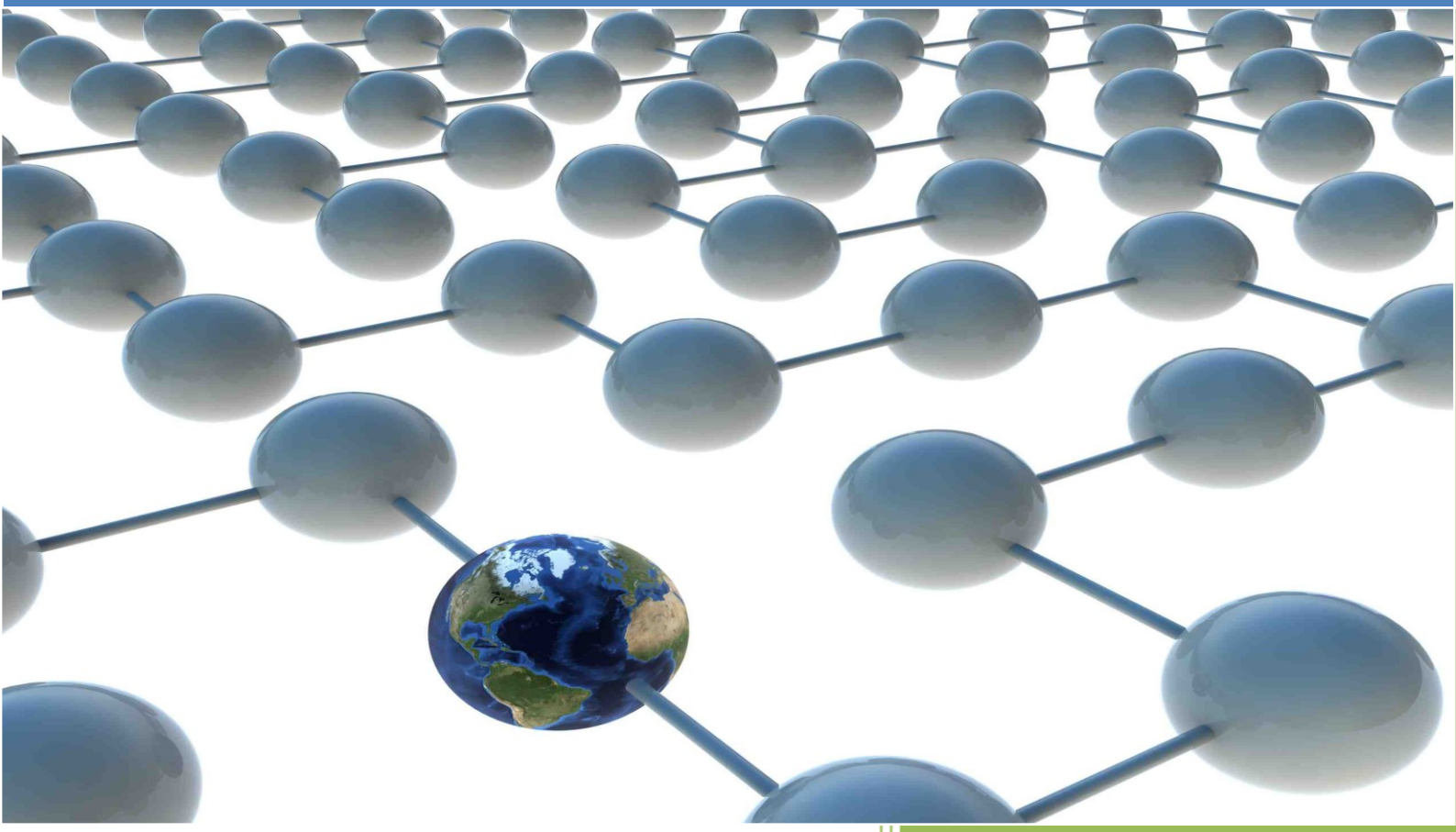
2013 版

计算机网络与应用

实验指示书



清华大学自动化系

目 录

前　　言

实验安排说明

结合我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. 在实验室进行的实验，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。

实验一　基本网络操作命令

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。

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 WINDOW XP 操作系统，Windows 7 下基本兼容；WIN98、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）。

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，确定本机和相邻微机的 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，察看本机、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、邻居微机、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；

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. 察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：
   a) 实验环境，包括网络环境和微机环境；

b) 实验内容及主要结果；

c) 回答实验思考中的问题；

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？

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。该参数可以禁用配置为自动获取 IP 地址的适配器的 TCP/IP
/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 *Adapter* [*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，并打印发送和接收把报文的数量。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：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 命令具体使用

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。该包将不被路由上的网关分段。
-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邮票。
-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* 或者键入 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，请在命令提示行键入：

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，请在命令提示符处键入下列内容：

tracert -d www.sina.com

利用“tracert 目的地址”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 cashe？

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 为目标地址，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，目标地址为 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，既可以又动态表项，也可以有静态表项。通过 arp－s net_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 Win7 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	计算机名/IP|*(广播) 传送内容，注意不能跨网段
net stop messenger	停止信使服务，也可以在控制面板－服务修改
net start messenger	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帐号列表 net user
3) 查看网络链接 net use

记录链接 net session

例如：C:\>net session

实验二 常用网络服务的配置

2.1 实验简介

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。

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；

实验环境

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

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

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 DN 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？

附：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，除了必需运行 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(RR，Resource Record)，资源记录是区域数据库文件中的条目。常用的资源记录有：

- A(Address，主机地址)：用于将域名映射到计算机使用的 IP 地址
- CNAME(Canonical Name，规范名称)：用于将 DNS 域名的别名映射到另一个主要的或规范的名称。
- MX(Mail eXchange，邮件交换器)：用于将 DNS 域名映射为交换或转发邮件的计算机的名称。

- NS(Name Server，名称服务器)：为区域中的授权 DNS 服务器指派 DNS 域名。
- 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) “开始”/“设置”/“控制面板”/“添加/删除程序”，在“组件”列表中选择“网络服务”。

(2) 鼠标点击“详细信息”，选中“域名系统（DNS）”，如图 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。

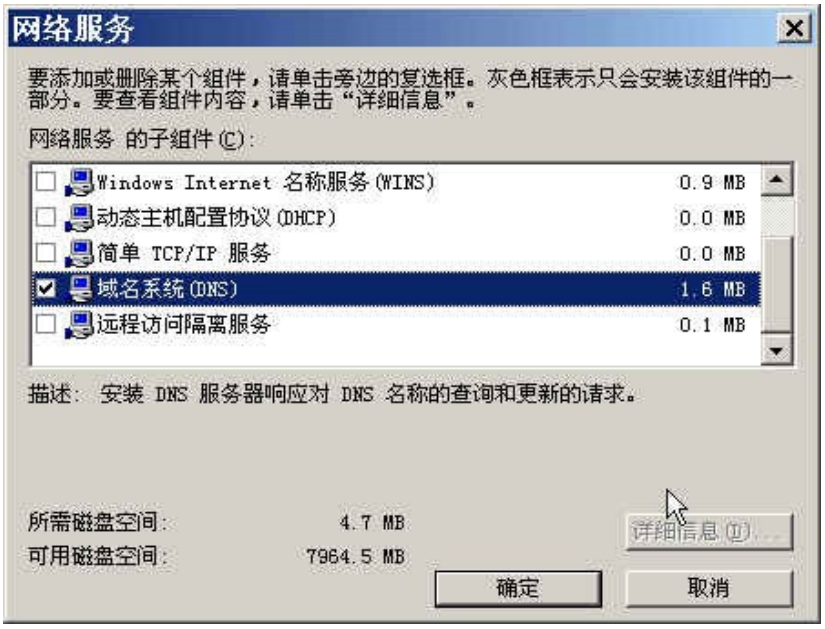


图 1 “Windows 组件向导”对话框和“网络服务”对话框

2. 配置新的 DNS 服务器

(1) 单击“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“配置服务器”命令，如图 2 所示，打开“配置 DNS 服务器向导(欢迎)”对话框。

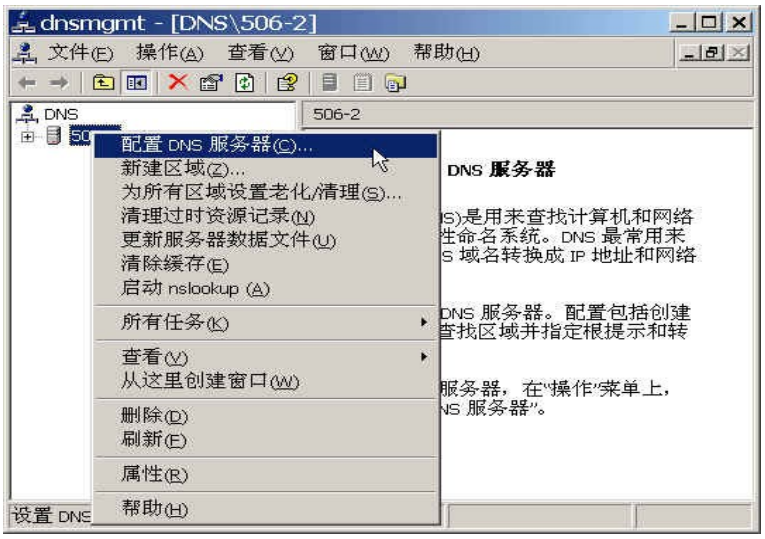


图 2 “DNS”控制台窗口

(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 3 所示。

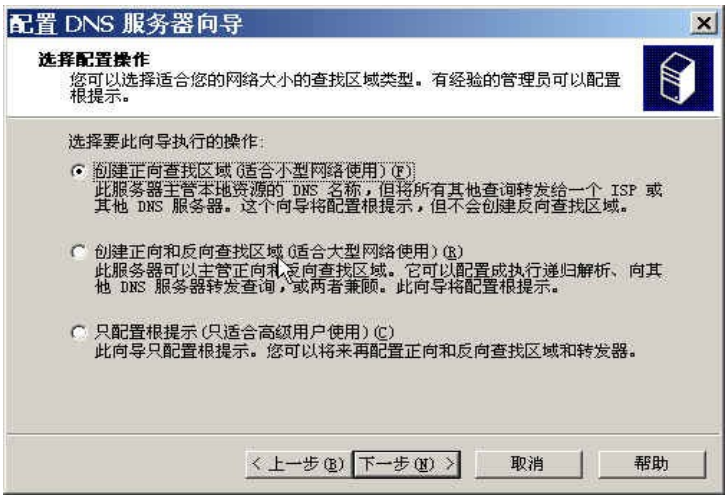


图 3 “配置 DNS 服务器向导—正向搜索区域”对话框

(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 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。

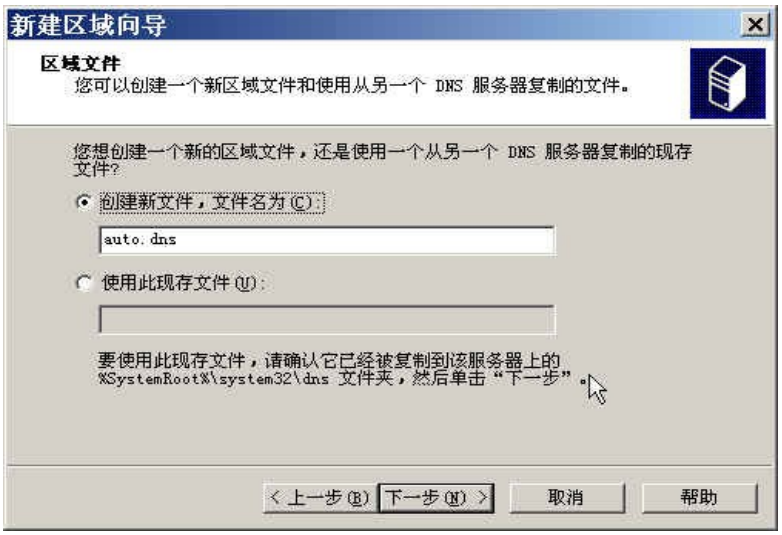


图 4 “区域文件”对话框

(6) 单击“下一步”，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”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 5 所示：起始授权机构(SOA)和名称服务器(NS)。

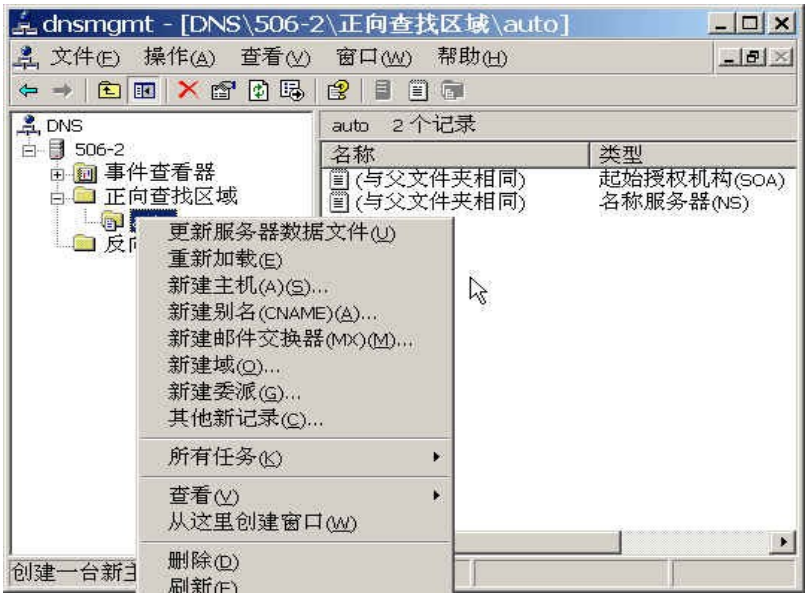


图 5 “DNS”管理控制台

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，单击“操作”菜单的“新建主机”命令，打开“新建主机”对话框。

② 在“名称”文本框中，键入新主机的 DNS 计算机名称 asp；在“IP 地址”文本框中，键入新主机的 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 6 所示。

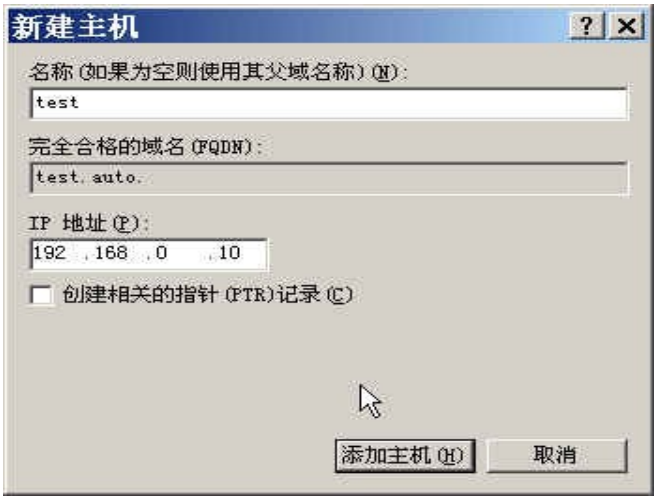


图 6　新建主机

(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 7-6-13 所示。

图 7　“DNS”管理控制台窗口

② 在“主机 ID 号”文本框中，输入主机的 IP 地址，如图 8 所示。

图 8 “新建资源记录”对话框

③ 在图 8 的“主机名”文本框中，键入 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-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。

