

遵循自顶向下的网络教学思路，简便易搭的自主实验平台

# 计算机网络 及应用实验指示书

程朋 贾庆山 曹军威 编著

清华大学出版社



## 作者简介

程朋，男，博士，清华大学自动化系副教授。1994年获学士学位，2000年获清华大学博士学位并留校任教。2003年至2006年，先后在美国普度大学和威斯康星大学进行访问研究。主要研究方向为复杂系统建模与优化、空中交通管理等。

贾庆山，男，博士，清华大学自动化系副教授。分别于2002年、2006年获得清华大学自动化系学士、博士学位，并留校任教。分别于2006年赴哈佛大学、2010年赴香港科技大学、2013年赴麻省理工学院任访问学者。主要研究方向为离散事件动态系统的仿真与性能优化，及在智能建筑与智能电网中的应用。

曹军威，男，博士，清华大学信息技术研究院研究员、副院长，清华信息科学与技术国家实验室（筹）公共平台与技术部主任。1991年至1998年，清华大学自动化系本科、硕士毕业。2001年英国Warwick大学计算机博士毕业。2002年至2006年先后在德国NEC欧洲实验室和美国MIT/LIGO实验室任Research Scientist。2006年回清华工作至今，主要从事分布式计算和网络系统技术及其在能源电力行业的应用研究。



# 计算机网络 及应用实验指示书

程朋 贾庆山 曹军威 编著

清华大学出版社  
北京

## 内 容 简 介

本书是清华大学自动化系“计算机网络及应用”课程的实验指导书。本书是根据 James F. Kurose 教授和 Keith W. Ross 教授编写的《计算机网络：自顶向下方法》教材设置的实验内容。本书内容涉及基本网络操作命令的使用、常用网络服务的配置、TCP/UDP 等数据包的捕获和分析、Socket 网络通信编程等。

本书适用于计算机科学与技术专业及相关专业的大学本科生和研究生，也可用于教学培训。本书能够帮助读者在实验中进一步理解计算机网络的相关知识，提高读者解决计算机网络相关实际问题的能力。

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

计算机网络及应用实验指示书/程朋,贾庆山,曹军威编著. —北京：清华大学出版社,2017

ISBN 978-7-302-46225-5

I. ①计… II. ①程… ②贾… ③曹… III. ①计算机网络—实验—高等学校—教材 IV. ①TP393

中国版本图书馆 CIP 数据核字(2017)第 019936 号

责任编辑：王一玲

封面设计：常雪影

责任校对：梁毅

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](mailto:c-service@tup.tsinghua.edu.cn)

质量反馈：010-62772015, [zhiliang@tup.tsinghua.edu.cn](mailto:zhiliang@tup.tsinghua.edu.cn)

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

印 装 者：清华大学印刷厂

经 销：全国新华书店

开 本：185mm×230mm 印 张：6

字 数：86 千字

版 次：2017 年 5 月第 1 版

印 次：2017 年 5 月第 1 次印刷

印 数：1~1500

定 价：29.00 元

---

产品编号：062437-01

# 前言

## FOREWORD

### 实验安排说明

结合清华大学自动化系计算机网络课程的教学内容,设计了该实验指导书。实验内容共分为 7 个实验环节,力求使学生通过这些实验加深理解网络基本概念,了解各项网络服务配置原理和方法,进而设计和开发网络通信程序,并通过对需要大量设备投入的实验进行软件模拟,了解网络相关设备的工作原理和实现方法。

### 实验要求

1. 预习实验指导书有关部分,做好实验内容的准备,就实验可能出现的情况提前做出思考。
2. 实验过程中认真进行相关实验和测试,观察出现的问题,记录主要情况,并做出必要说明和分析。
3. 编程实验要求提交源程序、程序设计文档及用户使用说明。
4. 在实验室进行实验,实验结束后,要求全部卸载实验中安装的软件。
5. 认真书写实验报告。实验报告包括主要实验内容,实验情况及其分析,并解答实验思考中的问题。

# 目 录

## CONTENTS

<b>实验一 基本网络操作命令</b>	1
1.1 实验目的	1
1.2 实验环境	1
1.3 实验内容	1
1.4 实验要求	2
1.5 实验思考	2
1.6 附录：网络常用命令	3
<b>实验二 常用网络服务的配置</b>	9
2.1 实验简介	9
2.1.1 实验目的	9
2.1.2 实验内容	9
2.1.3 实验环境	10
2.2 DNS 服务器的设置	10
2.2.1 实验步骤	10
2.2.2 实验思考	10
2.2.3 附录：实验参考资料	10
2.3 用 Apache HTTP Server 开设 WWW 服务	19
2.3.1 实验环境	19
2.3.2 实验步骤	19
2.3.3 实验要求	20

2.3.4 实验思考 .....	21
2.3.5 附录：实验参考资料 .....	22
2.4 架设 FTP 服务器 .....	32
2.4.1 实验环境 .....	32
2.4.2 实验内容 .....	32
2.4.3 实验步骤 .....	32
2.5 DHCP 服务器的配置 .....	37
2.5.1 实验目的 .....	37
2.5.2 实验环境 .....	37
2.5.3 实验内容 .....	37
2.5.4 实验思考 .....	37
2.5.5 附录：实验参考资料 .....	38
<b>实验三 捕获 TCP 数据包 .....</b>	<b>44</b>
3.1 实验目的 .....	44
3.2 实验环境 .....	44
3.3 实验内容 .....	44
3.4 实验报告要求 .....	45
3.5 实验步骤 .....	45
<b>实验四 HTTP 抓包分析 .....</b>	<b>53</b>
4.1 实验目的 .....	53
4.2 实验内容 .....	53
4.3 实验报告要求 .....	53
4.4 实验步骤 .....	54
<b>实验五 DHCP 抓包分析 .....</b>	<b>59</b>
5.1 实验目的 .....	59

5.2 实验环境	59
5.3 实验内容	59
5.4 实验报告要求	60
5.5 实验步骤	60
<b>实验六 DNS 抓包分析</b>	<b>64</b>
6.1 实验目的	64
6.2 实验内容	64
6.3 实验报告要求	64
6.4 实验步骤	65
<b>实验七 Socket 编程实现网络通信</b>	<b>70</b>
7.1 实验目的	70
7.2 实验要求	70
7.3 实验内容	71
7.3.1 邮件发送客户端实验(Simple SMTP)	71
7.3.2 课后完成内容: 带身份验证的 Simple SMTP	73
7.3.3 UDP Ping 实验	73
7.4 注意事项	74
7.5 实验结果	74
7.6 实验思考与分析题	75
7.7 附录: 配置实验环境	76
7.7.1 配置 Java 运行环境	76
7.7.2 在 Eclipse 中开发 Java 程序	76
7.7.3 在 Eclipse 中使用调试器	82
<b>致谢</b>	<b>85</b>



# 基本网络操作命令



## 1.1 实验目的

练习使用网络常用命令,进一步了解网络地址、子网掩码、域名、网关、路由、地址解析、协议和端口等基本概念;通过查看和测试网络状态,发现和解决网络可能存在的问题。

## 1.2 实验环境

安装并配置了 TCP/IP 协议的联网微机,Windows 系列操作系统(主要针对 Windows XP 操作系统,Windows 7 下基本兼容;Win 98、Win Me 等早期操作系统会与附录部分命令略有不同,可参考 Windows 命令帮助)。

## 1.3 实验内容

(1) 练习使用 ipconfig 工具,检测网络配置查看并记录本地微机的 IP (v4) 地址、子网掩码、DNS 服务器地址、默认网关地址,网卡物理地址等;

- (2) 使用 nbtstat 工具, 确定本机和相邻计算机的 netbios 信息;
- (3) 使用 netstat 工具, 查看并记录本机传输层协议统计信息和协议端口;
- (4) 熟悉 arp 命令的基本用法, 了解 IP 地址和物理地址间映射关系, 查看本机、相邻主机或网关的 IP 地址和物理地址的映射关系;
- (5) 练习使用 ping 命令, 测试网络连通性, 要求测试本机、邻居计算机、默认网关、域名服务器、远程网络地址等;
- (6) 练习使用 tracert 命令, 检测到达目的地址 166.111.8.28 所经过的路由器的 IP 地址。

## 1.4 实验要求

- (1) 阅读实验指示书和附录, 掌握常用网络命令及各种参数的使用方法。
- (2) 查看并记录使用命令后信息, 整理实验数据, 分析网络现状和问题。
- (3) 提交实验报告, 报告包含如下内容:
  - ① 实验环境包括网络环境和微机环境;
  - ② 实验内容及主要结果;
  - ③ 回答实验思考中的问题。

## 1.5 实验思考

- (1) 在 Internet 上进行网络通信, 主机必须包含的基本网络配置有哪些? 必须具有哪些地址?
- (2) 在使用 tracert 命令时, 在路由检测的过程中可能会出现“\*”, 是否一定代表路由不可到达? 为什么?
- (3) 分别使用 ping -r 和 tracert 检验到 166.111.8.28 所通过的路径, 分析到达该目标地址的相关路由, 获得的路由信息有何不同? 并画出到达目的地址的路径示意图。

(4) 实验中还出现了哪些你认为不该出现的或不能解释的现象？你是如何分析和理解的？

## 1.6 附录：网络常用命令

### 1. 利用 ipconfig 工具检测网络配置

/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。适配器可以代表物理接口(例如安装的网络适配器)或逻辑接口(例如拨号连接)。
/renew	更新所有适配器的 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可用。
/release	发送 DHCPRELEASE 消息到 DHCP 服务器, 以释放所有适配器当前 DHCP 配置并丢弃 IP 地址配置。
/flushdns	清理并重设 DNS 客户解析器缓存的内容。
/displaydns	显示 DNS 客户解析器缓存的内容。
/registerdns	初始化计算机上配置的 DNS 名称和 IP 地址的手工动态注册。
/showclassid	显示指定适配器的 DHCP 类别 ID。
/setclassid <i>Adapter</i> [ClassID]	配置特定适配器的 DHCP 类别 ID。
/?	在命令提示符显示帮助。

### 2. 利用 nbtstat 工具查看 NetBios 使用情况

-n	命令查看客户机所注册的 netbios 名称。
-c	显示本机 netbios 缓存信息。
-r	显示本机 netbios 统计信息。
-a	用来显示远程主机的 netbios 信息, 并能获远程主机的 MAC 地址。

### 3. 利用 netstat 工具查看协议统计信息

- a 显示所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口。
- e 显示以太网统计信息,如发送和接收的字节数、数据包数。
- n 显示活动的 TCP 连接。
- o 显示活动的 TCP 连接并包括每个连接的进程 ID (PID)。
- p *Protocol* 显示 *Protocol* 所指定的协议的连接。在这种情况下, *Protocol* 可以是 tcp、udp、tcpv6 或 udpv6。
- s 按协议显示统计信息。默认情况下,显示 TCP、UDP、ICMP 和 IP 协议的统计信息。
- r 显示 IP 路由表的内容。该参数与 route print 命令等价。

### 4. 利用 ping 工具检测网络连通性

ping 命令通过向计算机发送 ICMP 回应报文并且监听回应报文的返回,以校验与远程计算机或本地计算机的连接。只有在安装 TCP/IP 协议之后才能使用该命令。对于每个发送报文, ping 最多等待 1 秒,并打印发送和接收报文的数量。比较每个接收报文和发送报文,以校验其有效性。默认情况下,发送四个回应报文,每个报文包含 64 字节的数据(周期性的大写字母序列)。

通常在使用 ping 命令时,可以按照如下顺序测试网络连通性:

- |                |                        |
|----------------|------------------------|
| ping 127.0.0.1 | 检查本机的 TCP/IP 协议安装是否正确。 |
| ping 本机 IP     | 检测本机的服务和网络适配器绑定是否正确。   |
| ping 网关 IP     | 检测本机和网关连接是否正常。         |
| ping 远程主机 IP   | 检测网关是否能转发数据包。          |
| ping 某域名       | 检测 DNS 服务器是否能正常解释。     |

**注意:** Reply from 127.0.0.1: bytes=32 time<10ms TTL=128 通信正常。

Destination host unreachable 目标主机不可到达。

Request timed out

请求超时。

ping 命令的具体使用如下所示：

```
ping [ -t ] [ -a ] [ -n count ] [ -l length ] [ -f ] [ -i ttl ] [ -v tos ] [ -r count ] [ -s count ]
[ -j computer-list ] | [ -k computer-list ] [ -w timeout ] destination-list
```

- t 校验与指定计算机的连接,直到用户中断。
- a 将地址解析为计算机名。
- n count 发送由 count 指定数量的 ECHO 报文,默认值为 4。
- l length 发送包含由 length 指定数据长度的 ECHO 报文。默认值为 64 字节,最大值为 8192 字节。
- f 在包中发送“不分段”标志。该包将不被路上的网关分段。
- i ttl 将“生存时间”字段设置为 ttl 指定的数值。
- v tos 将“服务类型”字段设置为 tos 指定的数值。
- r count 在“记录路由”字段中记录发出报文和返回报文的路由。指定的 count 值最小可以是 1,最大可以是 9。
- s count 指定由 count 指定的转发次数的时间戳。
- j computer-list 经过由 computer-list 指定的计算机列表的路由报文。中间网关可能分隔连续的计算机(松散的源路由)。允许的最大 IP 地址数目是 9。
- k computer-list 经过由 computer-list 指定的计算机列表的路由报文。中间网关可能分隔连续的计算机(严格源路由)。允许的最大 IP 地址数目是 9。
- w timeout 以毫秒为单位指定超时间隔。
- destination-list 指定要校验连接的远程计算机。

## 5. 利用使用 tracert 命令跟踪路径

tracert *host\_name* 或者输入 tracert *ip\_address*

其中 *host\_name* 或 *ip\_address* 分别是远程计算机的主机名或 IP 地址。

例如,要跟踪从该计算机到 www. microsoft. com 的连接路由,请在命令提示行输入:

```
tracert www.sina.com
```

如果不希望 tracert 命令解析和显示路径中所有路由器的名称,请使用-d 参数。这会加速路径的显示。例如,要跟踪从该计算机到 www.microsoft.com 的路径而不显示路由器名称,请在命令提示符处输入下列内容:

```
tracert -d www.sina.com
```

利用“tracert 目的地地址”命令来检测到达目的地址所经过的路由器的 IP 地址。使用 Tracert 166.111.8.28,显示的结果为如下形式:

```
C:\Documents and Settings\Yangqing> tracert 166.111.8.28
Tracing route to dns - a.tsinghua.edu.cn [166.111.8.28]
over a maximum of 30 hops:
 1  < 1 ms    < 1 ms    < 1 ms 219.224.144.1
 2  3 ms      1 ms      1 ms 219.224.130.13
 3  < 1 ms    < 1 ms    < 1 ms 219.224.96.73
 4  < 1 ms    < 1 ms    < 1 ms 219.224.98.6
 5  < 1 ms    < 1 ms    < 1 ms dns - a.tsinghua.edu.cn [166.111.8.28]
Trace complete.
```

**6. 利用 ARP 命令显示和修改“地址解析协议(ARP)”缓存中的项目**  
可使用 arp/? 在命令提示符下显示帮助。

(1) 什么是 ARP 和 ARP cache

ARP (Address Resolution Protocol) 是个地址解析协议。在 TCP/IP 协议中,当 A 要给 B 发 IP 包时,需要填写 B 的 IP 为目地地址,但这个包含 IP 地址的包在以太网上传输时,还需要进行一次以太包的封装,在这个以太包中,目地地址为 B 的 MAC 地址。ARP 作用就是根据 B 的 IP 地址去获取其 MAC 地址。当 A 得到 B 的 MAC 地址后,会将 B 的 IP 地址和 MAC 地址一起存储在本机,以备下次使用。ARP cache 是个用来储存(IP, MAC)地址的缓冲区。当 ARP 被询问一个已知 IP 地址节点的 MAC 地址时,先在 ARP cache 查看,若存在,就直接返回 MAC 地址,若不存在,才发送 ARP request 向局域网查询。

## (2) 显示 cache 中的 ARP 表

显示高速 cache 中的 ARP 表可以使用 arp -a 命令,因为 ARP 表在没有手工配置之前,通常为动态 ARP 表项,因此,表项的变动较大,arp -a 命令输出的结果也不大相同。如果高速 cache 中的 ARP 表项为空,则 arp -a 命令输出结果为 No ARP Entries Found;如果 ARP 表中存在 IP 地址与 MAC 地址的映射关系,则 arp -a 命令显示该映射关系。

## (3) 添加 ARP 静态表项

存储在高速 cache 中的 ARP 表,既可以动态表项,也可以有静态表项。通过 arp -s inet\_addr eth\_addr 命令,也可以将 IP 地址与 MAC 地址的映射关系手工添加到 ARP 表中。其中,inet\_addr 为 IP 地址,eth\_addr 为与其相对应的 MAC 地址。通过 arp -s 命令加入的表项是静态表项,所以,系统不会自动将它从 ARP 表中删除,直到人为删除或关机。需要注意:在人为增加 ARP 表项时一定要确保 IP 地址与 MAC 地址的对应关系是正确的,否则将导致发送失败。

## (4) 删除 ARP 表项

无论是动态表项还是静态表项,都可以通过 arp -d inet\_addr 命令删除,其中 inet\_addr 为该表项的 IP 地址。如果要删除 ARP 表中的所有表项,也可以使用“\*”来代替具体的 IP 地址。

## 7. 域名解析命令 nslookup: 可用来诊断域名系统(DNS)基础结构的信息

例如:

```
C:\Documents and Settings\Automation> nslookup
Default Server: dns.au.tsinghua.edu.cn
Address: 166.111.72.2
> 输入要解析的域名或 ip 地址
```

## 8. 网络信使(在 Windows 7 和 Vista 系统中已经不提供信使服务,但提供了一个 msg 功能)

XP 用户:

net send {name/ \* /  
domain[:name] | /  
users} message

其中, name 为要接收发送消息的用户名、计算机名或通信名; \* 为将消息发送到组中所有名称; /domain [:name] 为将消息发送到计算机域中的所有名称; /users 为将消息发送到与服务器连接的所有用户; message 作为消息发送的文本

net stop messenger  
net start messenger

停止信使服务, 也可以在控制面板—服务修改  
开始信使服务

Win7 或 Vista 用户:

MSG username

示例: 给计算机名为 Tom 的用户发信息, msg Tom See you  
at 1PM today

## 9. 几个 net 命令

- (1) 显示当前工作组服务器列表 net view。
- (2) 查看计算机上的用户账号列表 net user。
- (3) 查看网络链接 net use, 记录链接 net session, 例如 C:\> net session。

## 常用网络服务的配置

### 2.1 实验简介

#### 2.1.1 实验目的

通过实验熟悉常用网络服务的基本原理和基于客户机/服务器的服务模式,掌握各项服务的服务原理,练习常用网络服务的配置方法。

#### 2.1.2 实验内容

- (1) 在 Windows 环境练习下配置 DNS 服务,理解域名服务的解析原理和层次关系及相关概念。
- (2) 在 Windows 环境中用 Apache HTTP Server 开设 WWW 服务,安装配置 PHP 动态网页编辑环境。
- (3) 利用 SERV-U 实现 ftp 服务,并针对不同用户、地址或端口进行授权访问。
- (4) 掌握 DHCP 服务器的安装与设置,了解 DHCP 的含义及工作原理,了解 DHCP 客户机的设置。

### 2.1.3 实验环境

在以太网环境中,安装 Windows Server 2003 操作系统的联网微机一台,既作为服务器也作为客户机。多台联网微机环境中,可分别指定服务器和客户机进行测试。

## 2.2 DNS 服务器的设置

### 2.2.1 实验步骤

- (1) 安装 DNS 服务器
- (2) 配置新的 DNS 服务器
- (3) 添加资源记录
- (4) 设置 DNS 的属性
- (5) 设置 DNS 客户机与测试

### 2.2.2 实验思考

- (1) 存储在 DNS 数据库中的数据是静态的还是动态的? 如何更新?
- (2) 在创建的 DNS 中添加了正向搜索的主机记录,为什么还要添加反向搜索记录?
- (3) 在上级域名服务器中修改某域名对应的 IP 地址且配置正确,在客户端测试中发现没有生效,为什么?
- (4) 实验中只给出了添加主机记录的部分,如果在该域中要添加一个下级子域,如何操作?

