程实现、内部路由协议核心算法的编程实现、端口扫描程序设计等。重点需要了解的是网络链路层、网络层和传输层协议，而网络应用层协议比较容易理解，应用设计案例也较多，在作者已出版的网络编程教材中已有大量案例，因此未列入本书内容。

（3）课后安排：每章的最后设计了多个“分析与设计题”，共计27道。这些题目既与正文案例相呼应，又有更新的设计要求，便于读者参考和选用。

3．教学条件

一方面，教材章节后的设计题具有通用性，书中所用工具软件全部来源于开放环境，利于读者自学，如Wireshark抓包软件、串口调试工具、网络调试工具等都可以免费下载。另一方面，系统设计的编程环境可自由选择。书中程序以C#语言为主，还有C++、Java语言和Matlab工具。在CSMA/CD和CSMA/CA、滑动窗口协议模拟、网络拥塞控制等方面，采用Matlab和OPNET等仿真软件将非常便利，读者能够把重点放在模型设计和系统优化方面。

本教材的设计案例主要来自作者的教学设计和实践指导过程，也有少量内容来自互联网

资源。同时，在网络课程设计指导过程中，本书部分案例得到了作者所在院校计算机系网络课程组老师们的积极实践和反馈，在此一并表示感谢。

感谢北京理工大学出版社对本书出版的大力支持和辛勤劳动。

张晓明

2016 年 5 月 20 日

CONTENTS 目录

第1章 网络环境搭建

本章首先介绍一些网络命令和网络测量工具，便于查找网络状况，及早诊断网络故障；然后介绍网络环境搭建，包括网线制作、无线网络配置和小型局域网设计。

本章的学习目标：

（1）通过常用网络命令的使用，具备网络故障诊断的基本能力；

（2）学会设计小型有线局域网络；

（3）具备有线和无线网络综合系统的设计能力。

1.1 常用网络命令

掌握常用的网络命令，便于网络配置方法以及 TCP/IP 协议的诊断。这些命令包括 Ping、Tracert、Netstat、Ipconfig 和 Nslookup 等。

1）Ping

Ping 是最为常用的测试网络故障的命令，它是测试网络连接状况以及信息包发送和接收状况的工具。它的主要作用是向目标主机发送一个数据包，并且要求目标主机在收到数据包时给予答复，来判断网络的响应时间及本机是否与目标主机相互联通。

如果执行 Ping 命令不成功，问题有可能是网线故障、网络适配器配置不正确、IP 地址不正确等。如果执行 Ping 命令成功而网络仍无法使用，那么问题很可能出在网络系统的软件配置方面。