(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。日志文件通常位于%systemroot%\System32\Dns 中，名为 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“自动获取 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 9 所示。

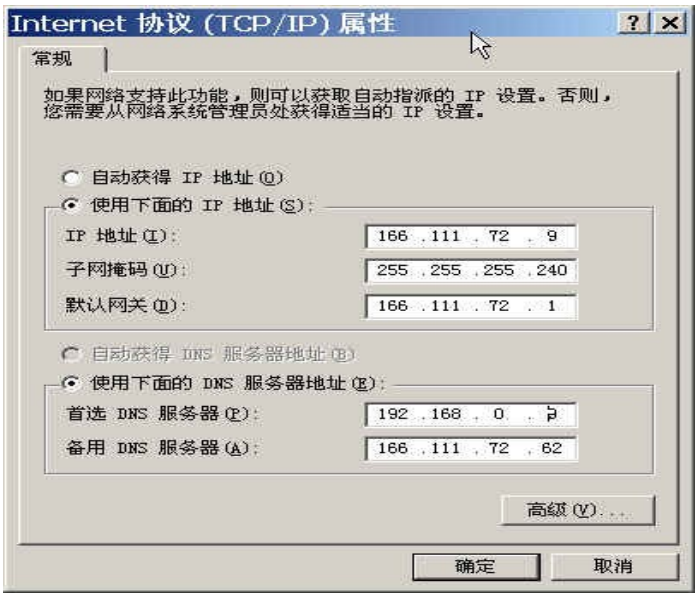


图 9 “Internet 协议(TCP/IP)属性”对话框

(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 10，能够正确解析 test.auto 为 192.168.0.10 。

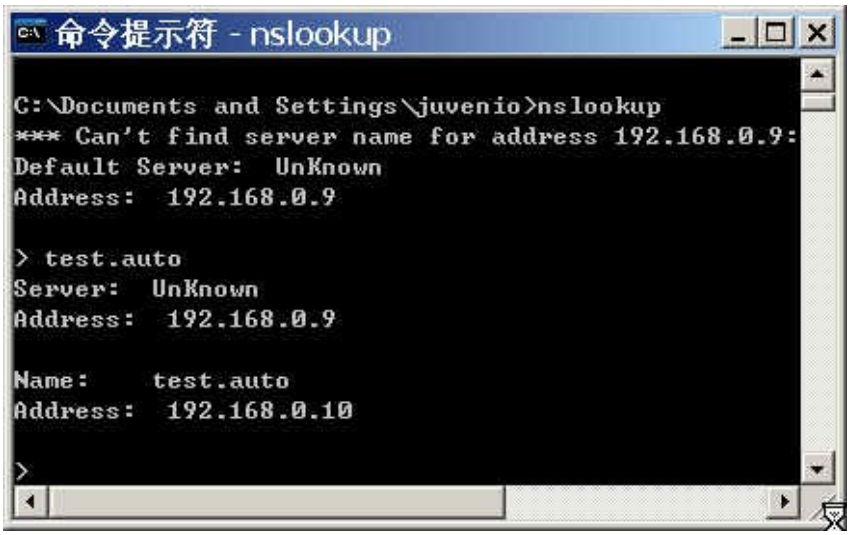


图 10 域名测试

2.3 用 Apache HTTP Server 开设 WWW 服务

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；

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

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

$myfile=fopen($c_file,"w"); //打开文件
fwrite($myfile,$t_num[0]); //写入新内容
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.

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 wingdows 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。

附：实验参考资料

1. Apache 服务器安装与配置

Apache 简介

Apache 是世界排名第一的 Web 服务器, 根据 Netcraft(www.netsraft.co.uk)所作的调查, 世界上百分之五十以上的 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, 以及其它的工作. 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"(MAYBE IT IS, MAYBE NOT):

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.[1]

校内很多的 web 站点都用这种方式开设服务。

获取 Apache

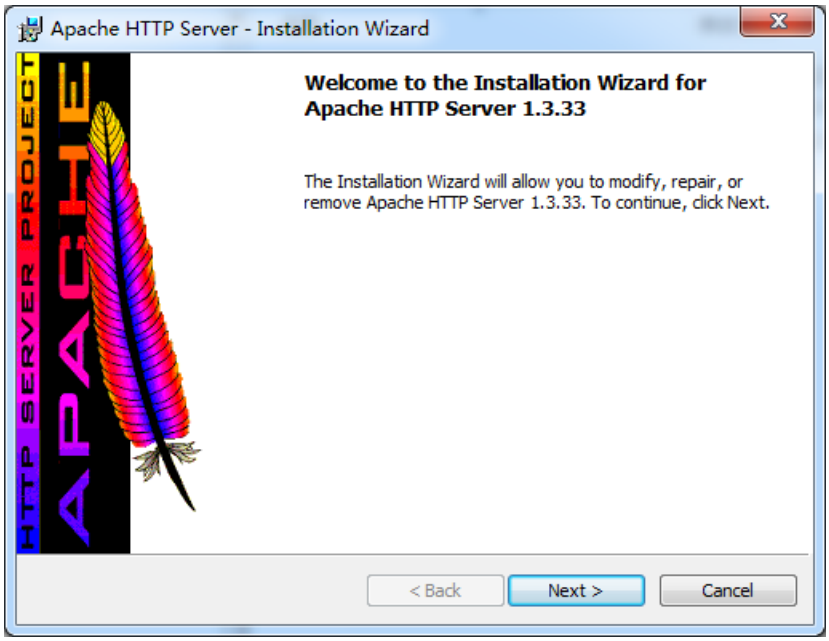
你可以直接从 Apache 的网站（http://www.apache.org）上下载 Apache 软件的 windows 版本，在 linux 或者其他 Unix 下面可以找到相应的二进制安装文件，或者直接下载源代码包进行编译安装。

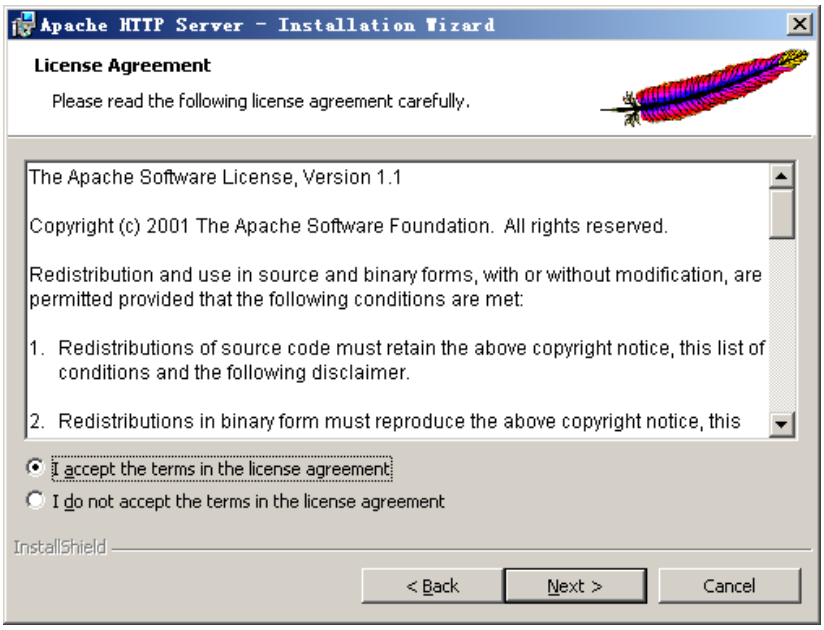
现在网络上能找到两类版本的 Apache 软件，版本号分别为 Apache1.3.xx 和 Apache2.0.xx，前者是从原来的 Apache 版本慢慢发展演变过来的，现在新出的版本大多是对原来版本的 bug 修改，因此是比较完善，几乎很难发现漏洞的版本。出于以上考虑我们选择 Apache1.3.xx 版本的 Apache HTTP Server 比较合适。

Apache 安装

以下以 Apache HTTP Server1.3.33 为例简要讲述 Apache 的安装过程。

Apache 的安装和其它 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。

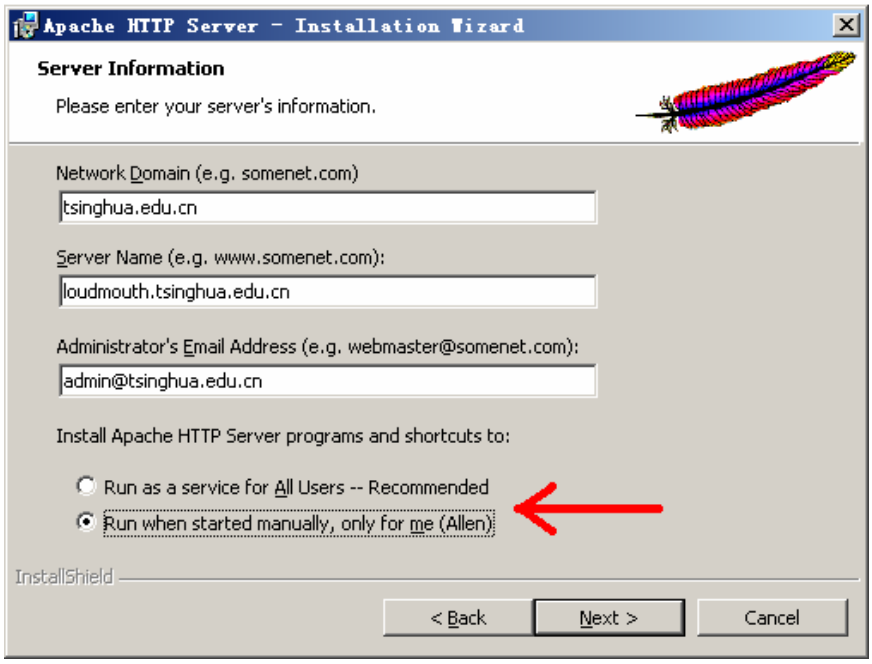




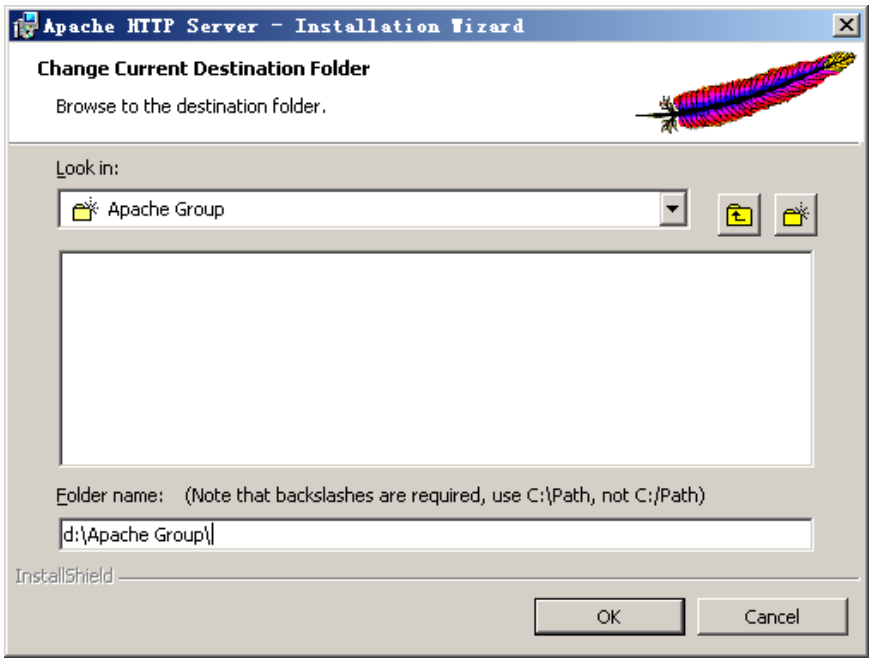
需要注意的是 Server Information 这一步，其中有一个运行方式的选项。

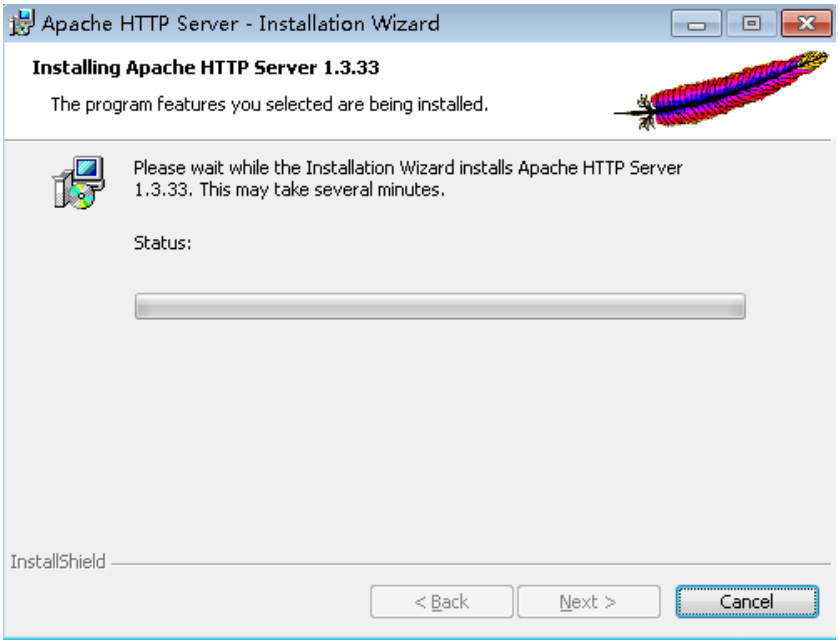
1、 作为一个 windows 的 service 来运行，这种方式下用户无须登陆 windows 启动 Apache 软件即可将 HTTP server 作为默认启动的服务运行，这个对于想长期开设 http 服务的用户来讲是必须的。

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 服务的话，那么可以选择手动启动的方式。这个实验中，我们应该选择**手动启动方式**。