### 2.2.3 附录: 实验参考资料

#### DNS 概述

DNS 是域名系统 (Domain Name System) 的缩写, 是一种组织成域层次结构的计算机和网络服务命名系统。DNS 命名用于 TCP/IP 网络, 如 Internet, 用来通过用户友好的名称定位计算机和服务。当用户在应用程序中输入 DNS 名称时, DNS 服务可以将此名称解析为与此名称相关的其他信息, 如 IP 地址。

所以, 如果想要建立内部网上的域名解析功能 (即翻译成 IP 地址), 就需要建立一个 DNS 服务器, 里面包含有域名和 IP 地址之间的映射关系。域名配置常用到的名词如下:

### (1) 区域

创建一个 DNS 服务器, 除了必须运行 DNS 服务的计算机外, 还需要建立一个新的区域即一个数据库才能正常运作。该数据库的功能是提供 DNS 名称和相关数据 (如 IP 地址或网络服务) 间的映射, 该数据库中存储了所有的域名与对应 IP 地址的信息, 网络客户机正是通过该数据库的信息来完成从计算机名到 IP 地址的转换。可以配置以下三种类型的区域。

Active Directory 集成的区域: Active Directory 集成的区域是一个新区域的主拷贝, 该区域用活动目录来存储和复制区域文件。

标准主要区域: 标准主要区域是一个新区域的主拷贝, 存放在一个标准文本文件中, 用户可以在创建该区域的计算机上管理和维护一个主控区域。默认区域类型为“标准主要区域”。

标准辅助区域: 标准辅助区域是一个现有区域的副本, 是只读的, 也存放在一个标准文本文件中。标准辅助区域帮助主服务器平衡处理的工作量, 并提供容错。

### (2) 资源记录

每个区域都拥有一组结构化的资源记录 (Resource Record, RR), 资源记录是区域数据库文件中的条目。常用的资源记录有以下几种。

A(Address, 主机地址): 用于将主机名映射到该主机名的 IP 地址。

CNAME(Canonical Name, 规范名称): 用于将主机别名映射为规范主

机名。

MX(Mail eXchange,邮件交换器): 用于将邮件服务器别名映射为规范主机名。

NS(Name Server,名称服务器): 用于指派域中权威 DNS 服务器的主机名。

SOA(Start Of Authority,起始授权机构): 为存储在区域中的信息指明授权机构的起点或初始点的记录。

PTR(PoinTeR,指针): 在 in-addr. arpa 域中创建的用于反向搜索区域中的资源记录,用来指定主机 IP 地址到主机 DNS 域名的反向映射。

### 1. 安装 DNS 服务器

添加 DNS 服务器之前必须首先安装 DNS 服务,方法如下:

(1) 选择“开始”→“设置”→“控制面板”→“添加/删除程序”,在“组件”列表中选中“网络服务”。

(2) 单击“详细信息”,选中“域名系统(DNS)”,如图 2.1 所示。

DNS 服务安装结束之后,在控制面板的“管理工具”中将出现 DNS 命令项。

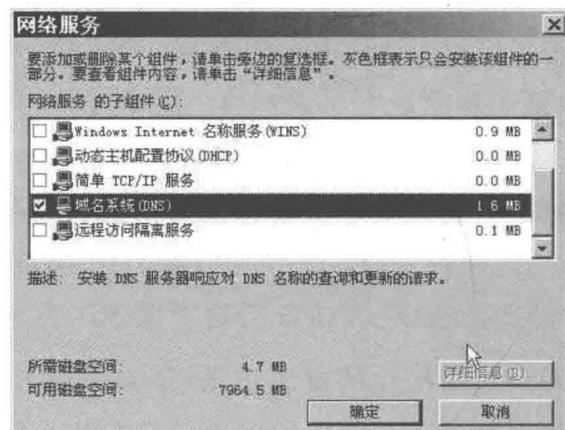


图 2.1 “网络服务”对话框

## 2. 配置新的 DNS 服务器

- (1) 选择“开始”→“程序”→“管理工具”→DNS，打开 DNS 控制台窗口。
- (2) 右击需要配置的 DNS 服务器，选择“配置 DNS 服务器”命令，如图 2.2 所示，打开“配置 DNS 服务器向导(欢迎)”对话框。

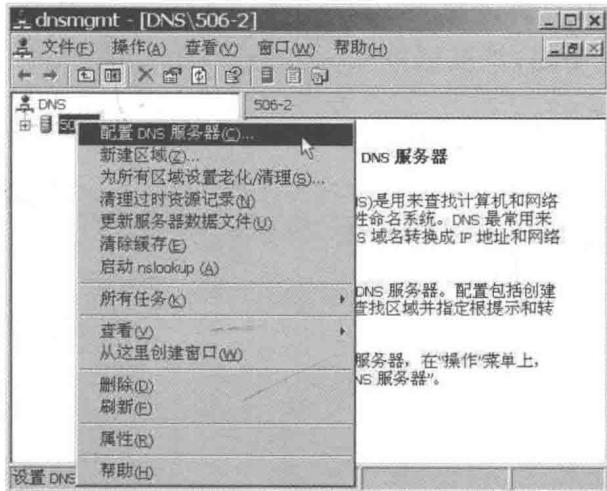


图 2.2 DNS 控制台窗口

- (3) 单击“下一步”按钮，打开“配置 DNS 服务器向导—正向搜索区域”对话框，如图 2.3 所示。

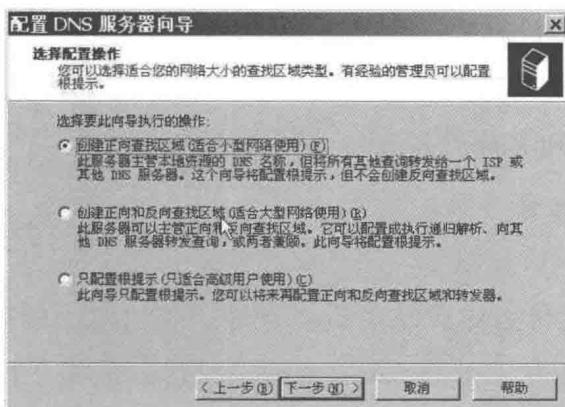


图 2.3 “配置 DNS 服务器向导—正向搜索区域”对话框

(4) 选择创建正向搜索区域或反向搜索区域：如果希望把域名映射到 IP 地址(常用于实现对服务器的访问)，应选定“正向搜索”单选按钮；如果希望把机器的 IP 地址映射到用户好记的域名(通过 IP 查询 DNS 名称)，应选定“反向搜索”单选按钮。

(5) 指定区域数据库文件，如图 2.4 所示。区域文件即区域数据库文件，其主名与区域名称相同，扩展名默认为.dns。

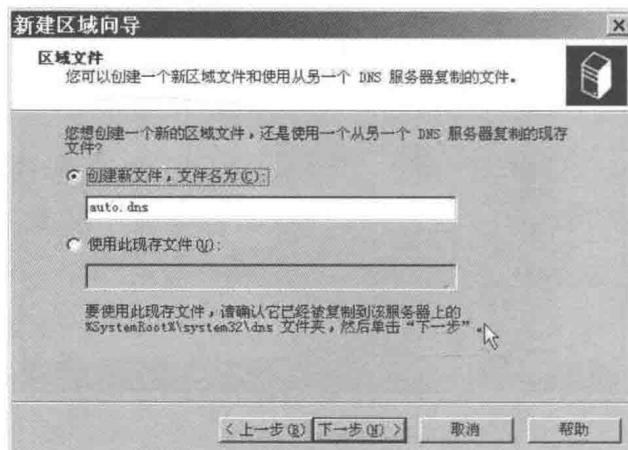


图 2.4 “区域文件”对话框

(6) 单击“下一步”按钮，打开“新建区域向导—完成”对话框，确认输入信息无误，单击“完成”按钮完成配置。

当创建一个区域时，DNS 会自动添加两个资源记录(如图 2.5 所示)：起始授权机构(SOA)和名称服务器(NS)。

### 3. 添加资源记录

#### (1) 添加主机(A)资源记录

创建区域后，就可以向区域中添加各种资源记录。例如：建立 IP 地址为 192.168.0.51，域名为 asp.gjy.com 资源记录的方法如下：

① 在 DNS 管理控制台的控制台树中，单击选择要添加资源记录的正向搜索区域，选择操作菜单的“新建主机”命令，打开“新建主机”对话框。

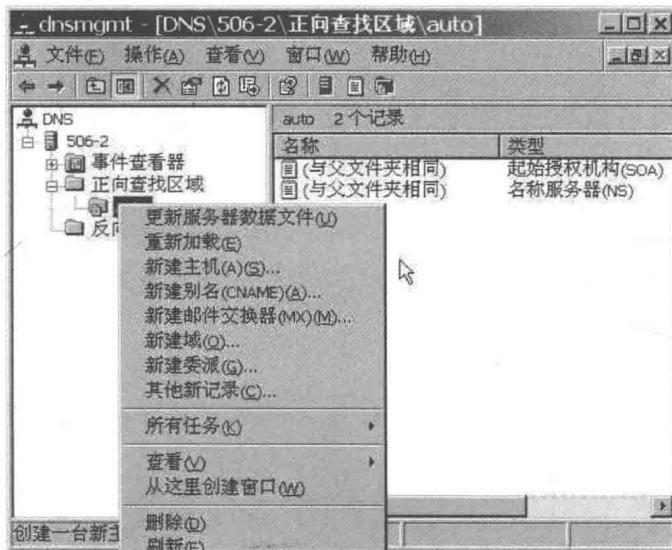


图 2.5 DNS 管理控制台

② 在“名称”文本框中,输入新主机的 DNS 计算机名称 test; 在“IP 地址”文本框中,输入新主机的 IP 地址 192.168.0.10; 如果选中“创建相关的指针(PTR)记录”复选框,可以根据在“名称”和“IP 地址”中输入的信息在此主机的反向区域中创建附加的指针记录。单击“添加主机”按钮,添加新主机记录,如图 2.6 所示。

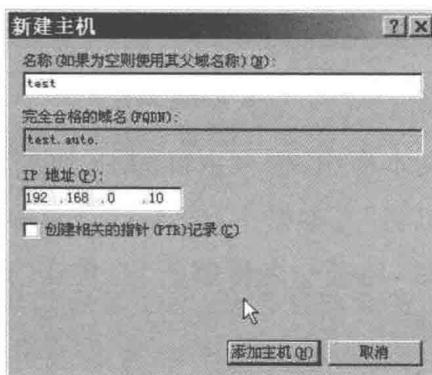


图 2.6 新建主机

## (2) 添加反向资源记录

添加了正向搜索的主机记录后,还可以添加反向搜索记录。因为通过前面的设置,客户机可以知道主机 test. auto 的 IP 地址是 192.168.0.10,但不知道 192.168.0.10 对应的域名是什么,所以还要在反向区域添加指针资源记录。操作如下:

① 在 DNS 控制台窗口中,右击某一反向搜索区域,选择“新建指针”命令,如图 2.7 所示。

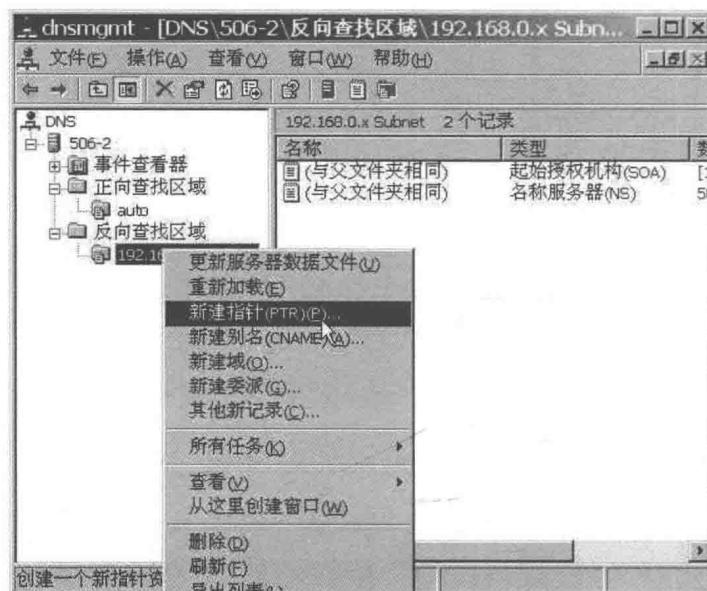


图 2.7 DNS 管理控制台窗口

② 在“主机 IP 号”文本框中,输入主机的 IP 地址,如图 2.8 所示。

③ 在图 2.8 的“主机名”文本框中,输入 DNS 主机的域名,该计算机使用此指针记录提供反向搜索(地址一名称解析)。单击“确定”按钮,可看到该区域中添加的新的主机记录。

## 4. 设置 DNS 的属性

在 DNS 控制台窗口的左窗格中选定服务器,选择操作菜单中的“属性”命令,打开该服务器的属性对话框。

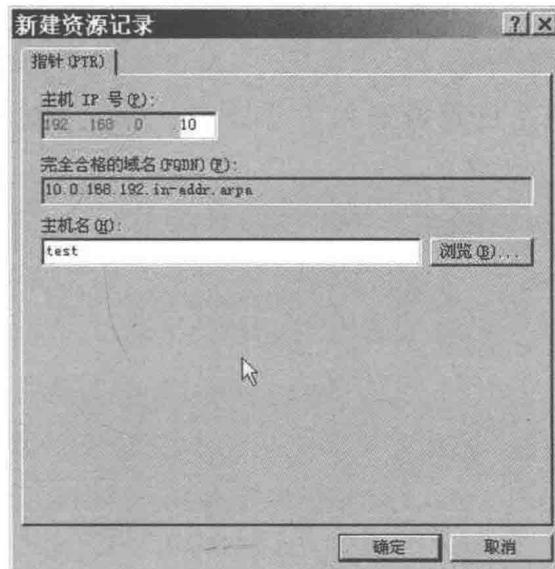


图 2.8 “新建资源记录”对话框

### (1) “接口”选项卡

在“接口”选项卡中选择对 DNS 请求进行服务的 IP 地址：有“侦听所有 IP 地址”和“只侦听指定的 IP 地址”两种侦听方式。

### (2) “监视”选项卡

在“监视”选项卡，选中“对此 DNS 服务器的简单查询”或者“对此 DNS 服务器的递归查询”复选框，可以单击“立即测试”来测试 DNS 服务器。

“简单查询”使用服务器计算机上的 DNS 客户机来查询本机 DNS 服务器，是本地测试；“递归查询”通过将查询转发给另一个 DNS 服务器来查询本机 DNS 服务器，是递归查询测试。

### (3) “日志”选项卡

在“日志”选项卡中可以设置 DNS 服务日志记录选项，从而对 DNS 服务的活动进行记录。日志文件通常为 %SystemRoot%\System32\DNS\DNS.log。

## 5. 设置 DNS 客户机与测试

### (1) 设置 DNS 客户端

首先确定客户机上已正确安装了 TCP/IP, 然后通过设置 TCP/IP 属性来配置 DNS 客户机。方法如下：

① 对于 Windows XP 客户机, 在“网络和拨号连接”窗口中, 右击“本地连接”→“属性”, 打开“本地连接属性”对话框, 双击“Internet 协议(TCP/IP)”, 打开“Internet 协议(TCP/IP)属性”对话框。

② 在“Internet 协议(TCP/IP)属性”对话框中可以选择“自动获得 DNS 地址”单选按钮配置自动获取 DNS 地址(由 DHCP 服务器提供), 或在“首选 DNS 服务器”文本框输入 DNS 服务器以及备用的 DNS 服务器的 IP 地址, 如图 2.9 所示。

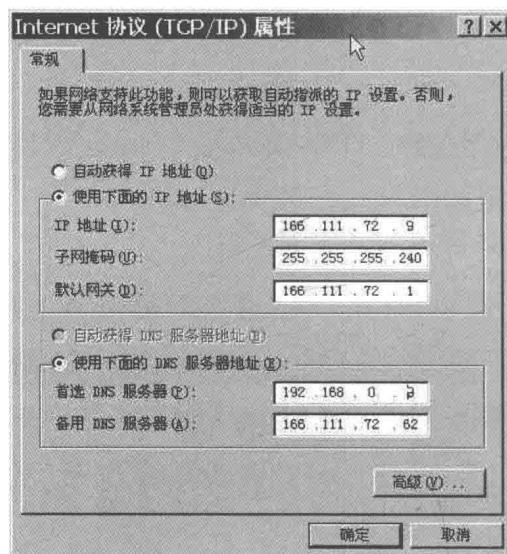


图 2.9 “Internet 协议(TCP/IP)属性”对话框

### (2) 测试 DNS

nslookup 命令行实用程序是 DNS 服务的主要诊断工具, 它提供了执行 DNS 服务器查询测试并获取详细响应作为命令输出的能力。使用 nslookup

可以诊断和解决名称解析问题、检查资源记录是否在区域中正确添加或更新,以及排除其他服务器相关问题,如图 2.10 所示,能够正确解析 test. auto 为 192.168.0.10。



图 2.10 域名测试

## 2.3 用 Apache HTTP Server 开设 WWW 服务

### 2.3.1 实验环境

操作系统: 几乎任意 Windows 版本。本实验是在 Windows XP 下实现的。

所需软件:

- (1) Apache HTTP Server1.3.33(版本可以不同)安装程序。
- (2) PHP4 安装包; php-4.4.6-Win32.zip。

### 2.3.2 实验步骤

- (1) Apache 服务器安装与配置,了解配置 Web 服务。
- (2) PHP 安装与配置。
- (3) 使用 PHP 完成网页计数器和动态显示图片功能。

### 2.3.3 实验要求

实验前：

(1) 准备好一个简单的主页 index. html 文件, (请采用这个文件名, 这是 Apache 默认的主页文件名), 测试 Apache Server 的服务是否正常。

(2) 准备好一个简单的 php 文件, 测试 php 环境是否运行正常。

例如：

test. php 文件, 文件内容如下：

```
<html>
  <body>
    <?
      phpinfo();
    ?>
  </body>
</html>
```

(3) 填写 visitorcounter. php 文件中网页计数器和动态显示图片代码中缺失的部分。

visitorcounter. php 代码如下：

```
<?php
$c_file = "counter.txt"; //文件名赋值给变量
if(!file_exists($c_file)) //如果文件不存在的操作
{
  $myfile = fopen($c_file, "w"); //创建文件
  fwrite($myfile, "0"); //置入"0"
  fclose($myfile); //关闭文件
}
$t_num = file($c_file); //把文件内容读入变量
echo "欢迎!";

//必做 1: 在下面添加代码统计访客数量

//必做 1 结束

echo "您是本站第". $t_num[0]. "位访客!"; //显示文件内容
```

```
//必做 2: 在下面空白处添加代码实现动态显示图片功能
//要求首次访问和非首次访问显示不同图片
//先准备两张图片保存在 htdocs 文件夹下, 或者新建文件夹保存

if( $t_num[0] != 1 )
    //在这里添加代码显示图片 1
else
    //在这里添加显示图片 2

//必做 2 结束

$c_file = fopen( $c_file, "w" );
fwrite( $myfile, $t_num[0] );
fclose( $myfile ); //关闭文件

//选作: 其他你想实现的功能, 比如表单收集、日期显示等

//选作结束
?>
```

实验后：

- (1) 实验完成后停掉 apache http server 在控制面板添加删除程序中卸载 Apache。
- (2) 删除 apache 的安装文件夹。
- (3) 从 Windows 系统目录中删除 php.ini。
- (4) 删除 php 的安装文件夹。
- (5) 删除 wdb 的安装文件夹和自己定义的文件夹。

#### 2.3.4 实验思考

- (1) 在 Apache Group\Apache\conf\httpd.conf 文件中, 了解其他选项, 比如, 如何修改服务器 IP 地址和端口, 默认首页文件名, 如何设置虚拟目录等。

- (2) 比较使用 Windows 网络组件 IIS 开设 Web 服务和 Apache 开设 Web

服务各自的优劣。

(3) 论坛实验中,没有涉及后台数据库。如果后台为 Access 数据库,如何使用 PHP 建立和数据库的连接?