命令格式：

```
Ping IP 地址或主机名 [-t] [-a] [-n count] [-l size]
```

参数含义：

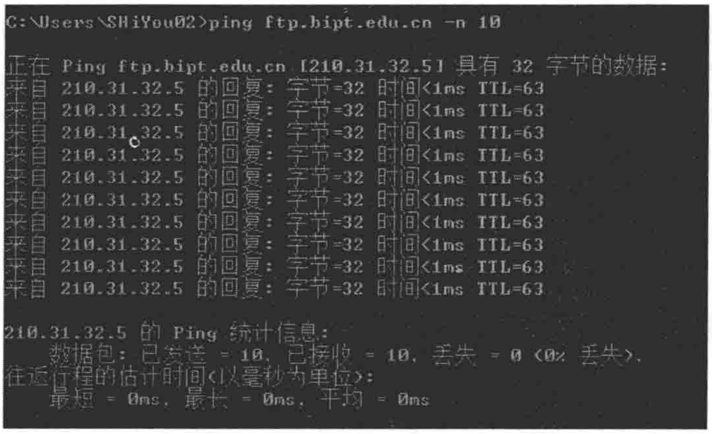
-t：不停地向目标主机发送数据；

-a：以 IP 地址格式来显示目标主机的网络地址；

-n count：指定要 Ping 多少次，具体次数由 count 来指定；

-l size：指定发送到目标主机的数据包的大小。

图 1.1 展示了 Ping 命令的执行情况，对主机 ftp.bipt.edu.cn 执行了 10 次 Ping 命令，回复了 10 次，延迟为 0ms；获得主机 IP 地址为 210.31.32.5。



```
C:\Users\SHiYou02>ping ftp.bipt.edu.cn -n 10

正在 Ping ftp.bipt.edu.cn [210.31.32.5] 具有 32 字节的数据:
来自 210.31.32.5 的回复: 字节=32 时间<1ms TTL=63
来自 210.31.32.5 的回复: 字节=32 时间<1ms TTL=63
来自 210.31.32.5 的回复: 字节=32 时间<1ms TTL=63
来自 210.31.32.5 的回复: 字节=32 时间<1ms TTL=63
来自 210.31.32.5 的回复: 字节=32 时间<1ms TTL=63
来自 210.31.32.5 的回复: 字节=32 时间<1ms TTL=63
来自 210.31.32.5 的回复: 字节=32 时间<1ms TTL=63
来自 210.31.32.5 的回复: 字节=32 时间<1ms TTL=63
来自 210.31.32.5 的回复: 字节=32 时间<1ms TTL=63
来自 210.31.32.5 的回复: 字节=32 时间<1ms TTL=63

210.31.32.5 的 Ping 统计信息:
    数据包: 已发送 = 10, 已接收 = 10, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

图 1.1 Ping 命令执行实例

2）Tracert

使用 Tracert（跟踪路由）命令可以显示数据包到达目标主机所经过的路径，并显示到达每个结点的时间。命令所获得的信息要比 Ping 命令较为详细，它把数据包所走的全部路径、结点的 IP 地址以及花费的时间都显示出来。

命令格式：

Tracert IP 地址或主机名 [-d][-h maximumhops][-j host_list] [-w timeout]

参数含义：

-d：不解析目标主机的名字；

-h maximumhops：指定搜索到目标地址的最大跳跃数；

-j host_list：按照主机列表中的地址释放源路由；

-w timeout：指定超时时间间隔，程序默认的时间单位是毫秒。

图 1.2 展示了该命令的执行情况，跟踪的目标主机是 www.baidu.com。

```
C:\Users\SHiYou02>tracert www.baidu.com

通过最多 30 个跃点跟踪
到 www.a.shifen.com [220.181.111.188] 的路由:

  1    <1 毫秒   <1 毫秒   <1 毫秒 210.31.40.1
  2     *        *        *     请求超时。
  3     2 ms     1 ms     1 ms  124.126.245.137
  4     5 ms     1 ms     *     253.234.120.106.static.bjtelecom.net [106.120.23
4.253]
  5     *        *        *     请求超时。
  6     *        *        *     请求超时。
  7     3 ms     2 ms     2 ms  220.181.182.38
  8     *        *        *     请求超时。
  9     *        *        *     请求超时。
 10     2 ms     2 ms     2 ms  220.181.111.188

跟踪完成。
```

图 1.2 Tracert 命令执行实例

3）Netstat

Netstat 是 DOS 命令，是一个监控 TCP/IP 网络的非常有用的工具，通过它可以了解网络的整体使用情况。它可以显示路由表、实际的网络连接以及每一个网络接口设备的状态信

息，一般用于检验本机各端口的网络连接情况。利用命令参数，可以显示所有协议的使用状态，这些协议包括 TCP 协议、UDP 协议以及 IP 协议等，另外还可以选择特定的协议并查看其具体信息，还能显示所有主机的端口号以及当前主机的详细路由信息。

TCP/IP 可以容许数据报导致出错数据或故障类型的错误，如果累计的出错情况数目占的百分比较大的时候，建议用 Netstat 命令查一查为什么会出现这些情况。Netstat 命令在这方面还是很有作用的。

命令格式：