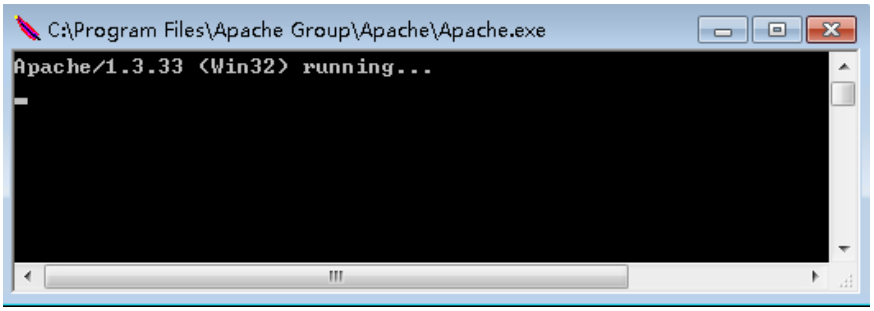


选择安装的目录之后就可以开始安装了。

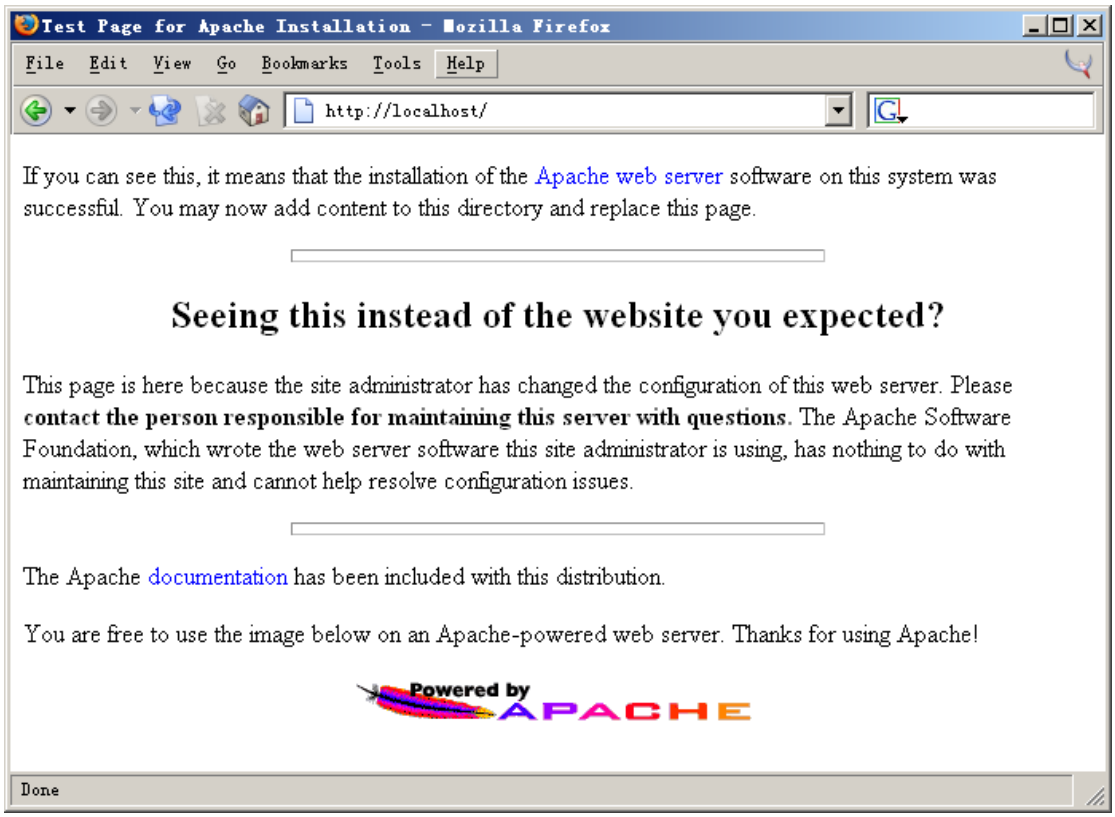




安装完成之后从程序菜单选择 Apache Http Server/Start apache in console 或者在 Apache Group\Apache 目录下双击打开 Apache.exe，就会弹出一个控制台窗口，显示 Apache/1.3.33（win32）running，表示 Apache 已经在后台运行了。



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，这说明 Apache 已经安装成功了。



发布自己的网页：

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 文件找到

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。此后的进一步配置管理。请参考[2].

2. PHP 的安装与配置

Php 简介

讲到 PHP 的全名就蛮有趣的，它是一个巢状的缩写名称，"PHP: Hypertext Preprocessor"，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 更快速的执行动态网页。PHP 最初是在公元 1994 年 Rasmus Lerdorf 开始计划发展。在 1995 年以 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 问市。第二版定名为 PHP/FI(Form Interpreter)。PHP/FI 并加入了 mSQL 的支援，自此奠定了 PHP 在动态网页开发上的影响力。在 1996 年底，有一万五千个 Web 站台使用 PHP/FI；在 1997 年中，使用 PHP/FI 的 Web 站台成长到超过五万个。而在 1997 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；加上它不断的更新及加入新的功能；并且它几乎支援所有主流与非主流资料库；再以它能高速的执行效率，使得 PHP 在 1999 年中的使用站台超过了十五万!!它的原始码完全公开，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，使得在程式设计方面有着更好的支援。

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更动，让程序的执行速度，满足更快的要求。在最佳化之后的效率，已较传统 CGI 或者 ASP 等程式有更好的表现。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，它将也是必修课程之一。 [3]

获取 php4

Php 的官方网站是 http://www.php.net，你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。我们以 php-4.4.6-Win32 为例来讲解 PHP 与 Apache 的。

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，我们可以在 d:\根目录下面新建一个 php 文件夹，将解压缩得到的文件拷贝到 php 文件夹下即可。

为了让 php 能够正常工作，我们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 目录下面找到，在这里，我们只介绍 php 与 apache 相互配合使用时的配置情况，需要其它类型的安装（php 与 IIS/PWS 等的配置，请参考此说明文档）

(1) 拷贝配置文件:

php 目录下面的 php.ini-dist 文件拷贝到 Windows 系统目录下面，一般来讲是 C:\WINDOWS（win95/98/xp）或者 C:\WINNT(win2000)目录，如果你在安装 windows 时使用了其它目录，那么就为你设置的那么目录。拷贝之后将文件名改为 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，将其修改为你 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?varible=value, 否则，你必须用 post 等其它隐式方式传递变量，因为这样相对来讲比较安全，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。

A．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，我们需要让 apache 知道在哪儿能够调用到它们.

方法是**将这两个文件拷贝到 apache 目录下面的 modules 子目录下.**

备注:

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拷贝到系统目录下面的 System32 文件夹下面;

二是可以将这两个文件拷贝到 apache 目录下面的 modules 子目录下;

三就是直接在配置文件中指定 php4apache.dll 的位置，但是必须拷贝一个 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，没有找到的话就会报错。

为了清晰方便，我们使用第二种方式。

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

拷贝完 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），我们在后面加入一行：

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

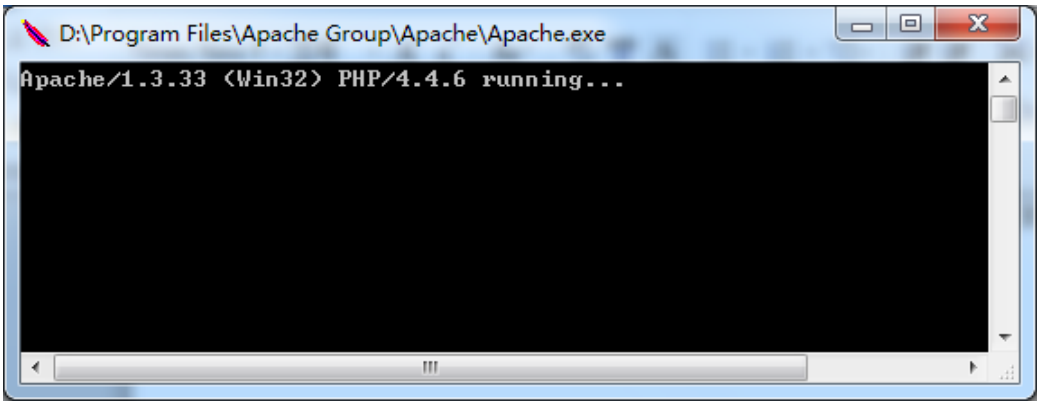
找到 AddType 部分，在后面添上：

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，如下图：



把准备好的 test.php 拷贝到 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 ，如果出现如下页面，表示配置成功。

用 Php 实现计数器和动态图片显示

根据 visitorcounter.php 中的提示，完成三个小任务

1. 必做：动态显示网页被访问次数
2. 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>";
3. 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

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

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。

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。

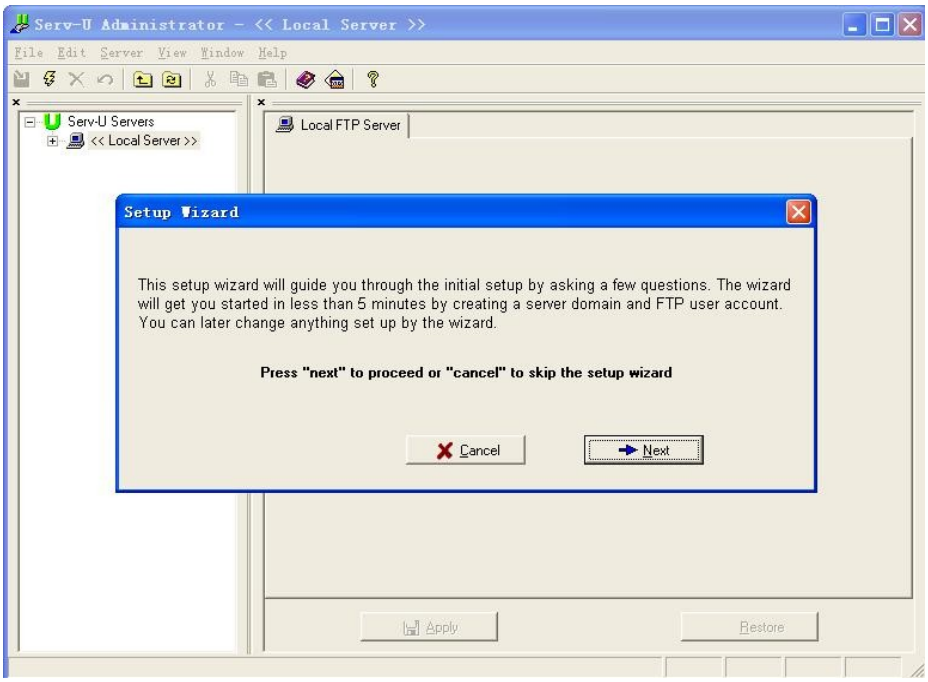
第一步：Serv-U 的下载和安装。

点击下载的 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，按“Next”完成每一步。安装完毕，在 Windows 的桌面上就出现 Serv-U 的图标，双击 Serv-U 图标，出现 Serv-U 主窗口，点击主界面右边窗口的“Start server”即可启动 FTP 服务器 。

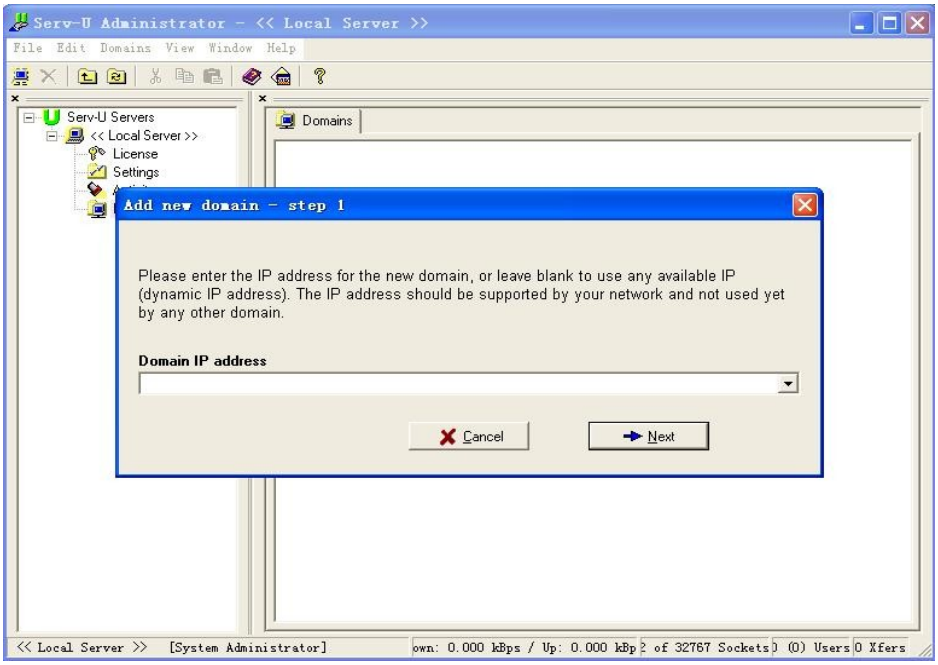
第二步：Serv-U 的配置。

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

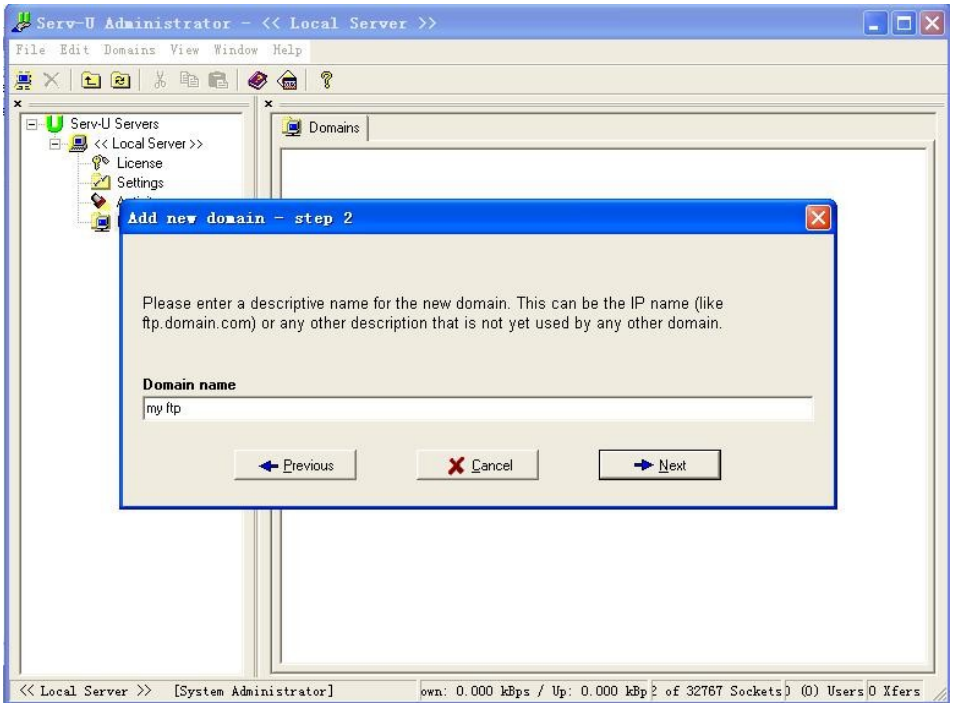
A.安装程序首先启动一个设置向导帮助你设置 FTP 服务器，点击“Next”继续。