(4) 了解 PHP 语言的使用以及除论坛外的其他应用。

### 2.3.5 附录: 实验参考资料

#### 1. Apache 服务器安装与配置

Apache 是世界排名第一的 Web 服务器,根据 Netcraft([www.netcraft.co.uk](http://www.netcraft.co.uk))所作的调查,世界上 50% 以上的 Web 服务器在使用 Apache。

1995 年 4 月,最早的 Apache(0.6.2 版)由 Apache Group 公布发行。Apache Group 是一个完全通过 Internet 进行运作的非盈利机构,由它来决定 Apache Web 服务器的标准发行版中应该包含哪些内容。准许任何人修改隐含错误,提供新的特征和将它移植到新的平台上,以及其他的工作。当新的代码被提交给 Apache Group 时,该团体审核它的具体内容,进行测试,如果认为满意,该代码就会被集成到 Apache 的主要发行版中。

Apache 的特性:

- (1) 几乎可以运行在所有的计算机平台上。
- (2) 支持最新的 HTTP 1.1 协议。
- (3) 简单而且强有力的基于文件的配置(HTTPD.CONF)。
- (4) 支持通用网关接口(CGI)。
- (5) 支持虚拟主机。
- (6) 支持 HTTP 认证。
- (7) 集成 PERL。
- (8) 集成的代理服务器。
- (9) 可以通过 Web 浏览器监视服务器的状态,可以自定义日志。
- (10) 支持服务器端包含命令(SSI)。
- (11) 支持安全 SOCKET 层(SSL)。

- (12) 具有用户会话过程的跟踪能力。
- (13) 支持 FASTCGI。
- (14) 支持 JAVA SERVLETS。

缺点是 Apache 没有为管理员提供图形用户接口 (GUI), 但最近的 Apache 版本已经有了 GUI 的支持。

很多的 Web 站点都用这种方式开设服务。

### 获取 Apache

可以直接从 Apache 的网站 (<http://www.apache.org>) 上下载 Apache 软件的 Windows 版本。在 Linux 或者其他 UNIX 下可以找到相应的二进制安装文件, 或者直接下载源代码包进行编译安装。

现在网络上能找到两类版本的 Apache 软件, 版本号分别为 Apache1.3.xx 和 Apache2.0.xx, 前者是从原来的 Apache 版本慢慢发展演变过来的, 现在新出的版本大多是对原来版本的 Bug 修改, 因此是比较完善, 几乎很难发现漏洞的版本。出于以上考虑, 选择 Apache1.3.xx 版本的 Apache HTTP Server 比较合适。

### Apache 安装

下面以 Apache HTTP Server1.3.33 为例简要讲述 Apache 的安装过程。

Apache 的安装和其他 Windows 软件安装方法并没有太大的不同, 直接按照提示一步一步往下进行即可, 如图 2.11~图 2.17 所示。

需要注意的是 Server Information 这一步, 有一个运行方式的选项。

(1) 作为一个 Windows 的 Service 来运行, 这种方式下用户无须登录 Windows, 启动 Apache 软件即可将 HTTP Server 作为默认启动的服务运行, 这个对于想长期开设 Http 服务的用户来讲是必需的。

(2) 手动启动方式。可能你没有那么大的权限, 或者你只是想在机器上测试网页, 而不是希望对外长期开始 Http 服务, 那么可以选择手动启动的方式。这个实验中, 应该选择手动启动方式。

选择安装的目录之后就可以开始安装了。

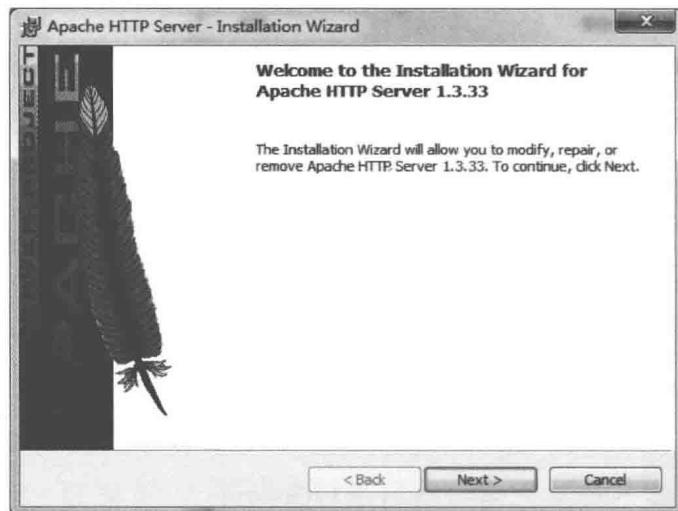


图 2.11 安装界面欢迎页

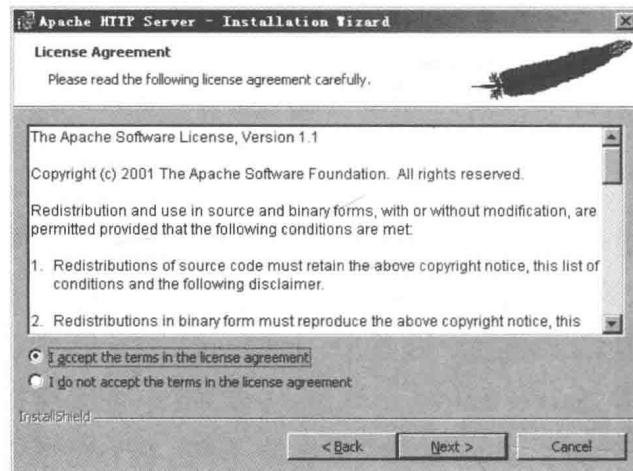


图 2.12 安装界面用户许可页

安装完成之后从程序菜单选择 Apache HTTP Server/Start Apache in console 或者在 Apache Group\Apache 目录下双击打开 Apache.exe, 就会弹出一个控制台窗口(见图 2.16), 显示 Apache/1.3.33(Win32)running, 表示 Apache 已经在后台运行了。

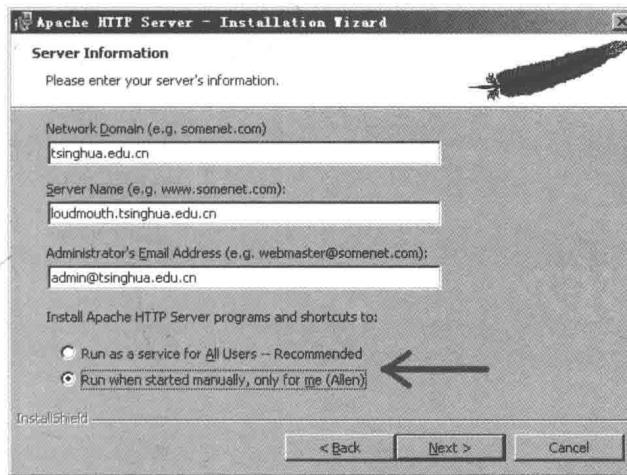


图 2.13 安装界面服务器信息填写页

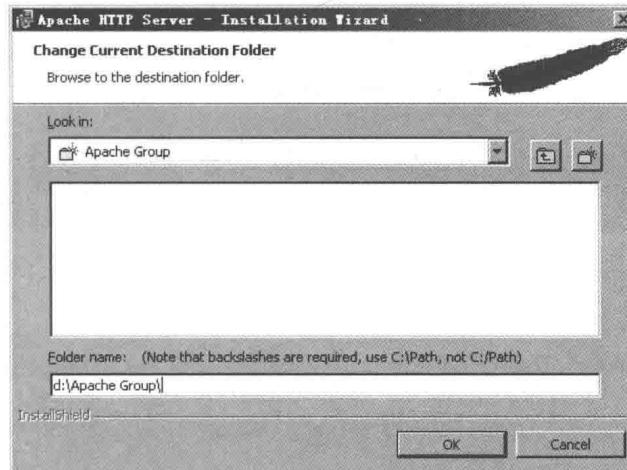


图 2.14 安装目录位置选择

打开浏览器，在地址栏中输入 `http://localhost`，应该就能看到 Apache 的默认 Web 页面了（见图 2.17），这说明 Apache 已经安装成功了。

发布自己的网页有两种方法：

- (1) 把自己的网页放到 `Apache Group\Apache\htdocs\` 目录下面。
- (2) 打开 `Apache Group\Apache\conf\httpd.conf`，文件即可找到。

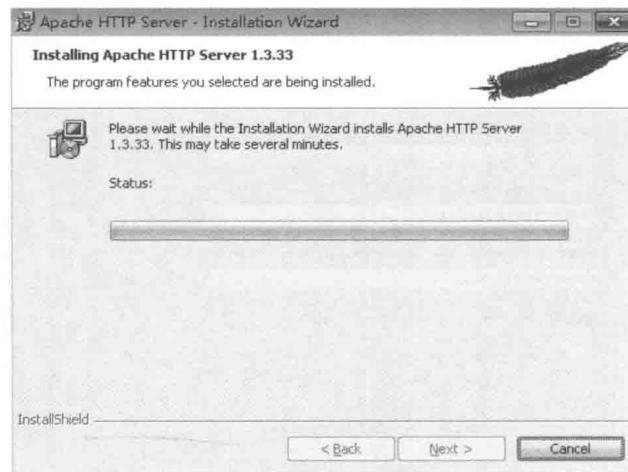


图 2.15 安装状态显示

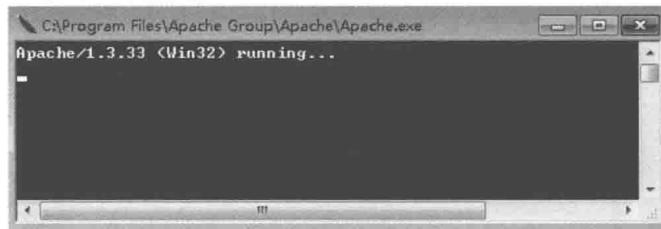


图 2.16 控制台窗口

DocumentRoot 一项把自己网页的存放目录写入。例如：如果把自己的 index.html 放在 d:\myweb 下面就写入 DocumentRoot "d:/myweb"。

至此，网页发布过程已经完成。

## 2. PHP 的安装与配置

PHP 是一个巢状的缩写名称，全称为“PHP：Hypertext Preprocessor.”。

从 PHP 的全称可以看出，仍包含 PHP，即“打开缩写还是缩写”。PHP 是一种 HTML 内嵌式的语言（类似 IIS 上的 ASP）。而 PHP 独特的语法混合了 C、Java、Perl 以及 PHP 式的新语法。它可以比 CGI 或者 Perl 更快速地执行动态网页。PHP 最初由 Rasmus Lerdorf 在 1994 年开始计划发展。在 1995 年

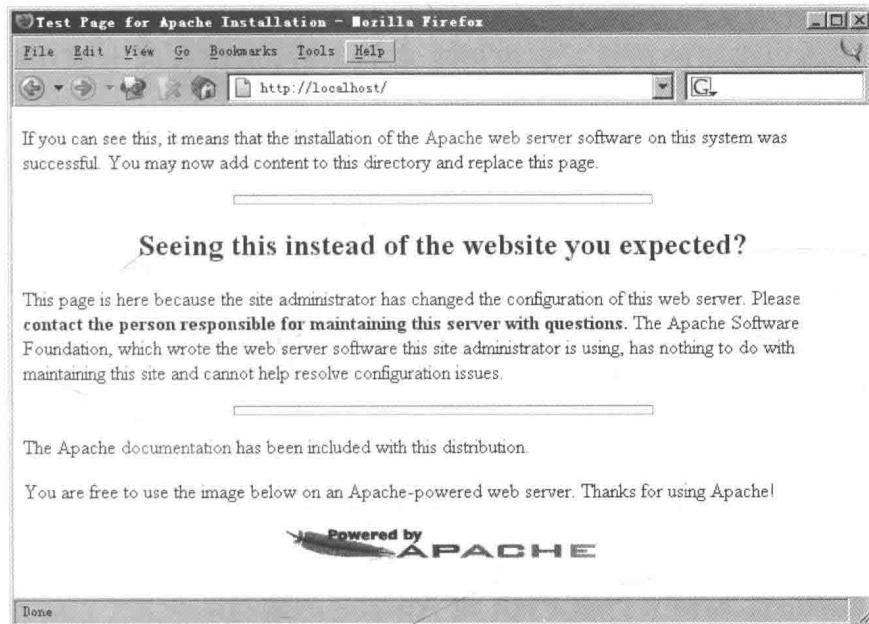


图 2.17 Apache 默认 Web 页面

以 Personal Home Page Tools (PHP Tools) 开始对外发表第一个版本。在这早期的版本中, 提供了访客留言本、访客计数器等简单的功能。随后在新的成员加入开发行列之后, 在 1995 年中, 第二版的 PHP 问世。第二版定名为 PHP/FI (Form Interpreter)。由于 PHP/FI 支持 MySQL 技术, 因而 PHP/FI 奠定了 PHP 在动态网页开发上的影响力。在 1996 年年底, 有 15000 个 Web 站台使用 PHP/FI; 在 1997 年年中, 使用 PHP/FI 的 Web 站台成长到超过 5 万个。而在 1997 年年中, 开始了第三版的开发计划, 开发小组加入了 Zeev Suraski 及 Andi Gutmans, 而第三版就定名为 PHP3。

PHP3 跟 Apache 服务器紧密结合, Apache 对于 PHP 的解析, 就是通过众多 Module 中的 php Module 来完成的; 由于 PHP 不断的更新及加入新的功能, 并且它几乎支持所有主流与非主流数据库; 同时 PHP 的执行效率高, 因而 PHP 在 1999 年年中的使用站台超过了 15 万! 它的原代码完全公开, 在 Open Source 意识抬头的今天, 它更是这方面的中流砥柱。不断地有新的函

数库加入,以及不停地更新的活力,使得 PHP 无论在 UNIX 或是 Win32 的平台上都可以有更多新的功能。它提供丰富的函数,从而有利于程序的设计及开发。

PHP 的第四代 Zend 核心引擎已经进入测试阶段。整个脚本程序的核心大幅变动,让程序的执行速度满足更快的要求。在优化之后的效率,已较传统 CGI 或者 ASP 等程序有更好的表现。而且还有更强的新功能、更丰富的函数库。PHP 将在 Web CGI 的领域上,掀起颠覆性的革命。对于一位专业的 Web Master 而言,它也是必修课程之一。

### 获取 PHP4

PHP 的官方网站是 <http://www.php.net>,可以在这个网站上直接获取,或者在教育网的各大 ftp 上直接下载一个 Win32 版的 PHP4。下面以 php-4.4.6-Win32 为例来讲解 PHP 与 Apache 的紧密结合。

### PHP 配置

网上得到的 php-4.4.6-Win32 是一个 zip 压缩包,直接将其解压缩就可以不必运行安装程序,为了设置方便,可以在 D:\根目录下面新建一个 php 文件夹,将解压缩得到的文件复制到 php 文件夹下即可。

为了让 php 能够正常工作,还需要作一些配置工作。这些工作都可以在 php 目录下面的 install.txt 找到,在这里,只介绍 php 与 Apache 相互配合使用时的配置情况。

#### (1) 复制配置文件

php 目录下面的 php.ini-dist 文件复制到 Windows 系统目录下面,一般来讲是 C:\WINDOWS(Win95/98/XP)或者 C:\WINNT(Win2000)目录,如果在安装 Windows 时使用了其他目录,那么就为你设置的那个目录。复制之后将文件名改为 php.ini。

#### (2) 编辑 php.ini,使用文本编辑工具(记事本/UltraEdit 等)打开。

找到 extension\_dir 项,将其修改为 php 目录的 extensions 文件夹,如

```
extension_dir = "d:\php\extensions"
```

找到 doc\_root 项,将其修改为 Apache 软件目录下的 htdocs 目录,这个目录是 Apache 默认的 Web 网页存放目录,如,

```
doc_root = "d:\Apache Group\Apache\htdocs"
```

找到 register\_globals 项,将其从 Off 改为 On,这个开关能够允许服务器从 url 中传递并得到变量(get 方式),具体格式为 `http://www. someone. com/somepage. php? variable=value`,否则,必须用 post 等其他隐式方式传递变量,因为这样相对比较安全,尤其是一些比较敏感的参数(比如密码)就必须这样处理,但是对于目前很多 php 网页来讲,很多都用到 get 方式,因此一般将它打开。

将对 php.ini 的修改保存下来。

### (3) 配置 php 以 module 的方式在 Apache 中调用。

① 在 Apache 中调用主要用到 `php4apache.dll` 和 `php4ts.dll` 这两个动态链接库,前面一个 `dll` 文件在 `php` 目录的 `sapi` 子目录下面,后一个在 `php` 目录下面。为了能在 Apache 中调用,需要让 Apache 知道在哪儿能够调用到它们。

方法是将这两个文件复制到 Apache 目录下面的 `modules` 子目录下。

注意:这里共有三种方法可以达到这一目的。一是可以将这两个文件复制到系统目录下面的 `System32` 文件夹下面;二是可以将这两个文件复制到 `apache` 目录下面的 `modules` 子目录下;三是直接在配置文件中指定 `php4apache.dll` 的位置,但是必须复制一个 `php4ts.dll` 到 `sapi` 目录下,因为 Apache 调用 `php4` 模块的时候需要在同一目录下面找那个 `dll`。如果未找到,就会报错。

为了清晰方便,使用第二种方式。

② 编辑 apache 的配置文件 `httpd.conf` (在 `Apache Group\Apache\conf` 目录下)。

复制完 dll 文件后,用文本编辑器打开 apache 目录 conf 子目录中的 httpd.conf 文件。

找到文件中 LoadModule 的部分(这部分中有很多行 LoadModule 语句),在后面加入一行:

```
LoadModule php4_module modules/php4apache.dll
```

注意,请不要在前面加#号,因为这个符号表示注释。

找到 AddModule 部分,在后面加上一行:

```
AddModule mod_php4.c
```

找到 AddType 部分,在后面添上:

```
AddType application/x-httpd-php .php
```

注意此处. php 前面有一个空格。

保存对 httpd.conf 的修改。

重启 Apache 服务器,这时候你就可以看到 PHP/4.4.6 运行的消息,如图 2.18 所示。



图 2.18 PHP 运行界面

把准备好的 test.php 复制到 htdocs 目录下面,来测试 PHP 是否正常运行,文件内容如下:

```

<html>
<body>
<?
    phpinfo();
?>
</body>
</html>

```

在浏览器中访问 `http://localhost/test.php`, 如果出现如图 2.19 所示的页面, 则表示配置成功。



图 2.19 PHP 测试界面

## 用 PHP 实现计数器和动态图片显示

根据 `visitorcounter.php` 中的提示, 完成三个以下小任务。

必做: 动态显示网页被访问次数。

必做: 动态显示图片(网站首次被访问时和非首次被访问时显示不同的图片)。显示图片的代码示例:

```
echo "<img src = example.gif>"
```

选作：实现其他功能，比如收集表单、显示日期等。

完成代码后，访问 <http://localhost/visitorcounter.php> 查看结果。

## 2.4 架设 FTP 服务器

### 2.4.1 实验环境

操作系统：几乎任意 Windows 版本。本实验是在 Windows XP 下实现的。

所需软件：Serv-U 6.4.0.2。

### 2.4.2 实验内容

用 Serv-U 软件安装 FTP 服务器，并用客户端上传和下载文件。

### 2.4.3 实验步骤

在 FTP 服务器的搭建中，Serv-U 是目前使用比较多的工具之一。它设置简单，功能强大，而且非常稳定。它适用于所有的 Windows 版本，是一款共享软件，可以让用户免费使用一个月。