```
Netstat [-r] [-s] [-n] [-a]
```

参数含义：

-r：显示本机路由表的内容；

-s：显示每个协议的使用状态（包括 TCP 协议、UDP 协议、IP 协议）；

-n：以数字表格形式显示地址和端口；

-a：显示所有主机的端口号。

图 1.3 描述的 Netstat 命令显示本机路由表的部分信息，执行命令是：Netstat -r。

图 1.3 Netstat 命令执行实例（一）

图 1.4 描述的是该命令用于监控地址和端口的情况。

4）Ipconfig

Ipconfig 是调试计算机网络的常用命令，人们通常使用它显示计算机中网络适配器的 IP 地址、子网掩码及默认网关，这些必要的信息是排除网络故障的必要元素。不过这只是 Ipconfig 的不带参数用法，而它的带参数用法在网络应用中也是很好用的。

总的参数简介(也可以在 DOS 方式下输入“Ipconfig /？”进行参数查询)

Ipconfig /all：显示本机 TCP/IP 配置的详细信息；

Ipconfig /release：DHCP 客户端手工释放 IP 地址；

Ipconfig /renew：DHCP 客户端手工向服务器刷新请求；

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 /showclassid：显示网络适配器的 DHCP 类别信息；

Ipconfig /setclassid：设置网络适配器的 DHCP 类别。

```
C:\Users\SHiYou02>netstat -n

活动连接

  协议  本地地址          外部地址        状态
  TCP    127.0.0.1:1113         127.0.0.1:21208        ESTABLISHED
  TCP    127.0.0.1:4025         127.0.0.1:4026         ESTABLISHED
  TCP    127.0.0.1:4026         127.0.0.1:4025         ESTABLISHED
  TCP    127.0.0.1:4027         127.0.0.1:4028         ESTABLISHED
  TCP    127.0.0.1:4028         127.0.0.1:4027         ESTABLISHED
  TCP    127.0.0.1:4091         127.0.0.1:5905         ESTABLISHED
  TCP    127.0.0.1:4092         127.0.0.1:5905         ESTABLISHED
  TCP    127.0.0.1:4123         127.0.0.1:5905         ESTABLISHED
  TCP    127.0.0.1:4124         127.0.0.1:5905         ESTABLISHED
  TCP    127.0.0.1:5905         127.0.0.1:4091         ESTABLISHED
  TCP    127.0.0.1:5905         127.0.0.1:4092         ESTABLISHED
  TCP    127.0.0.1:5905         127.0.0.1:4123         ESTABLISHED
  TCP    127.0.0.1:5905         127.0.0.1:4124         ESTABLISHED
  TCP    127.0.0.1:21208        127.0.0.1:1113         ESTABLISHED
  TCP    210.31.40.34:1113      210.31.40.34:21972     ESTABLISHED
  TCP    210.31.40.34:21251     222.161.227.152:80     CLOSE_WAIT
  TCP    210.31.40.34:21310     114.112.66.37:80       ESTABLISHED
  TCP    210.31.40.34:21966     54.223.186.91:80       CLOSE_WAIT
  TCP    210.31.40.34:21972     210.31.40.34:1113      ESTABLISHED
```

图 1.4　Netstat 命令执行实例（二）

图 1.5 展示的是执行命令 Ipconfig /all 后的部分内容。据此，可以查找本地网络连接的信息，包括已有 MAC 地址和分配的 IP 地址。

```
C:\Users\SHiYou02>ipconfig /all

Windows IP 配置

   主机名  . . . . . . . . . . . . . : ZhangXM
   主 DNS 后缀 . . . . . . . . . . . :
   节点类型 . . . . . . . . . . . . : 混合
   IP 路由已启用 . . . . . . . . . . : 否
   WINS 代理已启用 . . . . . . . . . : 否
   DNS 后缀搜索列表 . . . . . . . . . : bipt.edu.cn

无线局域网适配器 无线网络连接:

   媒体状态 . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : 1x1 11b/g/n Wireless LAN PCI Express Half
Mini Card Adapter
   物理地址. . . . . . . . . . . . . : 24-DE-2B-8E-36-DA
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是