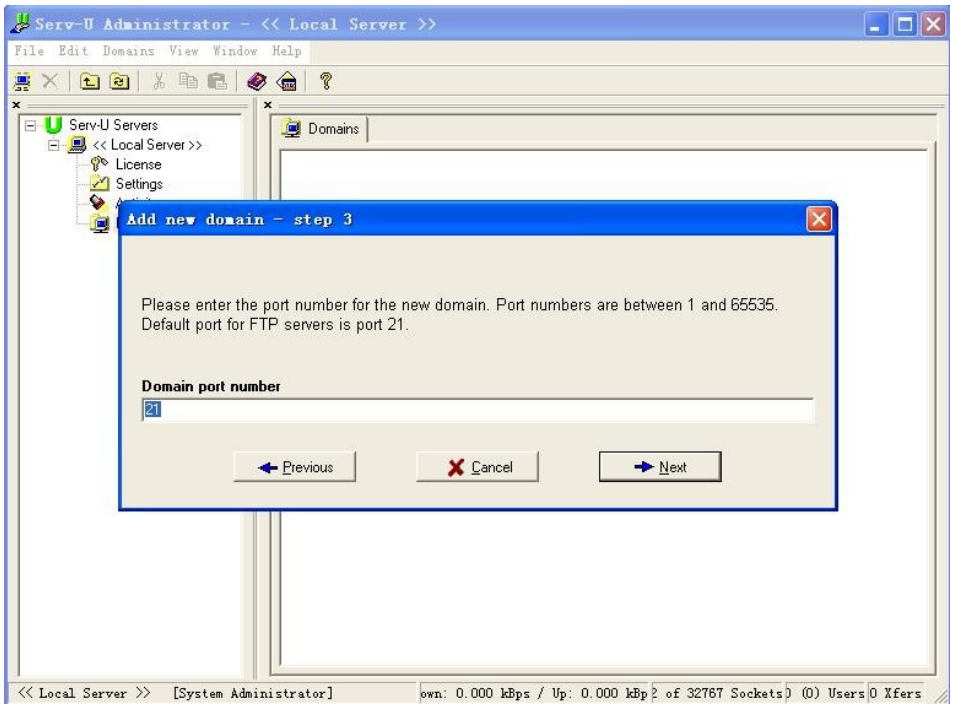
B.系统弹出输入 IP 的对话框，此项需要填入你准备为此 FTP 服务器绑定的 IP 地址。除非你的计算机有多个固定的 IP 地址，并且你只想其中一个被 FTP 服务器所使用，否则，建议不管你是否有固定的 IP 地址，都将此项保留为空（即让系统自动侦测），点击“Next”。



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



D.输入 FTP 访问的端口号，一般保持默认的 21 即可。



E.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帐号，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。

F.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，一般建议选是。

G.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，你的个人 FTP 就已经搭建完成了。不过这还只能实现 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。

A.对 FTP 用户的管理

欲增加一个新用户（包括增加 Anonymous 用户），则在 Serv-U 的一个域中选中 Users（用户），然后单击右键，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（如图 27）。

欲删除一个用户，则在此用户上单击右键，选 Delete User（删除用户）即可。

B.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（如图 28）。

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

C.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 处根据自己电脑的配置，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不完整文件。如果不要选中这项，就能让 Serv-U 支持断点上传功能（如图 29）。

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

实验目的

了解 DHCP 的含义及工作原理；

掌握 DHCP 服务器的安装与设置；

了解 DHCP 客户机的设置。

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。

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

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？在作保留 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，可以判断有什么问题？

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？

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中选择一个 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，如图所示。

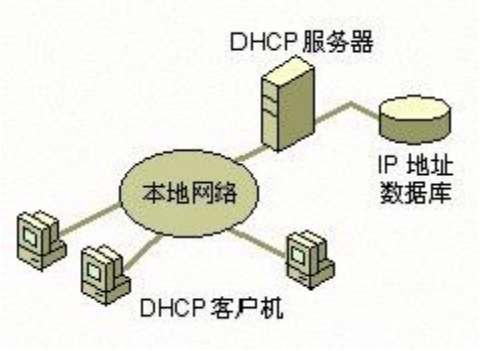


图 1 DHCP 的工作原理图

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，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 OFEER 信息直接送到客户机。DHCP OFEER 信息中包含了客户机的 MAC 地址，所提供 IP 地址，子网掩码以及 DHCP 服务器的 IP 地址。

DHCP 服务器发送 DHCP OFEER 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。

如果在一秒钟内 DHCP 客户机没有收到 IP 地址，就将 DHCPDISCOVER 消息重复广播四次，四次重试的间隔时间为 2、4、8、16 秒，另一次则在 0-1000 毫秒的随机时间。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 保留范围中采用一个 IP 地址。客户机仍将每隔五分钟尝试发现 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 OFEER 消息，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受的 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 DHCPREQUEST 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的客户。

图 2　获得租约要经过的四个步骤

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

在“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）”，按“确定”，接着按提示完成安装。

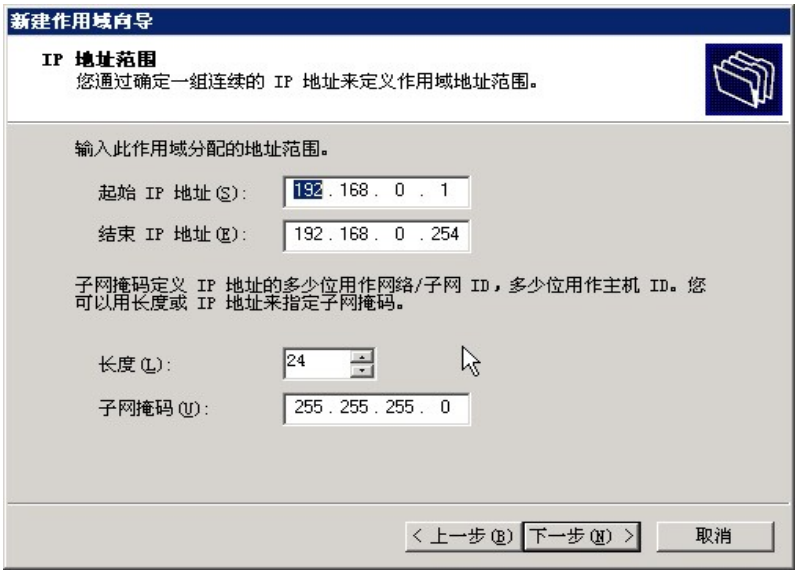
DHCP 服务安装结束之后，在“管理工具”中将出现“DHCP”命令项，并将自动建立一个默认的 DHCP 服务器。

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，在弹出的菜单中单击“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：

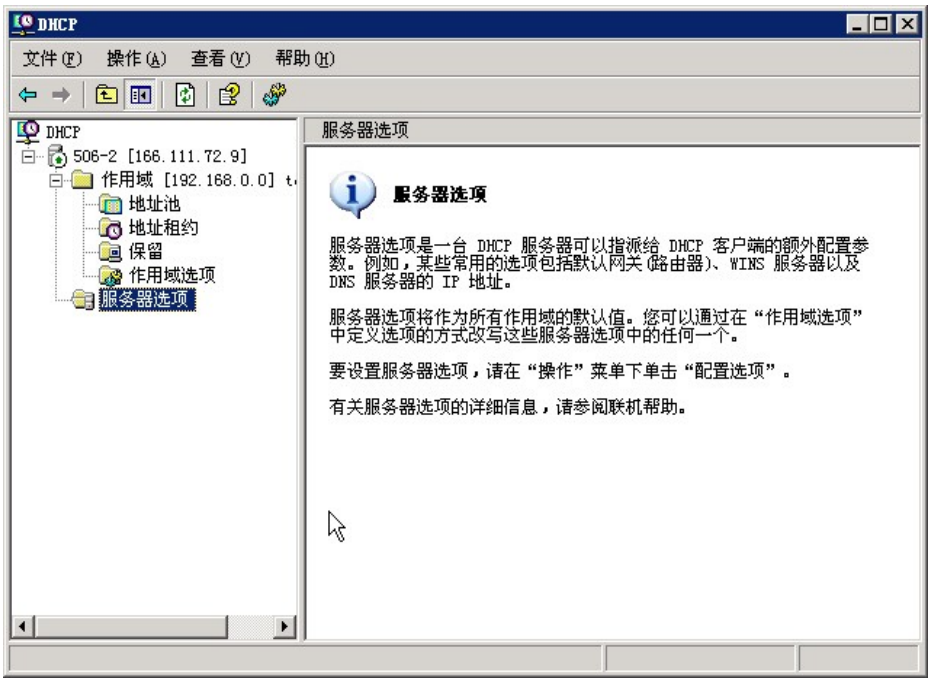
- 如图所示，设置 IP 地址范围 192.168.0.1～192.168.0.254 以及子网掩码 255.255.255.0，可包含排除的 DHCP 服务的 IP 地址:192.168.0.1～192.168.0.5
- 租约期限：默认的租约期是八天



(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，如下图所示：

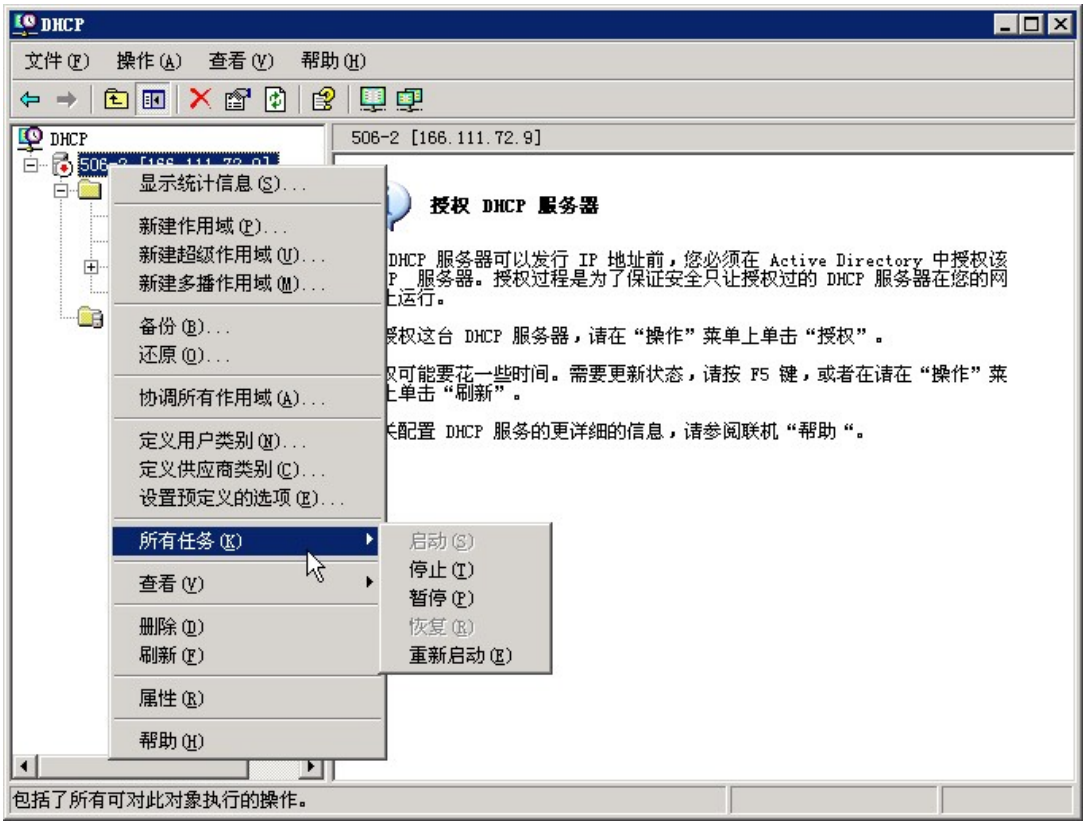


(3) 用户保留地址

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。如下图所示：



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”对话框中选择“自动获取 IP 地址”单选按钮，如图所示。

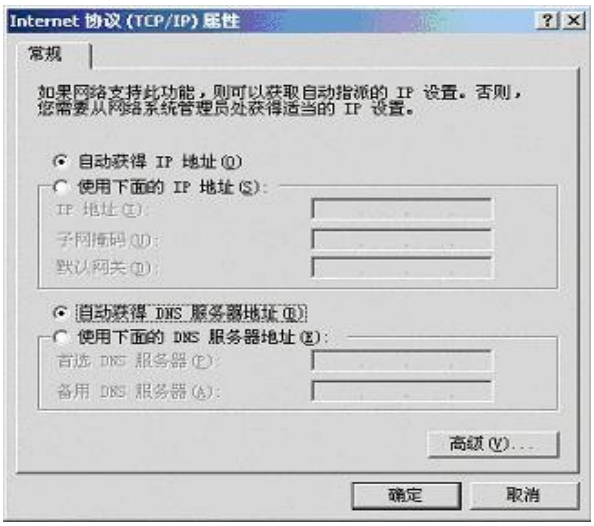


图 “Internet（TCP/IP）属性”对话框

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。

检查 DHCP 客户机租约状态信息，键入 ipconfig，或者键入 ipconfig /all。

释放 DHCP 客户机租约：键入 ipconfig /release。

续订 DHCP 客户机租约：键入 ipconfig /renew。

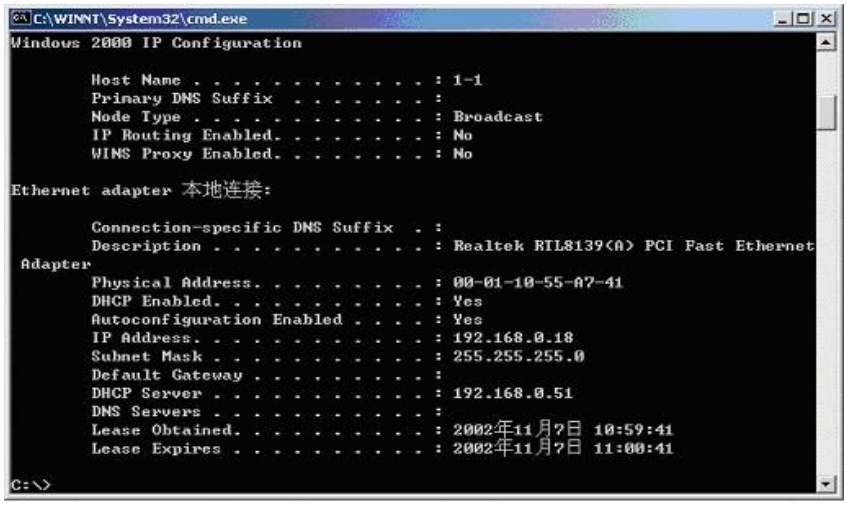


图 执行“ipconfig /all”命令窗口

实验三　捕获 TCP 数据包

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。

实验环境

1. 操作系统：几乎任意 windows 版本。本实验是在 windows xp 下实现的。
2. 所需软件：Wireshark-win32-1.10.2

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。

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。

实验步骤

1. Wireshark 的安装

Wireshark 基本安装过程与一般软件安装并无大异，均按默认设置安装即可。

2. 捕捉从自己 PC 机到远程服务器的 TCP 传输

在开始探索 TCP 奥秘之前，我们需要用 Wireshark 来得到一个从你 PC 到远程服务器的一个文件的 TCP 传输的数据包的跟踪。你需要进入一个网页，这个网页允许你输入在你的

PC 机上的一个文件的名字，然后将这个文件利用 HTTP POST 方法传输到 web 服务器（书 2.2.3 部分）。我们用 POST 方法而不是 GET 方法因为我们想要从你的 PC 上传输大量数据到另外一台 PC。当然，我们在做以上工作的时候，需要同时运行 Wireshark，以得到我们想要的从你 PC 上发送和接收到的 TCP 数据报的追踪。

需要做如下步骤：

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” 为文件名存入你的 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）