第一步：Serv-U 的下载和安装。

单击下载的 Serv-U 可执行文件即可开始安装了。安装过程很简单，所有设置保持默认值就可以，单击 Next 按钮完成。安装完毕，在 Windows 的桌面上会出现 Serv-U 的图标，双击 Serv-U 图标，出现 Serv-U 主窗口，单击主界面右边窗口的 Start Server 即可启动 FTP 服务器。

第二步：Serv-U 的配置。

在 Serv-U 的安装完成之后即可出现配置向导，可以通过这个向导进行配置，主要步骤如下。

① 安装程序首先启动一个设置向导帮助你设置 FTP 服务器,如图 2.20 所示,单击 Next 按钮继续。

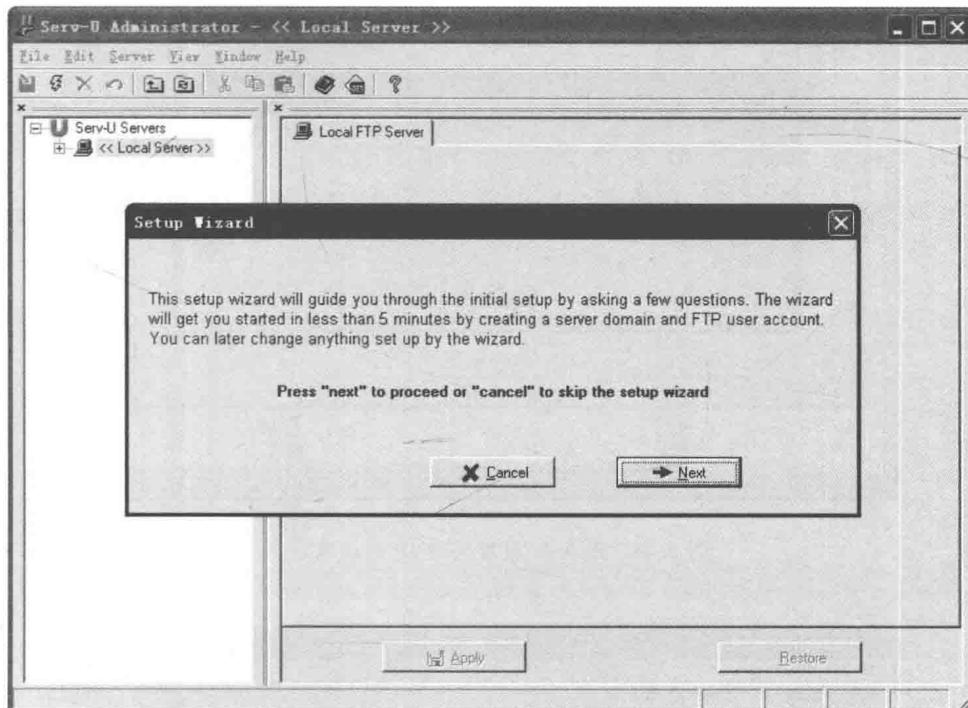


图 2.20 Serv-U 设置向导

② 系统弹出输入 IP 的对话框,如图 2.21 所示,此时需要填入准备为此 FTP 服务器绑定的 IP 地址。除非计算机有多个固定的 IP 地址,并且只想其中一个被 FTP 服务器所使用,否则,建议不管是否有固定的 IP 地址,都将此项保留为空(即让系统自动侦测),单击 Next 按钮。

③ 输入 Domain name(域名)。如图 2.22 所示,此处填入 FTP 服务器的域名。但域名由 DNS 解析而不是由这里决定,因此实际上可以填入任意内容,比如“我的个人 FTP 服务器”这种对 FTP 进行说明的文字。

④ 输入 FTP 访问的端口号,如图 2.23 所示,一般保持默认的 21 即可。

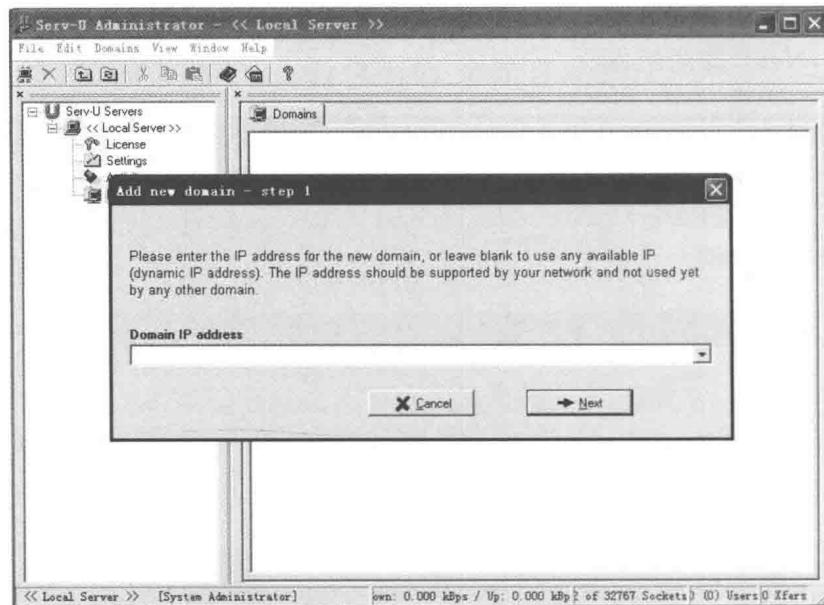


图 2.21 Serv-U 设置向导 IP 地址填写页



图 2.22 Serv-U 设置向导域名填写页

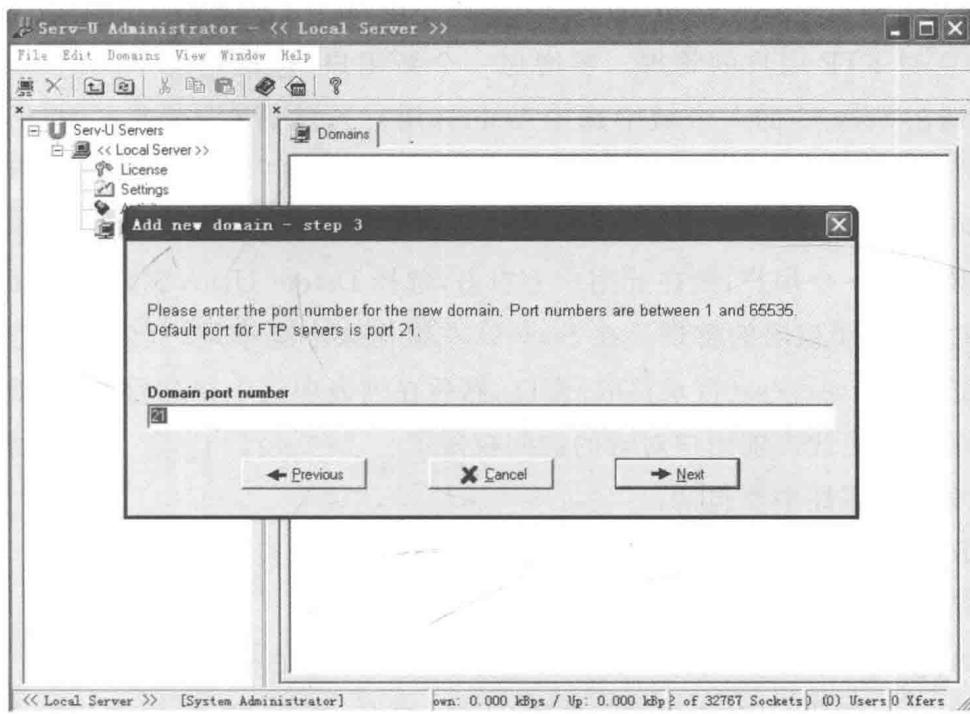


图 2.23 Serv-U 设置向导端口号填写页

⑤ 匿名用户的创建和访问目录的设定。首先向导会提示你是否要创建匿名账号,这里选择“是”,如果选择“不”,则用户需要用户名和密码才能访问FTP服务器。接下来安装向导提示输入匿名用户的主目录(Anonymous home directory),此处按照需要来设定匿名用户访问硬盘的位置。

⑥ 选择匿名用户是否将其限制在主目录里,如果选择“是”,则用户只能访问其主目录及以下的目录树;如果选择“否”,则可以访问其主目录的同级或更高级的目录树。从安全角度考虑,一般建议选择“是”。

⑦ 创建新用户和访问目录。按照向导的提示一步一步创建新用户并输入密码,接着指定该用户可访问的目录和用户权限即可。

到这里,个人FTP就已经搭建完成了。不过这只能实现Serv-U赋予的默认功能和权限,要真正让这个服务器能被控制和管理,则还需要经过以下

后续的操作,这主要包括如下几点。

① 对 FTP 用户的管理。要增加一个新用户(包括增加 Anonymous 用户),则在 Serv-U 的一个域中选中 Users(用户),然后右击,进入 New User(新用户),依次根据提示为它设置好 User Name(用户名)、Password(密码)、Home Directory(主目录)等即可完成。

要删除一个用户,则在此用户上右击,选择 Delete User(删除用户)即可。

② 对目录权限的管理。在 Serv-U 左边框架中选中用户名,再在右边框架中进入 Dir Access(目录存取)窗口,然后在列表中选中相应目录后,就可在窗口的右侧更改当前用户对它的访问权限了。

文件的属性主要包括:

Read(读): 对文件进行读操作(复制、下载,不含查看)的权力。

Write(写): 对文件进行写操作(上传)的权力。

Append(附加): 对文件进行写操作和附加操作的权力。

Delete(删除): 对文件进行删除(上传、更名、删除、移动)操作的权力。

Execute(执行): 直接运行可执行文件的权力。

List(列表): 对文件和目录的查看权力。

Create(建立): 建立目录的权力。

Remove(移动): 对目录进行移动、删除和更名的权力。

Inherit(继承): 如果选中此项,则以上设置的属性将对当前 Path(目录)及其下面的整个目录树起作用;否则就只对其当前目录有效。

③ 其他设置。在 Local Server 下的 Setting 处还可设置服务器的一些通用信息。在 max no. of users 处,设定同时登录该服务器的最大用户数。在 Max Speed 处根据自己计算机的配置,设置用户最大下载速度。

选择 Block users who connect more than XX times within YY seconds for ZZ minutes 复选框并设置相应的数值,可以防止有些恶意用户为达到攻击目的在短时间内对该服务器的频繁登录。

选择 Delete partially uploaded files 复选框,可以自动删除上传失败后留

在服务器上的不完整文件。如果不选中这一项,就能让 Serv-U 支持断点上传功能。

第三步: FTP 的访问。

利用专用的软件登录 FTP。此类软件有很多,比较著名的有 FlashFXP、 CuteFTP、LeapFTP 等(具体步骤略)。

## 2.5 DHCP 服务器的配置

### 2.5.1 实验目的

- (1) 了解 DHCP 的含义及工作原理;
- (2) 掌握 DHCP 服务器的安装与设置;
- (3) 了解 DHCP 客户机的设置。

### 2.5.2 实验环境

以太网环境,安装好 Windows 2003 Server 的联网计算机,一台安装好 Windows XP 的联网客户机。

### 2.5.3 实验内容

- (1) 了解 DHCP 服务的工作原理及相关概念。
- (2) 安装和配置 DHCP 服务器,熟悉实验步骤。
- (3) 设置 DHCP 客户机,测试 DHCP 服务配置是否正确。

### 2.5.4 实验思考

- (1) DHCP 服务器是否可以选择自动获得 IP 地址?
- (2) DHCP 服务为何要实现保留 IP 地址功能? 其在网络地址管理中有什么好处? 在保留 IP 地址时,为什么要先记录需保留 IP 地址的客户机的网

卡的物理地址？

(3) 客户计算机从 DHCP 服务器获得租约要经过几个步骤？

(4) 如果客户机设置了自动获取 IP 地址，当登录到局域网后，用 ipconfig 查看 IP 地址时，显示的 IP 地址为 169.254.16.2，判断有什么问题。

(5) 假设为 DHCP 服务器创建一个名为 shixun 的作用域，该作用域 IP 地址的范围是 192.168.0.1~192.168.0.254，可否包括 192.168.0.0 和 192.168.0.255 这两个地址？

## 2.5.5 附录：实验参考资料

DHCP 动态主机配置协议是 Dynamic Host Configuration Protocol 的缩写，DHCP 服务器主要作用是为网络客户机分配动态的 IP 地址，从而提供安全、可靠的 TCP/IP 网络配置。

### 1. DHCP 的工作原理

DHCP 采用客户/服务器模型，当 DHCP 客户端程序发出一个广播信息，请求一个动态的 IP 地址时，DHCP 服务器会根据目前已经配置的地址范围内选择一个 IP 地址，以地址租约形式提供一个可供使用的 IP 地址和子网掩码给客户端，如图 2.24 所示。

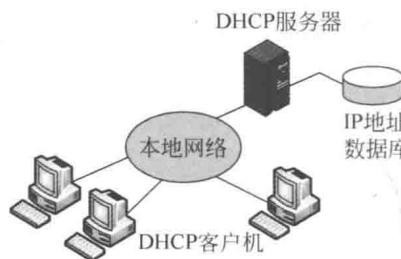


图 2.24 DHCP 的工作原理图

客户计算机从 DHCP 服务器获得租约要经过以下四个步骤：

(1) 请求 IP 租约

当 DHCP 客户计算机第一次启动或初始化 IP 时，其 IP 地址并没有任何

设置,而是使用 0.0.0.0 作为源地址,将 DHCP DISCOVER 消息广播发送给本地子网。

DHCP DISCOVER 消息中还包含客户的 MAC 地址和客户机名称,这样 DHCP 服务器可以确定是哪个客户机发来的请求。

#### (2) 提供 IP 租约

DHCP 服务器收到 DHCP DISCOVER 消息后,将 DHCP OFFER 信息直接送到客户机。DHCP OFFER 信息中包含了客户机的 MAC 地址、所提供的 IP 地址、子网掩码以及 DHCP 服务器的 IP 地址。

DHCP 服务器发送 DHCP OFFER 信息之后仍暂时保留发送给客户计算机的地址,并等待该地址客户的确认信息。

如果在 1s 内 DHCP 客户机没有收到 IP 地址,就将 DHCP DISCOVER 消息重复广播四次,四次重试的间隔时间为 2s、4s、8s、16s,另一次则为 0~1000ms 间的随机时间。在四次请求之后,如果仍没有收到,就从 169.254.0.1 到 169.254.255.254 保留范围内采用一个 IP 地址。客户机仍将每隔 5min 尝试发现 DHCP 服务器。

#### (3) 选择 IP 租约

因为客户可能收到网络上多个 DHCP 服务器的 DHCP OFFER 消息,需要决定使用哪一条消息。一般情况下,客户机使用第一条接到的信息,然后广播 DHCP REQUEST 消息作为响应,消息中还包括它所接收的 IP 租约的 DHCP 服务器的 MAC 地址,这样,其他 DHCP 服务器可在收到广播后将它们的 IP 地址释放回可用的地址池。

#### (4) 确认 IP 租约

当被选择 IP 租约的 DHCP 服务器收到 DHCP REQUEST 消息后,将用 DHCP ACK 消息应答。DHCP ACK 消息告诉客户计算机它现在具有有效租约。一旦客户机接收到 DHCP ACK 消息,就完成自己的 IP 配置并成为一个完全受租约的客户,如图 2.25 所示。

当 DHCP 客户机在租约期限过了一半的时候,尝试更新租约。DHCP 客

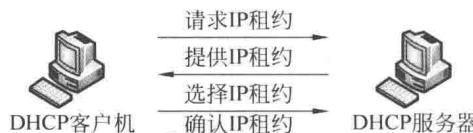


图 2.25 获得租约要经过的四个步骤

户机直接给 DHCP 服务器发送 DHCP REQUEST 消息。如果 DHCP 服务器可用,将发回 DHCP ACK 消息,其中包含新的租约和已更新的参数。DHCP 客户机在收到 DHCP ACK 消息后更新配置。如果 DHCP 服务器不可用,客户机将继续使用它的租约,然后在租约期限过了 87.5% 的时候,广播 DHCP DISCOVER 消息,接受任何 DHCP 服务器发出的租约。

如果租约到期,客户机必须停止使用当前的 IP 地址,然后开始新的租约过程。

在客户机请求一个非法的或重复的 IP 地址,DHCP 服务器用 DHCP NAK 消息拒绝,迫使客户机重新获得一个新的合法的地址。

## 2. 安装和配置 DHCP 服务器

### (1) 安装 DHCP 服务

选择“开始”→“设置”→“控制面板”,打开控制面板,双击“添加/删除程序”,选择“添加/删除 Windows 组件”,在打开的 Windows 组件列表框中选择“网络服务”,单击“详细信息……”按钮,在网络服务列表框中选中“动态主机配置协议(DHCP)”,单击“确定”按钮,接着按提示完成安装。

DHCP 服务安装结束之后,在“管理工具”中将出现 DHCP 命令项,并自动建立一个默认的 DHCP 服务器。

### (2) 配置 DHCP 服务器

#### ① 创建作用域

打开 DHCP 管理器,右击服务器名,在弹出的快捷菜单中选择“新建作用域”,打开新建作用域向导,输入作用域名称 shixun,设置 DHCP 作用域的属性。

如图 2.26 所示,设置 IP 地址范围 192.168.0.1~192.168.0.254 以及子网掩码 255.255.255.0,可包含排除的 DHCP 服务的 IP 地址:192.168.0.1~192.168.0.5。租约期限:默认的租约期是 8 天。

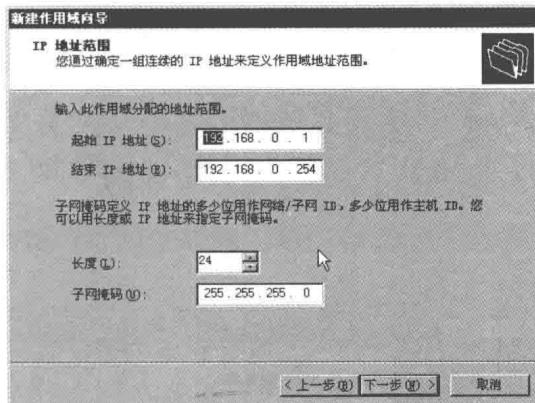


图 2.26 DHCP 管理器的 IP 信息填写

## ② 设置排除地址

右击“地址池”文件夹,在快捷菜单中选择“新建排除”,输入排除的 IP 地址 192.168.0.1~192.168.0.5 和 192.168.0.8。

设置完成后,如图 2.27 所示。

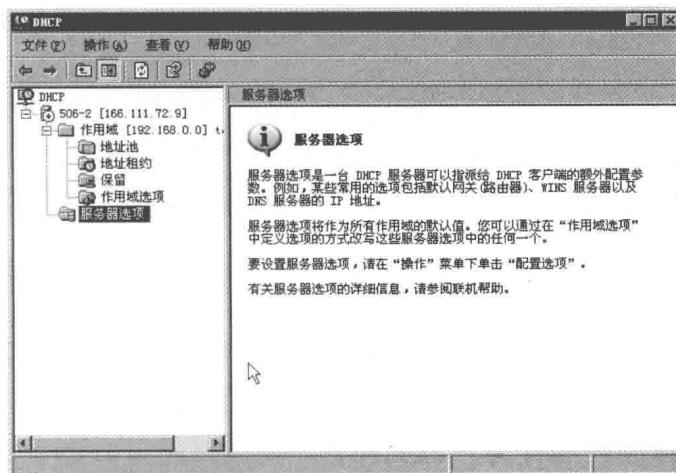


图 2.27 DHCP 管理器

### ③ 用户保留地址

右击“保留”文件夹，在快捷菜单中选择“新建保留”，输入标识、MAC 地址(00-01-30-55-B2-6A)和绑定的 IP 地址(192.168.0.100)。

## 3. 管理 DHCP 服务器

DHCP 服务器的数据库文件位于%systemroot%\system32\dhcp 文件夹内，其中的 DHCP. mdb 是其存储数据的文件。地址数据库可以通过控制台进行数据库的启动、停止、备份和恢复等工作，如图 2.28 所示。