以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . . . : bipt.edu.cn
   描述. . . . . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   物理地址. . . . . . . . . . . . . : F0-DE-F1-AA-DB-8B
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::ec4b:6b88:2618:f3e8%50(首选)
   IPv4 地址 . . . . . . . . . . . . : 210.31.40.34(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.254.0
   获得租约的时间  . . . . . . . . . : 2016年3月18日 13:57:56
   租约过期的时间  . . . . . . . . . : 2016年3月19日 13:57:55
```

图 1.5　Ipconfig 命令执行实例

1.2 网络测量软件

1.2.1 网络测量概述

网络测量是指遵照一定的方法和技术，利用软件和硬件工具来测试或验证表征网络性能指标的一系列活动的总和。

网络测量是一种技术，它通过收集数据或分组的踪迹来显示和分析在不同网络应用下网络中分组的活动情况。从研究的实质上看，网络测量可以把因特网从技术上升到科学，并且能够更好地指导应用。可以说，对因特网的测量是对因特网进行控制的基础和前奏。

网络测量可以为从事网络工作的人，比如负责网络日常运营维护的 ISP、网络工程建设的集成商、网络设备的生产商、互联网用户和网络研究人员等带来益处。其具体用途可分为以下几大类：网络故障诊断、网络协议排错、网络流量特征化、网络性能评价和其他用途，如发现网络恶意行为、网络病毒感染跟踪。

网络测量分类标准有多种：根据测量的方式，分为主动测量和被动测量；根据测量点的多少，分为单点测量与多点测量；根据被测量者知情与否，分为协作式测量与非协作式测量；根据测量所采用的协议，分为基于 BGP 协议的测量、基于 TCP/IP 协议的测量以及基于 SNMP 协议的测量；根据测量的内容，分为拓扑测量与性能测量。

主动测量是通过向网络中发送主动的探测包并观察延迟、丢包、路由变化情况来研究网络特征。其优点是具有很好的可控性，从而有利于突出人们最关心的一些描述网络业务特征的参数；其不足在于，主动测量的开销比较大，可能会改变网络性能参数。主动测量需要向网络中注入探测流量，因此会增加网络负荷，在某些情况下，甚至会对网络造成不必要的负担，影响网络性能。到目前为止，人们所做的大多数项目都涉及主动测量。典型的主动测量方法是使用 Ping、Traceroute/Tracert 等命令。

被动测量是通过在网络中选定的结点安装数据采集器（探针），再通过收集流经结点的网络业务流进行分析，提取业务特征，获得性能数据。被动测量经常用于测量业务量的特征。被动测量主要在一个特殊点观察网络的行为，并不向网络中发送测量探测分组，不增加和修改通过网络的数据负载，因此对网络的行为没有影响。但是，被动测量需要被测方支持以获取流经的业务流信息，从被动捕获得到的包中难以甚至不可能获得人们想要的某些信息，只能测得一些局部性参数，无法获得网络的整体性能参数和端到端性能参数，它与主动测量相比具有更多的不可控性。被动测量的典型例子是基于 tcpdump 的测量，利用 Wireshark 或 Sniffer 工具捕获数据包，其基本原理是利用在同一网段中，数据帧是以广播方式传输的，通过将本地某一主机网卡的工作方式设为混杂模式，截获流经本网段的数据包。