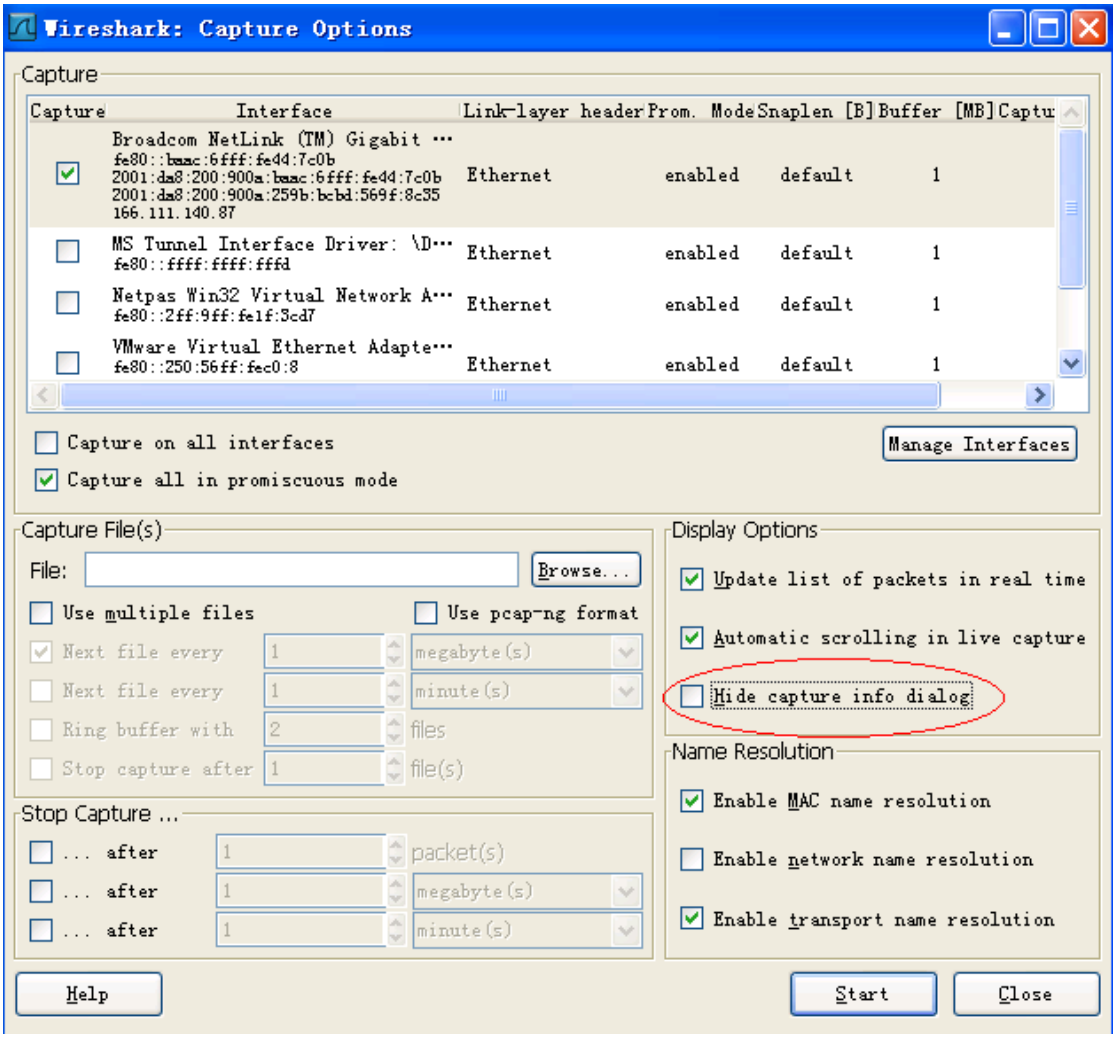
2) 进入 http://166.111.180.60:8080/upload/Lab3.jsp 。

你会看到下面样式的窗口：

点击“浏览”按钮进入包含 *Alice in Wonderland* 文件的文件夹，请先不要着急按“*提交文件 （学号）.txt*”按钮。

3) 用 Wireshark 开启数据包捕捉。

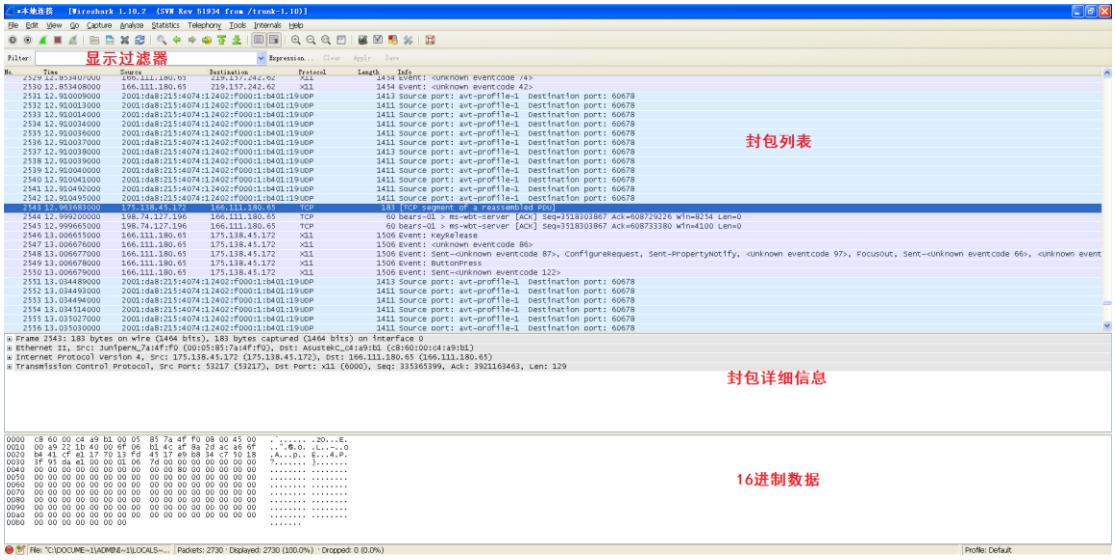
开始抓包之前，进入 Wirshark 的 Capture->Options，去掉“Hide capture info dialog”前面的“√”，以便在抓包过程中看到数据框。如下图所示。



安装好 Wireshark 后，点击 Capture->Start 开始抓包。回到浏览器，按“*提交文件（学号）.txt*”按钮来上传文件。一旦文件被上载成功，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 Inferface 项是否是你的计算机的默认网卡。

4) 停止 Wireshark 数据包捕捉。你的 Wireshark 窗口会出现类似下面的样式：



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”后回车，即可初步筛选所需数据。

如果在你的网络上 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。即使你已经成功捕捉到了你自己的追踪数据包并且已经解读，你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，我们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。在数据窗口中你将看到下面的消息：

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

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

   注：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。

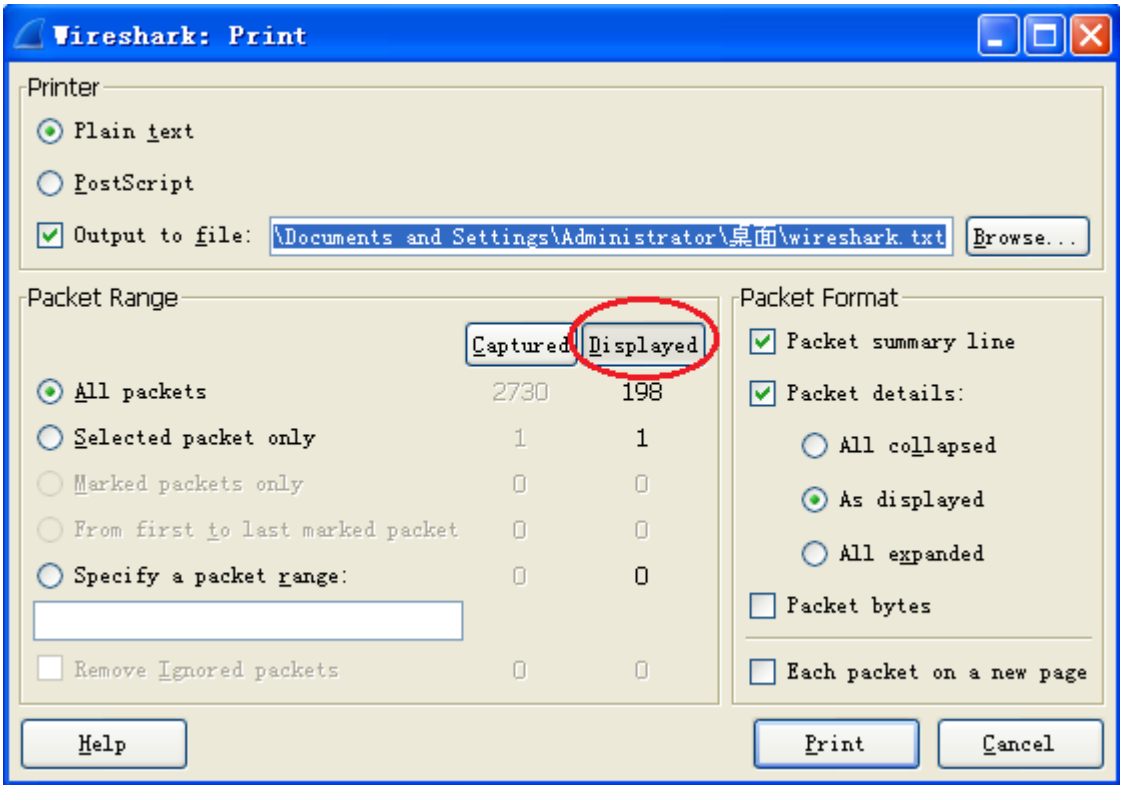
3) 从 http://166.111.180.60:8080/返回到你计算机的 TCP ACK 段。

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。

注（一种打印数据包的途径）：

File->Print,勾选 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 Caputred）。



现在，我们来改变 Wireshark 的“listing of captured packets (已捕获数据包清单)”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“✓ ”然后选择“OK”。在此次实验中我们还要查看 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勾除。

即我们需要查看的一系列往返于你的计算机和 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. TCP 基础

回答以下有关 TCP 报文段的问题：

1. 你的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，你需要在 Wireshark 窗口的底部发掘这个数据包内容域，找到一个在其 DATA 域中有标识 POST 的段。
5. 仔细思考一下作为 TCP 连接的第一个报文段的包含 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。

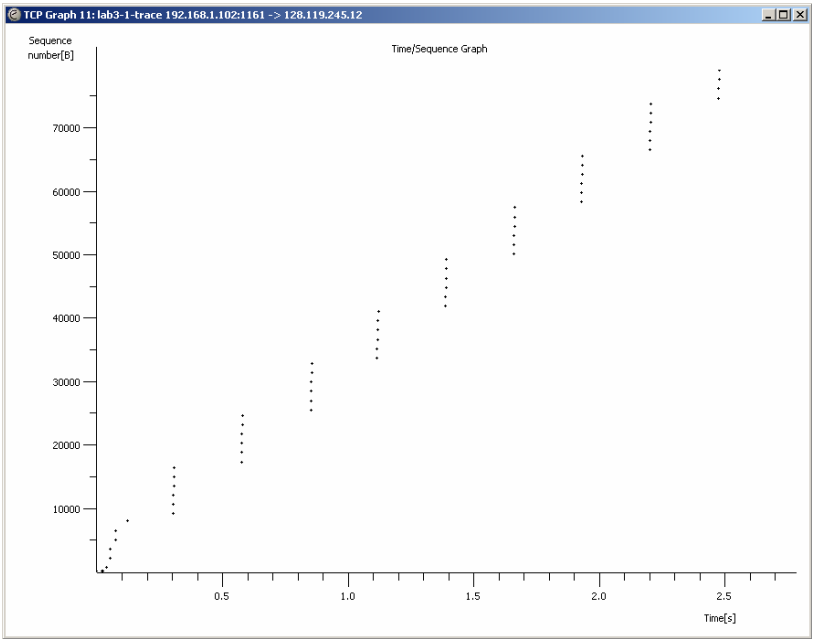
注意：Wireshark有一个很好的功能，它允许你画出发送的每一个TCP段的RTT。选择一个在“listing of the captured packets”窗口中的TCP段，此TCP正在从客户端到166.111.180.60，然后选择：*Statistics->TCP Stream Graph->Round Trip Time Graph*。

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，有重传的报文段么？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. TCP 拥塞控制

下面我们来观察单位时间内从客户端向服务器的数据量。我们不必对 Wireshark 窗口中的原始数据进行繁琐的计算，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)*，你会看到从捕获的数据包生成的如下图所示的图像。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。



这里，图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：

11. 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。你怎样判断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，不是所有的都像教材Figure 3.51那样简单漂亮的形式。同时还要注意在Time-Sequence-Graph(Stevens)中纵坐标所代表的变量与Figure 3.51中是不同的。

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

实验四　HTTP 抓包分析

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。

实验内容

4. 在 windows 环境进行 Wireshark 抓包。
5. 理解基本 GET/response 交互，HTTP 数据包的格式。
6. 获取较长的 HTML 文件，分析其数据包。
7. 获取有嵌入对象的 HTML 文件，分析器数据包。

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。

实验步骤

6. 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：

5) 打开网页浏览器；

6) 打开 Wireshark。本次试验中，我们只关注 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”（不带引号），并点击 Apply 按钮，这样只有 HTTP 数据包会在 packet-listing 窗口中显示；

7) 稍等片刻，然后开始 Wireshark 抓包；

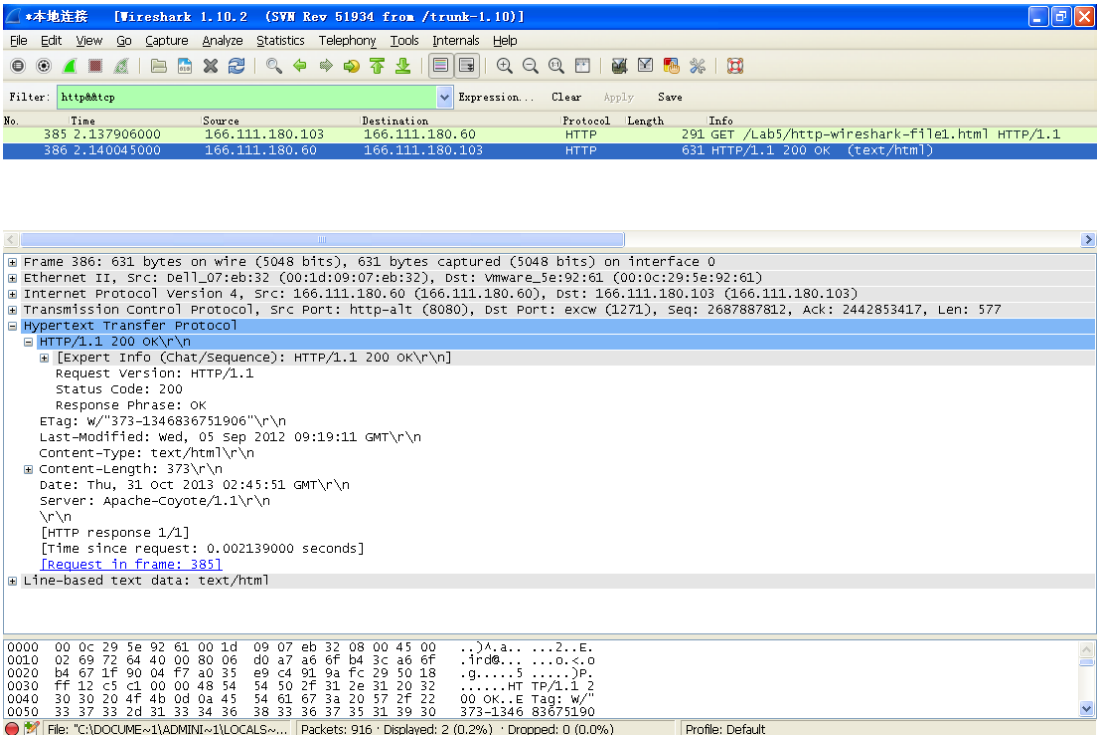
8) 在浏览器地址栏中输入以下 URL

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

你将在浏览器中看到一个只有两行文字的 html 文件；

9) 停止 Wireshark 抓包。

此时 Wireshark 窗口会出现类似如下的窗口：



上图所示的例子中，在 packet-listing 窗口中捕捉到了 2 个 http 数据包：GET 数据包（从你的浏览器到 166.111.180.60 服务器）以及从服务器到你的浏览器的 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。这里我们希望将在 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+号），只显示 http 数据报的具体内容（目录前的标志为-号）。

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，点击“删除文件”。

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（一种打印数据包的途径）：

File->Print,勾选 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？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?