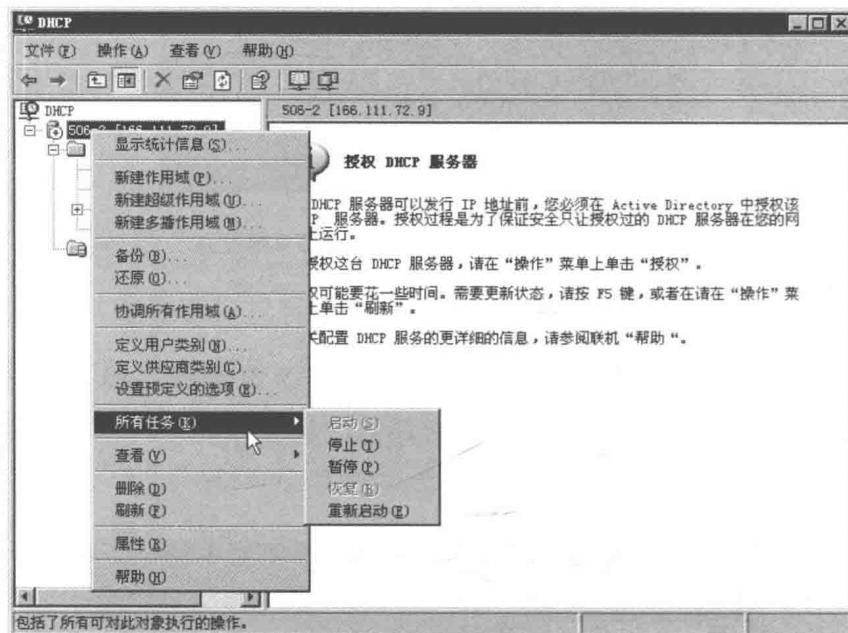


图 2.28 DHCP 服务器中地址数据库的管理

## 4. 设置 DHCP 客户机

### (1) 设置 TCP/IP 相应的常规属性

对于 Windows XP 客户机，在“Internet(TCP/IP)协议属性”对话框中单击“自动获得 IP 地址”单选按钮，如图 2.29 所示。

### (2) 检查、释放或续订客户机的租约

通过 ipconfig 命令行实用程序，可检查、释放或续订客户机的租约。

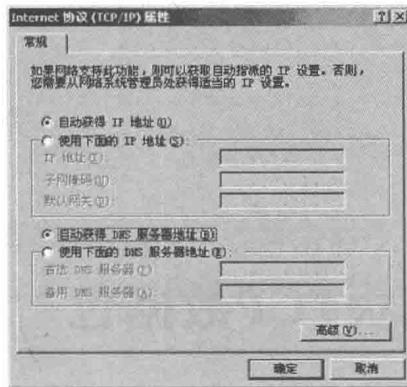


图 2.29 “Internet 协议(TCP/IP)属性”对话框

检查 DHCP 客户机租约状态信息, 输入 ipconfig, 或者输入 ipconfig /all, 如图 2.30 所示。

释放 DHCP 客户机租约: 输入 ipconfig /release。

续订 DHCP 客户机租约: 输入 ipconfig /renew。

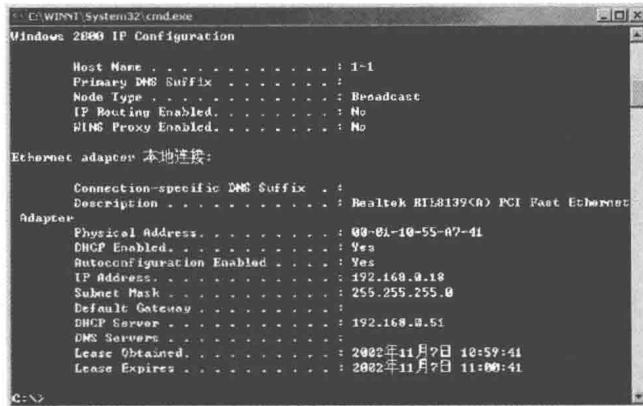


图 2.30 执行 ipconfig /all 命令窗口



## 捕获TCP数据包



### 3.1 实验目的

通过实验熟悉 Wireshark 抓包软件的使用方法,理解 TCP 传输过程,以及慢启动、拥塞避免等相关技术。

### 3.2 实验环境

操作系统:几乎任意 Windows 版本。本实验是在 Windows XP 下实现的。

所需软件: Wireshark-win32-1.10.2。

### 3.3 实验内容

- (1) 在 Windows 环境进行 Wireshark 抓包。
- (2) 在 Windows 环境 Wireshark 窗口中查看各种协议下的数据包。

(3) 在 Windows 环境上传文件到服务器, 同时观察 TCP 传输过程。

## 3.4 实验报告要求

按实验步骤完成所有实验内容, 回答实验思考题, 并从实验结果中提取必要的图表和分析数据来支持你对实验思考题的回答。

## 3.5 实验步骤

### 1. Wireshark 的安装

Wireshark 基本安装过程与一般软件安装基本相同, 均按默认设置安装即可。

### 2. 捕捉从自己 PC 到远程服务器的 TCP 传输

在开始探索 TCP 奥秘之前, 需要用 Wireshark 软件跟踪从 PC 到远程服务器的 TCP 传输数据包。需要进入一个网页, 这个网页允许输入在 PC 上的一个文件的名字, 然后利用 HTTP POST 方法将这个文件传输到 Web 服务器(教材 2.2.3 节)。用 POST 方法而不是 GET 方法, 是因为想要从 PC 上传输大量数据到另外一台 PC。当然, 在做以上工作的时候, 需要同时运行 Wireshark, 以捕获从 PC 上发送和接收到的 TCP 数据包。

需要进行如下步骤:

(1) 准备好 *Alice in Wonderland* (《爱丽丝漫游奇境记》) 的 ASCII 码文档, 并以“(你的学号).txt”为文件名存入 PC, 如 2004011000.txt。

文档可以去下面链接下载 <http://166.111.180.60:8080/upload/alice.txt> (将该网页另存为 txt 文件)。

(2) 进入 <http://166.111.180.60:8080/upload/Lab3.jsp>, 会看到如图 3.1 所示的窗口。

单击“浏览”按钮进入包含 *Alice in Wonderland* 文件的文件夹, 先不要着

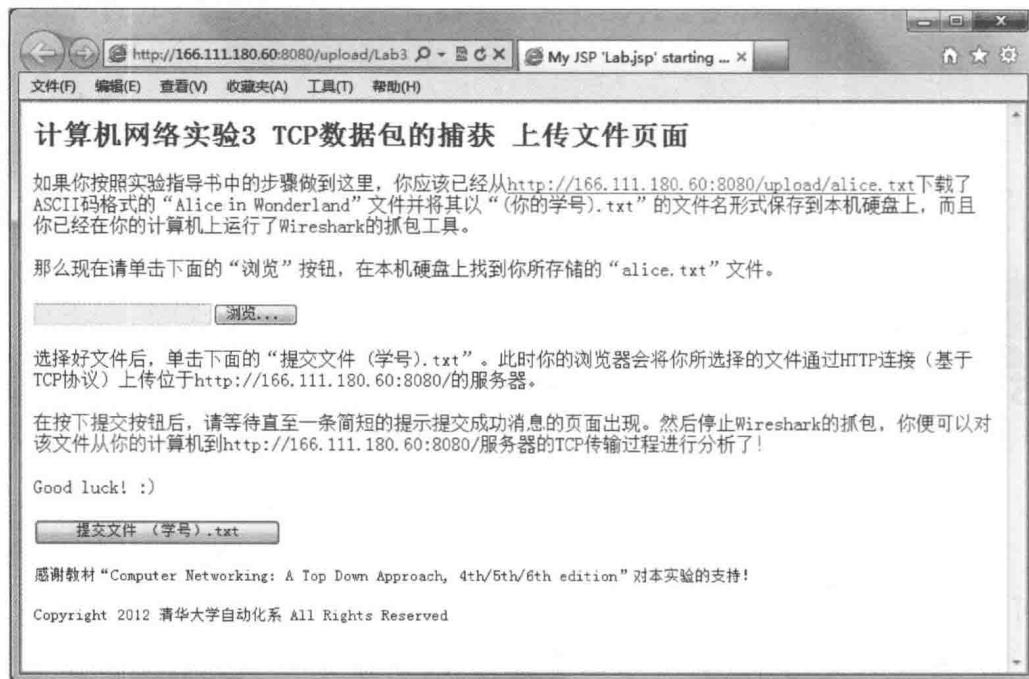


图 3.1 实验界面

急单击“提交文件(学号).txt”按钮。

(3) 用 Wireshark 开启数据包捕捉。开始抓包之前, 进入 Wireshark 的 Capture→Options, 去掉 Hide capture info dialog 前面的“√”, 以便在抓包过程中看到数据框, 如图 3.2 所示。

安装好 Wireshark 后, 选择 Capture→Start 开始抓包。回到浏览器, 单击“提交文件(学号).txt”按钮来上传文件。一旦文件上传成功, 将会有一个祝贺信息出现。

为简单起见, 在开始运行 capture 命令之前, 可以先定义对数据包进行捕捉的过滤器。具体操作如下: 选择菜单 capture→options, 出现一个对话窗口, 确认 Interface 项是否是当前计算机的默认网卡。

(4) 停止 Wireshark 数据包捕捉。你的 Wireshark 窗口会出现类似图 3.3 的界面。

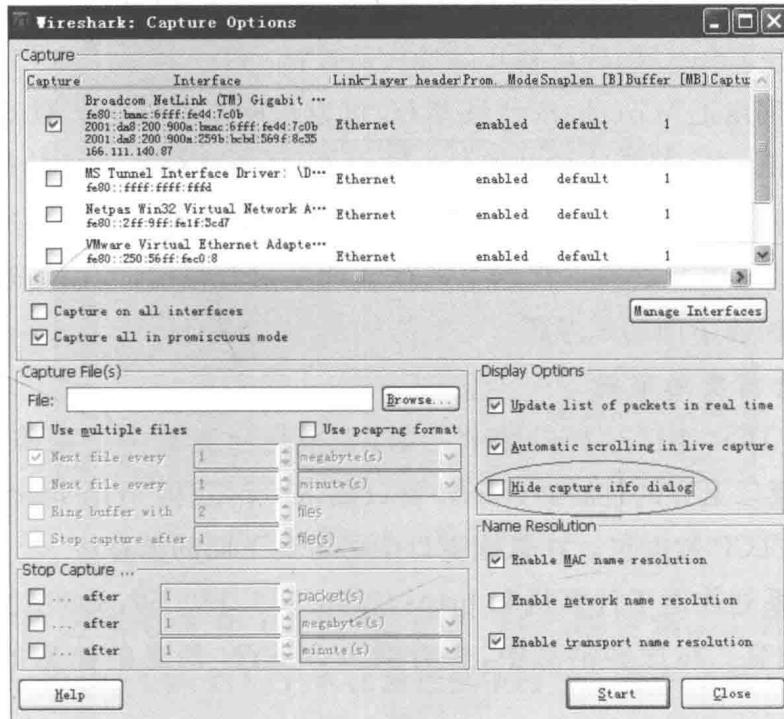


图 3.2 Wireshark 捕获选项设置

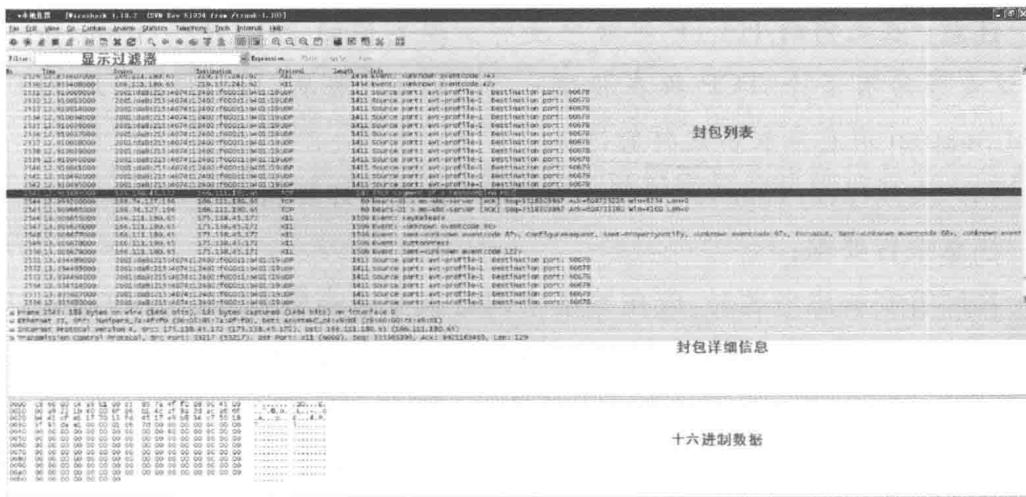


图 3.3 Wireshark 捕获结果

为方便分析数据,可在左上角的过滤器(filter)工具栏中输入“tcp. port == 8080”后按 Enter 键,即可初步筛选所需数据。

如果在网络上 Wireshark 无法运行,可以从网络学堂上下载 default\_test 文件。default\_test 是默认的数据包追踪文件,这个文件是在教师的计算机上按照上述操作步骤捕捉下来的。即使已经成功捕捉到了自己的追踪数据包并且已经解读,也会发现下载这个追踪文件是很有帮助的,因为这样可以帮助你更好地回答下面的思考题。

### 3. 查看捕获的跟踪

在分析 TCP 连接过程的细节之前,先来仔细查看一下跟踪。首先,在 Wireshark 窗口上方的过滤器(filter)窗口输入 tcp,使得 Wireshark 的数据窗口中只显示 TCP 数据包。在数据窗口中将看到下面的消息:

(1) 一系列往返于计算机和 `http://166.111.180.60:8080/` 之间的 TCP 和 HTTP 消息。在这些消息中,会看到包含 SYN 消息的初始的三次握手过程。

(2) 可能会看到从计算机发送到 `http://166.111.180.60:8080/` 的一个 HTTP POST 消息以及一系列的 HTTP Continuation 消息。

**注意:** 在之前的 HTTP 实验中没有出现类似的 HTTP Continuation 消息,这是因为有多个 TCP 段在传送一个 HTTP 消息,Wireshark 用 HTTP Continuation 消息来表示这样的情况。

(3) 从 `http://166.111.180.60:8080/` 返回到计算机的 TCP ACK 段。

**注意报告要求:**

在回答实验思考题时,应在答案中同时提交含有数据包以及跟踪的打印输出。在这些数据中添加注释来对相应的答案做出解释。

一种打印数据包的途径是:选择 `File→Print`,选中 `output to file`,将数据导出,然后打开文件,选择回答问题所需要的少量数据即可(即在 `Package Range` 选择 `Displayed`,而不是 `Captured`),如图 3.4 所示。

现在,改变 Wireshark 的“listing of captured packets (已捕获数据包清

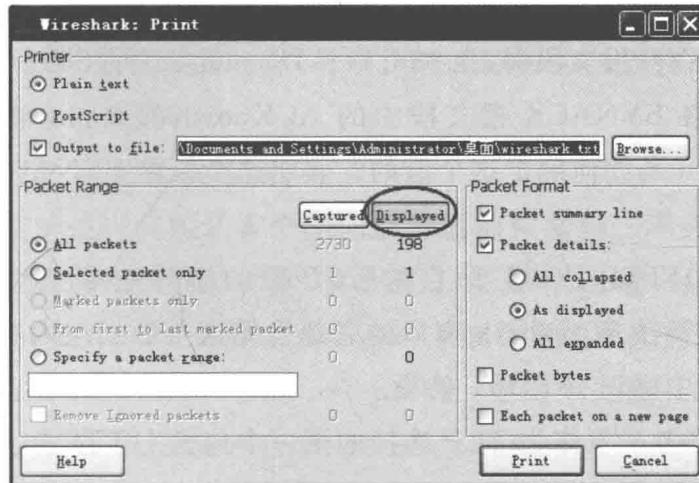


图 3.4 Wireshark 输出选项设置

单)”窗口,使它忽略含有 HTTP 消息的 TCP 段信息。选择 Analyze→Enabled Protocols,去除 HTTP 前面复选框中的“√”,然后单击 OK 按钮。在此次实验中还要查看 TCP 的 sequence numbers(不是 Wireshark 可能显示的 relative sequence numbers),选择 Edit→Preferences→Protocols→TCP,去除 relative sequence numbers 前面复选框中的“√”即可。事实上,Wireshark 在新版本中已经默认将上述两个复选框的“√”去除。

这就是需要查看的一系列往返于计算机和 `http://166.111.180.60:8080/` 之间的 TCP 段。我们将用这些捕获到的数据包和跟踪信息来完成此次实验。

#### 4. 分析 TCP 数据包

回答以下有关 TCP 报文段的问题:

(1) 客户端电脑传送文件到 166.111.180.60 的 IP 地址和端口是什么?  
从 166.111.180.60 接收文件的 IP 地址和端口是什么?

(2) 用来初始化客户端电脑和 166.111.180.60 的 TCP 连接的 TCP SYN 报文段的序号是什么?在报文段中,哪个地方表明这是一个 SYN 报

文段？

(3) 回复 SYN 报文段时,由 166.111.180.60 发送的 SYNACK 报文段的序号是什么? 在 SYNACK 报文段中的 ACKnowledgement 域的值是什么? 166.111.180.60 是如何确定这个值的? 表明这个段是 SYNACK 的标志位或者符号是什么?

(4) 包含 HTTP POST 命令的 TCP 段的序号是多少? 注意,要找到 POST 命令,需要在 Wireshark 窗口的底部发掘这个数据包内容域,找到一个在其 DATA 域中标识有 POST 的段。

(5) 仔细思考一下作为 TCP 连接的第一个包含 HTTP POST 的 TCP 报文段。TCP 连接(包括包含 HTTP POST 的报文段)的开头 6 个报文段的序号是多少? 每个报文段都在什么时间发送? 每个报文段接收到 ACK 的时间是多少? 假定每个 TCP 报文段发送事件和收到其确认信息的事件之间存在时间差,那么这 6 个报文段各自的 RTT 值是多少? 接收到每个 ACK 之后的 EstimatedRTT 数值是多少? (参见课本 160 页) 假设第一个报文段的 EstimatedRTT 值等于其观测到的 RTT 值,后续报文段的 EstimatedRTT 均按课本 160 页方程计算。

**注意:** Wireshark 有一个很好的功能,它允许画出发送的每一个 TCP 段的 RTT。选择一个在“listing of the captured packets”窗口中的 TCP 段,此 TCP 正在从客户端到 166.111.180.60,然后选择: Statistics→TCP Stream Graph→Round Trip Time Graph。

(6) 开始的 6 个 TCP 报文段的长度各自是多少?

(7) 在整个跟踪过程中,在接收端广告(advertise)的可用缓存空间的最小值是多少? 接收端有没有因缓存空间不足而限制发送端的发送?

(8) 在跟踪文件中,有重传的报文段吗? 回答这个问题,你需要检查哪个地方?