从测量点的数量来讲，网络测量分为单点和多点测量。在研究初期，许多工作都属于单点测量，但因为测量能力有限，搜集的信息不全面，分布式多点测量应运而生。尤其是多点主动测量，利用多个探测点得到的数据，能够综合出大规模的网络数据和单点测量所得不到的交叉路由信息。单点测量的典型例子是贝尔实验室的 InternetMapping 项目，这是一个非合作测量，该项目成功地描述了科索沃战争期间南斯拉夫和科索沃两个网络的拓扑变化情况，这表明在 IP 网络测量中，单点非合作测量具有相当强的网络探测能力，这也是网络测量在

军事领域中应用的典范。

网络拓扑测量主要是了解网络拓扑结构，用以指导资源调节和流量分配，多数项目显示的是逻辑拓扑关系图。随着测量范围的扩大，整张图的规模结构也随之扩大。这时，人们往往希望与实际地域位置相对应，也就是具有地理信息的拓扑图。

网络性能测量主要是通过监测网络端到端的时延、抖动、丢包率等特性，了解网络的可达性、利用率及网络负荷等。在性能测量方面的相关项目开展得较多，这一方面是为了对一个特定网络进行维护管理，保障服务质量；另一方面是为了预报网络性能，通过数值模型预测下一时段的 TCP/IP 端到端的吞吐量、延迟，主要用于广域网上的大规模计算的调度。

网络流量测量主要是对网络数据流的特性进行监测和分析，以掌握网络的流量特性，如协议的使用情况、应用的使用情况、用户的行为特征等。

1.2.2 网络测量的研究方向

1）IP 拓扑测量

其主要测量方法分为两类：基于 SNMP 协议、基于 ICMP 协议。前者主要通过访问 MIB 库进行拓扑关系的获取，由于权限的关系，其适合在具有管辖权的网络范围内测量，所以难以推广应用。后者通过 Tracert 实现，可用于 Internet 上的大规模网络测量，但当网络上安装有防火墙软件时，则无法进行测量。

测量过程如下：首先得到网络 IP 地址分段，然后利用路由追踪技术得到一个数据包从源 IP 地址到目的 IP 地址所经历的所有路由器的 IP 地址，对某一网络的所有 IP 地址进行路由追踪，就会得到该网络所有的路由器的 IP 地址及互联关系。路由追踪技术是基于下面的原理来实现的：首先以 TTL=1 向目的 IP 地址的一个不可达端口（通常是 10000 以上的端口）发一个 UDP 包，这个包在经过第 1 个路由器以后，将被路由器丢弃，同时路由器将向源主机发送一个 ICMP 包通知该包丢失。通过解开这个 ICMP 包，就可以得到该路由器的 IP 地址。然后，再以 TTL=2 向目的 IP 地址发 UDP 包。重复上面的操作，直到返回的 ICMP 包的类型为目的端口不可达，表明已经到达了目的主机，这样就得到从本机到目的主机所经过的路由器 IP 地址。目前，所有的路由器都支持这种实现方式。根据由数据搜集模块得到的路径总表，可以直接生成反映逻辑连接关系的路由 IP 拓扑图，结合各 IP 所在的地理位置，可以生成城市覆盖拓扑图。

2）AS 拓扑测量

总的来说，生成 AS 级拓扑图的方法可归结为基于 BGP 路由信息的 AS 图、基于 Traceroute 的 AS 图以及基于某些特性采用拓扑生成器合成的 AS 级拓扑图三类。其中，第 1 种方法较为普遍，该方法有被动测量和主动测量两种测量方式可供选择。前者在关键路由结点获取 BGP 数据包，再采用有限状态自动机技术，对捕获的 BGP update 报文进行处理；后者自备一台路由器，运行 BGP 协议，通过与 ISP 协商，与相应的路由器建立 BGP 对等连接，只接收路由更新报文，不转发用户数据，这需要对等双方对相应路由器正确配置，在大量测量数据的基础上，生成 AS 拓扑连接图，通过 AS 拓扑连接图，可以直观地了解各 AS 连接关系，分析出哪些 AS 起重要作用。这不仅可以为新 AS 的接入提供指导，而且还可以为将来信息战中的计算机攻防提供指导依据。

3）基于 TCP/IP 协议的网络性能测量与分析