7. 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，点击“删除文件”。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）。

1) 打开 Wireshark，在“display-filter-specification”窗口中输入“http&&tcp”（不带引号），并点击 Apply 按钮，然后开始抓包；

2) 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。

3) 快速的再次输入上述 URL，或者点击浏览器工具栏上的“刷新”按钮；

4) 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，服务器是否很清楚的传回了该 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 的状态代码是什么？服务器是否很清楚的传回了该 html 文件的内容？你如何知道的？

8. 获取较长的 HTML 文件

下面我们来获取一个较长的 html 文件，实验步骤如下：

1) 打开你的浏览器，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，你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。在我们的 http GET 数据包中，数据实体也就是我们需要查看的整个 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 数据包就会被拆成被 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？

9. 获取有嵌入对象的 HTML 文件

下面我们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) 打开你的浏览器，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。如果教材中所述，你的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。

实验五　DHCP 抓包分析

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。

实验环境

3. 操作系统：几乎任意 windows 版本。本实验是在 windows xp 下实现的。
4. 所需软件：wireshark-setup-1.6.1

实验内容

8. 在 windows 环境下执行 DHCP 相关命令。
9. 在 windows 环境通过 Wireshark 抓包。
10. 通过获取的数据包观察 DHCP 的工作过程。

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。

实验步骤

10. Wireshark 的安装

参见“实验三 捕获 TCP 数据包”实验指示书。

11. 执行 DHCP 相关命令

1) 打开 windows 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 Wirshark（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”。这条命令重新配置你主机的网络，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”。

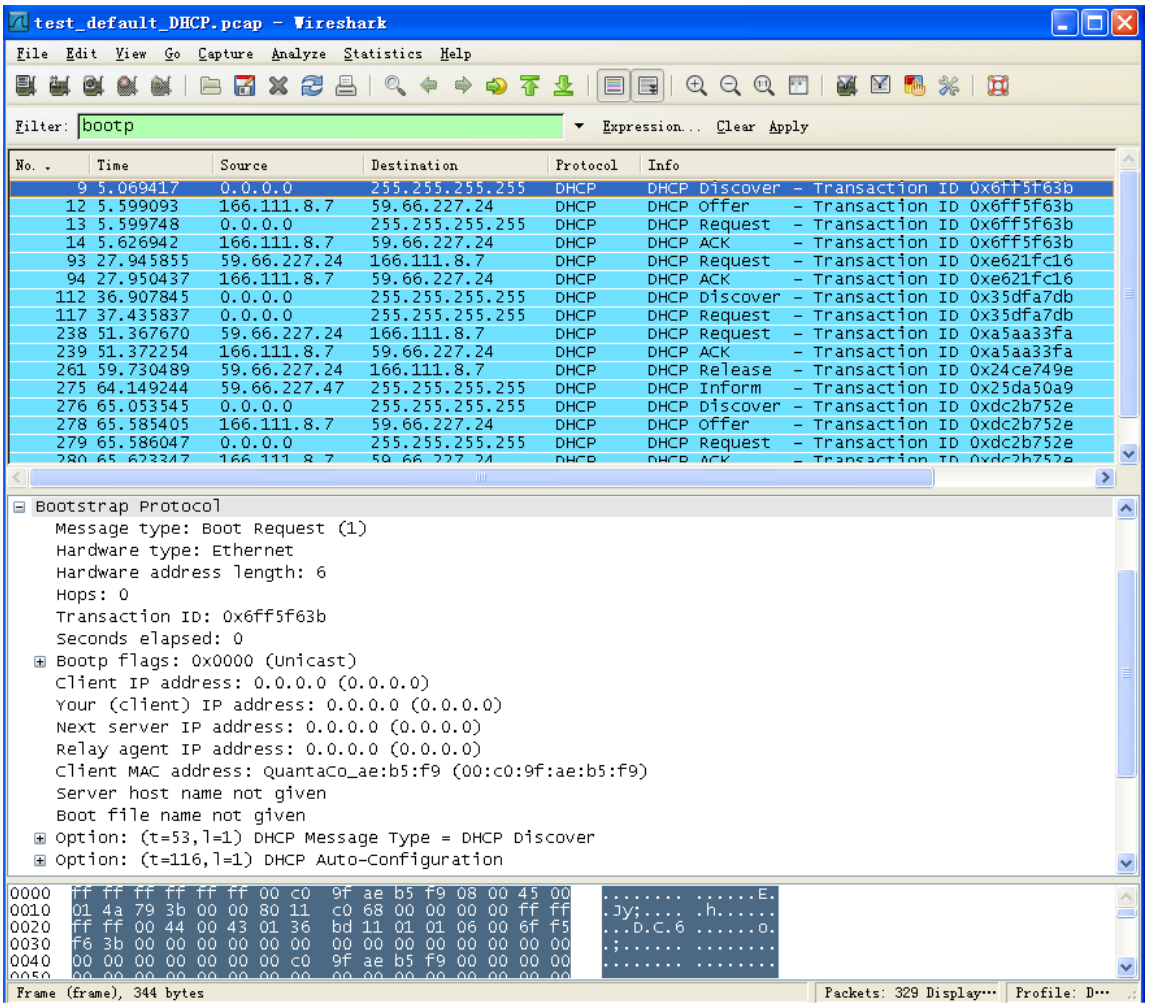
6) 在第二次“ipconfig /renew”命令执行结束后，输入“ipconfig /release”来再次释放先前获得的 IP 地址。

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。

12. 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。

13. 实验思考题

注意报告要求：

实验报告应包含如图 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 DCHP 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) 你所在主机链路层（例如，Ethernet）的地址是什么？
4) 通过什么值来 DHCP Descover 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 的只又是多少？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。
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) 在图 2 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么？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) 在图 2 所示的例子中，主机是在 DHCP Request 数据包中请求提供 IP 地址。你的试验中情况是怎样的？
12) 请解释设置租约时间（lease time）的作用。在你的试验中，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”的确认了么？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

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。

实验内容

11. 在 windows 环境进行 Wireshark 抓包。
12. 理解基本 GET/response 交互，HTTP 数据包的格式。
13. 获取较长的 HTML 文件，分析其数据包。
14. 获取有嵌入对象的 HTML 文件，分析器数据包。

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。

实验步骤

14. nslookup

在此次实验中，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，从该服务器接受一个 DNS 的回复，然后将结果显示出来。

下图显示了三个独立的 *nslookup* 命令运行的结果。在下图中，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。

1) 考虑第一个命令：

nslookup www.tsinghua.edu.cn

简单的说，该命令表是的意思是“请发给我 www.tsinghua.edu.cn 的 IP 地址”。如下图所示，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来得到该结果，如教材 2.5 节所述。

2) 考虑第二条命令

nslookup –type=NS tsinghua.edu.cn

在这条命令中，我们指定了 *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。简单的说，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 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。