(9) 接收方在一个 ACK 中,通常确认多少数据? 你能辨别出这样一种情形吗: 即接收方对收到的报文段,每隔一个确认一次? (参考教材 165 页

的表 3-2。)

(10) 这个 TCP 连接的吞吐量(每单位时间传输的字节数)是多少？解释你是如何计算这个数值的？

### 5. 分析 TCP 拥塞控制方法

下面来观察单位时间内从客户端向服务器的数据量。不必对 Wireshark 窗口中的原始数据进行烦琐的计算，而是通过 Wireshark 的 TCP 画图工具来完成：选择 Time-Sequence-Graph(Stevens)完成数据的图形显示。

在 Wireshark 的 listing of captured-packets 窗口中选择一个 TCP 段。然后在菜单中选择 Statistics → TCP Stream Graph → Time-Sequence-Graph (Stevens)，会看到从捕获的数据包生成的如图 3.5 所示的图像。注意，可用鼠标完成对图像的移动和缩进以得到满意效果，详见 help 选项。

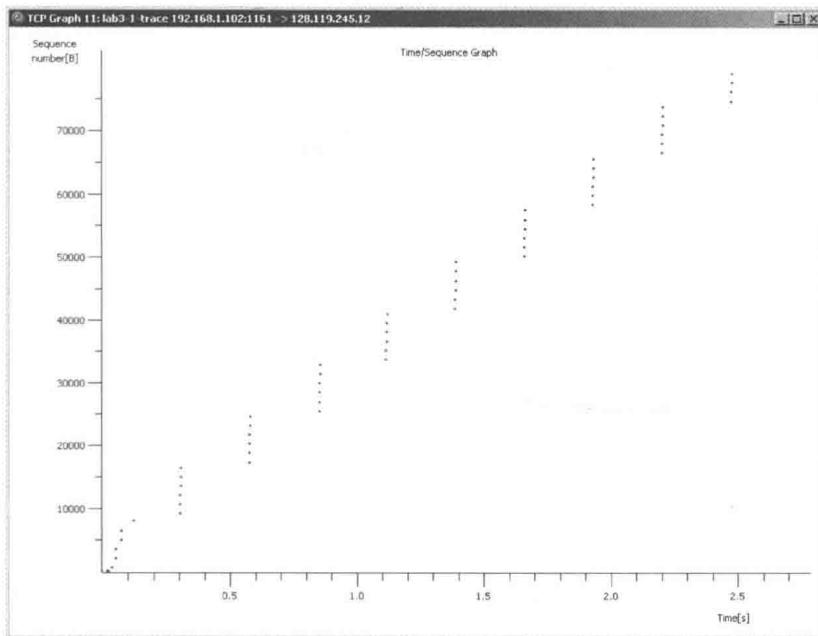


图 3.5 TCP 序列号时间衍变示意图

图 3.5 中的每个点代表一个发送的 TCP 段，横坐标代表时间，纵坐标代表 TCP 段的序列号。注意那些堆叠在一起的点代表从发送方背靠背连续发

送的一系列数据包。

回答下面的问题：

(1) 用 Time-Sequence-Graph(Stevens)中的画图工具观察从客户端发送到 166.111.180.60 服务器的 TCP 段的序列号—时间图。怎样判断 TCP 的慢启动(slowstart)开始和结束？拥塞避免在什么地方开始起作用的？注意在实际的跟踪中，不是都像教材图 3.5 那样具有简单漂亮的形式。同时还要注意在 Time-Sequence-Graph(Stevens)中纵坐标所代表的变量与教材图 3.5 中是不同的。

(2) 总结这次实验中所得到的 TCP 数据与在教材中所学的理想情况有什么不同？



## HTTP抓包分析



### 4.1 实验目的

通过实验熟悉 Wireshark 抓包软件的使用方法,理解有关 HTTP 协议的各方面内容。

### 4.2 实验内容

- (1) 在 Windows 环境下进行 Wireshark 抓包。
- (2) 理解基本 GET/response 交互,HTTP 数据包的格式。
- (3) 获取较长的 HTML 文件,分析其数据包。
- (4) 获取有嵌入对象的 HTML 文件,分析其数据包。

### 4.3 实验报告要求

按实验步骤完成所有实验内容,回答实验思考题,并从实验结果中提取必要的图表和分析数据来支持对实验思考题的回答。

## 4.4 实验步骤

### 1. 基本 HTTP 的 GET/response 交互

为了了解基本的 HTTP 协议相关内容, 我们从一个最简单 HTML 文件开始, 该 HTML 文件非常简短, 不包含嵌入对象。实验步骤如下:

(1) 打开网页浏览器。

(2) 打开 Wireshark。本次试验中, 只关注 HTTP 协议, 不希望在抓包窗口中看到其他协议的数据包, 因此在 display-filter-specification 窗口中输入 http&&tcp, 并单击 Apply 按钮, 这样只有 HTTP 数据包会在 packet-listing 窗口中显示。

(3) 稍等片刻, 然后开始 Wireshark 抓包。

(4) 在浏览器地址栏中输入以下 URL

`http://166.111.180.60:8080/Lab5/http-wireshark-file1.html`

将在浏览器中看到一个只有两行文字的 html 文件。

(5) 停止 Wireshark 抓包。

此时 Wireshark 窗口会出现类似图 4.1 的窗口。

在图 4.1 所示的例子中, 在 packet-listing 窗口中捕捉到了两个 http 数据包: GET 数据包(从浏览器到 166.111.180.60 服务器)以及从服务器到浏览器的 response 数据包。在下面的 packet-contents 窗口中可以看到相应消息的细节内容。复习一下数据包的内容: http 数据包包含在 TCP 段里, TCP 段包含在 IP 数据报里, IP 数据报包含在 Ethernet 框架里, 因此 Wireshark 捕捉了以上所有数据报的信息。这里希望将在 packet-contents 窗口中显示出来的非 http 数据量减到最低, 所以将 Fream, Ethernet, IP 以及 TCP 的相应目录下的具体内容隐藏(目录前的标志为十号), 只显示 http 数据报的具体内容(目录前的标志为一号)。

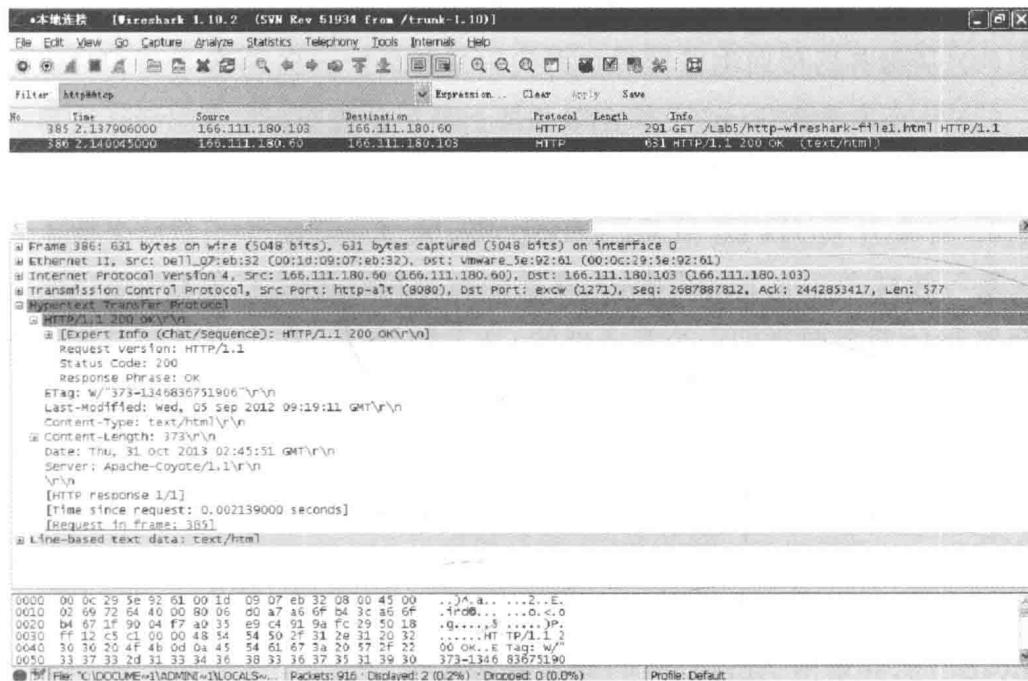


图 4.1 Wireshark 的捕获界面

**注意：**在做实验之前，请确认 Analyze→Enabled Protocols 中 HTTP 已经被选中，否则在 packet-listing 中不会显示 HTTP 数据包。另外，实验前先清空网页浏览器的缓冲区：在浏览器工具栏里选择工具→Internet 选项，单击“删除文件”按钮。

观察 http 的 GET 和 response 数据报，回答下列问题。

在回答实验思考题时，应在答案中同时提交含有数据包以及跟踪的打印输出。在这些数据中添加注释来对相应的答案做出解释。

**注意(一种打印数据包的途径)：**选择菜单 File→Print，选中 output to file，将数据导出，然后打开文件，选择回答问题所需要的少量数据即可。

(1) 你的浏览器所运行的是 Http 协议的 1.0 版本还是 1.1 版本？服务器用的是什么版本的 Http 协议？

(2) 你的浏览器可以支持多少种语言(如果有)？

- (3) 你自己的 IP 地址是多少？服务器呢？
- (4) 从服务器传回浏览器的状态代码是什么？
- (5) 你所看到的 html 文件在服务器上最后的修改时间是什么？
- (6) 传回浏览器的内容的大小是多少 bytes？

## 2. 有条件的 HTTP 的 GET/response 交互

复习教材 2.2.5 节的内容，大多数网页浏览器提供了对象缓冲功能从而在获取 http 对象时送回一个有条件的 GET 数据包。在实施下面的实验步骤前，先清空网页浏览器的缓冲区：在浏览器工具栏里选择工具→Internet 选项，单击“删除文件”按钮。然后实施以下实验步骤：

(1) 打开浏览器清空浏览器缓存。（以 IE 浏览器为例，打开菜单栏中的工具→Internet 选项，选择删除文件。）

(2) 打开 Wireshark，在 display-filter-specification 窗口中输入 http&.&.tcp，并单击 Apply 按钮，然后开始抓包。

(3) 在浏览器地址栏中输入以下 URL

`http://166.111.180.60:8080/Lab5/http-wireshark-file2.html`

在浏览器中将会显示一个简单的具有 5 行文字的 html 文件。

(4) 快速地再次输入上述 URL，或者单击浏览器工具栏上的“刷新”按钮。

(5) 停止 Wireshark 抓包。

回答下面的问题：

(1) 在 packet-content 窗口中观察第一个从浏览器向服务器发出的 HTTP GET 请求的数据包，是否看到一行显示“IF-MODIFIED-SINCE”？

(2) 观察从服务器传回的 response 数据包，服务器是否很清楚地传回了该 html 文件的内容？你如何知道的？

(3) 观察第二个从浏览器向服务器发出的 HTTP GET 请求的数据包，是否看到一行显示 IF-MODIFIED-SINCE？如果有，在 IF-MODIFIED-

SINCE 报头后显示的是什么？

(4) 从服务器传回的对第二个 HTTP GET 的 response 状态代码是什么？服务器是否很清楚地传回了该 html 文件的内容？你如何知道的？

### 3. 获取较长的 HTML 文件

下面来获取一个较长的 html 文件，实验步骤如下：

(1) 打开浏览器，确认浏览器的缓冲器已经被清空。

(2) 打开 Wireshark，开始抓包。

(3) 在浏览器地址栏中输入以下 URL

`http://166.111.180.60:8080/Lab5/http-wireshark-file3.html`

在浏览器中将会显示一个介绍故宫的 html 文件。

(4) 停止 Wireshark 抓包，在 display-filter-specification 窗口中输入 `http&&.tcp`。

在 packet-listing-window 中，会看到向服务器发出的 HTTP GET 数据包，在其后有多种针对 GET 的 response 数据包。复习教材中的 2.2 节（参见教材图 2.9），http 的 response 数据包包含一个状态行，其后有报头行，再其后有一个空行，然后是数据实体。在 HTTP GET 数据包中，数据实体也就是需要查看的整个 html 文件。该 html 文件较长以至于一个 TCP 包已经不能满足数据量的要求，此时 HTTP response 数据包就会被 TCP 拆成几块，每一块被一个 TCP 段所包含（参见教材图 3-30）。每个 TCP 段在 Wireshark 中被作为一个单独的数据包来记录。

回答下面的问题：

(1) 浏览器向服务器发送了多少个 HTTP GET 请求的数据包？

(2) 该 HTTP response 数据包需要多少个含有数据的 TCP 段来传送？

(3) 与 HTTP GET 对应的 response 数据包的状态代码是什么？

### 4. 获取有嵌入对象的 HTML 文件

下面将了解含有嵌入对象的 html 文件的数据包，实验步骤如下（本次实

验需要主机与本校以外的网络建立连接):

- (1) 打开浏览器,确认浏览器的缓冲器已经被清空;
- (2) 打开 Wireshark,开始抓包;
- (3) 在浏览器地址栏中输入以下 URL

`http://166.111.180.60:8080/Lab5/http-wireshark-file4.html`

在浏览器中将会显示一个含有两个图片的 html 文件。这两个图片是被该 html 文件所引用的图片,也就是说该 html 文件并不包含这些图片文件,而是含有这些图片文件的 URL 地址。正如教材中所述,浏览器必须从相应的 URL 地址获取这些图片。其中 Google 中国的 logo 图片是从 `www.google.com` 服务器上获得的,我校校徽图片是从 `www.tsinghua.edu.cn` 服务器上获得的。

- (4) 停止 Wireshark 抓包,在 display-filter-specification 窗口中输入 `http&&tcp`。

回答下面的问题:

- (1) 浏览器向服务器发送了多少个 HTTP GET 请求的数据包? 这些数据包发送的目的网址是什么?
- (2) 浏览器是从两个服务器上连续下载这两个图片还是并行下载的? 请做相应解释。



## DHCP抓包分析

### 5.1 实验目的

通过执行 DHCP 有关命令并获取 DHCP 包, 观察 DHCP 工作过程。

### 5.2 实验环境

操作系统: 几乎任意 Windows 版本。本实验是在 Windows XP 下实现的。

所需软件: Wireshark-setup-1.6.1。

### 5.3 实验内容

- (1) 在 Windows 环境下执行 DHCP 相关命令。
- (2) 在 Windows 环境通过 Wireshark 抓包。
- (3) 通过获取的数据包观察 DHCP 的工作过程。

## 5.4 实验报告要求

按实验步骤完成所有实验内容,回答实验思考题,并从实验结果中提取必要的图表和分析数据来支持对实验思考题的回答。

## 5.5 实验步骤

### 1. Wireshark 的安装

参见“实验三 捕获 TCP 数据包”实验指示书。

### 2. 执行 DHCP 相关命令

(1) 打开 Windows,选择菜单“开始”→“运行”,输入 cmd 打开 Windows 命令提示符程序。

(2) 输入 ipconfig /release。这条命令释放当前 IP 地址,此时主机的 IP 地址变为“0.0.0.0”。

(3) 打开 Wireshark(相关设置请参考实验三指示书),并开始抓包。

(4) 回到 Windows 命令提示符窗口,输入 ipconfig /renew。这条命令重新配置主机的网络,包括一个新的 IP 地址。

(5) 一直等待直到 ipconfig /renew 这条命令执行结束(在 Wireshark 抓包窗口中观察,没有新捕获的 DHCP 数据包即为命令执行结束),再次输入 ipconfig /renew。

(6) 在第二次 ipconfig /renew 命令执行结束后,输入 ipconfig /release 来再次释放先前获得的 IP 地址。

(7) 最后再次输入 ipconfig /renew 给主机重新获得 IP 地址。

(8) 停止 Wireshark 抓包。

### 3. 观察数据包

观察 Wireshark 所获取的数据包。在数据包上方的过滤器(filter)窗口中

输入 bootp,使其只显示 DHCP 数据包。(DHCP 从一个较早版本的 BOOTP 协议发展而来。BOOTP 和 DHCP 使用同样的端口号,67 和 68。在 Wireshark 中观察 DHCP 数据包时,需要输入的是 bootp 而不是 dhcp。)

从得到的数据包结果可以看出,在第一个 ipconfig /renew 命令执行以后,产生了 4 个 DHCP 数据包: DHCP Discover, DHCP Offer, DHCP Request 和 DHCP ACK。

#### 4. 实验思考题

注意报告要求:

实验报告应包含如图 5.1 所示的命令行执行过程。在回答实验思考题时,应在答案中同时提交含有数据包以及跟踪的打印输出。在这些数据中添加注释来对相应的答案做出解释。

回答下列问题:

- (1) DHCP 数据包传送的是 UDP 还是 TCP?
- (2) 画出时间-数据包图,说明第一组 4 个 DHCP 数据包 (Discover/Offer/Request/ACK) 在客户端和服务器端之间的交换过程。对每个数据包,指出源端口号和目的端口号。
- (3) 所在主机链路层(例如 Ethernet)的地址是什么?
- (4) 通过什么值来选择 DHCP Discover 数据包与 DHCP Request 数据包?
- (5) 在第一组 4 个 DHCP 数据包中, Transaction-ID 的值分别是多少? 第二组 DHCP 数据包中的 Request 和 ACK 数据包的 Transaction-ID 的值又是多少? 设置 Transaction-ID 的目的是什么?
- (6) 主机通过 DHCP 来获取 IP 地址,但主机的 IP 直到 4 个 DHCP 数据包交换完毕以后才得以确认。如果 IP 地址在这 4 个 DHCP 数据包交换完毕后才得以确认,那么这 4 个 DHCP 数据包中的 IP 数据报所使用的 IP 值是什么? 对于这 4 个 DHCP 数据包中的每一个数据包,指出其封装在 IP 数据报中的源端和目的端的 IP 地址。

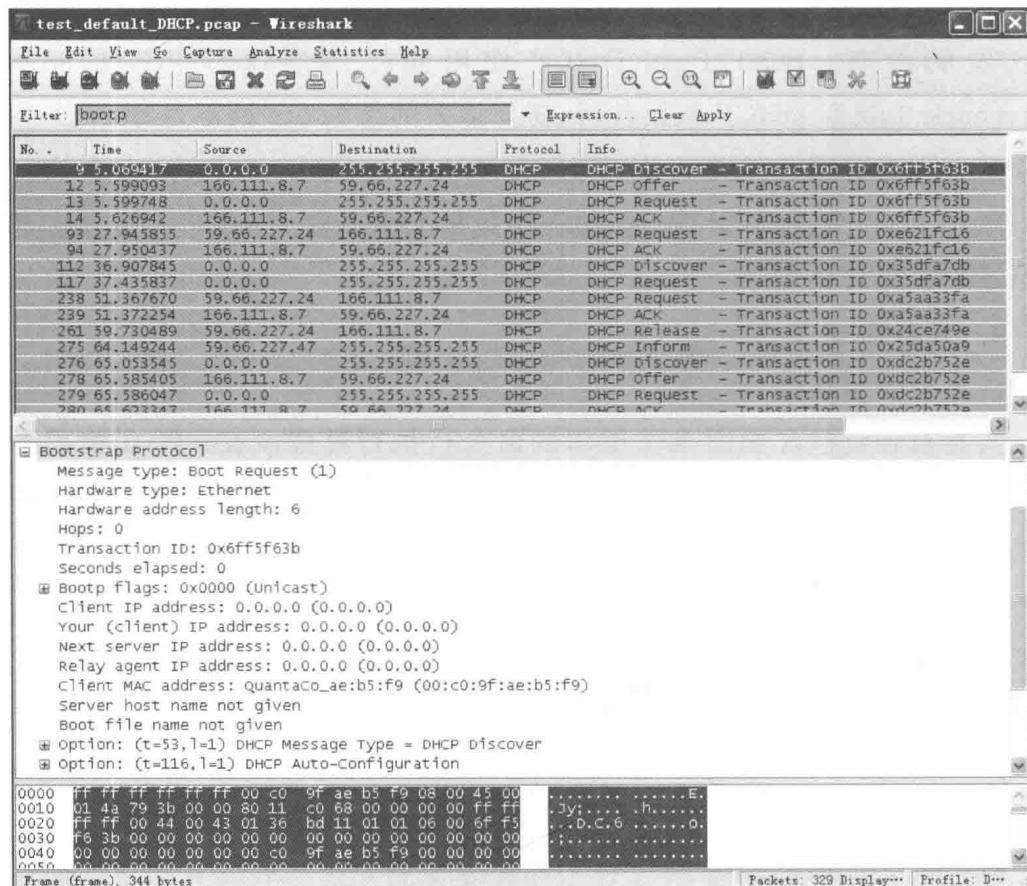


图 5.1 Wireshark 的 DHCP 捕获界面

(7) DHCP 服务器的 IP 地址是什么？

(8) 在 DHCP Offer 数据包中显示的 DHCP 服务器提供给主机的 IP 地址是什么？请指出哪个 DHCP 数据包包含了所提供的 DHCP 地址。

(9) 如图 5.1 所示的例子中，在主机和 DHCP 服务器之间没有延迟代理 (relay agent)。从数据包中的什么内容中可以看出没有延迟代理呢？在你的实验中有延迟代理吗？如果有，该代理的 IP 地址是什么？

(10) 请解释在 DHCP Offer 数据包中 router 和 subnet mask 内容的作用。

(11) 如图 5.1 所示的例子中, 主机是在 DHCP Request 数据包中请求提供 IP 地址。试验中的情况是怎样的?