为了考察网络的稳定性、可达性、可靠性及网络服务质量，需要周期性、连续测量的性能参数，包括丢包率、RTT、流量、路径的平均跳数等。在此基础上，以时间为主线分析各路径上各项指标的动态变化，以空间为主线统计分析某一时刻整个网络的整体态势，如处于不同量级时延的结点总体数量分布等，分析端到端路由变化（或跳数的路由变化）等。其他分析还包括对探测得到的数据进行数据挖掘，或者利用已有的模型（Petri 网、自相似性、排队论）研究其自相似特征。由于对网络性能测量的实时性要求较高，所以探测频率往往很高，但必须保证不要由此对网络造成较大的额外负荷，同时注意隐藏探测踪迹。

4）网络运行态势综合分析

基于多个监测点，在不同时段收集的测量数据，生成被测网络的综合态势战略图，真正实现“决胜于千里之外”。该图除了具有不同层面属性的即时播放功能以外，还可以通过颜色标注、声音提示等进行流量异常、故障报警，为防范大规模网络攻击提供预警手段；同时，从网络攻击的角度，研究发展具有隐蔽性、高效的分布式网络侦察测量方法。另外，进行综合分析，为用户提供 QoS 指数、病态路由报告，为改正病态路由、制定网络路由策略、进行网络破坏后的网络资源自组织等提供第一手资料。

5）测量与分析结果的可视化

网络测量与分析结果的可视化是一个关键环节。通过研究，采用图形用户界面 GUI、电子地图的任意缩放及拖动、电子地图的多层表示法、直方图、二维及三维坐标曲线、扇形图、表格、报表、二维平面图形、三维立体图形等手段，结合 GIS 技术，对态势图进行层次化、可拖动、交互式分级显示，直观、形象地表示出测量分析结果。折中点在于，既要全面而客观地显示库中的数据，又要具有良好的视觉效果。

6）网络行为建模、网络仿真、网络趋势预测

网络拓扑发现和测量已经成为研究网络行为学的主要方法，网络行为的测量是整个网络行为学研究的基础。网络行为的建模分析可采用排队论、Petri 网、马尔可夫链、Poisson 过程等理论。由于 Internet 环境的复杂性、多变性、异构性，网络行为的建模分析和仿真分析变得步履维艰。

7）网络测量的体系结构

随着时间的推移，网络测量将不断扩展升级，所以在设计实施之初，就要充分考虑测量体系的可扩展性、可裁剪性及兼容性、容错性。

1.2.3 网络测量工具软件

几个典型的测量工具如表 1.1 所示。

表 1.1 网络测量工具示例

工具名称	所属类型	主要功能	下载地址	服务性质
PingPlotter	主动测量	数据采集和延迟计算	www.pingplotter.com	注册
NetWorx	主动测量	流量测量	www.softperfect.com	免费
WireShark	被动测量	协议数据包分析	www.wireshark.org	免费

1）PingPlotter 工具介绍

PingPlotter 是一款路由跟踪软件，它界面简单，结合了数据与图形两种表达方式，检测分析结果更为直观和易于理解。PingPlotter 是一个多线性的跟踪路由程序，它能最快地揭示当前网络出现的瓶颈与问题。例如，与 Windows 中的 TraceRT 相比，它具有信息同时反馈的速度优势。图 1.6 描述了自本地到达清华大学网站的测量结果。

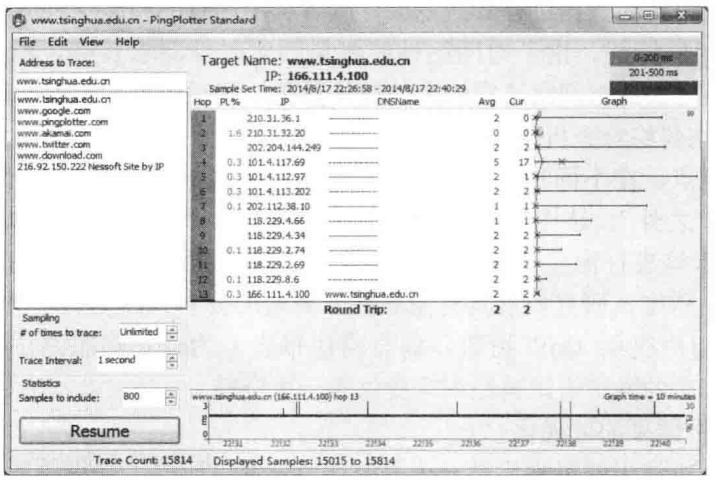
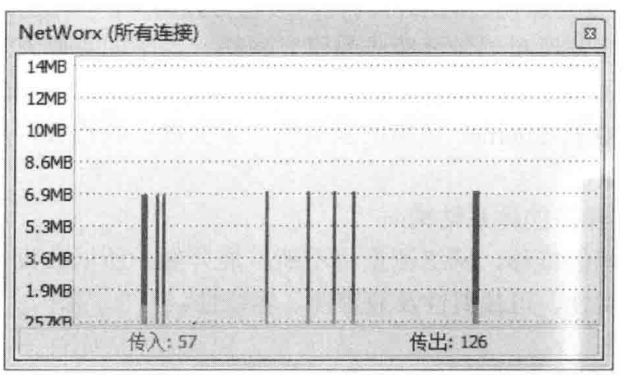


图 1.6　PingPlotter 工具的应用示例

2）流量测量工具 NetWorx 5.3.2 介绍

NetWorx 工具功能较多，包括流量测量、流量统计、速度计算，以及主机和端口扫描、路由追踪等，同时它能够设置流量限制和导出数据。图 1.7 所示是几个典型应用界面。

（a）



（b）

（c）

图 1.7　NetWorx 工具的应用实例