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

Name:       www.d.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
```

15. ipconfig

ipconfig 对主机中 DNS 信息的管理也是有用的命令。在教材 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 /dispalydns

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。

16. 利用 Wireshark 跟踪 DNS

熟悉 *nslookup* 和 *ipconfig* 两个命令后，首先我们来捕获正常浏览网页时生成的 DNS 数据包。（DNS_default_test1.pcap）

2) 用 ipconfig 命令清空 DNS 缓存。
3) 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）
4) 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。
5) 开始抓包。
6) 在浏览器中打开网页：http://www.baidu.com 。
7) 停止抓包。

回答下面的问题：

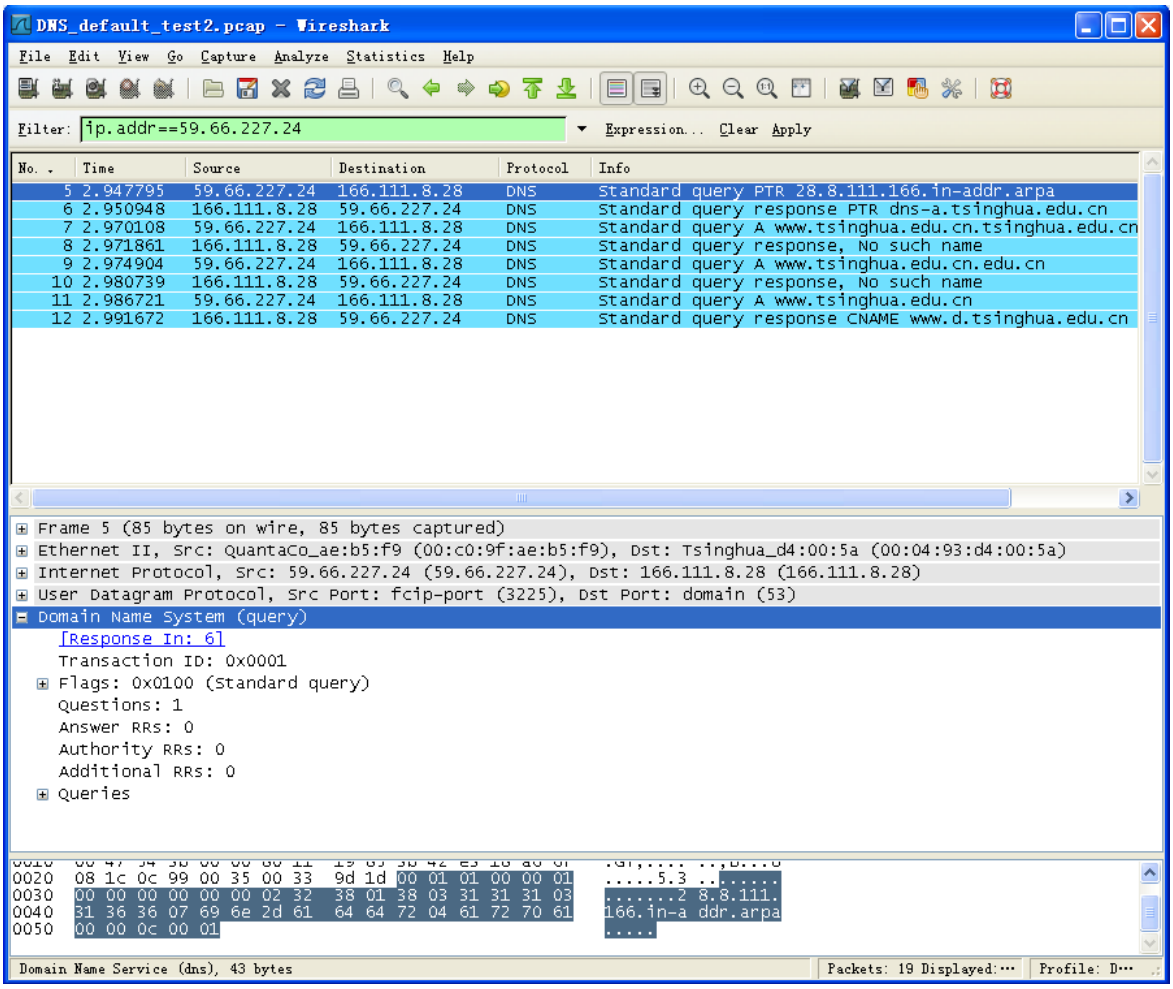
1. 观察 DNS 查询和回答数据包。他们发送的是 UDP 还是 TCP 包？
2. 该 DNS 查询数据包的目的端口号是什么？DNS 回答数据包的源端口号是什么？
3. DNS 查询数据包发送给了哪个 IP 地址？利用 ipconfig 来确定本地 DNS 服务器的 IP 地址，这两个地址是同一个吗？
4. 观察 DNS 查询数据包。该 DNS 查询是什么类型（Type）的？该数据包含有查询结果（answer）信息吗？
5. 观察 DNS 回答数据包。该数据包提供了多少个结果（answer）？每个结果包含什么信息？
6. 观察主机发送的子序列 TCP SYN 数据包。SYN 数据包的目的地 IP 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？

下面分析 *nslookup*：（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：

8. 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？
9. 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？
10. 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？
11. 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？
12. 请提供抓包的截屏图。

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：

13. 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？
14. 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？
15. 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？

16. 观察 DNS 回答数据包。回答数据包所提供的哪个 tsinghua 名字服务器？该回答服务器提供了 tsinghua 服务器的 IP 地址了吗？
17. 请提供抓包的截屏图。

实验七　Socket 编程实现网络通信

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。

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。若准备不充分出现问题过多，调试时间过长，可能会给后面的实验同学带来不便。
4. 课后须提交任务清单（提交时请打包提交到网络学堂上）：
   a) 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)。
   b) 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。

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。其中不带身份验证的 Simple SMTP 为课上必做，带身份认证的 Simple SMTP 为课后必做，UDP Pinger 课堂选作，如果课上做不完，那么一定在课后完成，并完成课后实验思考题。

3.1 邮件发送客户端实验（Simple SMTP）

实验环境

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

实验内容

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”，要求同学们须分析，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。

实验要求

1. 在给出的实验程序模版上填上相应合适的端口和命令，完成程序的调试。
2. 程序，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)拷贝到实验报告上。调试程序成功后，找助教老师验收。
3. 完成课后思考题。

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。

附录

邮件发送的命令可以参考教材 P78 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。之后可以再加上 SUBJECT 命令用以指定邮件的主题，然后正文，之后的流程跟书上一样，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。

…到了输入 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.

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（如果你是用 mails.tsinghua.edu.cn 发送信件的话）以外的邮件服务器由于登入注销需要涉及 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 HELO 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）拷贝出来，加到实验报告内。

3.2 UDP Ping 实验

实验内容

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。

实验要求

1. 读懂并运行已给的 UDP Pinger 程序，观察实验现象。
2. 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，并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。