(12) 请解释设置租约时间(lease time)的作用。在试验中, 租约时间是多长?

(13) DHCP Release 数据包的作用是什么? DHCP 服务器对于客户端的 DHCP 请求发出“已收到”的确认了吗? 如果客户端的 DHCP Release 数据包丢失会产生什么结果?

## 实验六

# DNS抓包分析

### 6.1 实验目的

通过执行 DNS 有关命令并获取 DNS 包, 观察 DNS 工作过程。

### 6.2 实验内容

- (1) 在 Windows 环境进行 Wireshark 抓包。
- (2) 理解基本 GET/response 交互, HTTP 数据包的格式。
- (3) 获取较长的 HTML 文件, 分析其数据包。
- (4) 获取有嵌入对象的 HTML 文件, 分析其数据包。

### 6.3 实验报告要求

按实验步骤完成所有实验内容, 回答实验思考题, 并从实验结果中提取必要的图表和分析数据来支持对实验思考题的回答。

## 6.4 实验步骤

### 1. nslookup

在此实验中,将进一步利用 nslookup 命令来查看相关信息。在 Windows 系统下,打开 Windows 命令提示符窗口中运行 nslookup。

在 nslookup 的基本应用中,该命令允许主机查询任何指定的 DNS 服务器。被查询的 DNS 服务器可以为 root 级的 DNS 服务器、一个顶级域名 (top-level-domain) DNS 服务器、一个权威 (authoritative) DNS 服务器,以及中间 (intermediate) DNS 服务器。为了达到查询目的,nslookup 命令给指定的 DNS 服务器发送一个 DNS 查询请求,从该服务器接收一个 DNS 的回复,然后将结果显示出来。

图 6.1 显示了三个独立的 nslookup 命令运行的结果。在图 6.1 中,用户主机在清华大学校内,当地的 DNS 服务器为 dns-a.tsinghua.edu.cn。当运行 nslookup 时,如果没有指定 DNS 服务器,则该命令返回的是默认的 DNS 服务器地址,在此例中也就是 dns-a.tsinghua.edu.cn。

考虑第一个命令:

```
nslookup www.tsinghua.edu.cn
```

简单地说,该命令表示的意思是“请发给我 www.tsinghua.edu.cn 的 IP 地址”。如图 6.1 所示,该命令的运行结果提供了两条信息:

- (1) 提供该结果的 DNS 服务器的名字和 IP 地址;
- (2) DNS 服务器主机的名字和 IP 地址。

该结果来自清华大学的本地服务器,但也有可能该 DNS 服务器与其他 DNS 服务器反复进行了连接得到该结果,如教材第 2.5 节所述。

考虑第二条命令:

```
nslookup -type = NS tsinghua.edu.cn
```

```
C:\>nslookup www.tsinghua.edu.cn
Server: dns-a.tsinghua.edu.cn
Address: 166.111.8.28

Name: www.tsinghua.edu.cn
Address: 166.111.4.100
Aliases: www.tsinghua.edu.cn

C:\>nslookup -type=NS tsinghua.edu.cn
Server: dns-a.tsinghua.edu.cn
Address: 166.111.8.28

tsinghua.edu.cn nameserver = ns2.net.edu.cn
tsinghua.edu.cn nameserver = dns.tsinghua.edu.cn
tsinghua.edu.cn nameserver = dns2.tsinghua.edu.cn
tsinghua.edu.cn nameserver = ns2.cuhk.hk
dns.tsinghua.edu.cn     internet address = 166.111.8.30
dns2.tsinghua.edu.cn   internet address = 166.111.8.31
```

图 6.1 nslookup 命令查询结果

在这条命令中,指定了 nslookup 的可选参数“-type = NS”以及域名“tsinghua. edu. cn”。此时 nslookup 命令给本地默认 DNS 服务器发送了查询 type-NS 记录的请求。简单地说,该命令表示的意思是“请发给我 tsinghua. edu. cn 的权威 DNS 的主机名”。(如果没有指定-type 参数,nslookup 利用其默认值查询 type A 的记录,参考教材第 2.5.3 节。)该命令的结果首先显示了提供该结果的 DNS 服务器以及四个 tsinghua 名字服务器,其中每一个服务器都是为清华大学校内主机提供服务的权威 DNS 服务器。最后该结果显示了清华大学校内权威 DNS 的 IP 地址。

## 2. ipconfig

ipconfig 对主机中 DNS 信息的管理也是有用的命令。在教材第 2.5 节中提到最近获取的 DNS 记录将保存在主机的缓存中,运行下面的记录可以查看这些缓存中的 DNS 记录:

```
ipconfig /displaydns
```

该命令显示剩下的 TTL。清空 DNS 缓存,运行以下命令:

```
ipconfig /flushdns
```

该命令清空 DNS 缓存中的所有记录。

### 3. 利用 Wireshark 跟踪 DNS

任务 1：熟悉 nslookup 和 ipconfig 两个命令后，首先来捕获正常浏览网页时生成的 DNS 数据包(DNS\_default\_test1.pcap)。

- (1) 用 ipconfig 命令清空 DNS 缓存。
- (2) 打开浏览器清空浏览器缓存(以 IE 浏览器为例，打开菜单栏中的工具→Internet 选项，选择删除文件)。
- (3) 打开 Wireshark 在过滤器中输入“ip. addr == 你的 IP 地址”。该过滤器隐藏了由其他主机发出或获取的数据包。
- (4) 开始抓包。
- (5) 在浏览器中打开网页：<http://www.baidu.com>。
- (6) 停止抓包。

回答下面的问题：

- (1) 观察 DNS 查询和回答数据包。发送的是 UDP 还是 TCP 包？
- (2) 该 DNS 查询数据包的目的端口号是什么？DNS 回答数据包的源端口号是什么？
- (3) DNS 查询数据包发送给了哪个 IP 地址？利用 ipconfig 来确定本地 DNS 服务器的 IP 地址，这两个地址是同一个吗？
- (4) 观察 DNS 查询数据包。该 DNS 查询是什么类型(Type)的？该数据包含有查询结果(answer)信息吗？
- (5) 观察 DNS 回答数据包。该数据包提供了多少个结果(answer)？每个结果包含什么信息？
- (6) 观察主机发送的子序列 TCP SYN 数据包。SYN 数据包的目的地 IP 地址与 DNS 回答数据包中的 IP 地址有对应的吗？
- (7) 该网页含有图片。在获取每个图片前，主机发出了新的 DNS 查询请

求了吗？

任务 2：下面分析 DNS 数据包：(DNS\_default\_test2. pcap)。

- (1) 开始 Wireshark 抓包。
- (2) 运行

```
nslookup www.tsinghua.edu.cn
```

- (3) 停止抓包。

回答下面的问题：

(1) DNS 查询数据包的目的端口号是什么？DNS 回答数据包的源端口号是什么？

(2) DNS 查询数据包发送给了哪个 IP 地址？与本地 DNS 服务器的 IP 地址是同一个吗？

(3) 观察 DNS 查询数据包。该 DNS 查询是什么类型(Type)的？该数据包含有查询结果(answer)信息吗？

(4) 观察 DNS 回答数据包。该数据包提供了多少个结果(answer)？每个结果包含什么信息？

- (5) 请提供类似图 6.2 的抓包截屏图。

任务 3：运行 nslookup -type = NS tsinghua.edu.cn，重复上述实验：(DNS\_default\_test3. pcap)。

回答下面的问题：

(1) DNS 查询数据包的目的端口号是什么？DNS 回答数据包的源端口号是什么？

(2) DNS 查询数据包发送给了哪个 IP 地址？与本地 DNS 服务器的 IP 地址是同一个吗？

(3) 观察 DNS 查询数据包。该 DNS 查询是什么类型(Type)的？该数据包含有查询结果(answer)信息吗？

- (4) 观察 DNS 回答数据包。回答数据包所提供的哪个 tsinghua 名字服

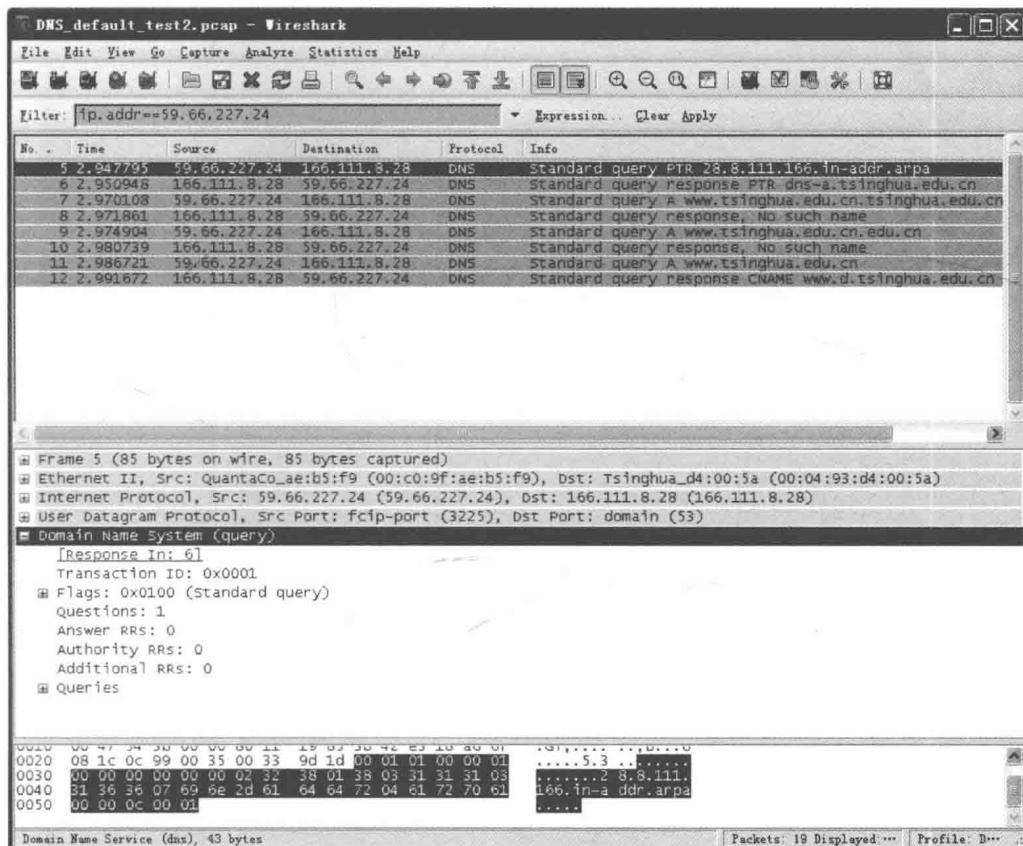


图 6.2 DNS 数据包捕获结果

务器？该回答服务器提供了 tsinghua 服务器的 IP 地址了吗？

(5) 请提供抓包的截屏图。

## 实验七

# Socket编程实现网络通信



## 7.1 实验目的

掌握 Socket 编程思想,并实现简单的 Socket 应用的连接通信过程。

## 7.2 实验要求

- (1) 编程语言: 使用 Java 编程语言进行 Socket 编程。
  - (2) 基本要求: 实验要求定位在调试“半成品”Java 程序, 即给出基本程序, 仅在部分地方需要同学加入自己的内容, 分析实验现象, 完成实验思考题。
  - (3) 时间要求: 建议同学们在课前将程序准备充分, 争取在课堂快速通过检查。
  - (4) 课后须提交任务清单。
- 几个程序:
- 不带服务器身份验证的 Simple SMTP 的 Java 程序 (SMTPSender.java);

- 课后需作的带服务器身份验证的 Simple SMTP 的 Java 程序 (AuthSender.java);
- 带自己注释的 UDP Pinger 的 Java 客户端程序(UDPClient.java)。

实验报告：包括实验现象，实验运行结果和实验思考题。

(5) 实验报告要求各部分内容完整，并总结通过该次实验所获得的经验和知识，另外也将关键代码及其注释张贴到报告中。

## 7.3 实验内容

本次实验主要做 Simple SMTP 和 UDP Pinger 程序的调试、分析和改进。

### 7.3.1 邮件发送客户端实验(Simple SMTP)

#### (1) 实验环境

安装配置了 Eclipse 的 Java 开发环境的联网计算机(具体请参见后面附录)。

#### (2) 实验任务

本实验要求按照 SMTP 通信协议(RFC2821)编写一个简单的邮件发送程序。实验采用学校的 SMTP 服务器(mails.tsinghua.edu.cn)作为邮件发送服务器。此次实验已经给出了程序的“半成品”，要求同学们先分析，读懂程序，然后添加必要的代码，程序即能运行。为了简化实验，本实验在课堂上不要求编写发送服务器验证需要身份验证的发送程序，这个留在课后完成，详情见后面实验思考题要求。需服务器身份验证要求加上 SMTP 扩充协议(RFC2554)进行用户信息验证。在不使用服务器身份验证的情况下，学校的 SMTP 服务器只能把邮件发送到同一个服务器上，而不能把邮件发送到其他服务器上。如服务器为 mails.tsinghua.edu.cn，则只能发送到 xx@mails.tsinghua.edu.cn 的邮件地址。

### (3) 实验要求

- 在给出的实验程序模板上填上相应的端口和命令,完成程序的调试。
- 把邮件发送到自己校内邮箱内,并把程序的结果(包括控制台输出的信息和邮箱里面显示的邮件信息)复制到实验报告上。调试程序成功后,找助教老师验收。
- 完成课后思考题。

### (4) 课上检查内容

看程序运行结果是否正确(参考后面实验结果部分)。

### (5) 附录

邮件发送的命令可以参考教材第 78 页。按照书上的发送方式即可。值得注意的是在 DATA 命令之后,需要增加一些命令以保证邮件信息的完整性,首先是 DATE 命令,指定邮件发送的日期,这个程序会自动生成,不需要编程工作。另一个 From:< mail address >和 To:< mail address >命令,指定了邮件里显示收件人和发件人的邮箱地址。然后可以再加上 Subject 命令用以指定邮件的主题,后面流程跟书上一样,不再详述。以下是上述命令的工作流程。以下 S 代表 Server,C 代表 Client,//为注释。此流程仅供同学理解 Simple SMTP 程序的工作过程。

输入 DATA 命令后:

```
C: DATA
S: 354 Start mail input; end with < CRLF >.< CRLF >
//DATE 命令.格式 DATE: < date >
C: DATE: Saturday, May 12, 2007 11:51:22 PM CST
From:abc@hey.com //From 命令.格式 From:< mail address >
To:addrMayDiffer@computer.networking //To 命令.格式 To:< mail address >
SUBJECT:Test msg //Subject 命令.格式 Subject:< subject >
//正文 ...
//内容结束符
S: 250 Requested mail action okay, completed. Message - ID = < vC929487764871. 19081 @
mail3 >
C: QUIT //退出
S: 221 mails.tsinghua.edu.cn closing connection.
```

### 7.3.2 课后完成内容：带身份验证的 Simple SMTP

参考 RFC2554 扩展协议, 实现发送服务器的身份验证功能。因为只有采用了身份验证, 才能把邮件发送到 mails. tsinghua. edu. cn(如果用 mails. tsinghua. edu. cn 发送信件)其他的邮件服务器由于登录注销需要涉及 Base64 编码, Java 内提供了相应的类进行处理。

sun. misc. BASE64Encoder 提供了相应的 encode 方法, 把字符串流转换成基于 Base64 编码的字符串。只要 import 该类, 再进行相应的操作即可。

示例代码：

```
BASE64Encoder encoder = new BASE64Encoder();
String encodedStr = encoder.encode("sample string".getBytes());
```

验证部分加在 Hello 命令的响应之后, 验证后可以发送到校外邮件, 详细要求请见后面思考题, 并把输出信息(包括控制台输出信息和邮箱内的邮件信息)复制出来, 加到实验报告内。

### 7.3.3 UDP Ping 实验

#### (1) 实验任务

运行已给的 UDP Pinger 的客户端和服务器程序, 分析实验现象, 思考本程序与 Windows 自带的 ping 程序的异同。实验给定的 UDP Pinger 的客户端和服务器程序都是可以完整运行的, 不需要同学修改什么。同学需要在运行之后, 仔细观察实验结果, 并一点一点读懂程序, 对关键的需要注释的地方(助教老师已经在程序中做了说明, 共 5 处), 给出自己分析的代码的作用, 写到注释中。在运行的过程中, 两个同学一组(可以自己组合, 最好相邻同学), 一位运行客户端, 一位运行服务器端, 观察实验现象。完成课后思考题, 并比较本程序与 Windows 自带的 ping 程序的异同。

### (2) 实验要求

- 读懂并运行已给的 UDP Pinger 程序, 观察实验现象。
- 对程序中需要加注释的代码部分, 仔细分析其在程序中的作用, 在注释处给出自己的分析结果, 并将这些内容粘贴到报告中。
- 完成课后思考题。

### (3) 检查内容

此为课堂选作内容, 课上如果完成, 可以请助教老师验收, 主要看实验是否调通, 注释是否正确。

## 7.4 注意事项

(1) 实验前做好准备工作, 课前认真阅读课本 2.4 节, 理解 SMTP 原理。

(2) 实验前, 认真阅读课本 2.7.2 节, 理解 TCP 编程原理。

(3) 实验前, 认真阅读课本 2.8 节, 理解 UDP 编程原理。

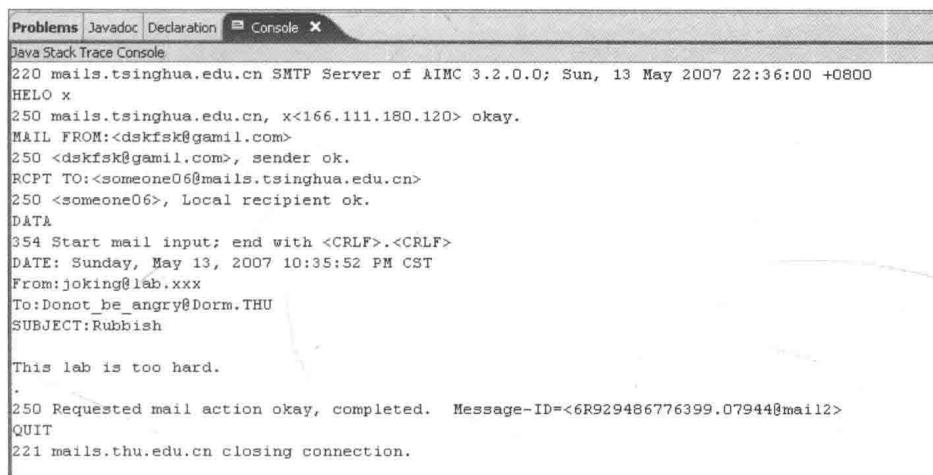
(4) 本实验要求编程环境统一为 Java 环境, 后面附录里有如何配置的情况, 同学请遵照附录情况进行配置, 以免带来版本问题的麻烦。其中软件可以从网络学堂上下载。对 Java 编程了解不深的同学, 附录是不错的手把手入门教程, 希望多投入一些时间学习, 也可以请教有经验的同学。

(5) 实验报告要求各部分内容完整, 并总结通过该次实验所获得的经验和知识。

(6) 大家可以互相讨论, 但严禁复制代码, 一经发现抄袭者和被抄袭者将严肃处理!

## 7.5 实验结果

对于不带身份验证的 Simple SMTP 实验, 控制台输出的结果如图 7.1 所示。同学不一定要得出相同的结果, 只要程序正确运行, 功能实现即可。



```
220 mails.tsinghua.edu.cn SMTP Server of AIMC 3.2.0.0; Sun, 13 May 2007 22:36:00 +0800
HELO x
250 mails.tsinghua.edu.cn, x<166.111.180.120> okay.
MAIL FROM:<dskfsk@gamil.com>
250 <dskfsk@gamil.com>, sender ok.
RCPT TO:<someone06@mails.tsinghua.edu.cn>
250 <someone06>, Local recipient ok.
DATA
354 Start mail input; end with <CRLF>.<CRLF>
DATE: Sunday, May 13, 2007 10:35:52 PM CST
From:joking@lab.xxx
To:Donot_be_angry@Dorm.THU
SUBJECT:Rubbish

This lab is too hard.

250 Requested mail action okay, completed. Message-ID=<6R929486776399.07944@mail2>
QUIT
221 mails.thu.edu.cn closing connection.
```

图 7.1 不带身份验证的 Simple SMTP 实验结果

## 7.6 实验思考与分析题

- (1) 实验报告中提交完整的程序代码(前面提到过),完成必要的注释。
- (2) 记录实验结果,讨论实验现象:
  - Simple SMTP 程序和常用的 E-mail 客户端在功能、结构上的比较;
  - UDP Pinger 与 Windows 自带的 ping.exe 程序在功能、协议和输出结果上的比较。
- (3) 课后完成对 Simple SMTP 的改进,提交具有进行身份验证功能的改进版 SMTP 程序代码。随实验报告上交 Java 代码,根据代码本身和收到的 E-mail 判断是否正确添加身份认证功能。

规定: subject 内容为“Simple SMTP”。

邮件正文的内容:

“Hi TA

I am very glad to inform you that I successfully complete the Simple SMTP with authentication.

I am XXX. My studentID is XXXXXXXX. ”。

发送完成,提交程序清单时,考虑到个人隐私问题,同学可以把代码中的“User/Password”用“XXXX/XXXX”代替。

(4) 针对程序调试中出现的问题及解决办法,写出实验体会。

## 7.7 附录：配置实验环境

### 7.7.1 配置 Java 运行环境

先从网络学堂下载所需的文件,包括:

- 执行 Java 应用程序的 Java Runtime Environment (JRE): jre-6u1-windows-i586-p. exe;
- 编辑环境 Eclipse IDE: eclipse-SDK-3.2.2-win32. zip;
- 可选的 Java API 文档: j2se6\_documentation. zip。

其中第三个为 Java 6.0 的 API 文档,用来查阅各个类的方法及属性,对编程没有影响。

下载完成后先安装 JRE,执行 jre-6u1-windows-i586-p. exe 安装程序,完成后就可执行 Java 应用程序。之后解压 eclipse-SDK-3.2.2-win32. zip,执行文件夹内的 eclipse. exe 即可运行 Eclipse,运行后它会询问你设置工作目录 workspace,就是存放工作时源代码及其他相关文件的目录,按喜好指定一个,单击 Ok 按钮即可。

### 7.7.2 在 Eclipse 中开发 Java 程序

打开程序后界面如图 7.2 所示,先关闭 Welcome 标签页。

在建立 Java 程序前先要创建 Java 项目,以下以图示的方式讲述如何运行简单的 Hello 程序。



图 7.2 Eclipse 欢迎界面

### (1) 新建 Project

在菜单中选择 File→New→Project, 如图 7.3 所示。

### (2) 选择 Java Project, 单击 Next 按钮, 如图 7.4 所示。

(3) 输入 Project 名字, 这例子中设为 HelloWorld, 之后单击 Finish 按钮即可, 如图 7.5 所示。

### (4) 在菜单中选 File→New→Class, 如图 7.6 所示。

(5) 在 Name 中输入类的名字, 然后单击 Finish 按钮, 如图 7.7 所示。

### (6) 在 HelloWorldNTimes 中输入如下程序代码, 如图 7.8 所示。

(7) 输入完成后, 在右边的 Package Explorer 中右击, 选 Run As→Java Application 执行程序, 如图 7.9 所示。

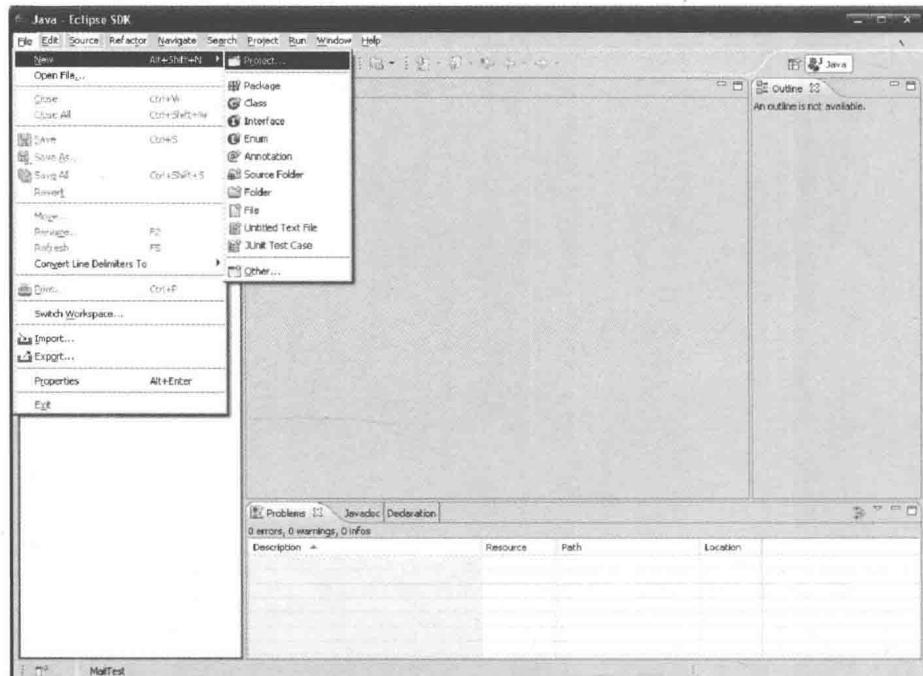


图 7.3 新建工程

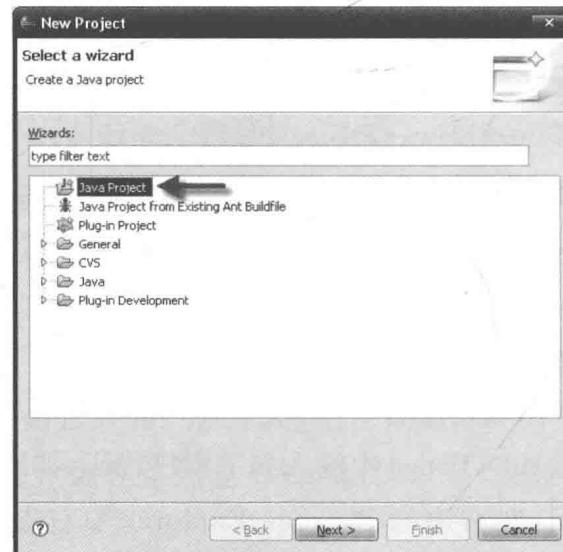


图 7.4 选择工程类型

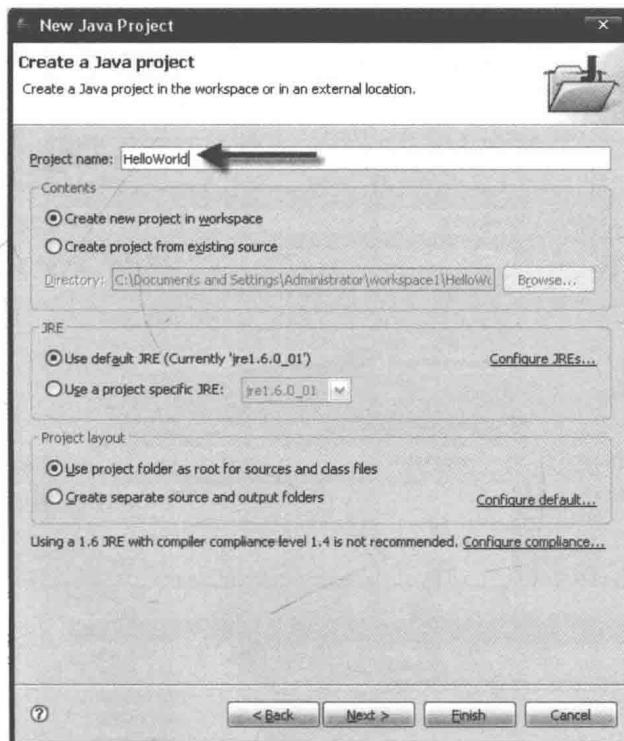


图 7.5 工程相关信息填写

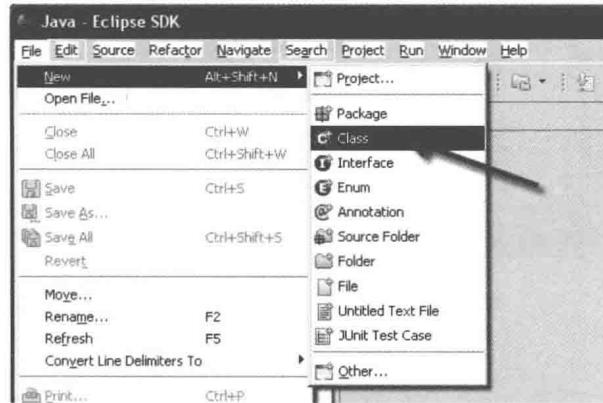


图 7.6 新建类

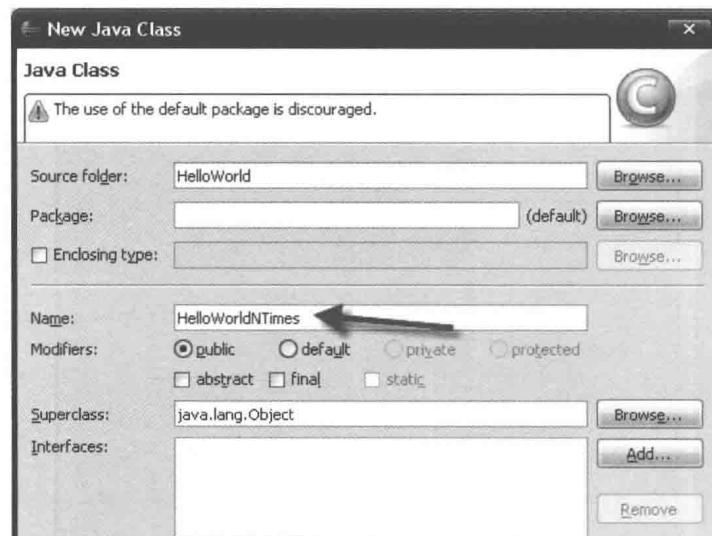


图 7.7 类信息填写

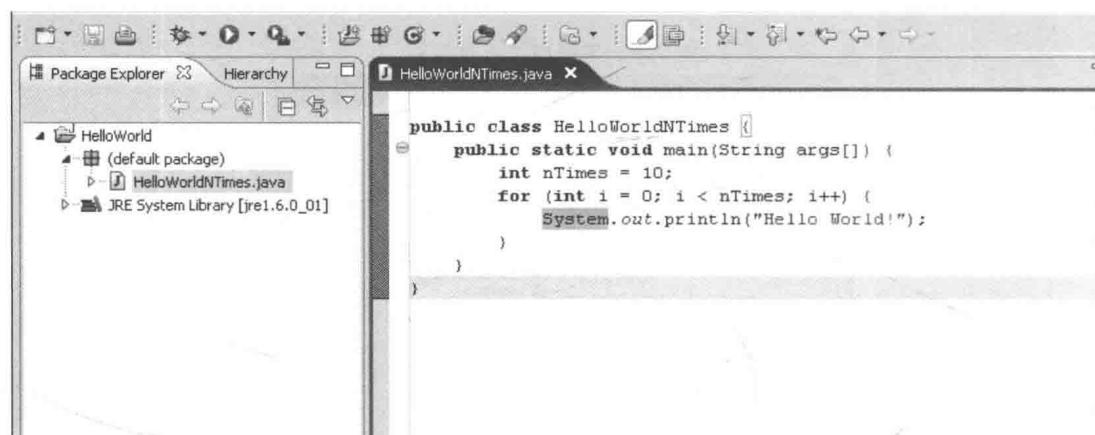


图 7.8 代码输入

(8) 结果输出在 Console 中,如图 7.10 所示。

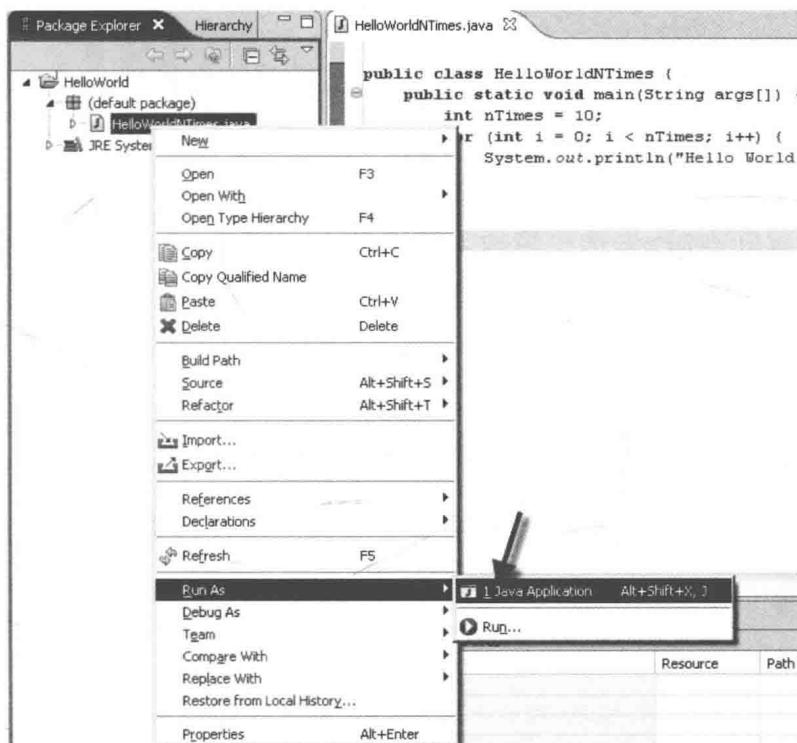


图 7.9 程序执行



图 7.10 控制台输出

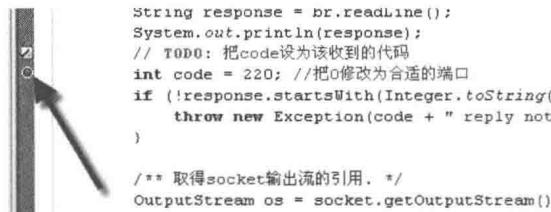
### 7.7.3 在 Eclipse 中使用调试器

Eclipse 中的调试器十分强大,除了可以帮助找出程序出错原因外,还可以帮助了解程序的运行过程。

进行调试时要先设置断点,设置方法有几种。

(1) 设置断点时,先选中想插入断点的行,然后:

① 如图 7.11 所示的第 3 行,然后在该行最前端的位置(如图中箭头所指的位置),双击鼠标。



```

String response = br.readLine();
System.out.println(response);
// TODO: 把code设为该收到的代码
int code = 220; //把0修改为合适的端口
if (!response.startsWith(Integer.toString(code))) {
    throw new Exception(code + " reply not received from server.");
}

/** 取得socket输出流的引用. */
OutputStream os = socket.getOutputStream();

```

图 7.11 断点插入

② 选中菜单中的 Run→Toggle Line Breakpoint,如图 7.12 所示。

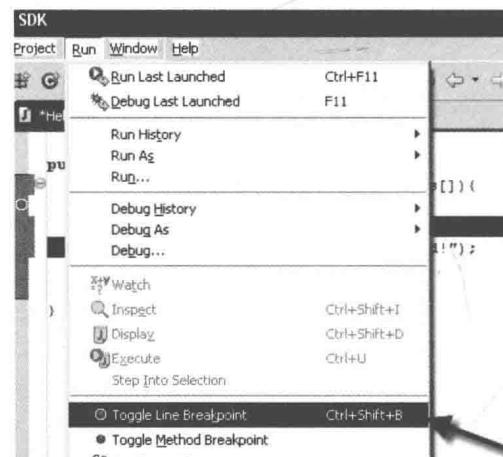


图 7.12 断点设置

(2) 执行程序,与运行程序相似,不过这次选中期望执行的程序右击后选

Debug As→Java Application, 如图 7.13 所示。



图 7.13 执行程序

然后出现 Save and Launch 窗口, 单击 Ok 按钮即可。接着会弹出询问转换视图(Perspective)的对话框, 单击 yes 按钮即可。Perspective 是 Eclipse 的特色之一, 如图 7.14 所示。它能够切换到不同的布局, 方便使用。

**注意:** 若没有自动切换视图, 可在菜单上选择 Window→Open Perspective→Other...之后在弹出的窗口中选 Debug, 再单击 Ok 按钮即可。

(3) 执行语句时, 使用图 7.15 的执行控制器, 其中绿色的 Play 按键为继续执行, 红色的 Stop 为停止。图 7.15 的 1, 2, 3 分别对应 Step Into, Step Over 和 Step Return 3 种执行方式。

Step Into 为程序单步运行, 遇到其他方法调用时, 跳转到被调用方法内部继续执行。

Step Over 也是单步运行, 但在遇到方法调用时, 不跳转到方法内部执行, 而是执行整句完整语句。

Step Out 主要是配合 Step Into 使用, 当 Step Into 到某个被调用的方法

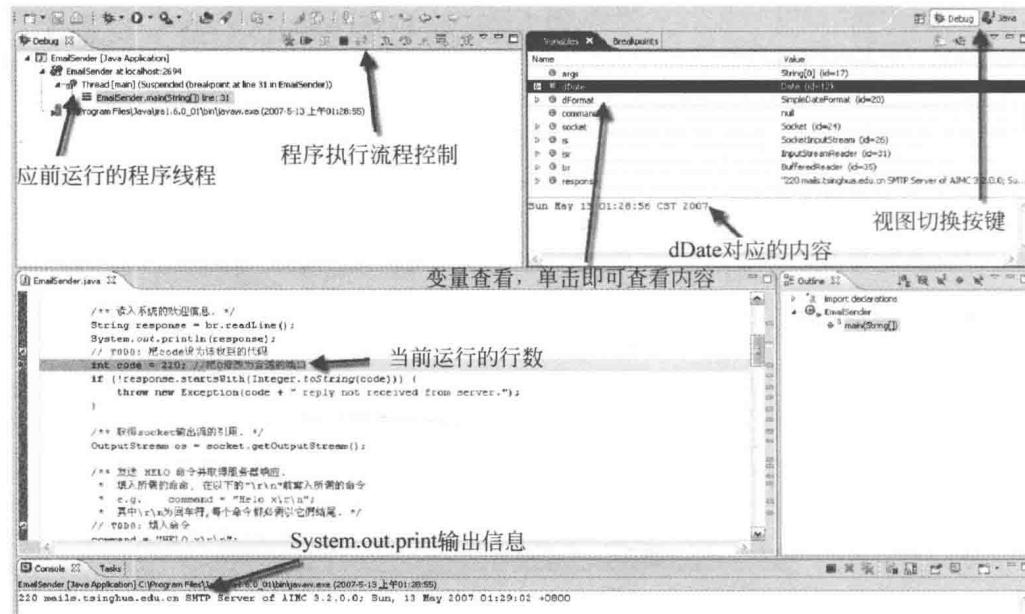


图 7.14 Eclipse 的视图窗口界面

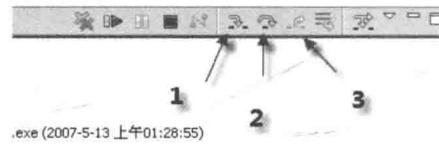


图 7.15 程序运行状态的控制

内,一步一步地执行该方法可能会花费大量的时间,此时可使用 Step Out 跳出。

**注意:**由于这次实验较为简单,几乎没有什么方法调用,有需要调试,为了免去不必要的麻烦,建议只使用 Step Over 按键。

(4) 程序按以上步骤单步执行下去,不想执行时单击图 7.15 中红色的 Stop 按键即可。