3. 完成课后思考题。

检查内容

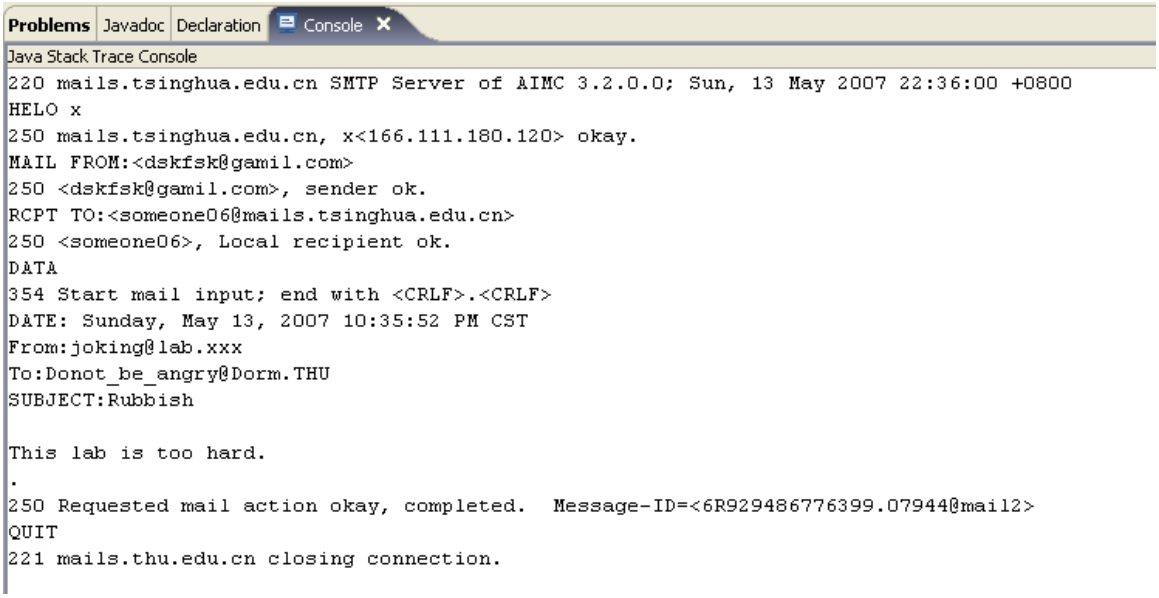
此为课堂选作内容，课上如果完成，请助教老师验收，主要看实验是否调通，注释是否正确。

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，也可以请教有些经验的同学。
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，但严禁拷贝代码，一经发现抄袭者和被抄袭者将严肃处理!!*

实验结果

对于不带身份验证的 Simple SMTP 实验，控制台输出的结果类似如下：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，此仅供参照。



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：

   A）simple SMTP 程序和常用的 email 客户端在功能、结构上的比较；

   B）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，根据代码本身和你收到的 email 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/XXXXX”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。

祝大家最后一个实验顺利通过！！！^_^

附录：配置实验环境

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，按 Ok 即可。

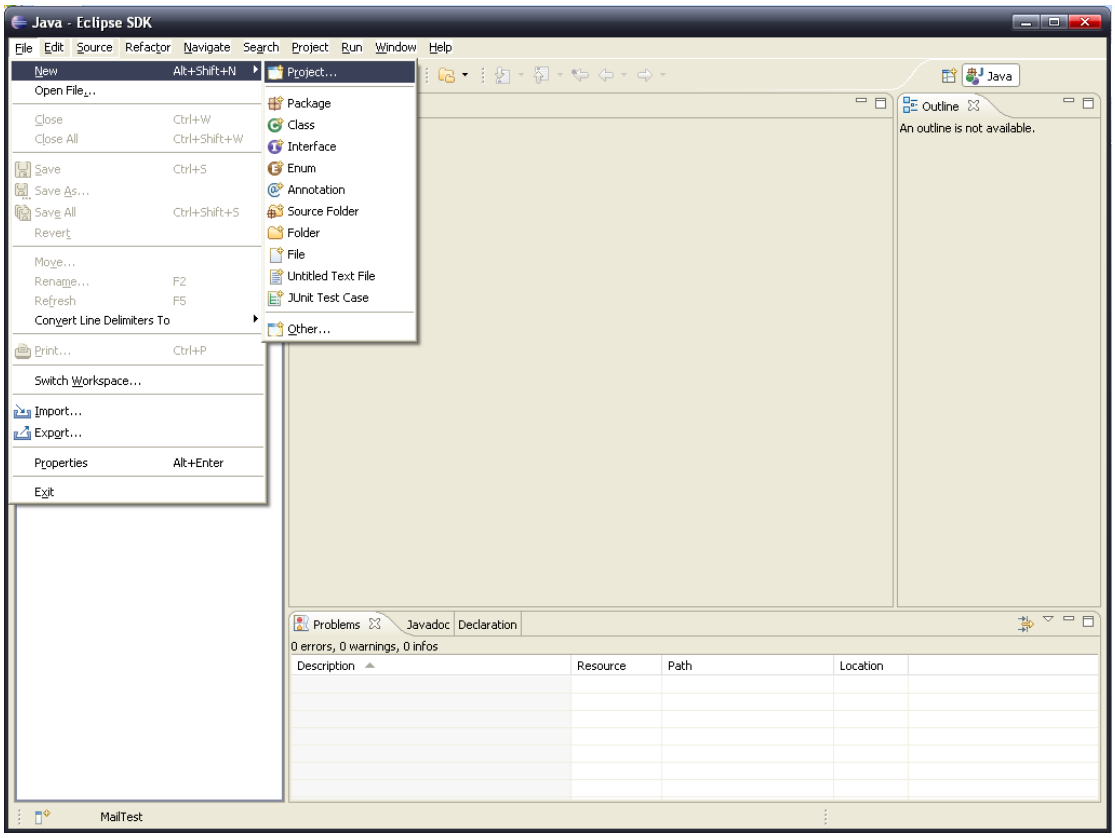
在 Eclipse 中开发 Java 程序

打开程序后如下图，先关闭 Welcome 标签页。

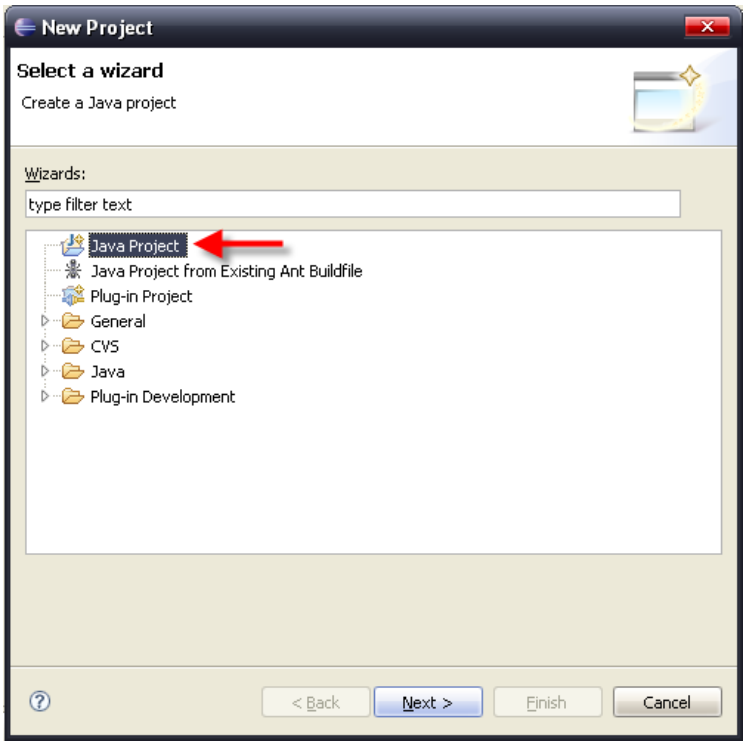
在建立 Java 程序前先要建 Java 项目，以下以图示的方式讲述如何运行简单的 Hello 程序。

1) 新建 Project

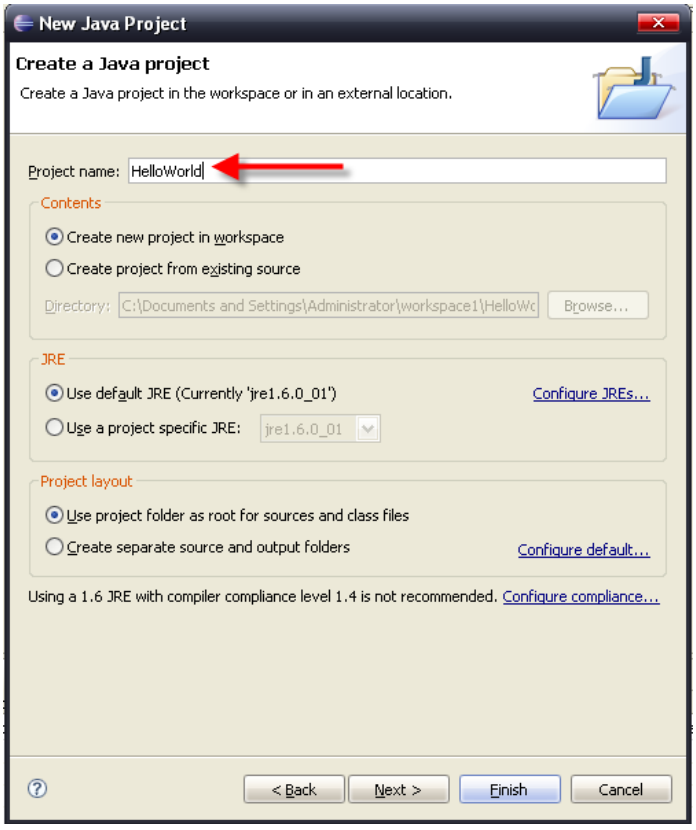
选择 File->New->Project



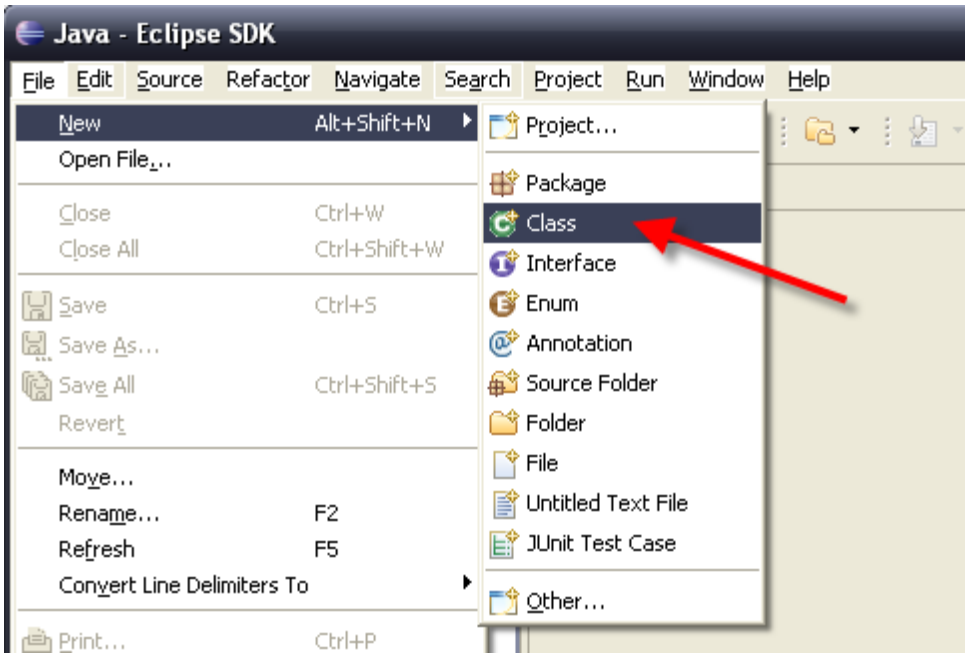
2) 选择 Java Project，按 Next。



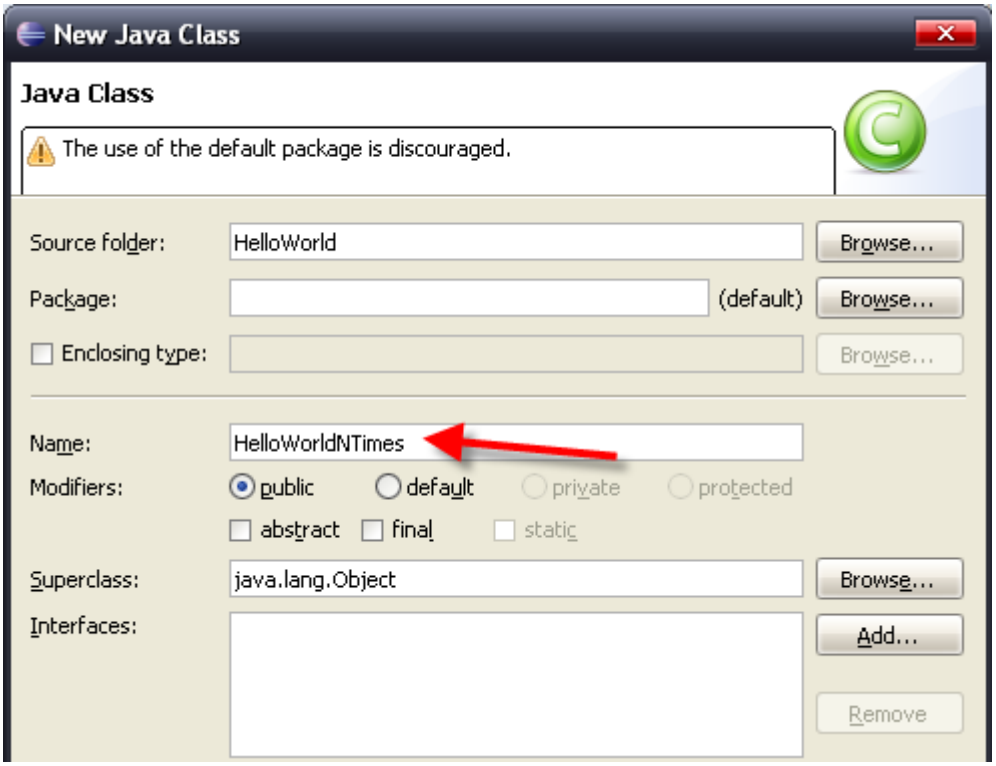
3) 输入 Project 名字，这例子中设为 HelloWord，之后点 Finish 即可。



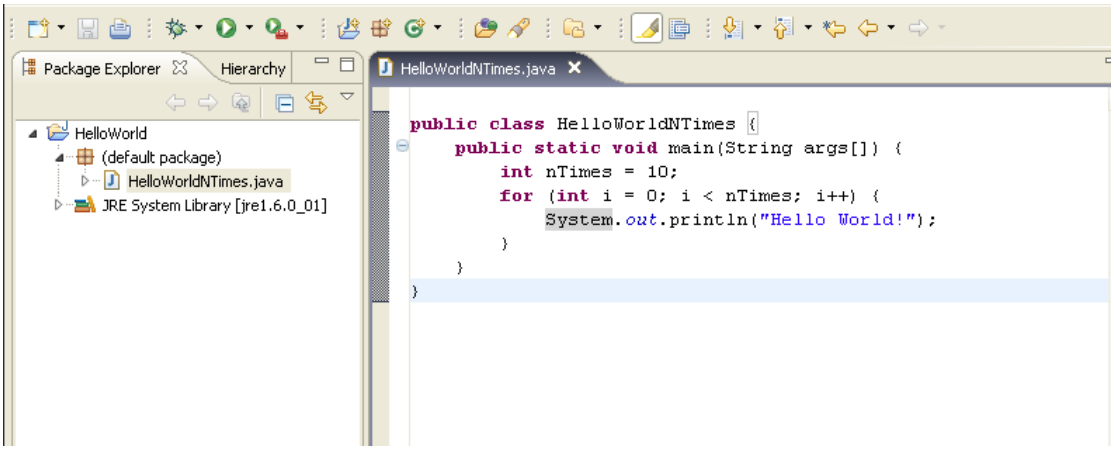
4) 在菜单中选 File->New->Class.



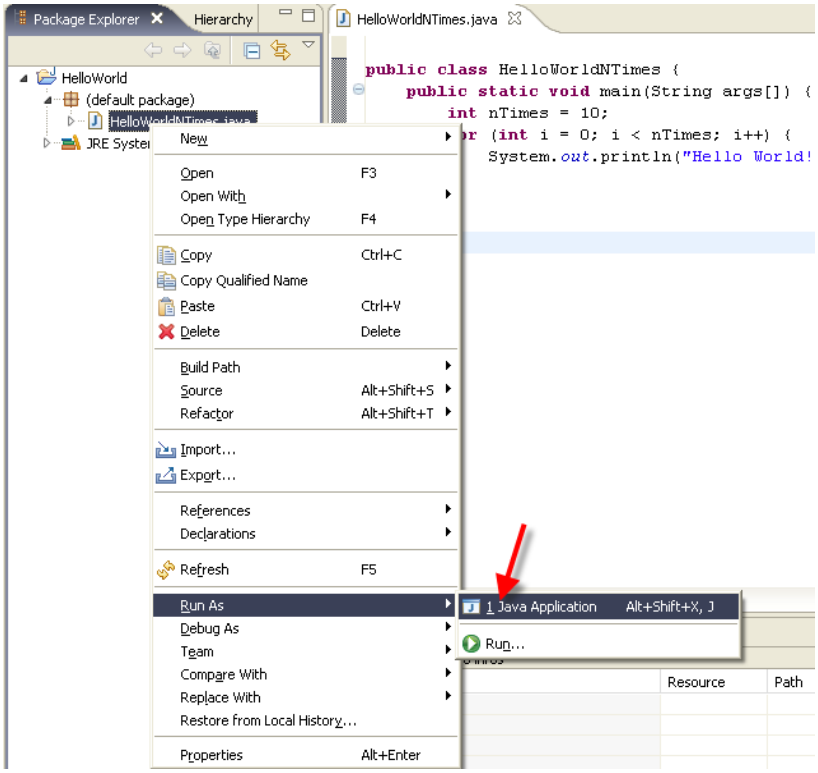
5) 在 Name 中输入类的名字，然后点 Finish.



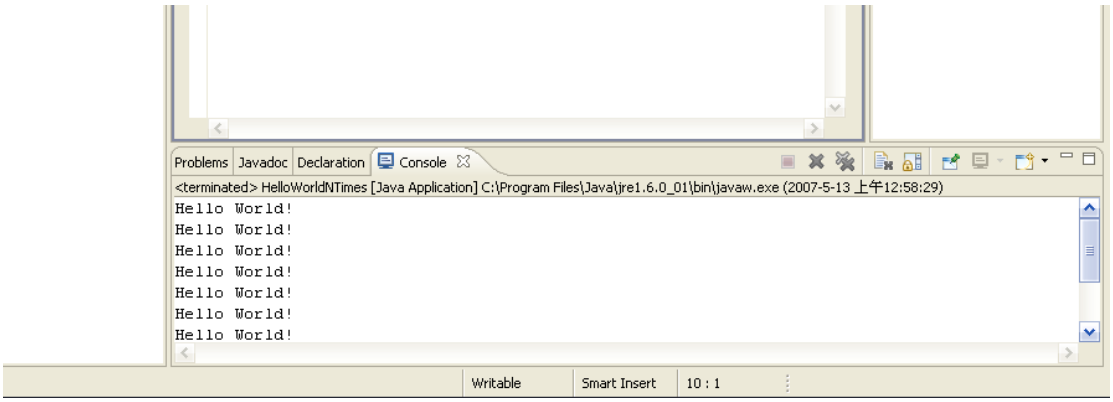
6) 在 HelloWorldNTimes 中输入如下程序代码。



7) 输入完成后，在右边的 Package Explorer 中点右键，选 Run As->Java Application 执行程序。



8) 结果输出在下图的 Console 中。



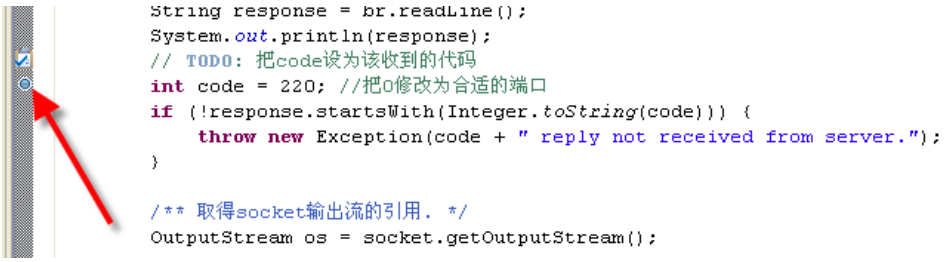
在 Eclipse 中使用调试器

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。

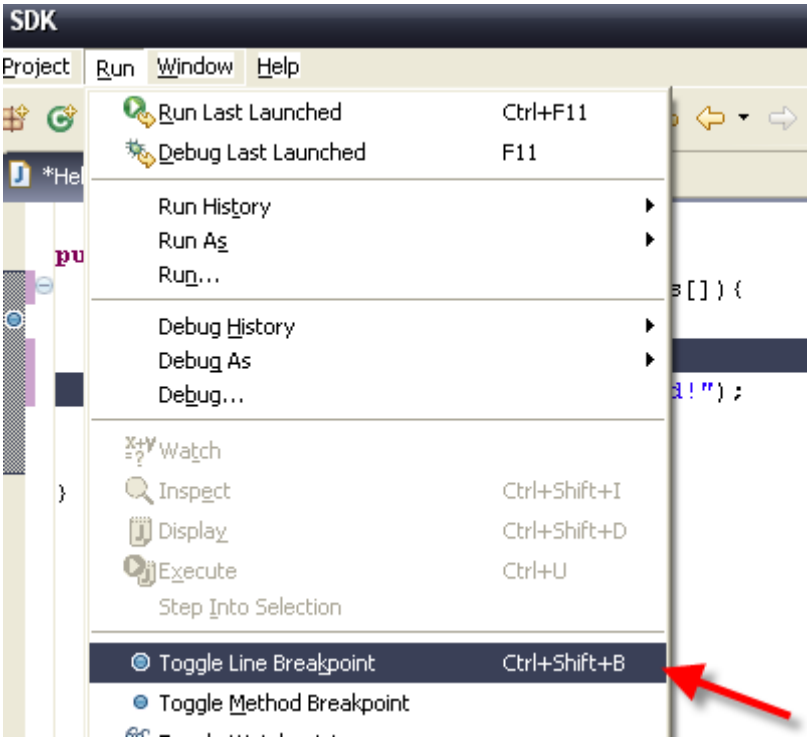
进行调试时先要设置断点，设置方法有几种。

1. 设置断点时，先选中想插入断点的行，然后：

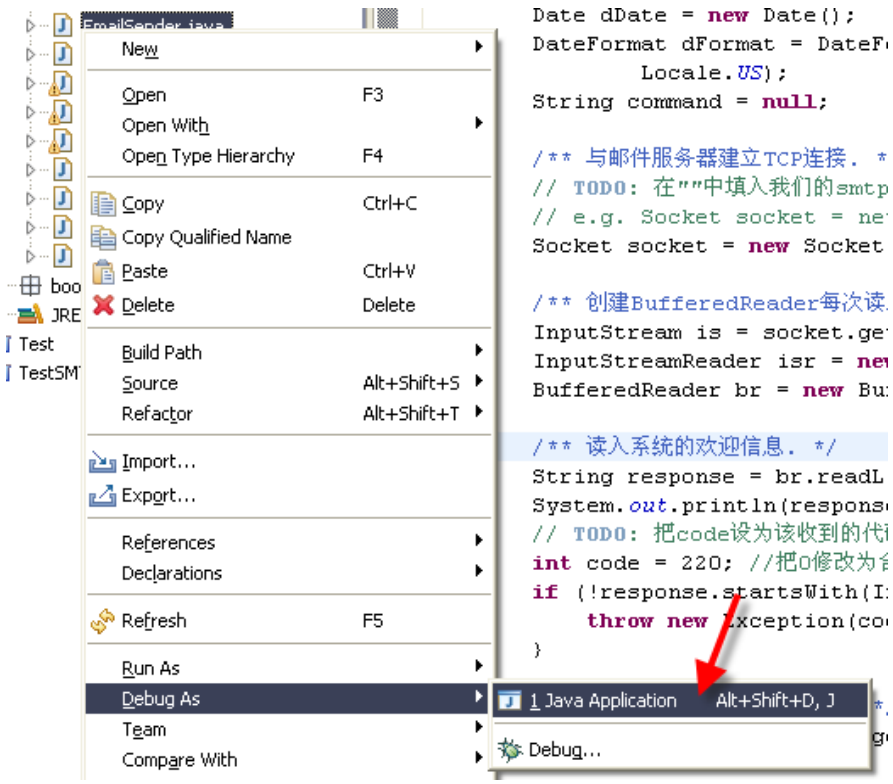
a) 如图中的第三行，然后在该行最前端的位置（如下图红箭头所指的位置），双击鼠标。



b) 选中菜单中的 Run->Toggle Line Breakpoint.

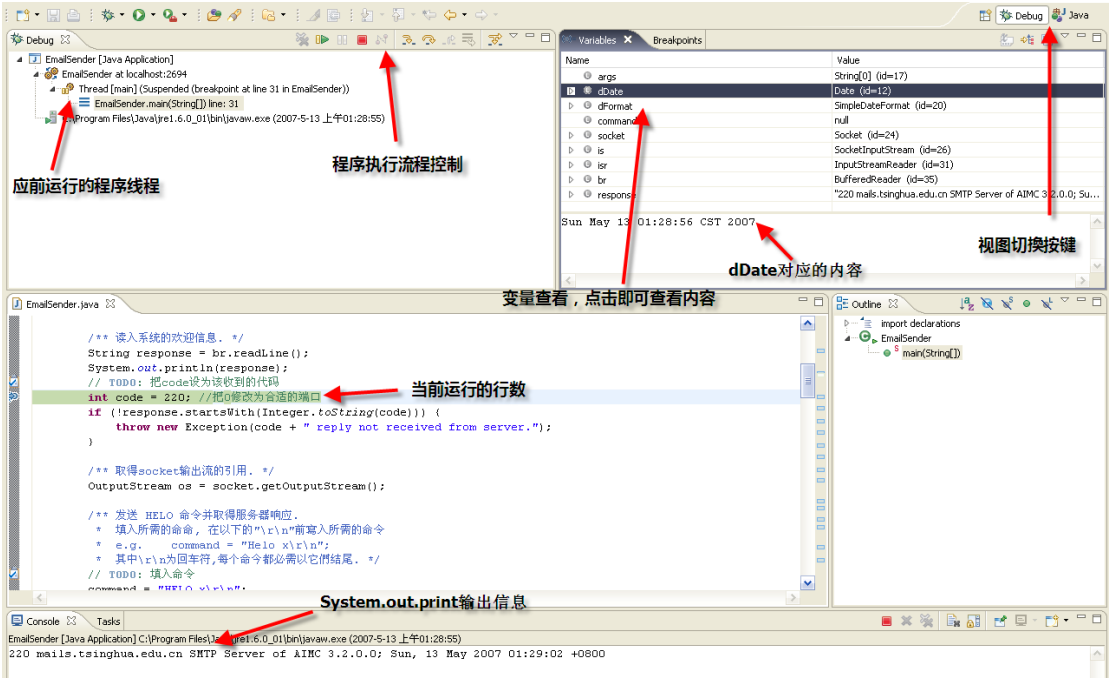


2. 执行程序，与运行程序相似，不过这次我们选中期望执行的程序点右键后选 Debug As->Java Application



之后出现 Save and Launch 窗口，选 Ok 即可。之后会弹出询问转换视图(Perspective)的对话框，选 yes 即可。Perspective 是 Eclipse 的特色之一，在使用不用的模式时，方便切换到不同的布局，方便使用。

注：若没有自动切换视图，可在菜单上选 Window->Open Perspective->Other…之后在弹出的窗口中选 Debug，再选 Ok 即可。



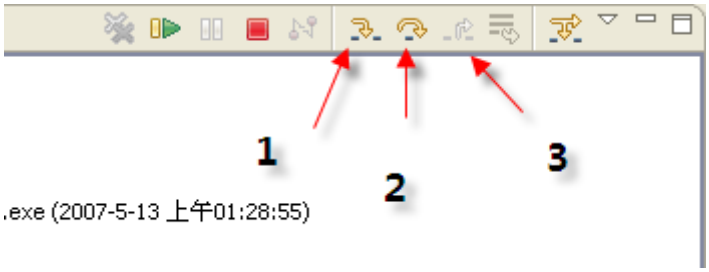
3. 执行语句时，使用下图的执行控制器，其中绿色的 Play 按键为继续执行，红色的 Stop 为停止。下图的 1，2，3 分别对应 Step Into，Step Over 和 Step Return 三种执行方式。

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：由于这次实验较为简单，几乎没有什么方法调用，有需要调试的话，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，不想执行时点上图红色的 Stop 按键即可。

致　谢

本实验指示书（2007 版）是为 2006-2007 学年度春季学期《计算机网络及应用》课程而编写的，由于本学期课程采用了原版教材“Computer Networking : A Top-Down Approach Featuring Internet (3rd Edition)”,在实验安排上较之以前作了相应的调整。两位助教博士生李欣、瞿莉为本版实验指示书的成型，以及辅导各次实验做了大量辛勤的工作，在此对他们表示衷心的感谢。

感谢实验中心的李振刚老师为两次课内实验——实验二和实验四的顺利完成所提供的帮助。

我的研究生梁荣达参与了实验四 Socket Programming 指示书的编写，准备了 Eclipse 编程环境和 Java 代码调试，并参与了实验四的辅导，在此表示特别感谢。

2007 版实验指示书中的实验一和实验二基本上参照了 2006 版的内容，稍加了改动。在此也对 2006 版的编写者关敬敏老师、张佐教授以及助教何勇等表示衷心感谢。没有他们的工作积累，本版指示书无法顺利完成。

实验三、实验四的内容设计参考了原版教材网站提供的内容，在此对两位作者 Kuross 和 Ross 教授，以及 Pearson 出版公司表示感谢。

当然，本版指示书还有许多需要改进的地方，本应该包含更多的内容: 例如，基于实验三还可以演化出两到三个新的实验，帮助学生理解应用层、网络层协议的内容和分组结构；在实验四的基础上也可以设计出更多的 Socket Programming 实验。由于课时有限，这些实验不能一一完成了。我们将在今后的工作中逐步丰富实验内容，完善实验环境。

课程主讲教师　程　朋

清华大学自动化系 副教授

2007.5.24.